www.ip-com.com.cn

User Guide

9GE+1SFP Cloud Managed Switch With 8-Port PoE

G2210P-8-102W

IP-COM
World Wide Wireless

V1.0

Copyright statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM! This user guide helps you configure, manage and maintain the product.

Conventions

This user guide is applicable to 9GE+1SFP Cloud Managed Switch With 8-Port PoE G2210P-8-102W. The web UI screenshots and related parameters mentioned herein are only for reference. Please refer to the actual product.

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	Choose **System** > **Live Users**.
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
UI control	Bold	On the **Policy** page, click the **OK** button.

The symbols that may be found in this document are defined as follows.

Item	Meaning
	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
	This format is used to highlight a procedure that will save time or resources.

For more documents

Go to our website at www.ip-com.com.cn and search for the latest documents for this product.

Product materials

Document	Description
Data sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.
Quick installation guide	It introduces how to set up the switch quickly, including the description of installation and management, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.
User guide	It introduces how to set up more functions of the device for more requirements, including all functions on the web UI of the device.
Lightning protection guide	It introduces lightning protection of the switch.

Technical support

If you need more help, contact us using any of the following means. We will be glad to assist you as soon as possible.



(86 755) 2765 3089	info@ip-com.com.cn	www.ip-com.com.cn

Revision history

IP-COM is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the user guide was released.

Version	Date	Description
V1.0	2022-07-21	Original publication.

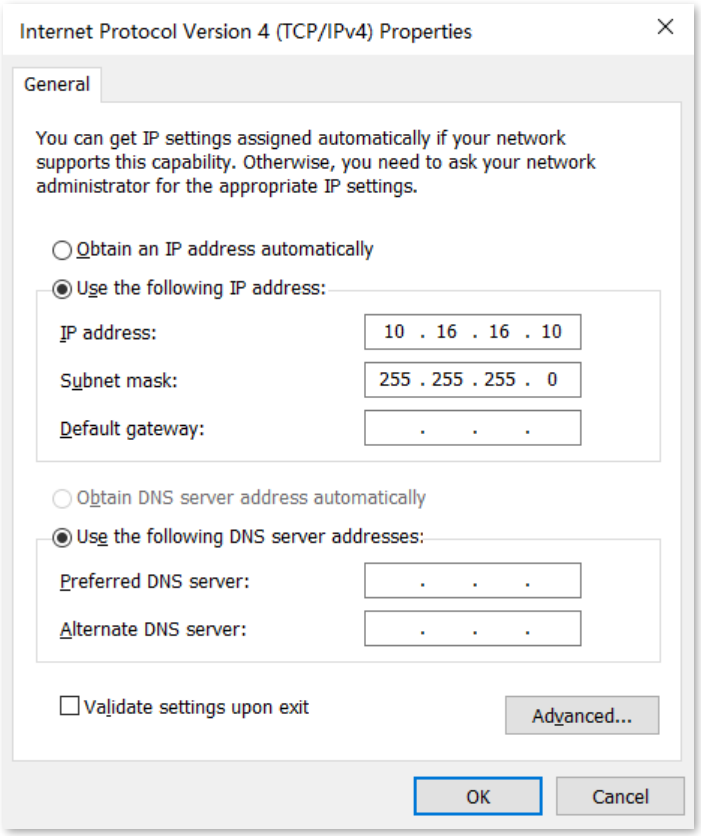
Contents

1 Web login

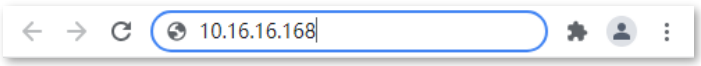
1.1 Login

1. Connect the computer to one of the RJ45 ports of the switch using an Ethernet cable.
2. Set the IP address of Ethernet (or Local Area Connection) of the computer to an unused one belonging to the same network segment of the IP address of the switch.

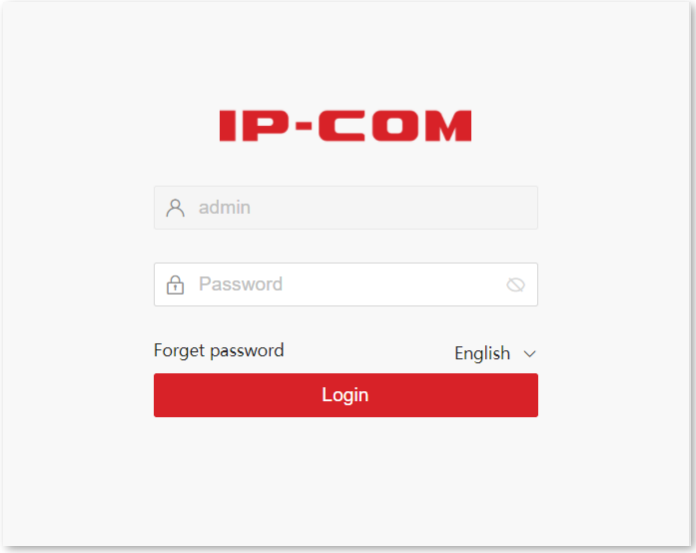
   For example, the default IP address of the switch is **10.16.16.168**, you can set the IP address of the computer to **10.16.16.*X*** (*X* ranges from 2 to 254 excluding 168 and is not occupied), and subnet mask to **255.255.255.0**.



3. Start a browser (such as Chrome) and enter the IP address of the switch (default: **10.16.16.168**) in the address bar to access the login page.



4. Enter your password (**admin** by default) and click **Login**.



----End

Tip

If the above page does not appear, try the following solutions:

- Clear the cache of the web browser or try another web browser.
- If there is a DHCP server in the LAN where the switch is deployed, the switch automatically obtains IP address from the DHCP server. Under such circumstance, check the new IP address of the switch at the client list of the DHCP server first, and use the new IP address to log in to the web UI of the switch.
- If the problem persists, reset the switch and try again. Reset method: When the **SYS** LED indicator is blinking, press down the reset button using a sharp item (such as a pin) for about 10 seconds, and then release it when all LED indicators are solid on. When the **SYS** LED indicator blinks again, the switch is reset successfully.

After logging in to the web UI, you can start to configure the switch.

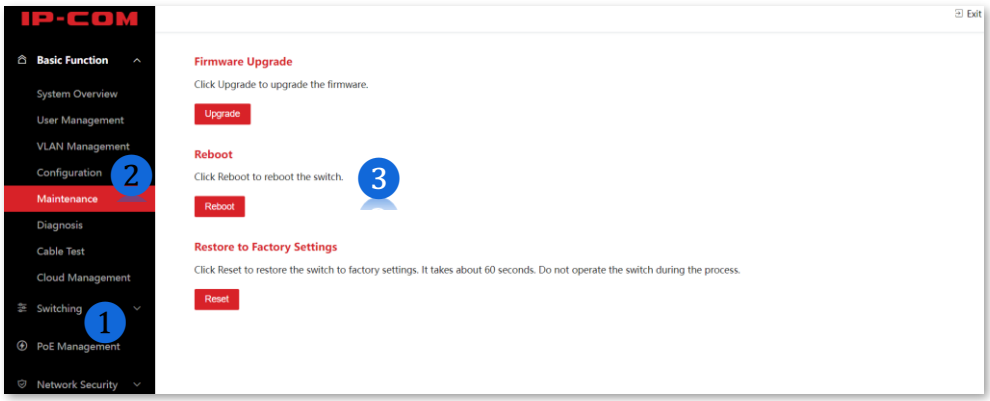
1.2 Logout

After you log in to the switch's web UI page, the system will automatically log you out if there is no operation within five minutes. Alternatively, you can directly click **Exit** on the upper right corner to exit the web UI page.

2 Web UI introduction

2.1 Web layout

The Web UI page can be divided into three parts: level-1 navigation bar, level-2 navigation bar and configuration area.



No.	Name	Description
1	Level-1 navigation bar	The navigation bars display the function menu of the switch. When you select a function in navigation bar, the configuration of the function appears in the configuration area.
2	Level-2 navigation bar	
3	Configuration area	This area enables you to view and modify configuration. Tip Features and parameters in gray indicate that they are not available or cannot be changed under the current condition.

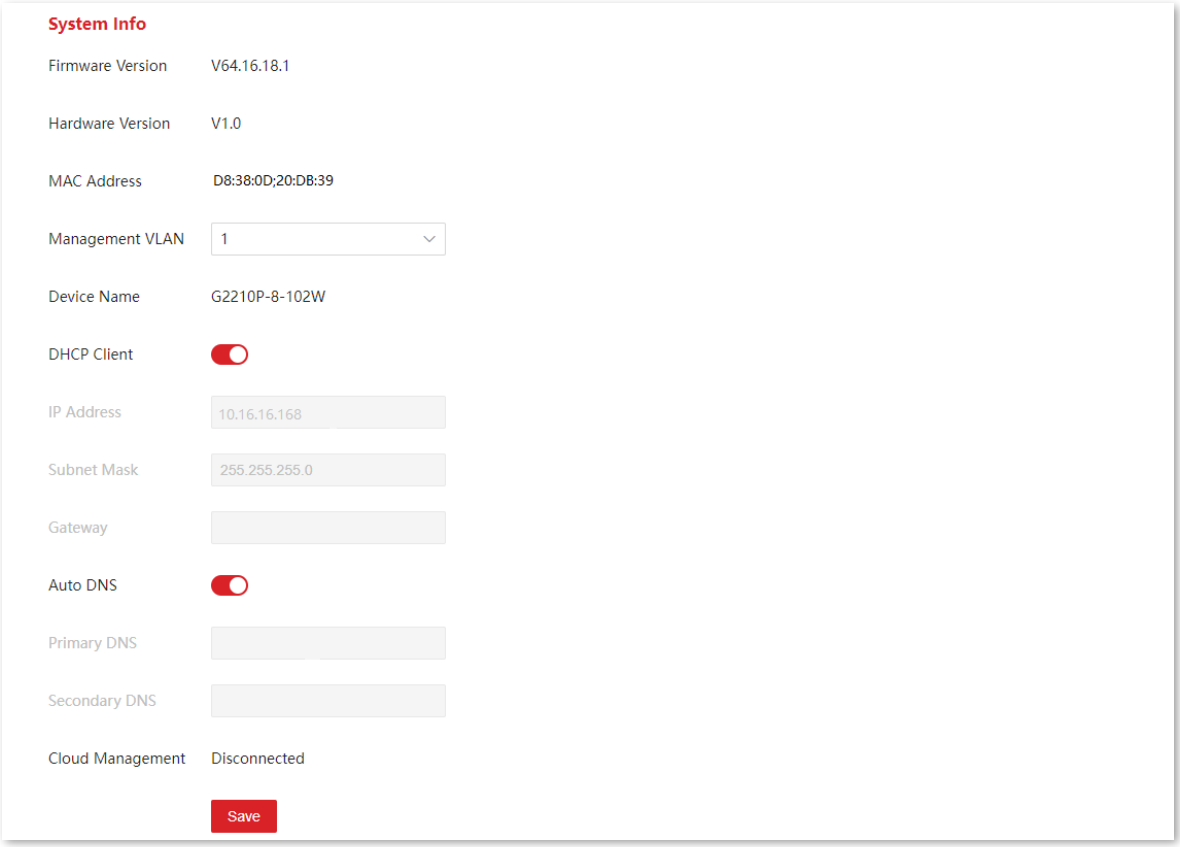
2.2 Commonly used buttons

Common buttons	Description
Add	Used for adding new rules on the current page.
Delete	Used for deleting the rules on the current page.
	Used for selecting ports or rules.
Cancel	Used for restoring the original configuration without saving the configuration on the current page.
Save	Used for saving all current configurations of the switch.
Edit	Used for configuring the settings on the current page in batches.
Refresh	Used for refreshing displayed contents on the current page.
OK	Used for saving the configurations on the current page and enabling the configurations to take effect.

3 Basic function

3.1 System overview

Choose **Basic Function** > **System Overview** to enter the page. On this page, you can view and modify basic parameters of the switch.



Parameter description

Name	Description
Firmware Version	It displays the firmware version of the switch.
Hardware Version	It displays the hardware version of the switch.
MAC Address	It displays the MAC address of the switch.

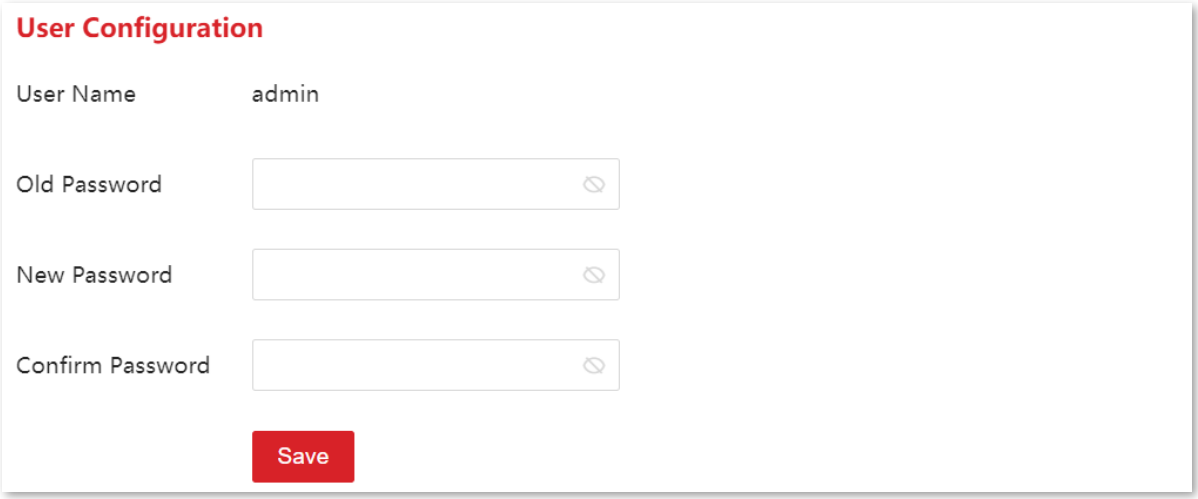
Name	Description
Management VLAN	The management VLAN of the switch is 1 by default. This function is only valid when the switch enables VLAN management. Note The switch can be visited only when the computer is connected to the VLAN port member (all ports are in VLAN 1 by default).
Device Name	It displays the name of the switch. By default, the device name is the model of the device.
DHCP Client	Enable/Disable DHCP client function. By default, this function is enabled. – Enable: The switch will automatically acquire IP address, subnet mask and gateway from the DHCP server. – Disable: Manual settings are required for IP address, subnet mask and gateway to manage the device and connect to Internet.
IP Address	The IP address of the switch. The default IP address is 10.16.16.168 and can be modified when DHCP client is disabled. Also, it is the management IP address of the switch which can be used to log in to the web UI.
Subnet Mask	The subnet mask of the IP address. The default subnet mask is **255.255.255.0**, and can be modified when DHCP client is disabled.
Gateway	The gateway address of the switch by default. It can be modified when DHCP client is disabled.
Auto DNS	Enable/Disable auto DNS function. – Enable: The switch will automatically acquire primary and secondary DNS server address from the DHCP server. – Disable: Manual settings are required for primary and secondary DNS server address.
Primary DNS Secondary DNS	The primary/secondary DNS server address of the switch. It can be modified when **Auto DNS** is disabled.
Cloud Management	It displays whether the switch is connected to the IP-COM ProFi Cloud platform. – **Connected**: The switch is connected to the IP-COM ProFi Cloud platform. – **Disconnected**: The cloud management function is disabled, or the switch fails to connect to the IP-COM ProFi Cloud platform.

3.2 User management

Choose **Basic Function** > **User Management** to enter the page. Here, you can change the login password.

Tip

To ensure network safety, it is strongly recommended to set a login password with a certain complexity.



When you click **Save** to save the change, the switch will redirect to the login page. Enter the new user password to log in to the web UI.

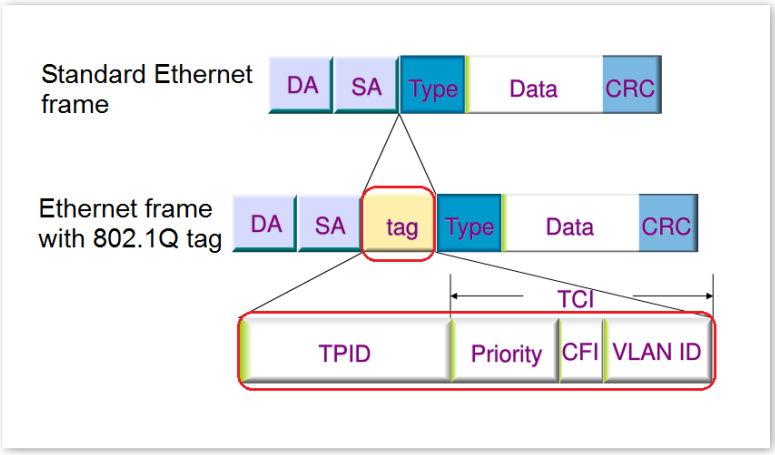
3.3 VLAN management

3.3.1 Overview

Virtual Local Area Network (VLAN) is a technology that divides devices in LAN into different logical, instead of physical, network segments to form virtual working groups. VLANs allow a network station constituted by switches to be logically segmented into different domains for broadcast isolation. All members in a VLAN are treated as in the same broadcast domain and communicate as if they were on the same network segment, regardless of their physical locations. Different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer-3 devices that are able to perform layer-3 forwarding.

The switch supports 802.1Q VLAN and can communicate with devices that support 802.1Q VLAN in VLAN as well.

As defined by IEEE 802.1q protocol, one 4 bytes 802.1Q VLAN tag is bound to be wrapped behind the destination MAC address and the source MAC address of the Ethernet frame for identifying the relevant information of VLAN. As shown below, the Ethernet frame with 802.1Q tag is produced by adding an 802.1Q VLAN tag behind the destination MAC address and the source MAC address of the standard Ethernet frame.

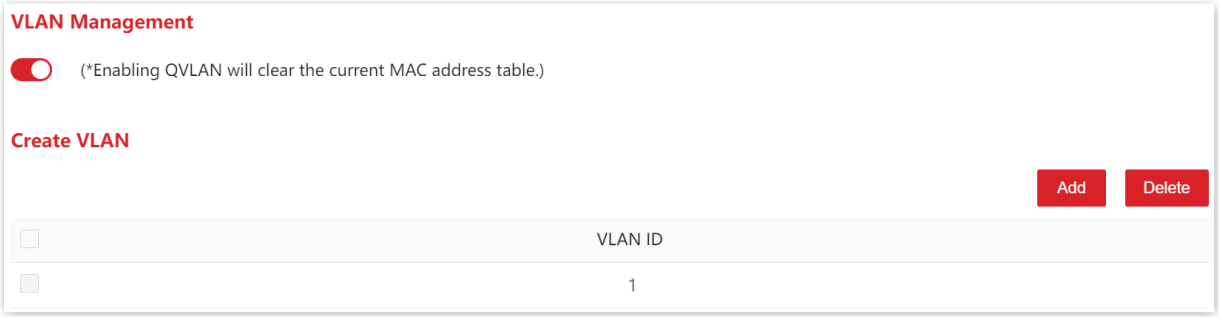


3.3.2 Configure 802.1Q VLAN

Create VLAN rules

Choose **Basic Function** > **VLAN Management** to enter the page. On this page, you can configure the rules of 802.1Q VLAN. By default, this function is disabled. At this time, the switch works in VLAN transparent mode and forwards data of all VLANs.

A VLAN rule is created by default to ensure communication between switches in factory settings. All ports are set to be members of this VLAN by default with the VLAN ID of **1**. This rule cannot be deleted.

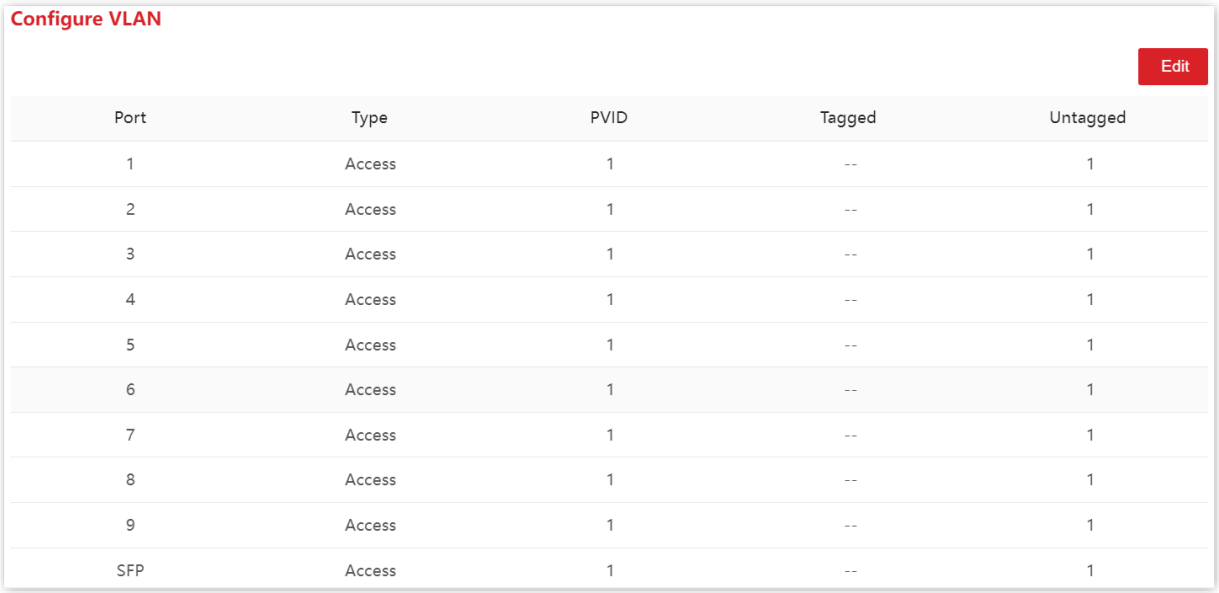


Parameter description

Name	Description
VLAN ID	It specifies the VLAN ID, used for identifying the VLAN to which the packet belongs. The management VLAN ID is **1** and cannot be deleted.
Add	It is used to add VLAN.
Delete	It is used to delete VLAN.

Configure VLAN port members

Choose **Basic Function** > **VLAN Management** to enter the page. On this page, you can configure link type, PVID and Tag treatment policies of each port to realize VLAN isolation.



Parameter description

Name	Description
Port	It specifies the ID of the port.
Type	It specifies the link type of the port. Two VLAN link types are supported: **Access** and **Trunk**. – **Access**: An access port only belongs to one VLAN and transmits untagged messages. It is commonly used to connect to terminals, such as computers. – **Trunk**: A trunk port can receive and transmit messages belonging to multiple VLANs, usually used as a cascade-connected port between switches.
PVID	It specifies the default VLAN ID of the port. By default, the PVID of each port is **1**. When receiving untagged packets, the port forwards them to the corresponding VLAN based on the PVID of the port itself.
Tagged	If the VLAN ID of the tagged packets received by the port is the same with the tagged VLAN, the port retains the tags of the packets and transmit them.
Untagged	If the VLAN ID of the tagged packets received by the port is the same with the untagged VLAN, the port removes the tags of the packets and transmit them.

3.3.3 Example of 802.1Q VLAN configuration

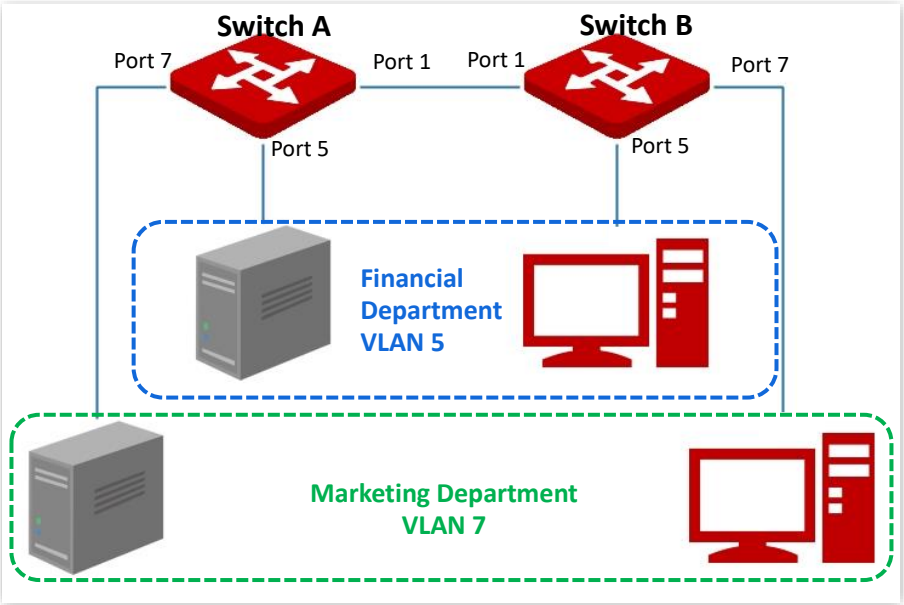
Networking requirement

The staff in the financial department and marketing department of a company work on the second floor, while the servers for these two departments are on the third floor. Now it is required that the communication is available within each department and the servers can be accessible respectively, but the two departments cannot communicate with each other.

Solution

Configure 802.1Q VLAN for two switches:

- Create two VLANs for the switches. Assign the ports connected to the financial department's devices to VLAN 5, and the ports to the marketing department's devices to VLAN 7.
- Add the ports that connect two switches to both VLAN 5 and VLAN 7.



Configuration procedure

I. Configure Switch A

1. Create VLANs.

(1) Log in to the web UI of Switch A and choose **Basic Function** > **VLAN Management**.

(2) Enable **VLAN Management** function.

(3) Click **Add** and enter the **VLAN ID** to **5**. Then click **OK**.

(4) Repeat step (2) and add another VLAN with the **VLAN ID** of **7**.

2. Configure port attribute.

(1) Choose **Basic Function** > **VLAN Management**.

(2) Click **Edit**. Select port 5 and set **PVID** to **5**. Then click **OK**.

(3) Click **Edit**. Select port 7 and set **PVID** to **7**. Then click **OK**.

(4) Click **Edit**. Select port 1, set **Type** to Trunk, set **Tagged** to **5, 7**. Then click **OK**.

II. Configure Switch B

Refer to the steps of configuring Switch A.

----End

Verification

The staff can access the server of their department, but cannot access the server of the other department. The staff in the same department can communicate with each other but cannot communicate to the staff of other departments.

3.4 Configuration

Choose **Basic Function** > **Configuration** to enter the page. On this page, you can back up system configurations and import configuration files.

3.4.1 Back up system configurations

If you have made extensive configurations on the switch for better performance, it is recommended to back up the configuration to facilitate troubleshooting and save configuration time later.

The switch supports two backup methods: local backup and cloud backup.

Tip

Only when the switch is managed by the ProFi Cloud platform can the configurations be backed up to the ProFi Cloud platform.

3.4.2 Import configuration file

If you need to make same configuration on several switches, or performance degradation of switch occurs due to wrong operations, you can click **Select File** to select the backup configuration file, and then click **Import** to import the file to the switch.

3.5 Maintenance

Choose **Basic Function** > **Maintenance** to enter the page. On this page, you can upgrade firmware of the switch, reboot the switch and restore the switch to factory settings.

3.5.1 Firmware upgrade

On **Basic Function** > **Maintenance** page, you can upgrade firmware of the switch, getting better user experience.

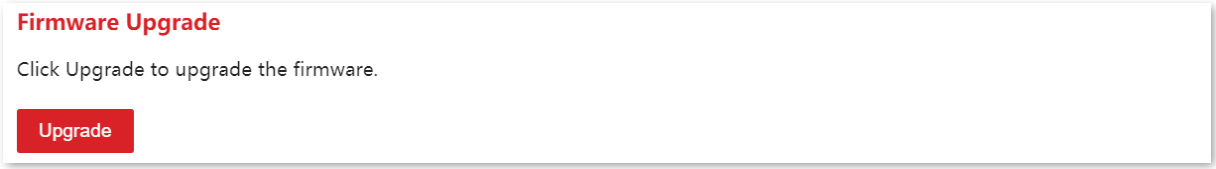
Note

To avoid damages to the switch, ensure that the switch is upgraded properly. Please note that:

- Before upgrading, you can download the latest firmware of the switch on the IP-COM official website: www.ip-com.com.cn. Generally, the filename extension of the upgrading file is **.bin**.
- During the upgrading process, ensure stable power supply to the switch.

Configuration procedure

1. Choose **Basic Function** > **Maintenance**.
2. Click **Upgrade** in the **Firmware Upgrade** module.



3. Find and load the upgrading file in the corresponding directory.
4. Click **OK** after confirming the prompt message.

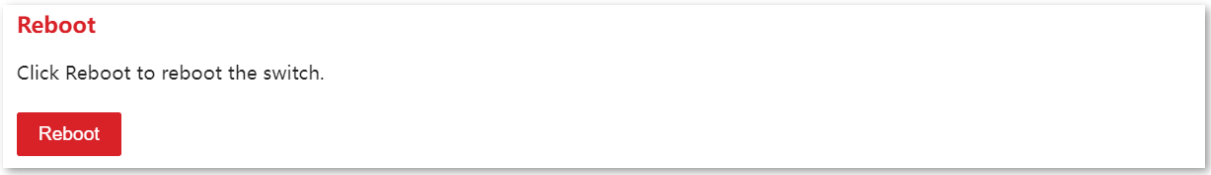
----End

Wait for the progress bar to finish. After the progress bar is completed, you can log in to the switch again, choose **Basic Function** > **System Overview**, and check the firmware version of the switch to confirm whether the upgrade is successful.

3.5.2 Reboot

When a parameter you set does not work properly, you can try to reboot the switch to fix this issue.

On **Basic Function** > **Maintenance** page, you can click **Reboot** to restart the switch.


Reboot
Click Reboot to reboot the switch.
Reboot

3.5.3 Restore to factory settings

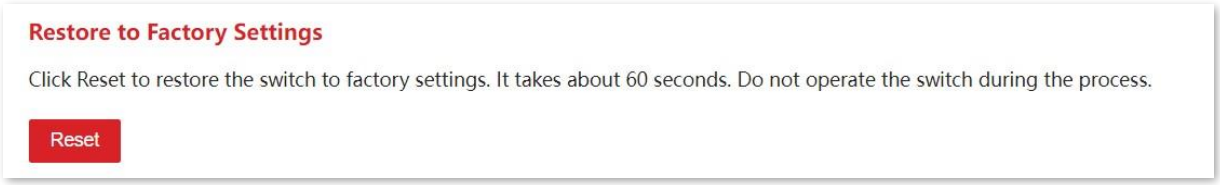
If you cannot solve certain network issues, or you forget your user password when logging in to the web UI of the switch, you can restore the switch to factory settings, and then use the default password (**admin**) to log in. This switch supports software reset and hardware reset.

Software reset

On **Basic Function** > **Maintenance** page, you can click **Reset** to restore the switch to factory settings.

Note

To avoid any damages, please ensure stable power supply to the switch during the resetting process.

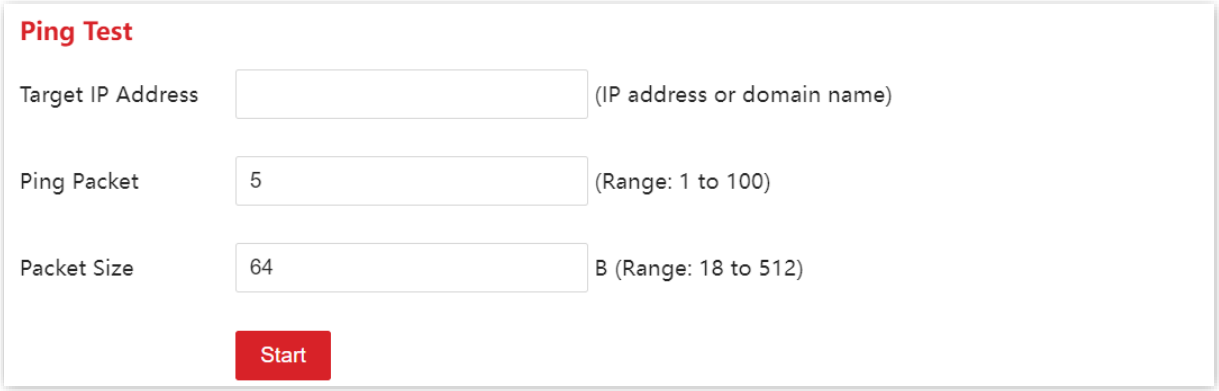


Hardware reset

When the **SYS** LED indicator is blinking, press down the reset button on the switch using a sharp item (such as a pin) for about 10 seconds, and then release it when all indicators are solid on. When the **SYS** LED indicator blinks again, the switch is restored to factory settings.

3.6 Diagnosis

Choose **Basic Function** > **Diagnosis** to enter the page. On this page, you can perform Ping test to test network connection and connection quality.

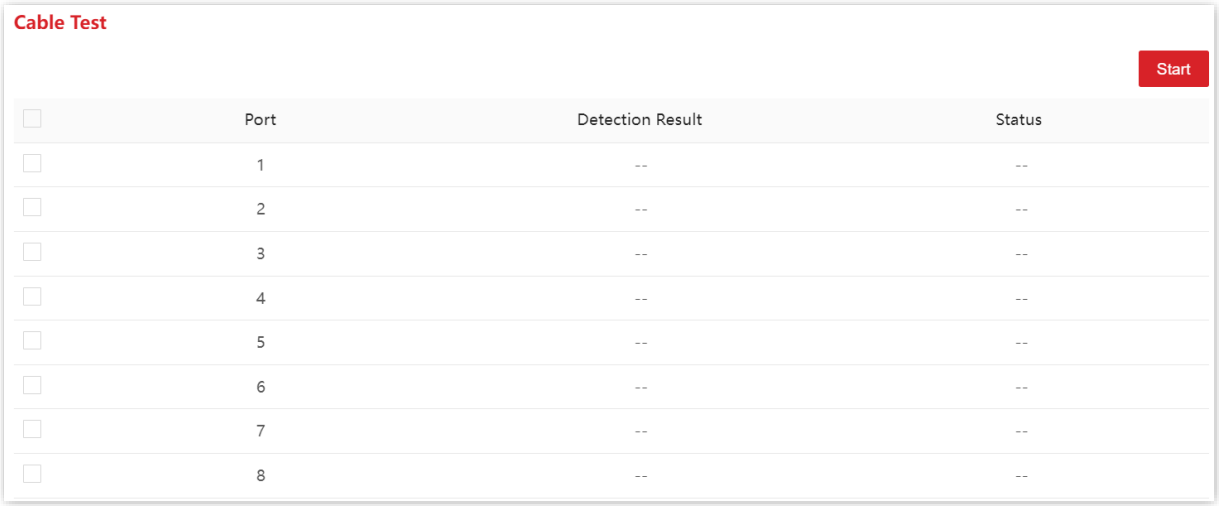


Parameter description

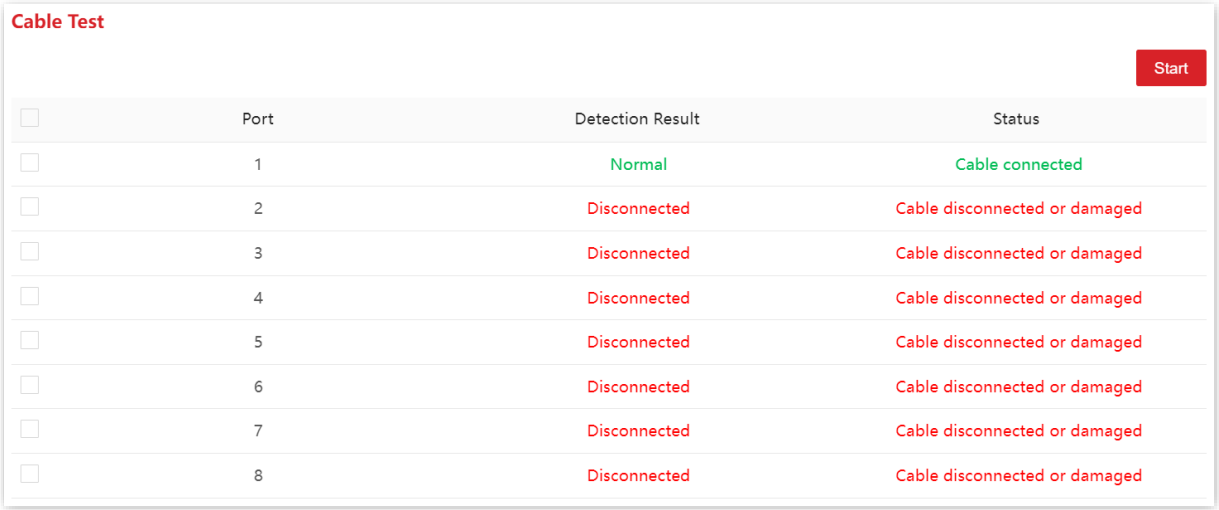
Name	Description
Target IP Address	It specifies the IP address or domain name of the destination device to be pinged.
Ping Packet	It specifies the number of data packets sent by Ping.
Packet Size	It specifies the size of data packets sent by Ping.

3.7 Cable test

Choose **Basic Function** > **Cable Test** to enter the page. On this page, you can test current cabling situations of each port.



Choose the port number you wish to test, click **Start** and then you can view **Detection Result** and **Status** as shown in the figure below.



3.8 Cloud management

IP-COM ProFi Cloud Platform is a cloud platform established by IP-COM, providing central management for IP-COM devices that support ProFi cloud management.

With this switch managed by the ProFi Cloud platform, you can configure and check the parameters of the switch on the ProFi Cloud platform. You can also configure and check these parameters on the web UI of the switch.

To enable ProFi Cloud Management function of the switch, choose **Basic Function** > **Cloud Management** to enter the page.

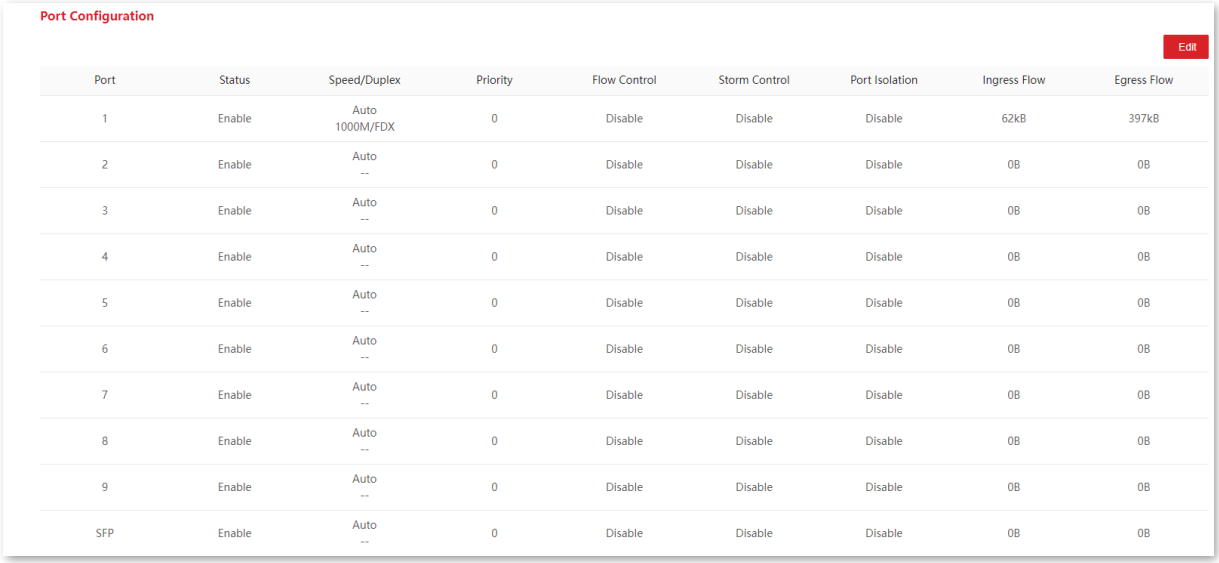
Tip

- For how to add the switch to the IP-COM ProFi Cloud platform, refer to the **Quick Installation Guide** of the switch.
- Please ensure that the switch can access the internet, otherwise it cannot be managed by the ProFi Cloud platform.
- With the switch managed by the ProFi Cloud platform, you can modify the parameters of the switch on both the ProFi Cloud platform or web UI of the switch. The parameters of the switch take effect based on the last modification.

4 Switching

4.1 Basic configuration

Choose **Switching** > **Basic Configuration** to enter the page. On this page, you can view and configure the basic parameters of the ports.



Port Configuration

Edit

Port	Status	Speed/Duplex	Priority	Flow Control	Storm Control	Port Isolation	Ingress Flow	Egress Flow
1	Enable	Auto 1000M/FDX	0	Disable	Disable	Disable	62kB	397kB
2	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
3	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
4	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
5	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
6	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
7	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
8	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
9	Enable	Auto --	0	Disable	Disable	Disable	0B	0B
SFP	Enable	Auto --	0	Disable	Disable	Disable	0B	0B

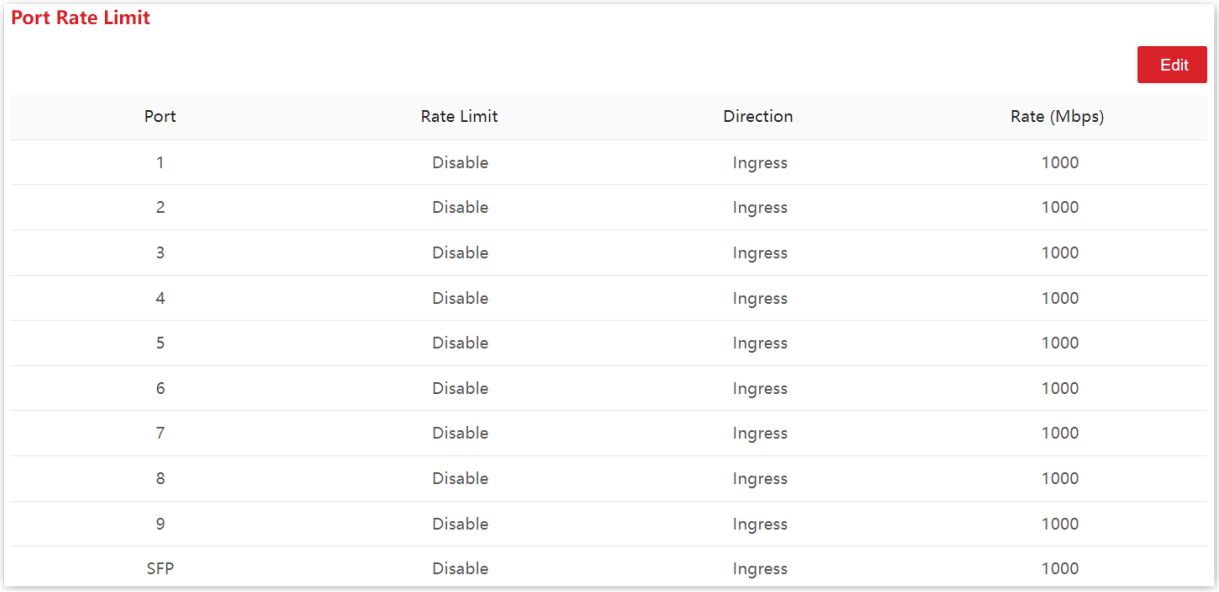
Parameter description

Name	Description
Port	It specifies the ID of the port.
Status	It specifies the current connection status of the port, including **Enable**, **Disable**, and **No Change**.
Speed/Duplex	It specifies the transmission speed and duplex mode of the port. – **Auto**: The port automatically negotiates the speed and duplex mode with the peer device. – **10M/HDX**: The negotiation speed of the port is 10Mbps and the duplex mode is half duplex mode. – **10M/FDX**: The negotiation speed of the port is 10Mbps and the duplex mode is full duplex mode. – **100M/HDX**: The negotiation speed of the port is 100Mbps and the duplex mode is half duplex mode. – **100M/FDX**: The negotiation speed of the port is 100Mbps and the duplex mode is full duplex mode. – **1000M/FDX**: The negotiation speed of the port is 1000Mbps and the duplex mode is full duplex mode. – **No Change**: Keep the original negotiation speed and duplex mode of the port.  If not connected or negotiated failure, it will be shown as “--”.
Priority	It specifies the data packets with a higher priority are transmitted preferentially if port congestion occurs. A larger value of Priority indicates a higher priority.
Flow Control	Enable/Disable the flow control function of the selected port. By default, the port flow control is disabled. When the flow control of the switch and the terminal equipment are all enabled, if some port congestion of the switch occurs, the port will send the pause frame to the terminal equipment that will be suspended to send data after receiving the pause frame. Meanwhile, when one port of the switch receives a pause frame, the port also will be paused to send data.  Enable the flow control to avoid the data packet loss caused by the inconsistency of the sending and receiving rate. Yet that will also affect the communication rate of the data source port and other facilities. Please be careful with this function when linking the network port.

Name	Description
Storm Control	Enable/Disable the broadcasting storm control function of the selected port. By default, the storm control is disabled. Broadcast storm means that the broadcasting frame quantities are soaring up due to the continuous transmissions, which brings negative effect on the communication, degrades the system performance and even results in breakdown of the network. While enabling the storm control, the switch will discard the excessive broadcast traffic as the broadcast traffic on the port exceeds the limited value (10Mbps), thus reducing the proportion of the broadcast traffic to the limited range.
Port Isolation	Enable/disable port isolation function of the selected port. By default, the port isolation is disabled. While enabling the port isolation, isolated ports are isolated from each other and can only communicate with ports that are not isolated.
Ingress Flow	It specifies the statistics of data traffic received by the port.
Egress Flow	It specifies the statistics of data traffic transmitted by the port.

4.2 Port rate limit

Choose **Switching** > **Port Rate Limit** to enter the page. On this page, you can enable or disable the ingress rate limit for each port.



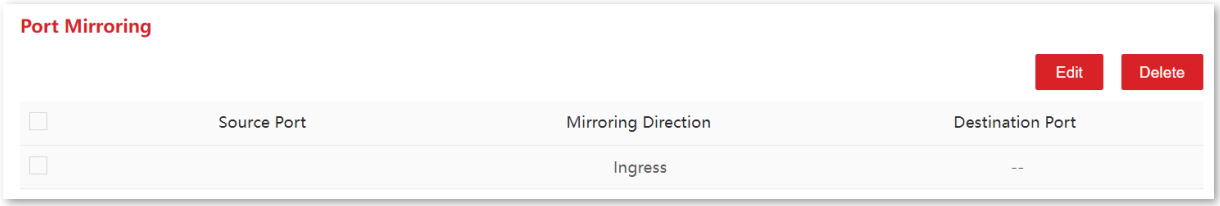
Parameter description

Name	Description
Port	It specifies the ID of the port.
Rate Limit	Enable/Disable the rate limit of the selected port.
Direction	It specifies the direction of the port rate limit. – **Ingress**: The rate at which the port receives packets will be limited. – **Egress**: The rate at which the port sends packets will be limited. – **Two-way**: The rate at which the port sends and receives packets will be limited.
Rate (Mbps)	It specifies the maximum rate of the port after the port rate limit is set.

4.3 Port mirroring

Port mirroring is a method of copying and sending data from a port or multiple ports (source ports) to a specified port (destination port) of the switch. The destination port is usually connected to a data monitoring device, enabling you to monitor data traffic, analyze performance and diagnose faults.

Choose **Switching** > **Port Mirroring** to enter the page. On this page, you can configure the port mirroring rules.

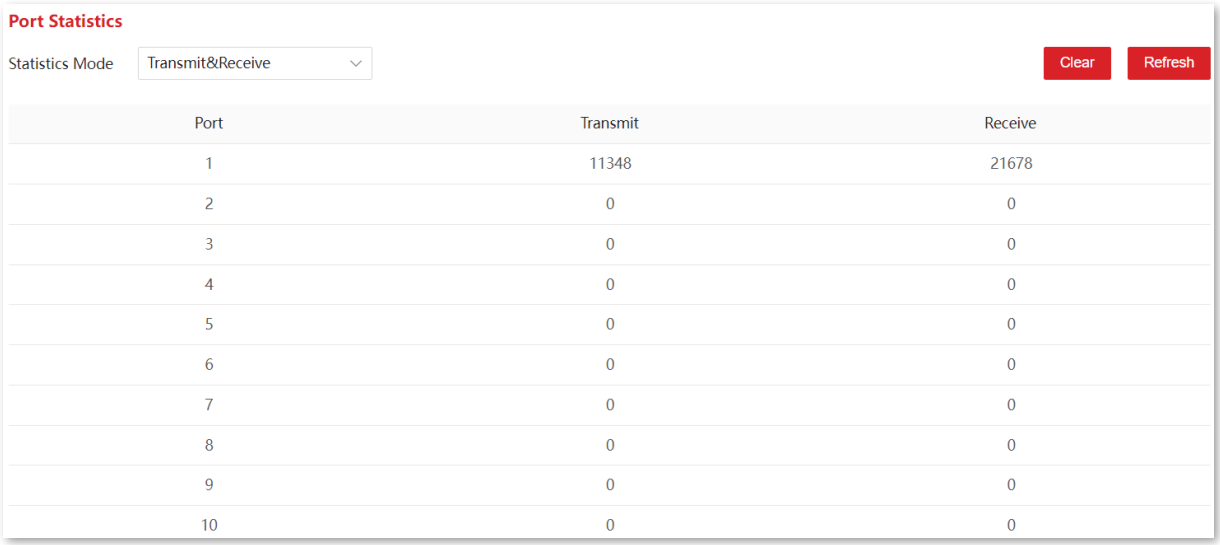


Parameter description

Name	Description
Source Port	It specifies the ports whose packets will be copied. Multiple ports can be selected.
Mirroring Direction	It specifies the packet type. – **Ingress**: Packets received by source ports will be copied to the destination port. – **Egress**: Packets transmitted by source ports will be copied to the destination port. – **Two-way**: Packets transmitted and received by source ports will be copied to the destination port.
Destination Port	Packets of source ports will be copied to this port. A mirroring group can contain only one destination port.

4.4 Port statistics

Choose **Switching** > **Port Statistics** to enter the page. On this page, you can view and clear the packet statistics of each port.



Parameter description

Name	Description
Port	It specifies the ID of the port.
Statistics Mode	It specifies the statistics mode of port packets. – **Transmit & Receive**: It specifies the number of transmitted and received packets. – **Conflict & Transmit**: It specifies the number of collision packets and the number of transmitted packets. – **CRC Error & Receive**: It specifies the number of CRC verification error packets and received packets.
Clear	Clear port statistics of all ports.
Refresh	Refresh port statistics of all ports.

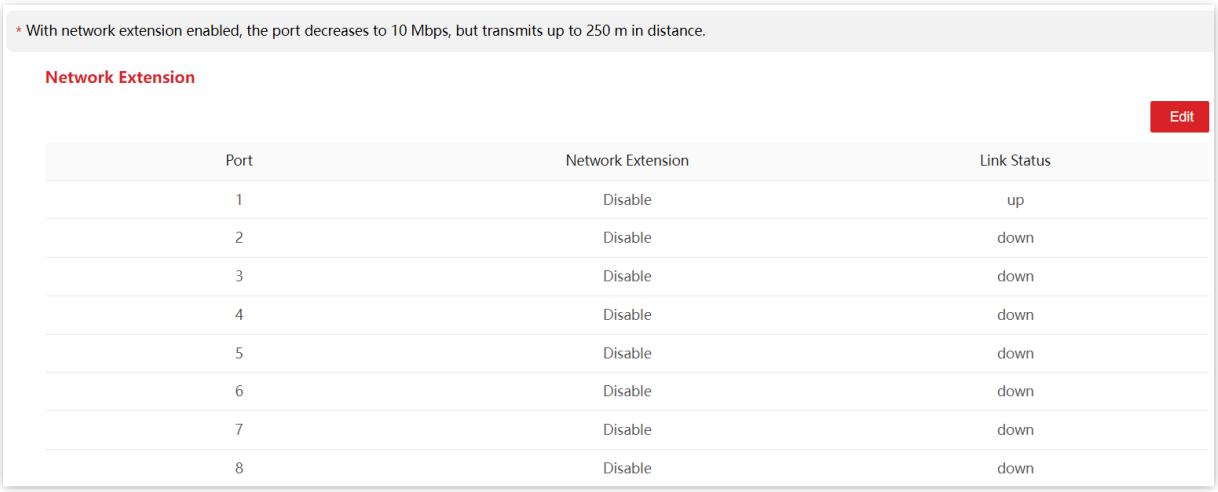
4.5 Network extension

The switch offers you the network extension function, which can extend the data transmission of downlink ports to make network deployment more convenient.

Once network extension is enabled, the port link speed will be automatically negotiated to 10Mbps. In this situation, if using the CAT5, CAT5E cable or better, the transmission distance of port data can break 100 meters, and the maximum distance can reach 250 meters.

It is recommended to enable the function when IP cameras are connected to the switch with long distance (>100m).

Choose **Switching** > **Network Extension** to enter the page.



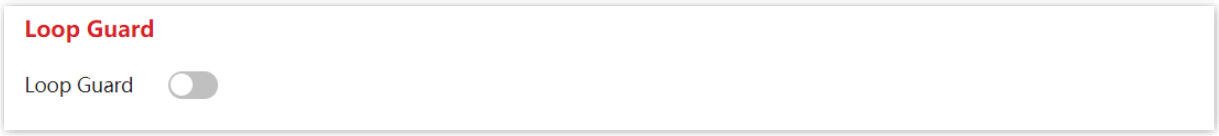
Parameter description

Name	Description
Port	It displays the number of the port which can supply PoE power.
Network Extension	Enable/Disable network extension of the selected port.
Link Status	It displays the link status of the port. If the port is connected normally, it will be shown as **up**. If the port is not connected or the connection is abnormal, it will be shown as **down**.

4.6 Loop guard

Choose **Switching** > **Loop Guard** to enter the page. On this page, you can enable or disable the loop guard function of the switch.

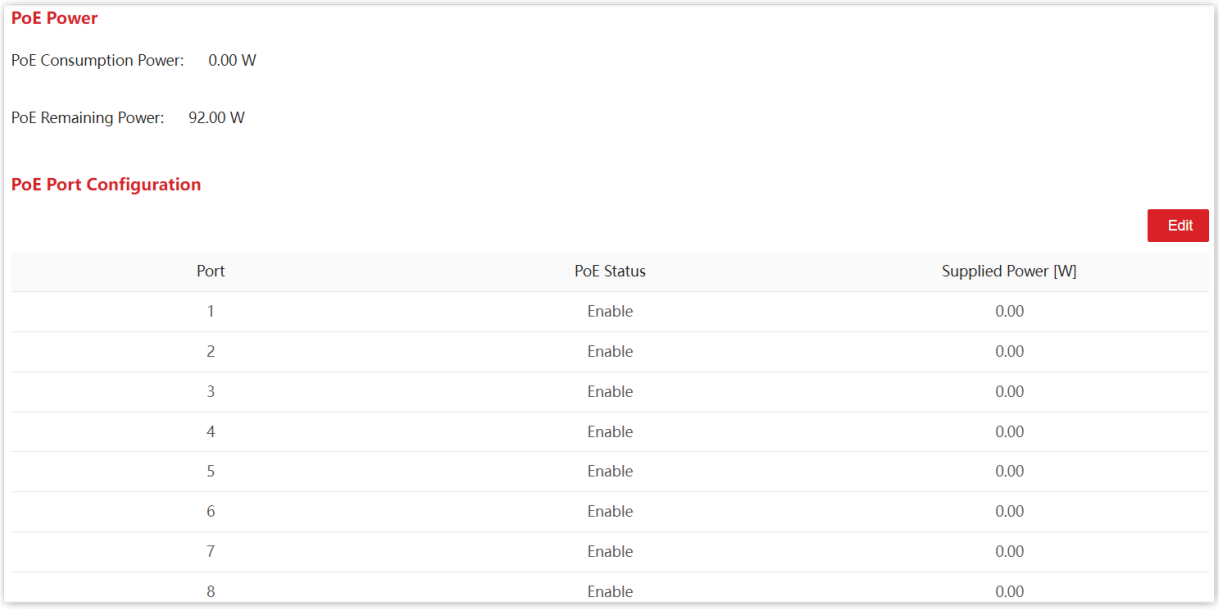
After loop protection is enabled, if there is a loop on the current device, the port where the loop occurs will be set to Blocking state and will not forward data packets. After the loop is eliminated, the port will automatically resume forwarding state. By default, this function is disabled.



5 PoE management

All downlink ports support PoE power supply and conform to IEEE 802.3af and IEEE 802.3at. The switch will automatically supply required PoE power to the powered device which is connected to the PoE port.

Click **PoE Management** to enter the page. You can check the PoE power status of the current switch and enable/disable the PoE power function of the downlink port as well.



Parameter description

Name	Description
PoE Consumption Power	It displays the total output power of the switch supplied by PoE.
PoE Remaining Power	It displays the remaining output power of the switch supplied by PoE.
Port	It displays the downlink port number of the switch.
PoE Status	Enable/Disable the PoE power function of the selected port.
Supplied Power [W]	It displays the output power of the downlink port supplied by PoE.

6 Network security

MAC binding

MAC binding provides the function of static MAC address table: After a port is bound with a MAC address, the device that matches the designated MAC address can access the network only through this port, not through other ports.

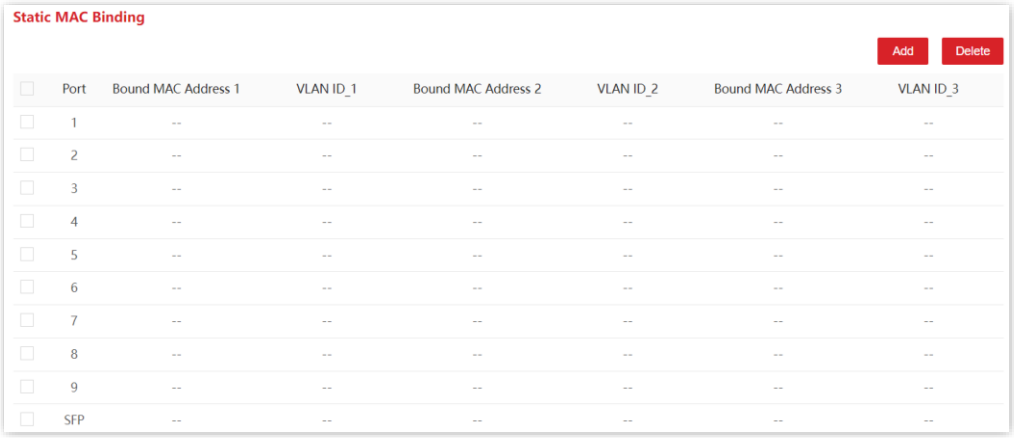
The MAC binding function ensures network security and user authority and effectively prevents unauthorized users from gaining data by cheating and performing loiter net.

Tip

Bound MAC addresses are manually added and deleted, and will not be aged over time.

Configure MAC binding

Choose **Network Security** > **MAC Binding** to enter the page. On this page, you can perform static MAC address binding.



Parameter description

Name	Description
Port	Select a port whose static MAC address binding function needs to be configured.

Name	Description
Bound MAC Address 1/2/3	It displays the bound MAC address.
MAC Address 1/2/3	Enter an access device MAC address bound to this port. The switch supports binding up to three access devices. Note Broadcast or multicast address binding is not allowed.
VLAN ID_1/2/3	It specifies the VLAN to which the MAC address belongs.

Example of configuring MAC binding

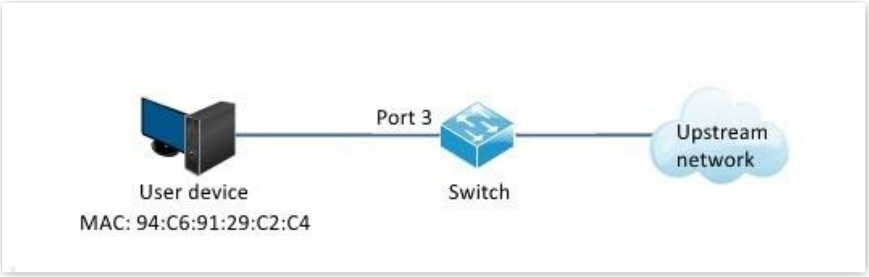
Networking requirement

The MAC address of the user device is 94:C6:91:29:C2:C4. Connect it to port 3 of the switch to prevent other unauthorized users from performing loiter net or MAC addresses pretending to be the authorized user from gaining data from other ports of the switch.

Solution

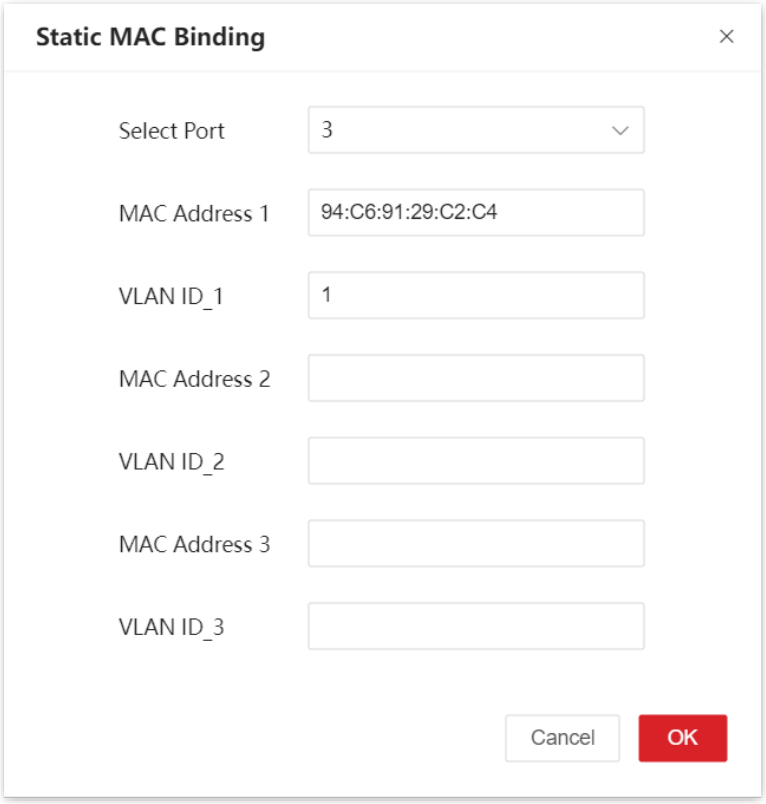
Bind the MAC address of the user device to port 3 of the switch.

Assume that the user device belongs to VLAN 1.



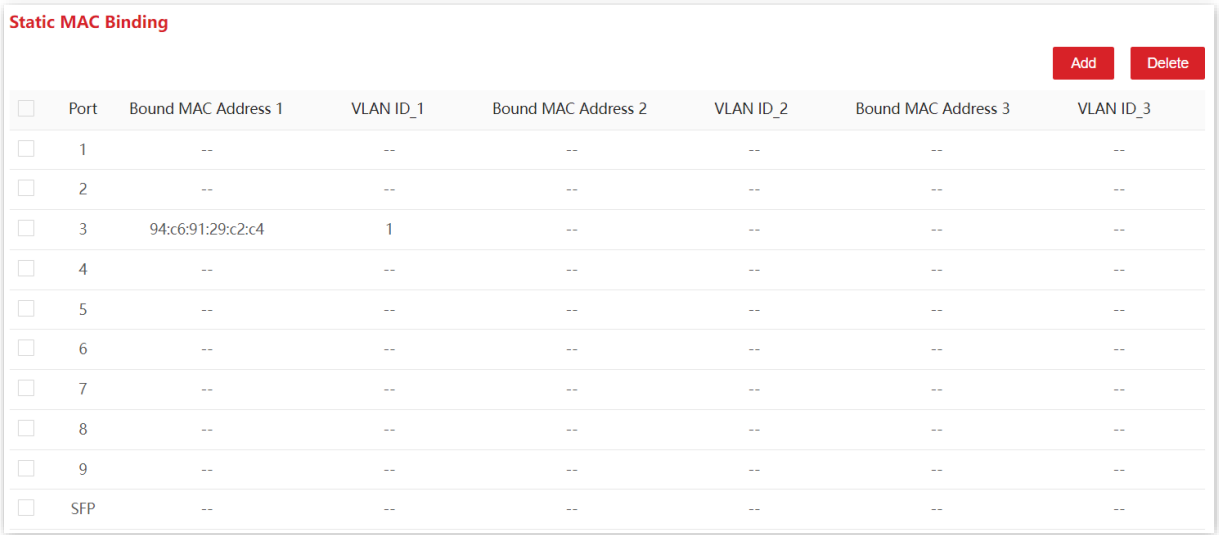
Configuration procedure

1. Log in to the web UI of the switch and choose **Network Security** > **MAC Binding**.
2. Select Port **3**.
3. Enter the user device MAC address **94:C6:91:29:C2:C4** in the **MAC Address 1** column, and set **VLAN ID_1** to **1**.
4. Click **OK**.



----End

MAC address is bound successfully. See the following figure.



Verification

The device with MAC address **94:C6:91:29:C2:C4** must be connected to port 3 of the switch to access the higher-level network. If the device with MAC address **94:C6:91:29:C2:C4** is connected to other ports of the switch, this device cannot access the higher-level network.

Appendix

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
CRC	Cyclic Redundancy Check
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FDX	Full Duplex
HDX	Half Duplex
IP	Internet Protocol
LAN	Local Area Network
MAC	Medium Access Control
PoE	Power over Ethernet
PVID	Port-based VLAN ID
QoS	Quality of Service
SA	Source Address
VLAN	Virtual Local Area Network
WAN	Wide Area Network

Configure the switch to access the internet

Networking requirement

You want to configure the switch to access the internet.

Tip

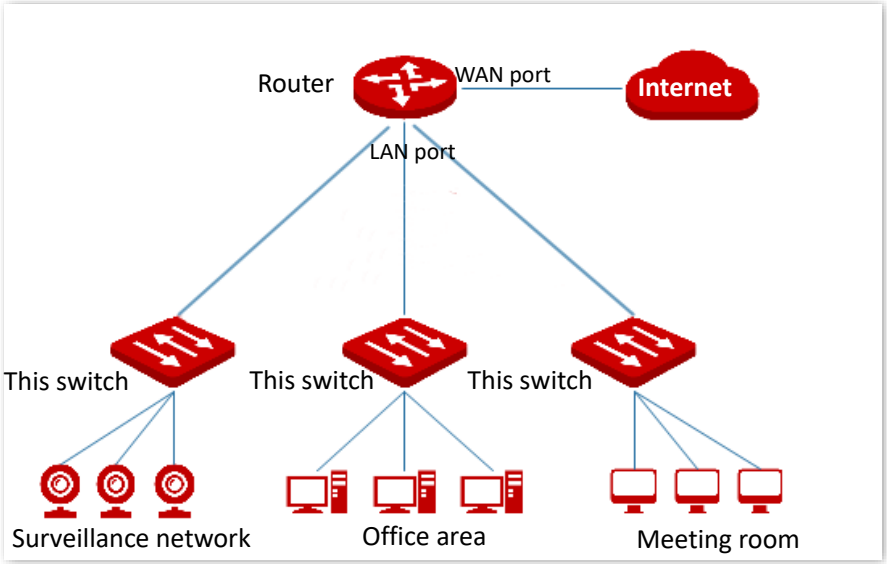
The following shows the steps to access the internet when the switch's DHCP client is disabled.

(When DHCP client and DNS are enabled, the switch automatically obtains IP address and other parameters from the upstream router.)

Assume that:

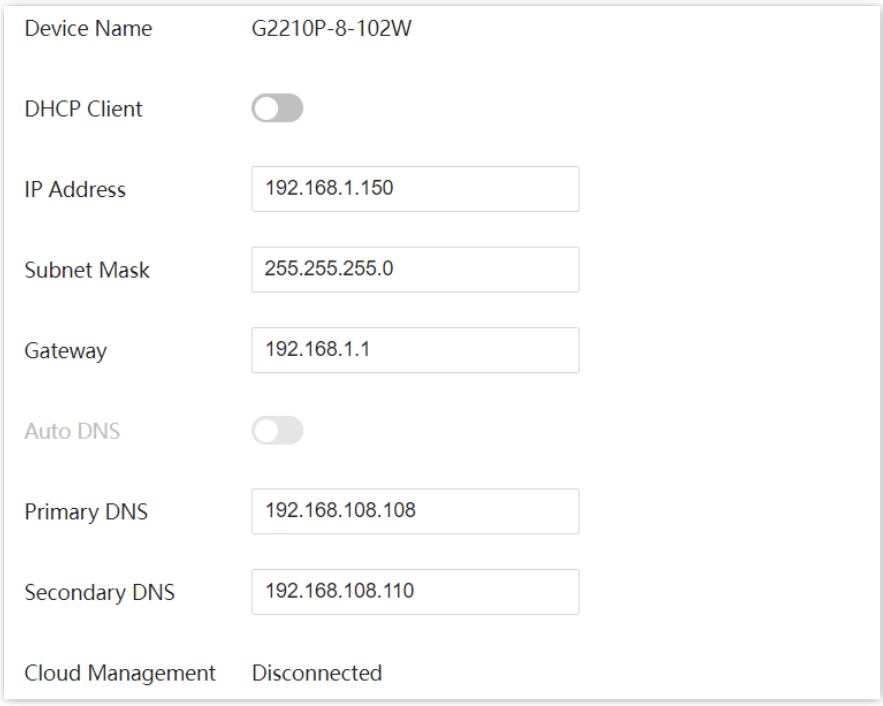
- LAN IP address/subnet mask of the upstream router: 192.168.1.1/255.255.255.0
- Primary & secondary DNS server address: 192.168.108.108, 192.168.108.110

The network topology is as shown below.



Configuration procedure

1. Log in to the web UI of the switch.
2. Configure the IP address, subnet mask, gateway and DNS server address of the switch.
   (1) Choose **Basic Function** > **System Overview**.
   (2) Disable **DHCP Client**.
   (3) Set **IP Address** to an IP address in the same network segment as that of the LAN IP address of the router, which is **192.168.1.150** in this example.
   (4) Set **Subnet Mask** to **255.255.255.0**, **Gateway** to **192.168.1.1**.
   (5) Set the **Primary DNS** and **Secondary DNS** to DNS server addresses that can properly resolve the URL of the ProFi Cloud platform, which are **192.168.108.108, 192.168.108.110** respectively in this example.
   (6) Click **Save**.



----End

Verification

After configuration, you can test whether the switch can access the internet through the Ping test by navigating to **Basic Function** > **Diagnosis**.

You can Ping a domain name to test the internet connection status, which is **www.bing.com** in this example. The switch accesses the internet successfully if the test results are as shown below.