# Wi-Tek Cloud Easy Smart PoE Switch

# WEB User Manual

www.wireless-tek.com

## This manual applies to the following switch models

Product Model

| Product Model | Interface |
|---|---|
| WI-PCES310G | 8-port Gigabit PoE+ RJ45 and 2-port Gigabit RJ45 |
| WI-PCES320GFH | 16-port Gigabit PoE+ RJ45 and 2-port Gigabit RJ45, 2 Gigabit SFP |
| WI-PCES328GFH | 24-port Gigabit PoE+ RJ45 and 2-port Gigabit RJ45, 2 Gigabit SFP |

# Preface

## Manual Introduction

This manual primarily describes web-based operations for the Wi-Tek Cloud Easy Smart PoE switch. We try to group each system function into its own chapter, so that when you need to use a particular function, you only need to refer to the corresponding chapter. For overlapping functions that cannot be grouped together, this manual will specifically indicate their use.

We hope this manual will be helpful to your work!

## Target Audience

This manual is mainly intended for the following persons:

Software debugging engineer

On-site maintenance engineer

System maintenance engineer

## Conventions in this manual

Icon Symbol Conventions

| Format | illustrate |
|---|---|
| **illustrate:** | Supplement or emphasize the previous content. |
| **Attention:** | Indicates the content that requires attention during the installation or use of the equipment, which is the key to the correct installation and operation of the equipment. |
| **Warning:** | Prohibited operations or operations that must be performed in accordance with prescribed steps, otherwise personal injury or equipment damage may result. |

# Content

# 1 Introduction

Device WEB management is network management software for a single device. It provides a visual configuration method for business functions, helping operation and maintenance personnel to quickly complete device configuration, view the current configuration information of various business functions, and understand the current working status of the device.

Device web management allows you to manage network devices, such as routers or switches, using browsers like IE , Firefox , and Chrome . This is primarily used to simplify device configuration and improve product usability.

Device web management consists of two parts: a web server and a web client. The web server, integrated into the device, receives and processes requests from the client and returns the results to the client. The web client is typically a web browser, such as Internet Explorer, Firefox, or Chrome .

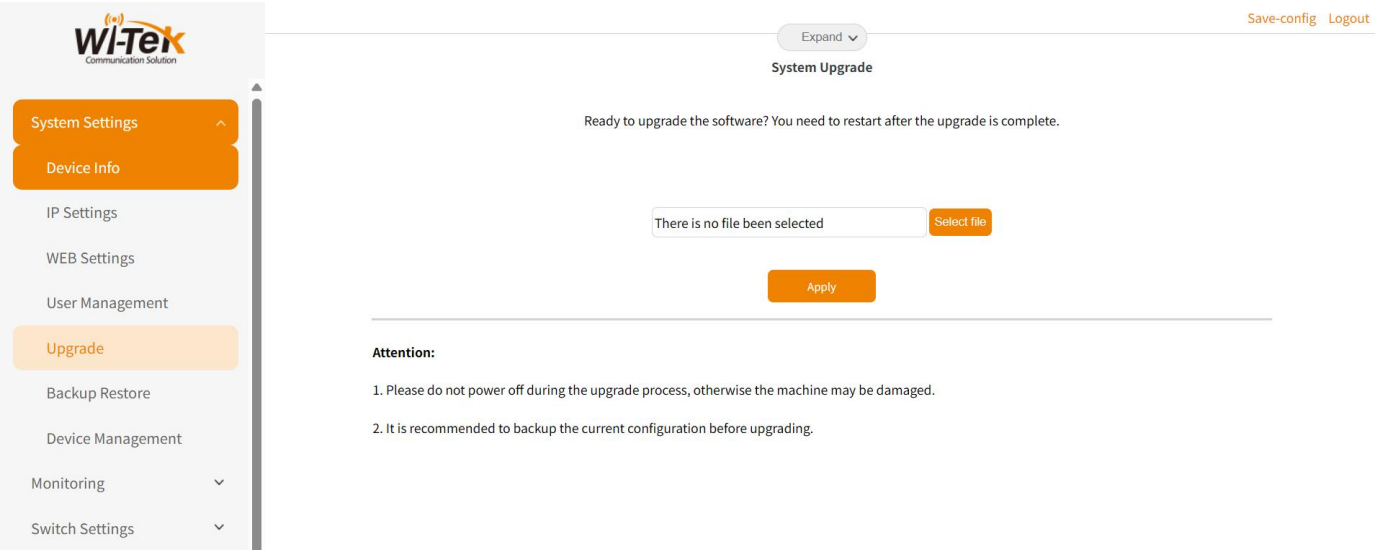
# 2 Download device WEB package and device upgrade

## 2.1 Download the device WEB package

First, download the device WEB package  WI-PCES310G_V1000SP10_20241112_host.img and put it in a local folder.

## 2.2 Equipment upgrade

After logging in to the device using a web browser, upgrade the device in the "System Management" - " Device Upgrade " page. For details, see Section 4.5.




## 2.3 Restore factory settings

If the user needs to restore the device to its default configuration, press and hold the "reset" button on the device panel for 10 seconds and then release it. After all electrical ports are turned off, ports 9 and 10 will light up orange first, followed by ports 1-8.

# 3 WEB LOGIN

## 3.1 Web login

Open a browser (Chrome, Firefox, 360, and Edge are currently supported, but IE is not recommended), enter the switch management address, and enter the login page (as shown in Figure 3-1 ). The default switch IP address is 192.168.0.1 , and the default subnet mask is 255.255.255.0.

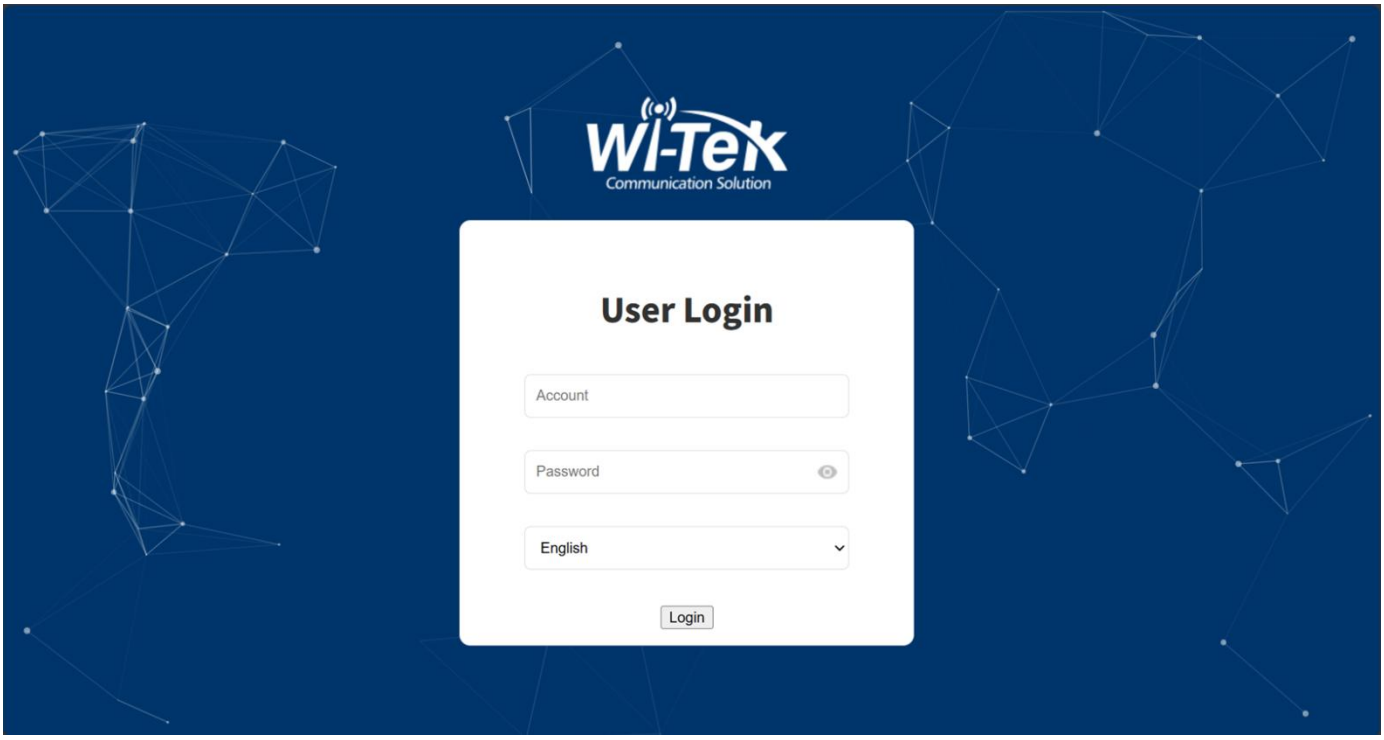



Figure 3 - 1

## 3.2 User account and password configuration

The user account and password for web management must be configured on the System Management - Account Settings page. The default user name is admin, and the default password must be changed for the first login . See Figure 3-2.

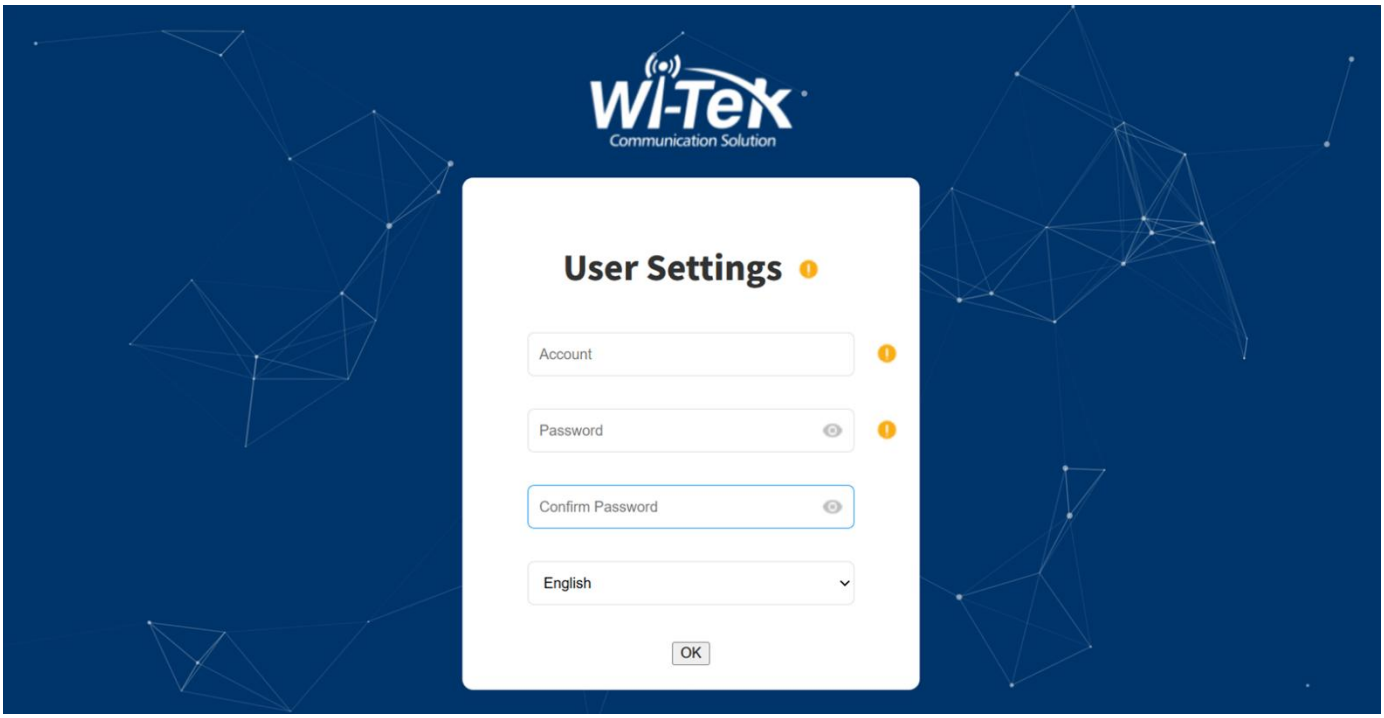



Figure 3 - 2

## 3.3 Device IP address and gateway configuration

Before managing the switch through the web, users can configure the device 's IP address, subnet mask, and gateway address through the "System Management" - " IP Settings " page. You can choose a static IP address or obtain an address through DHCP. The default is a static IP address.

For example: Configure IP address: 192.168.1.1, subnet mask: 255.255.255.0, click " Apply " to take effect (as shown in Figure 3-3 ), and the device will automatically jump to the newly configured IP address and log in to the device again.

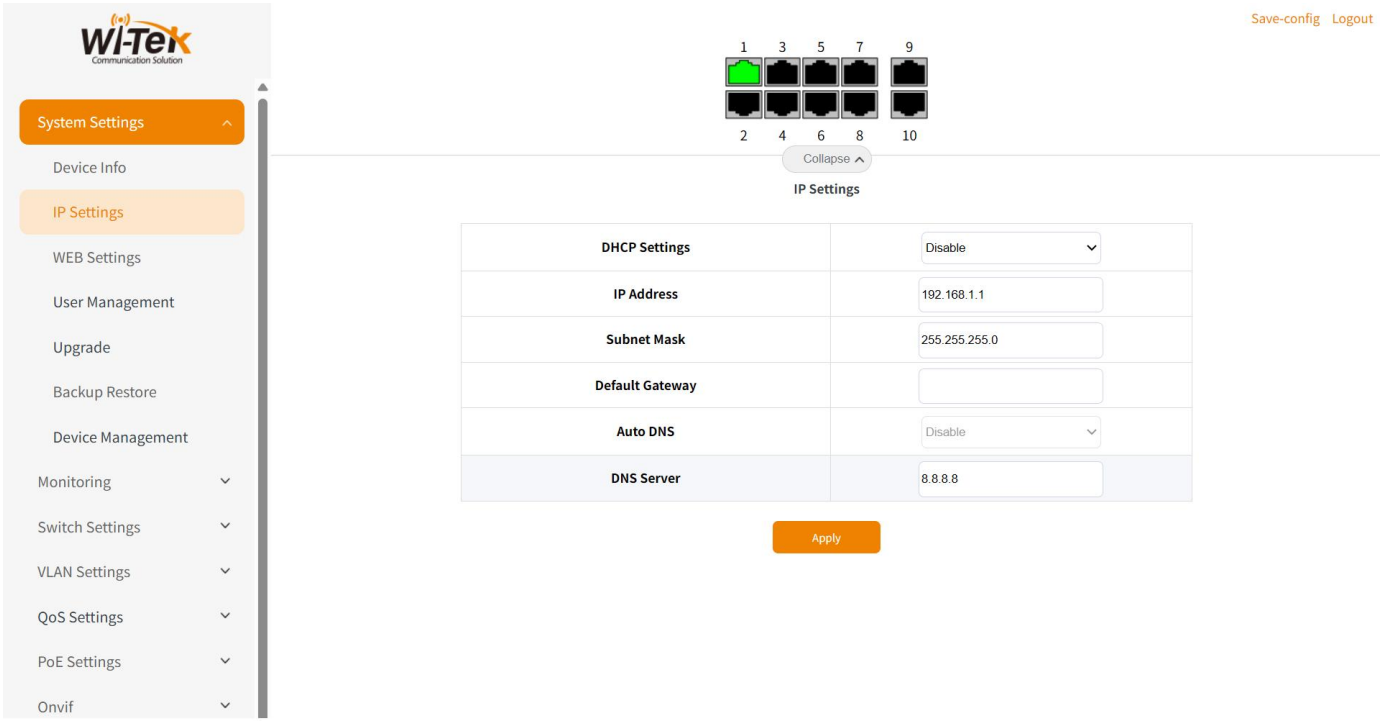



Figure 3- 3

**Attention：**

- IP address is 192.168.0.1 , the default subnet mask is 255.255.255.0, and the default gateway is blank.

## 3.4 Error message

When the user enters an incorrect username or password, he or she cannot successfully log in to the operation interface. At this time, the interface will give a corresponding prompt (as shown in Figure 3-4 ) .

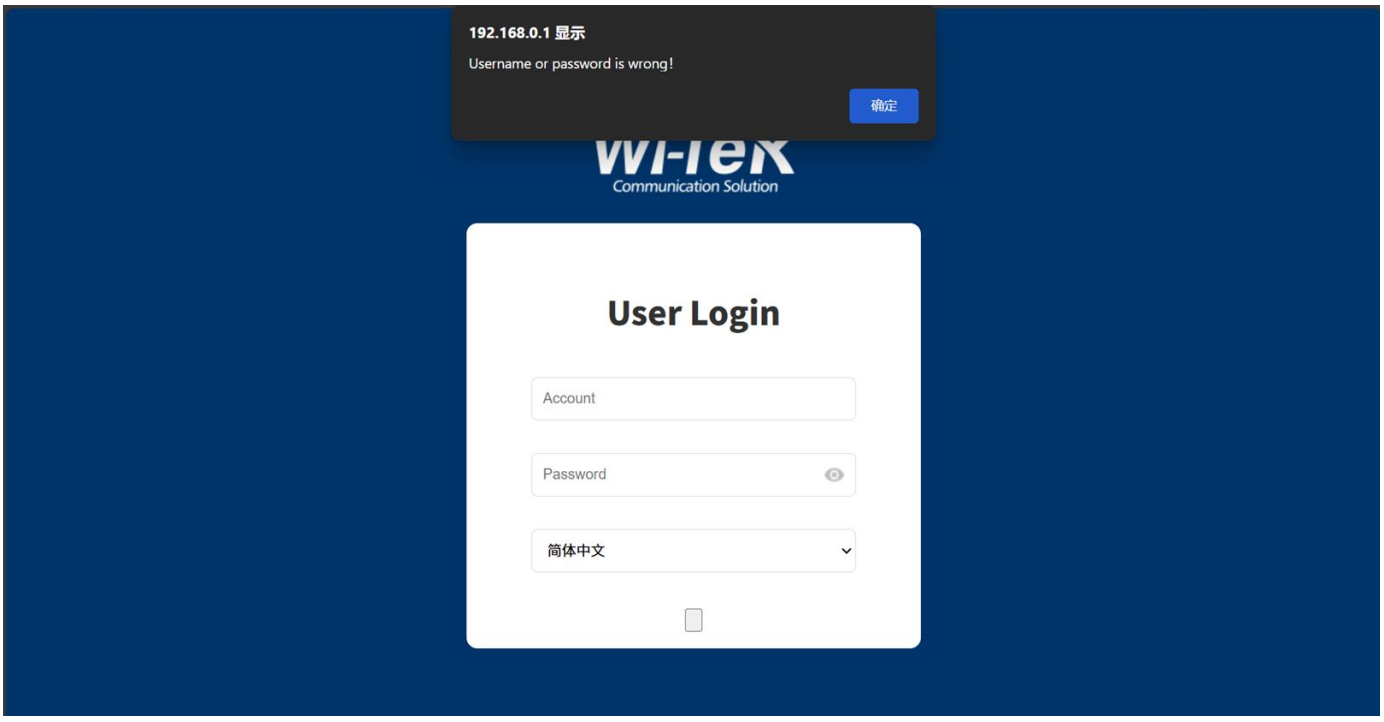



Figure 3 - 4

## 3.5 Language settings

Click the drop-down option above the login interface to choose Simplified Chinese or English mode to log in (as shown in Figure 3-5 ) . The default is English.


Figure 3 - 5

Sign out

After completing the configuration of the device, the user can log out of the operation interface by clicking the " Log Out " button.

" Logout " button is located in the upper right corner of the operation page (as shown in Figure 3-6 ) .

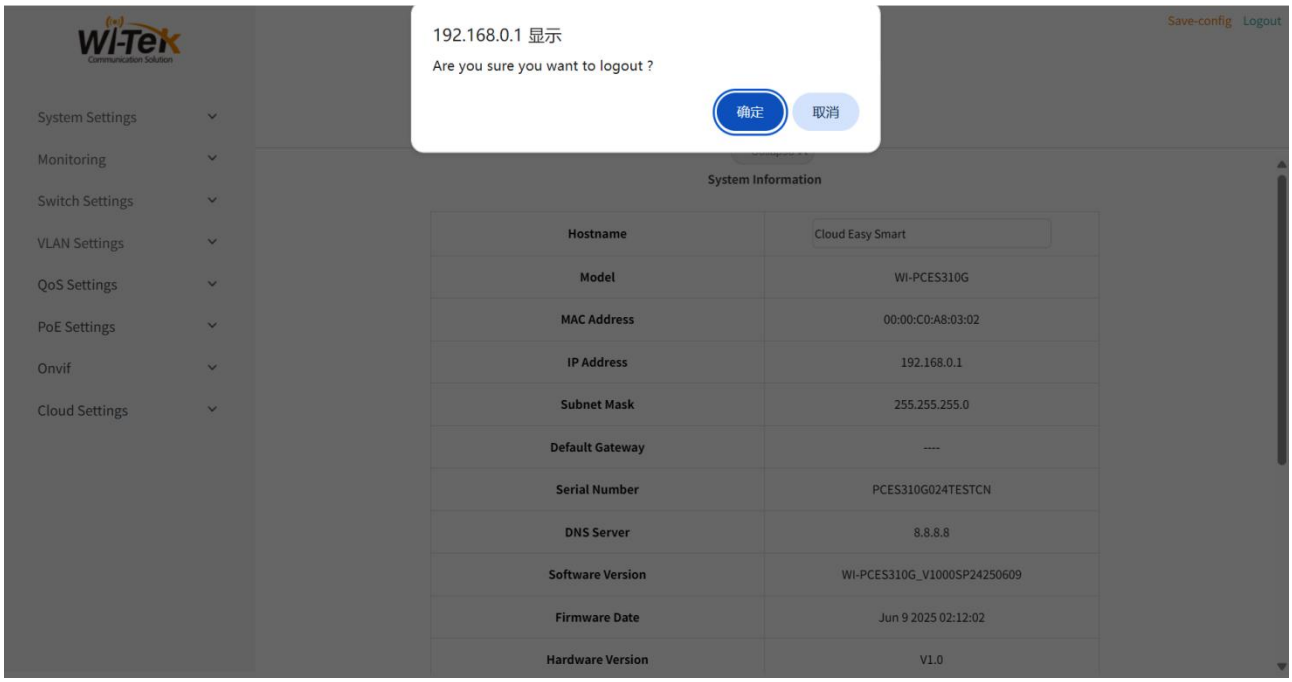



Figure 3 - 6

## 3.6 Save Configuration

To save the configuration, click the " Save Configuration " button in the upper right corner of the operation page . Click "Save Configuration" and then "OK" (as shown in Figure 3 - 7 ). After saving, a message "Save Configuration Successfully" will be displayed.

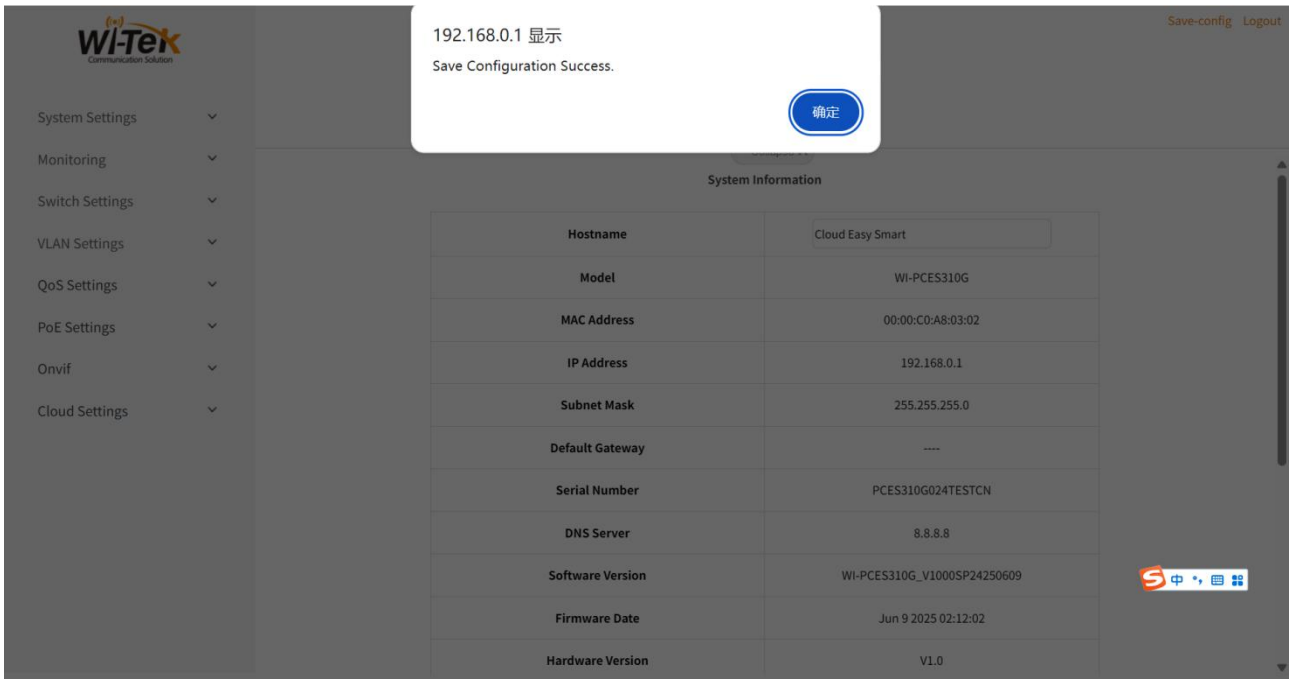



Figure 3 - 7

## 3.7 Restart

To soft restart the device, click "System Management - Device Management - Device Restart" and "OK" (as shown in Figure 3-8 ) . During the restart process, all LED lights will go out and then light orange .

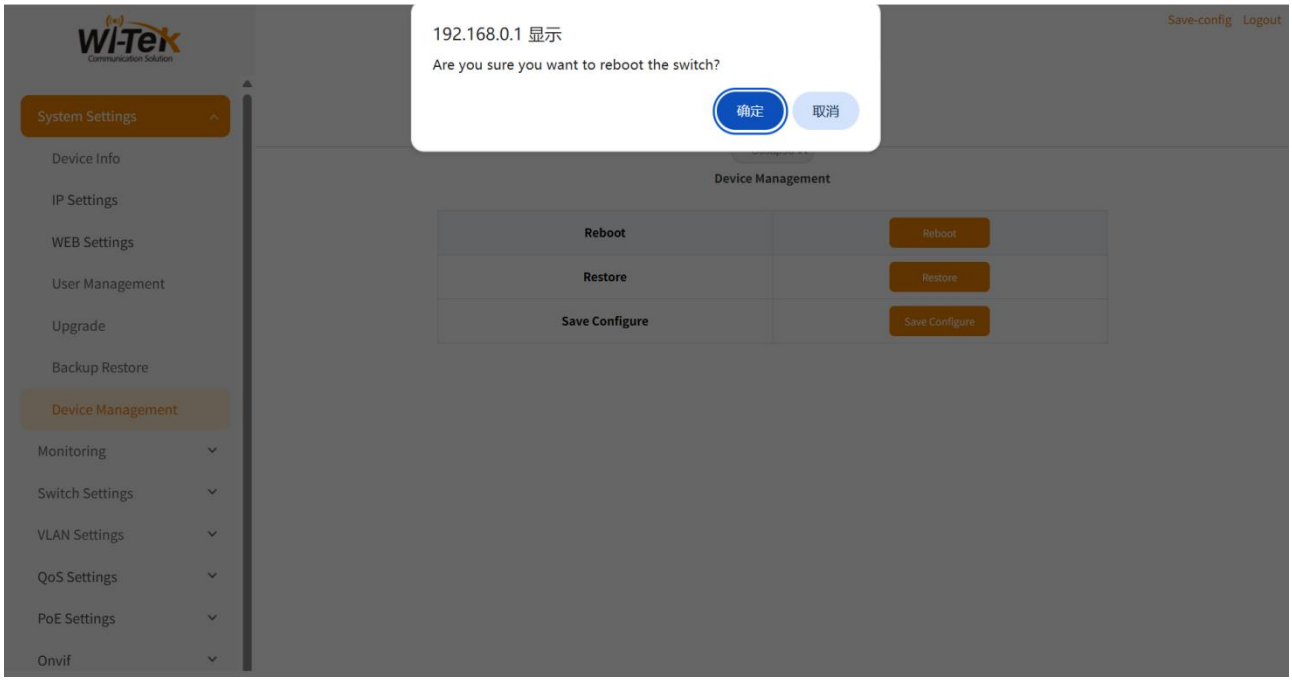



Figure 3 - 8

## 3.8 Port status display

After the user logs in successfully, the device panel is displayed on the operation page. The port status can be displayed or hidden by " Expand,Collapse " from left to right , with single on top and double on bottom (as shown in Figure 3-9 ) . If the port speed is configured to other speeds, the light color is yellow (as shown in Figure 3-10) .

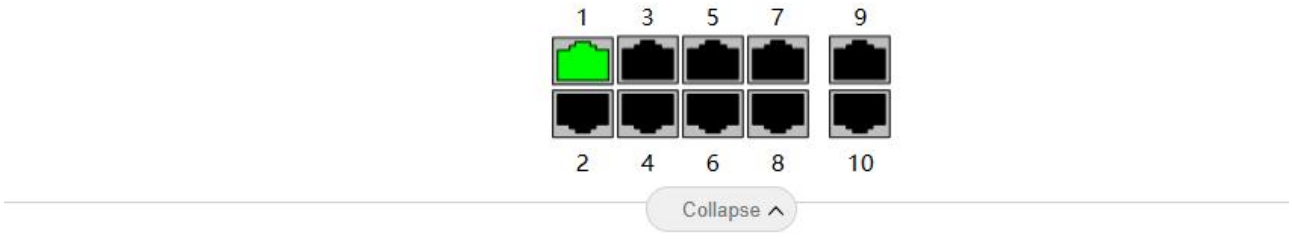



Figure 3 - 9

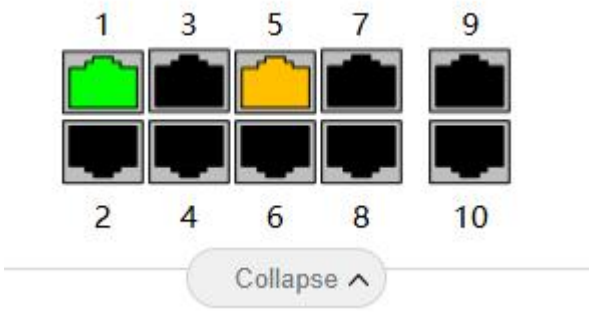



Figure 3 - 10

# 4 System Management

## 4.1 System Information

This page displays basic information about the device, allowing users to configure the system name, device contact, and location . Click "System Management" - " System Information " to enter ( as shown in Figure 4-1 );

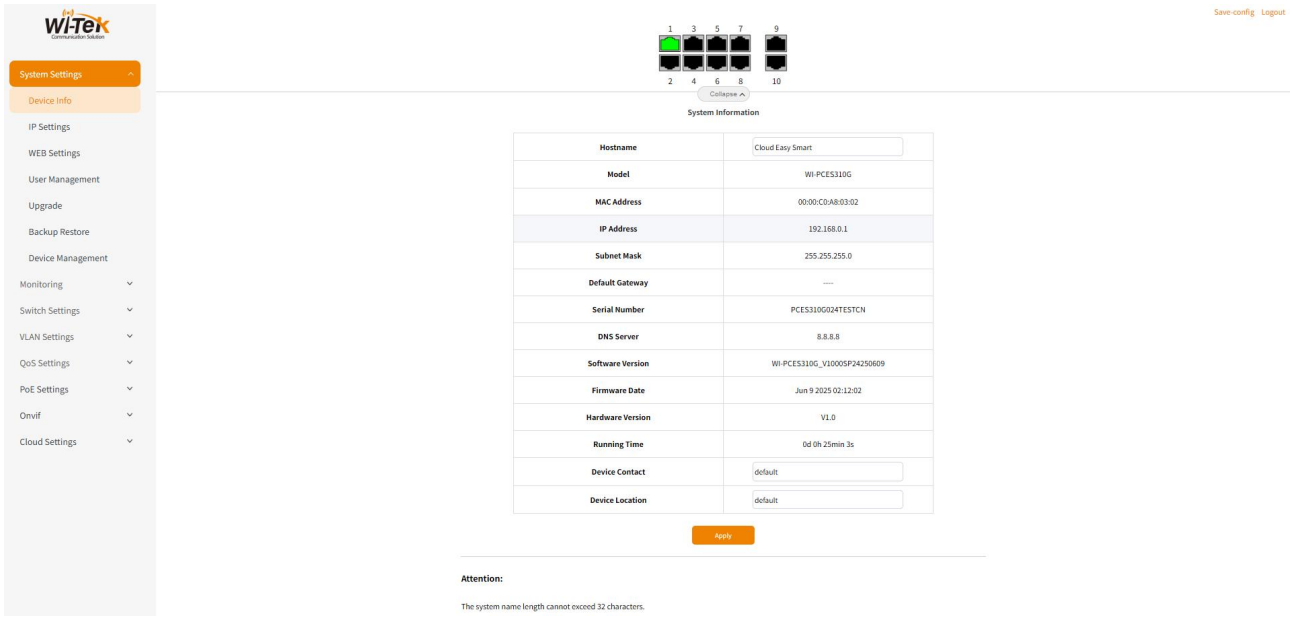



Figure 4-1

### 4.1.1 System information configuration

This page is used to modify the system name, device contact, and location . ( As shown in Figure 4-2 ). The system name defaults to Cloud Easy Smart, and there are no default settings for the device contact and

location .

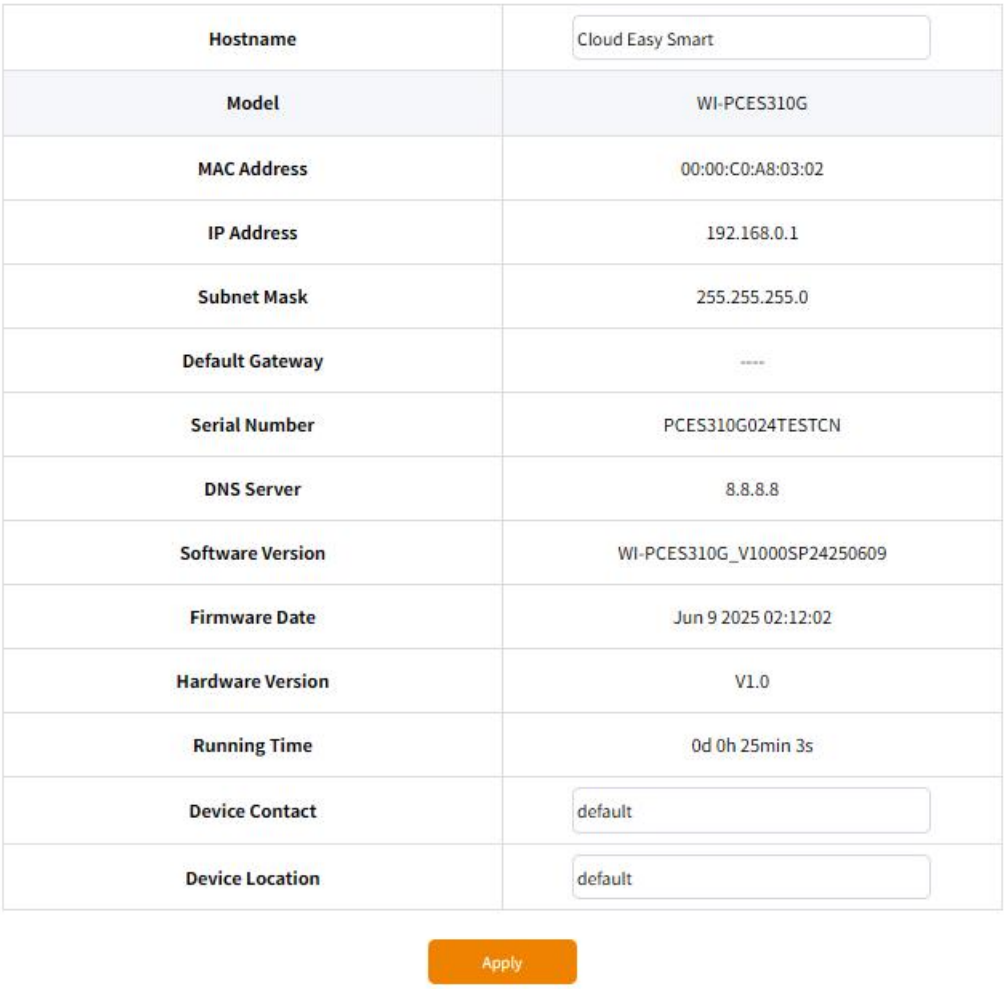



Figure 4-2

**Attention：**

- The system name cannot exceed 32 characters .
- The device contact and location cannot exceed 15 characters.

## 4.2 IP address configuration

This page allows users to configure the device management IP address , including the " IP Configuration" function. Click "System Management" - " IP Configuration" to enter ( as shown in Figure 4-3 ) ;

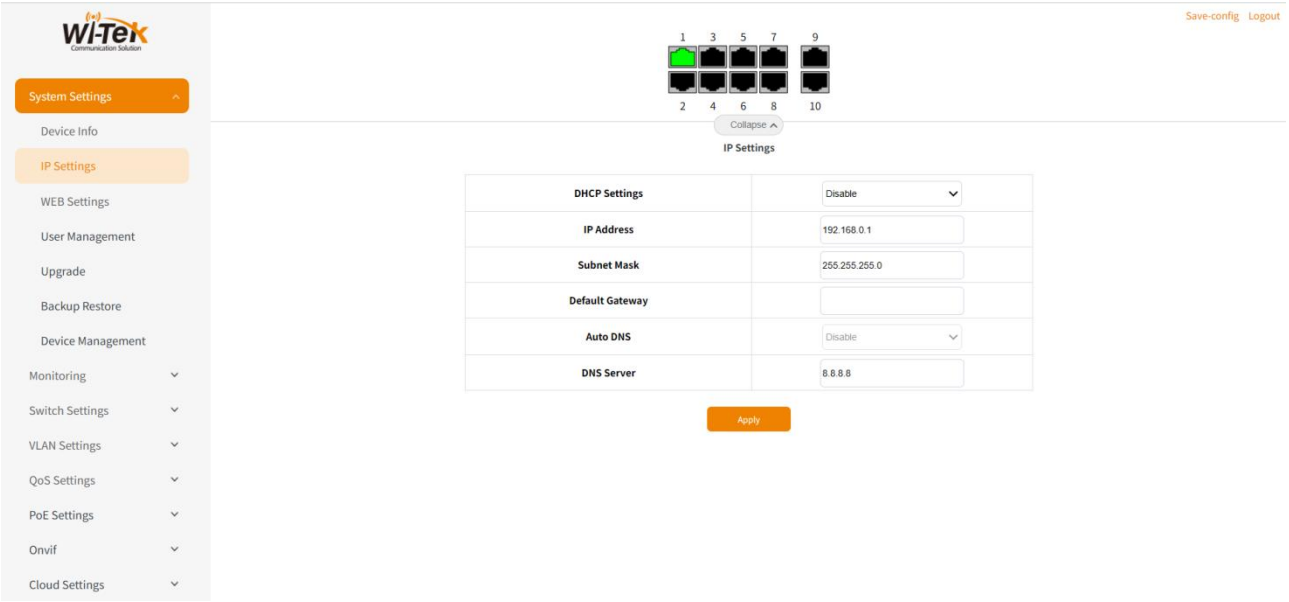



Figure 4-3

### 4.2.1 IP address configuration

DNS acquisition method , network mask, gateway , and DNS server for logging into the management device ( as shown in Figure 4-4 ) . By default, DHCP and automatic DNS are disabled, the IP address is 192.168.0.1 , the subnet mask is 24 bits, there is no default gateway configuration, and the DNS server is 8.8.8.8.


picture 4- 4

**Attention：**

- Automatic DNS can only be configured after enabling DHCP settings ;

## 4.3 WEB settings

### 4.3.1 WEB settings

Click "System Management" - " WEB Settings " in sequence to enter, configure the WEB timeout, and then click " Apply " ( as shown in Figure 4-5 ).

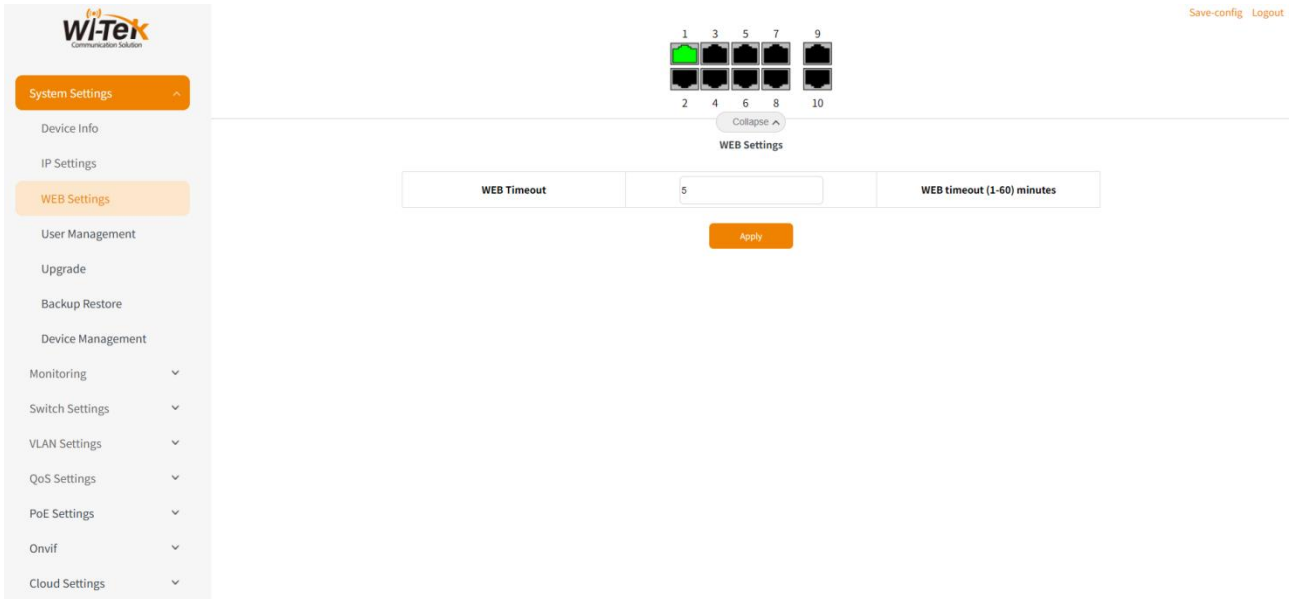



Figure 4-5

## 4.4 Account Settings

This page allows users to configure the device login user , and can modify the account password at the same time. You can also choose to modify one and use the modified account when logging in . Click "System Management" - " Account Settings " in sequence to enter (such as Figure 4-6);

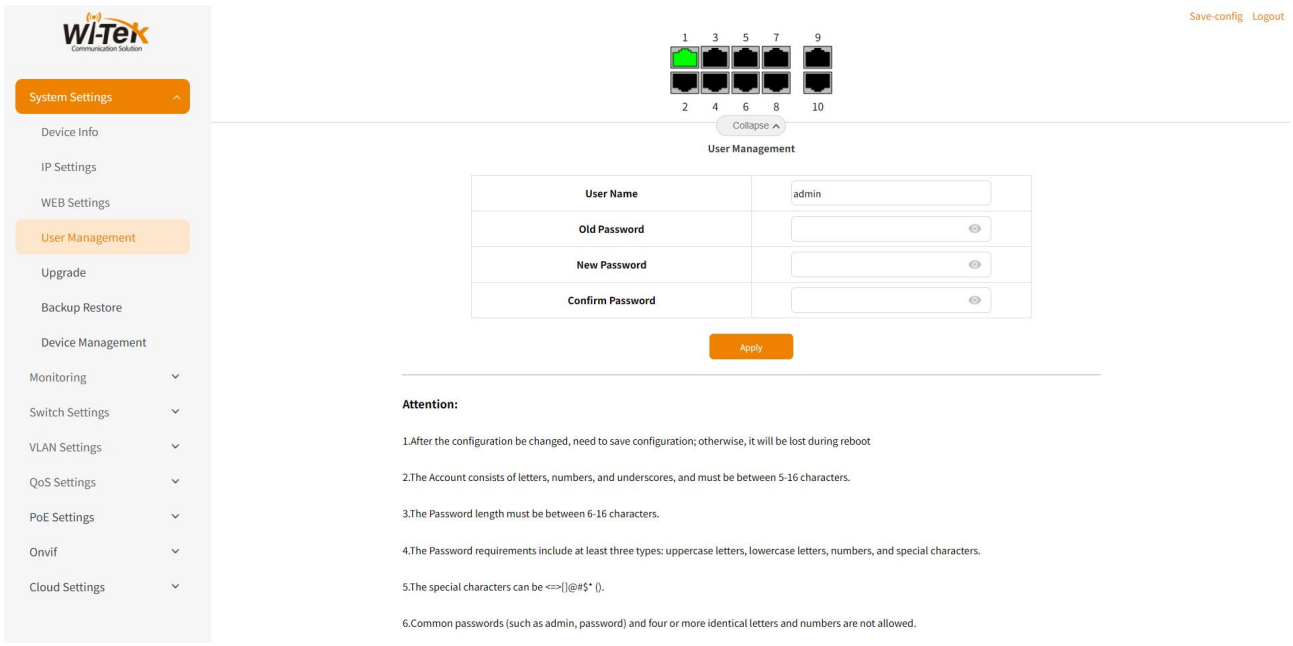



Figure 4-6

### 4.4.1 User Configuration

Used to configure the password for the login user. The default username and password are both admin. The login user can be modified . The length is no more than 16 characters , and letters , Figure , and underscores are allowed ( as shown in Figure 4-7) .

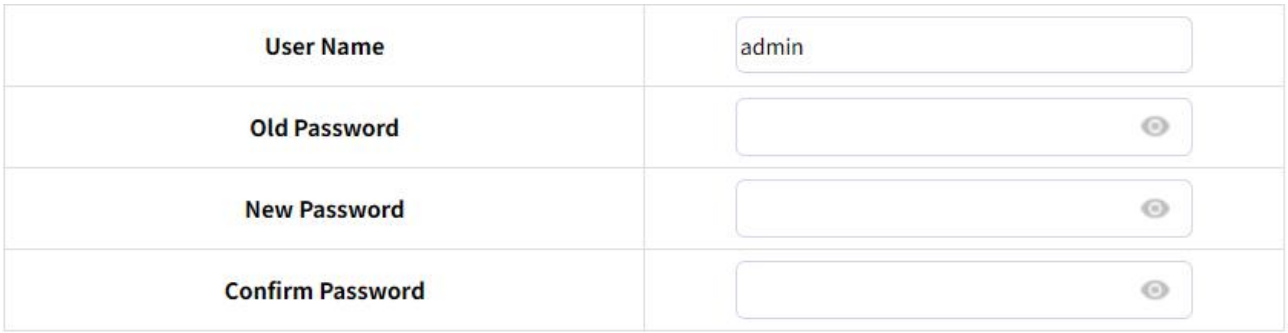



Figure 4-7

## 4.5 Equipment upgrade

### 4.5.1 Equipment upgrade

Click "System Management" - "System Upgrade " in sequence to enter , click Browse to select the host file to be updated, and then click " Apply " ( as shown in Figure 4-8 ).

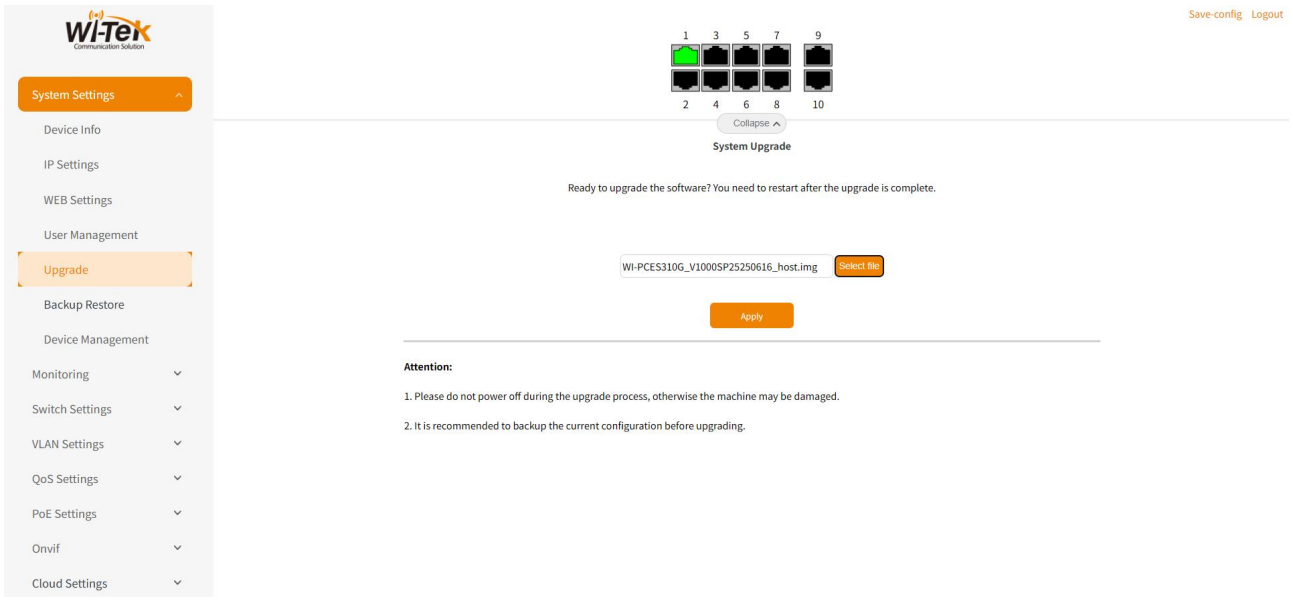



Figure 4-8

# 4.6 Backup and Restore

## 4.6.1 Backup Configuration

Before backing up the configuration , ensure normal communication with the device and confirm that the current configuration has been saved .

Click the " Download Configuration File " button to directly download the configuration file (the save dialog box is built into the browser and may vary slightly depending on the browser). The save path is the browser's default path ( as shown in Figure 4-9).

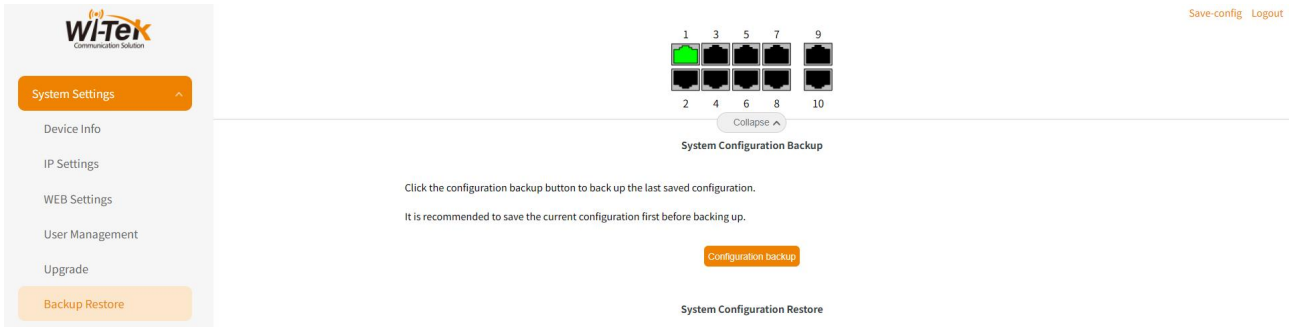



Figure 4-9

## 4.6.2 Restore Configuration

Before restoring the configuration , you need to ensure normal communication with the device .

Click to select the file path , and then click Restore Configuration. The restored configuration will take effect only after the device restarts ( as shown in Figure 4-10 ).

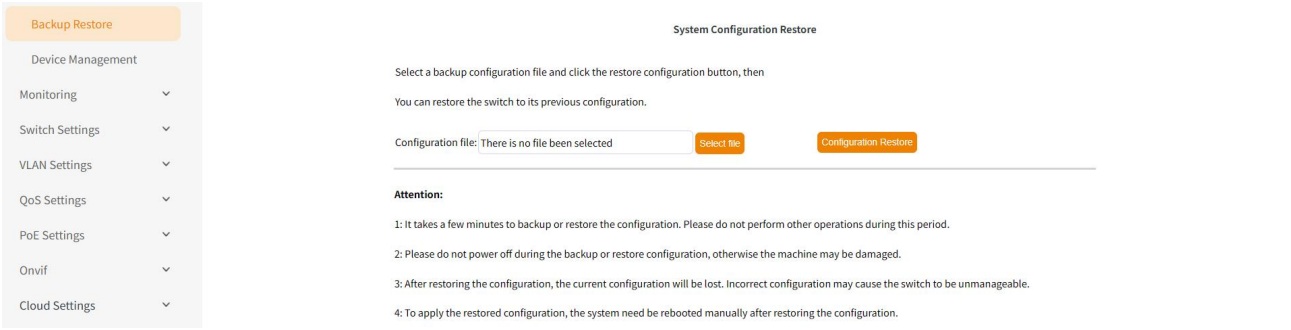



Figure 4-10

# 4.7 Device Management

## 4.7.1 Restart and restore to factory settings

Click "System Management" - " Device Management " in sequence to enter , click Device Restart - Confirm to complete the device restart operation. The steps for restoring the factory settings are similar to those for restarting the device (as shown in Figure 4-11).

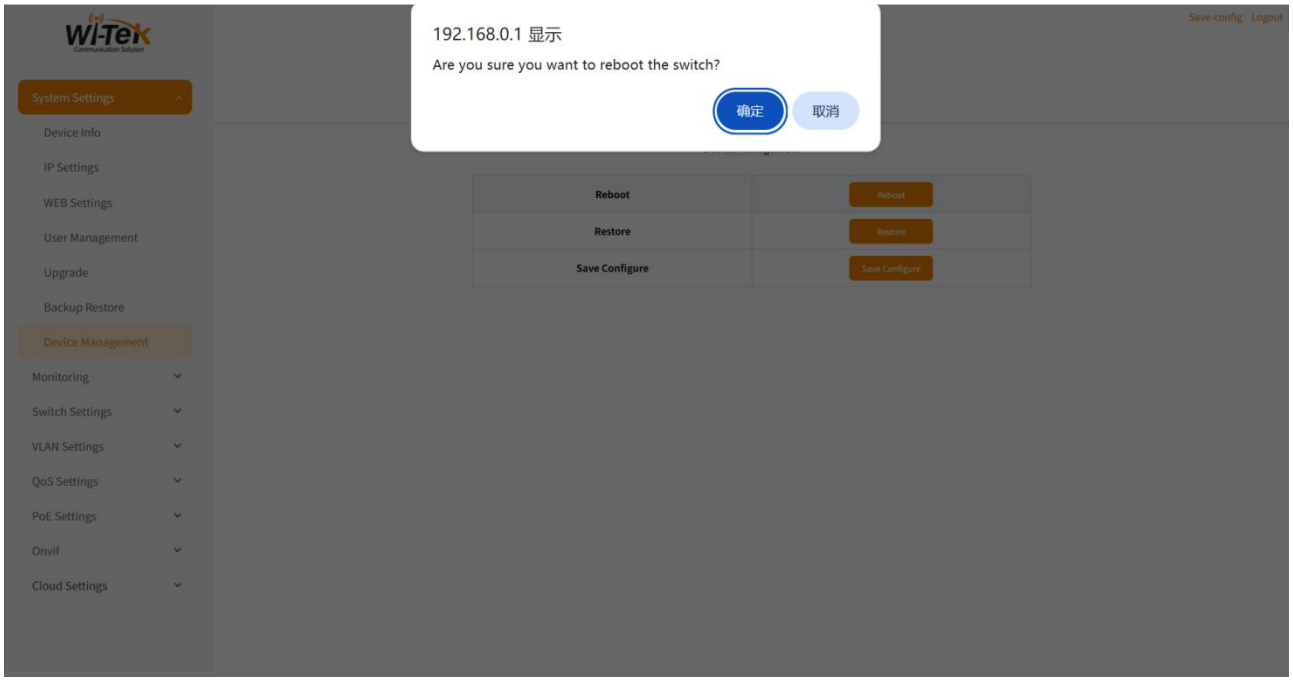



Figure 4-11

## 4.7.2 Save Configuration

There are two ways to save the configuration. Click "System Management" - " Device Management " to save the configuration. You can also directly click Save Configuration in the upper right corner of the web interface. The two ways have the same functions (as shown in Figure 4-12).


Figure 4-12

# 5 Monitoring and Management

## 5.1 Port Statistics

### 5.1.1 Overview

The number of packets and bytes received and sent by each port .

### 5.1.2 Enter the port statistics interface

Select "Port Statistics" under "Monitoring Management" in the menu bar to enter the traffic monitoring interface (as shown in Figure 5-1 ) .

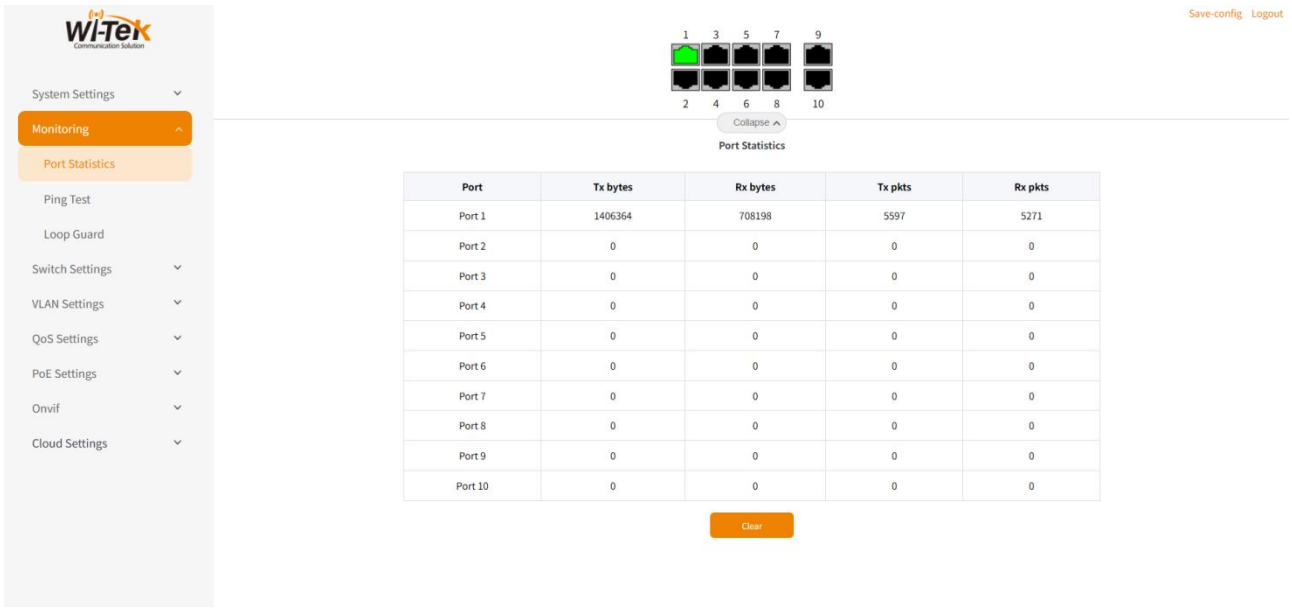



Figure 5- 1

### 5.1.3 View port statistics

In the traffic monitoring interface, you can view the port's message statistics and clear the statistical messages by clicking the Clear button (as shown in Figure 5-2 ).

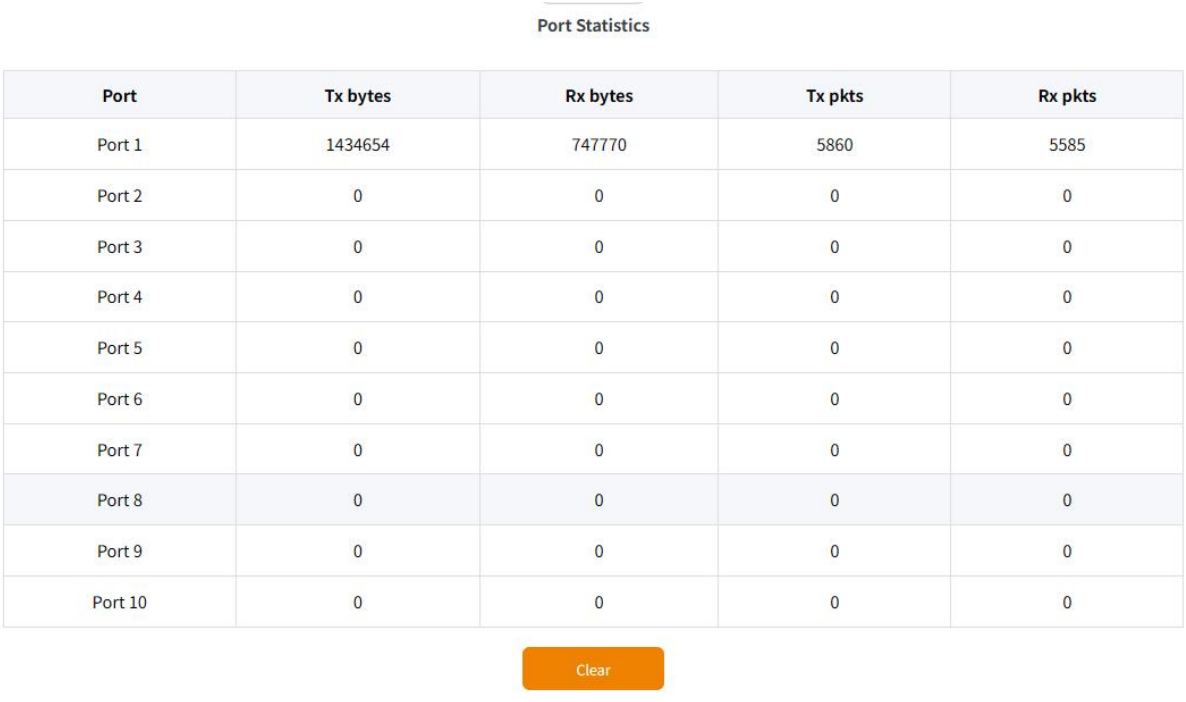



Figure 5- 2

Parameter Description

| Parameter items | illustrate |
|---|---|
| port | Display port name |

| | |
|---|---|
| Number of bytes sent | Number of bytes sent |
| Number of bytes received | Number of bytes received |
| Number of sent messages | Number of messages sent |
| Number of received messages | Number of received messages |

## 5.2 Ping Tool

### 5.2.1 Overview

Used to test network connection reachability and measure network latency. It detects network connectivity and performance by sending ICMP (Internet Control Message Protocol) echo request messages to the target host and waiting for the target host to return ICMP echo reply messages.

### 5.2.2 Enter the Ping tool page

Select " Ping Tool " under " Monitoring Management " in the menu bar to enter the Ping Tool page (as shown in Figure 5-4 ).

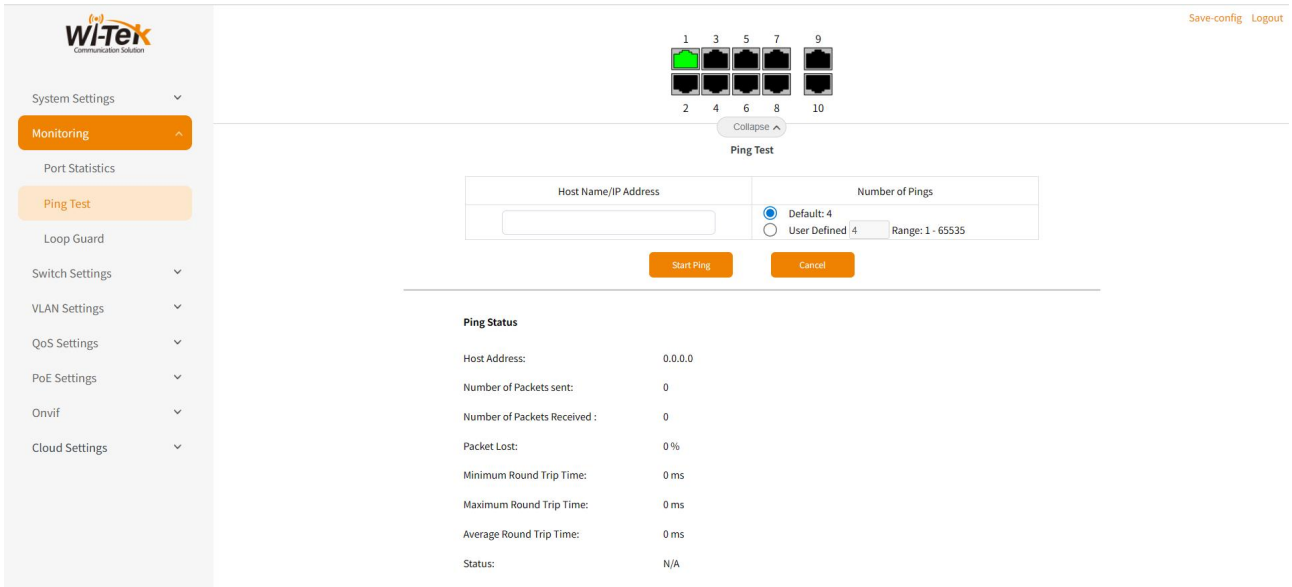



Figure 5 - 4

### 5.2.3 Using the Ping Tool

In the Host Name/IP Address box . You can configure the number of pings and click Start Ping. (As shown in Figure 5-5 ) The address can be pinged 50 times .

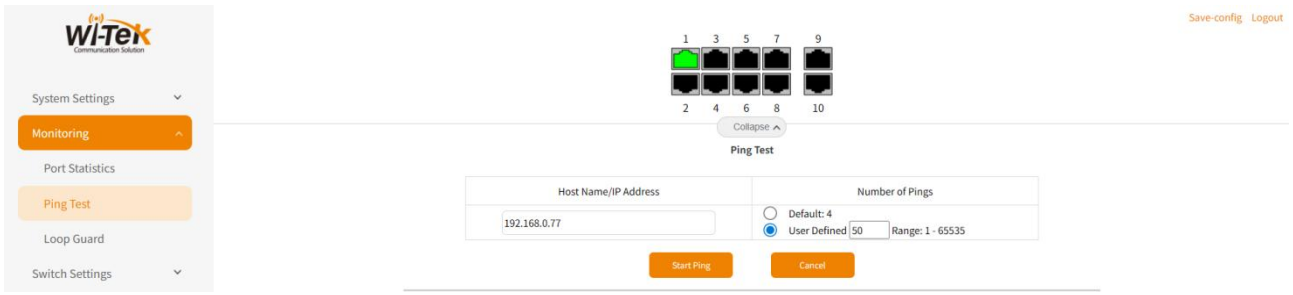



Figure 5-5

The Ping status display can show success/failure, etc. (as shown in Figure 5-6 ).

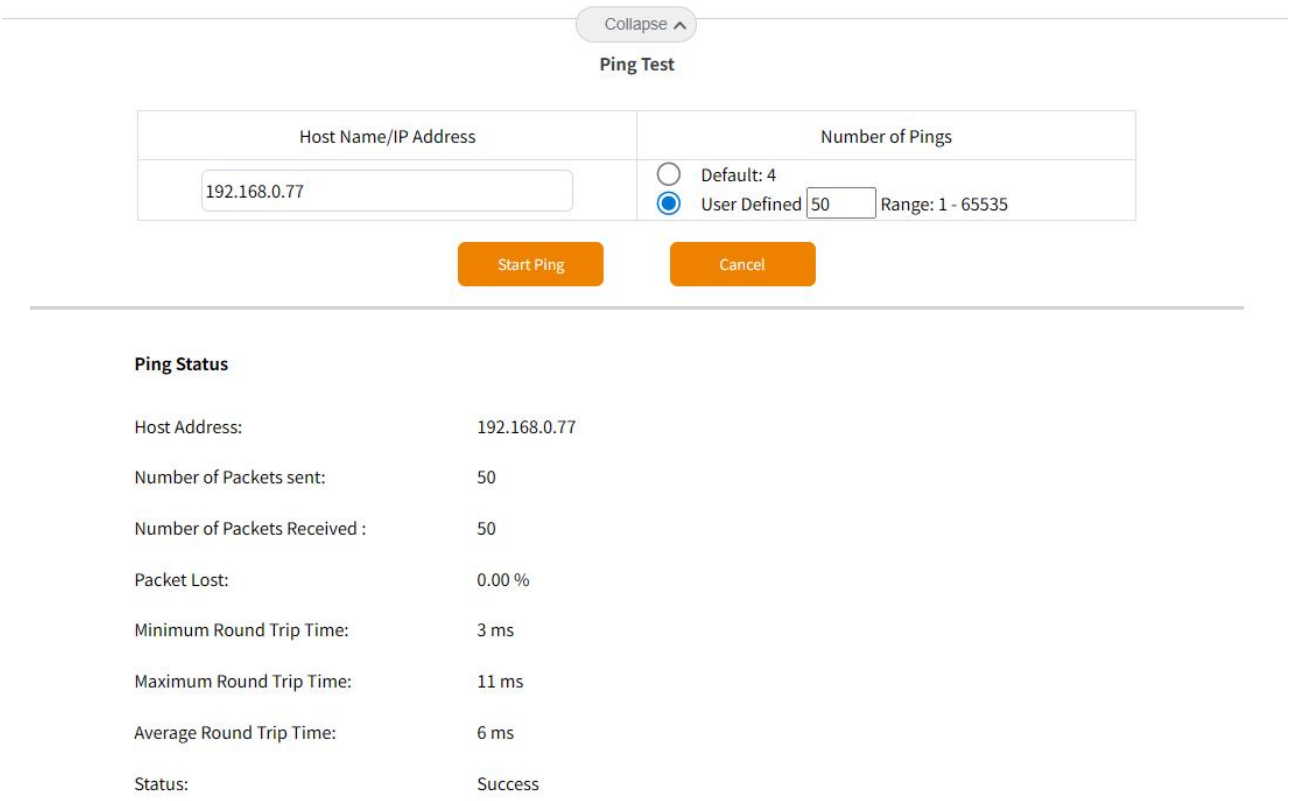



Figure 5-6

Parameter Description

| Parameter items | illustrate |
|---|---|
| Hostname/IP address | IPv4 address or domain name |
| Ping times | The default number of pings is 4. If the number of pings is too high, you can cancel the ping |

## 5.3 Loopback protection

### 5.3.1 Overview

Loopback Detection (LBD) periodically sends detection packets from a port to check whether the packets return to the device (it doesn't have to be the same port for both sending and receiving). This technology then determines whether a loop exists between the port, the connected network or device, or between device ports. If a loop is detected, it takes action on the port to keep it under control, minimizing the impact of the loop on the device and the entire network.

### 5.3.2 Enter the loopback protection interface

Select " Loopback Protection " under " Monitoring Management " in the menu bar to enter the loopback protection settings interface (as shown in Figure 5-7 ).

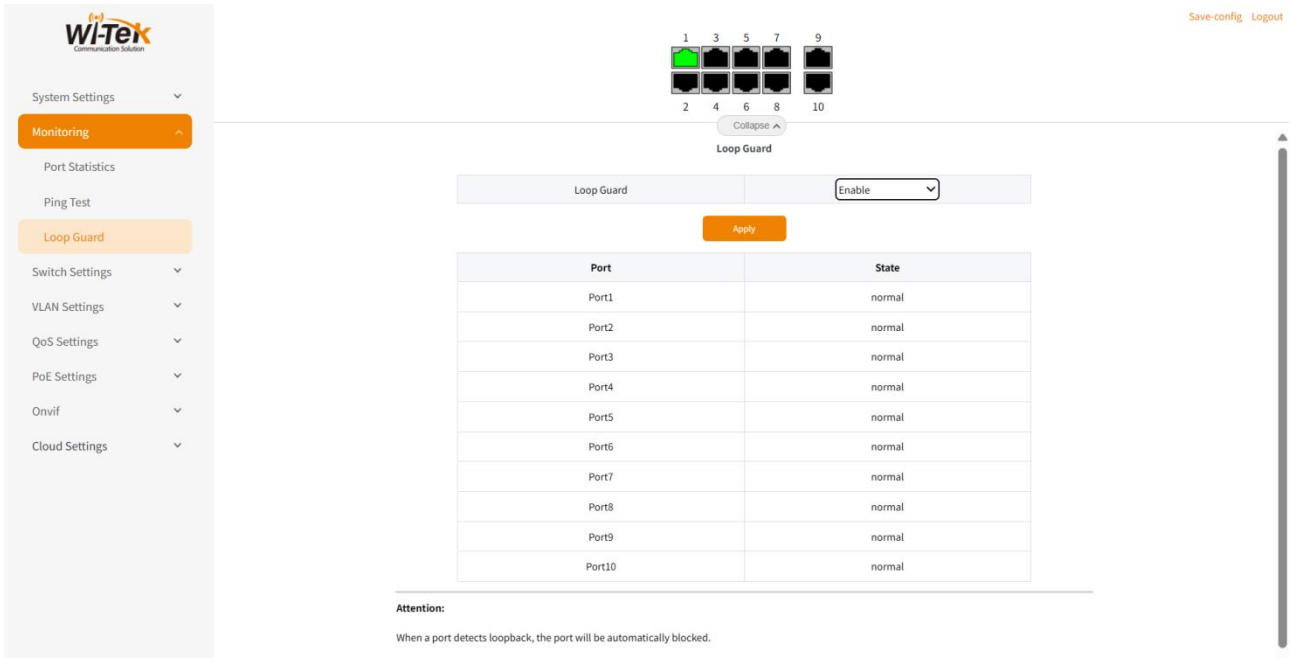



Figure 5-7

Parameter Description

| Parameter items | illustrate |
|---|---|
| Enable | loopback protection globally , enabled by default |
| Disable | Disable loopback protection globally |
| port | Port Name |
| state | Nomal: Normal data transmission and reception<br>blocked: blocked port<br>Loop: Only loopback protocol packets are allowed to be sent and received |

### 5.3.3 Configuring loopback protection

Enable the loopback protection function on the loopback protection settings page. When the port detects a loopback, it will be automatically blocked (as shown in Figure 5-8 ).

**Loop Guard**

| Loop Guard | Enable |
|---|---|

Apply

| Port | State |
|---|---|
| Port1 | normal |
| Port2 | normal |
| Port3 | normal |
| Port4 | normal |
| Port5 | loop |
| Port6 | normal |
| Port7 | blocked |
| Port8 | normal |
| Port9 | normal |
| Port10 | normal |

Figure 5-8

In the port status display page, the blocked port is shown as  , and the loop port is shown as  (as shown in Figure 5-9 )

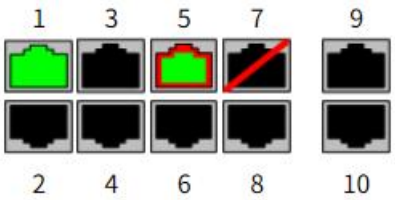



Figure 5 - 9

# 6 System Configuration

## 6.1 Port Management

### 6.1.1 Overview

The Port Status page displays port information and allows you to modify port configurations. Ports support configuration status, speed / duplex, and flow control. When the port status is "Up", it will function normally with a properly connected cable. When the port status is "Down", it will not function regardless of whether a cable is connected.

### 6.1.2 Enter the port management interface

Select "Port Management" under "System Configuration" in the menu bar to enter the port configuration interface (as shown in Figure 6-1 ).

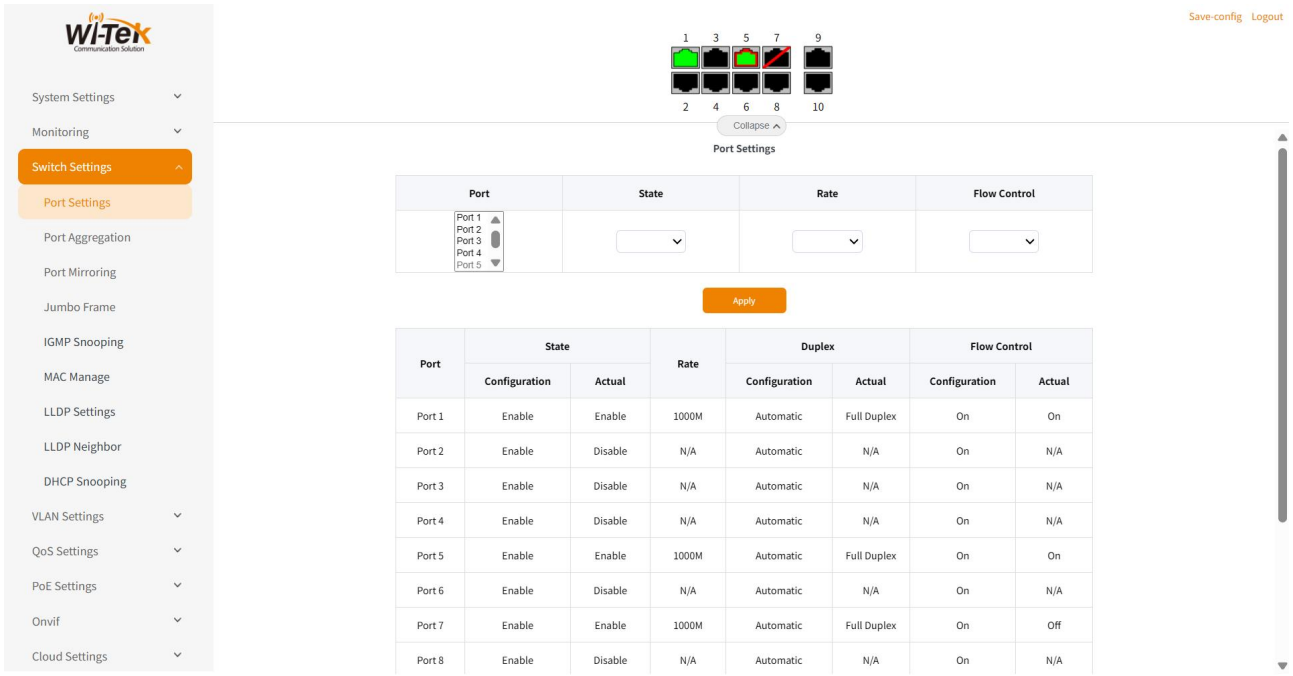



Figure 6 - 1

### 6.1.3 Configure the port

Select a port on the port configuration page and configure it according to user needs and the specific support of the device (as shown in Figure 6-2 ).


Figure 6 - 2

Parameter Description

| Parameter items | illustrate |
|---|---|
| port | Display port name |
| state | Contains two options: enable and disable state |
| Speed /Duplex | Includes 6 types: auto, 1000M, 100M- Half, 100M-Full, 10M- Half, 10M-Full |
| Flow Control | Is it enabled? Flow control function |

# 6.2 Convergence Management

## 6.2.1 Overview

An aggregation group is a logical link formed by bundling multiple physical interfaces together to increase link bandwidth. If one physical interface fails, the link remains connected as long as the other interfaces are connected normally.

## 6.2.2 Enter the aggregation management interface

Select "Convergence Management" under "System Configuration" in the menu bar to enter the convergence configuration page (as shown in Figure 6-3 ).

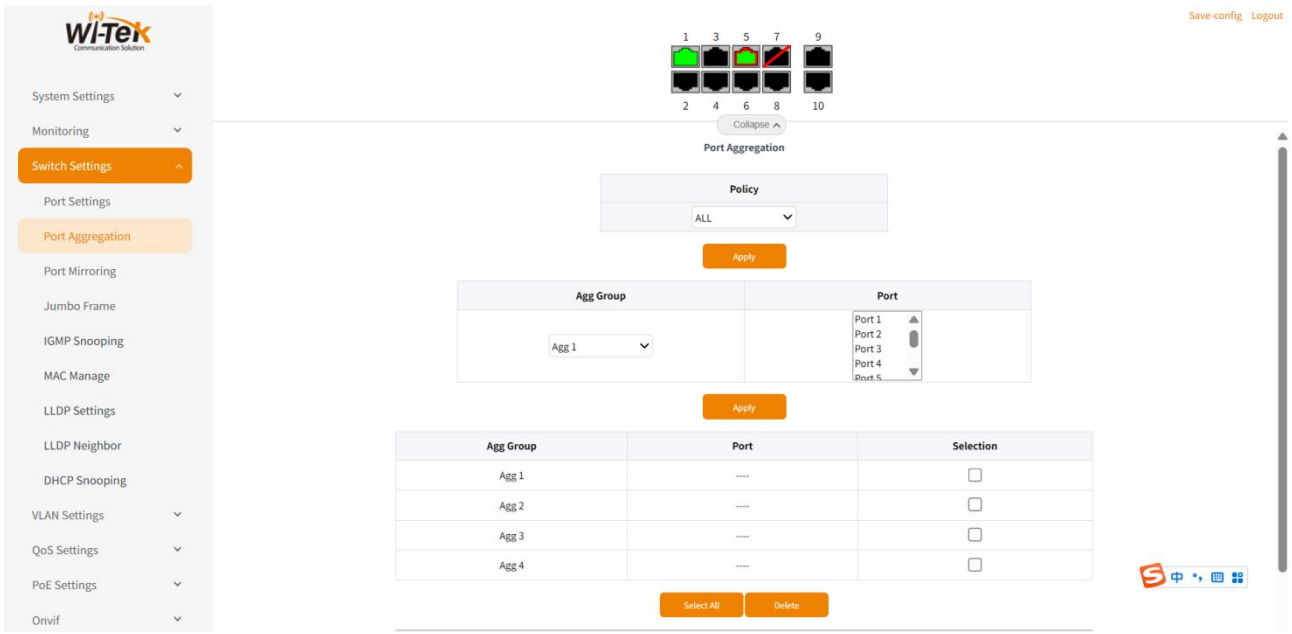



Figure 6-3

## 6.2.2 Configuring an aggregation group

On the aggregation configuration page, you can choose to configure the aggregation group and forwarding port (as shown in Figure 6-4 ). Configure ports 1-3 as an aggregation group, press the ctrl key to select the port, and click Apply .

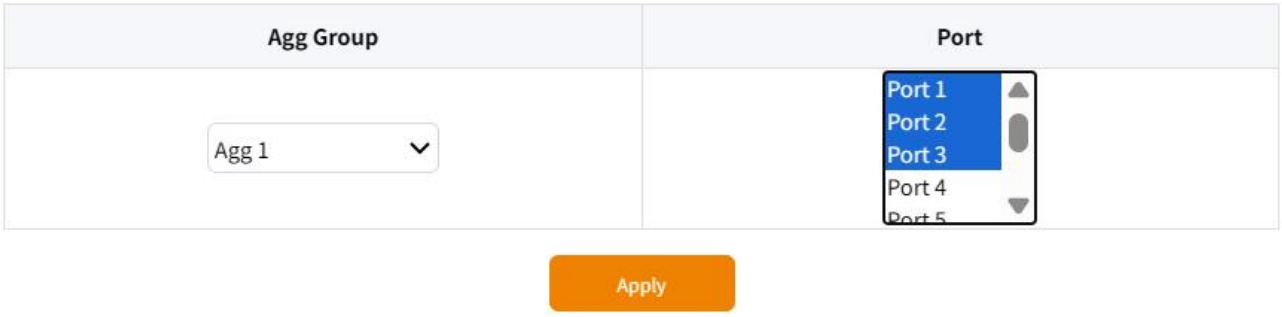



Figure 6-4

After the configuration is complete, the aggregation group member ports are displayed (as shown in Figure 6-5 ).

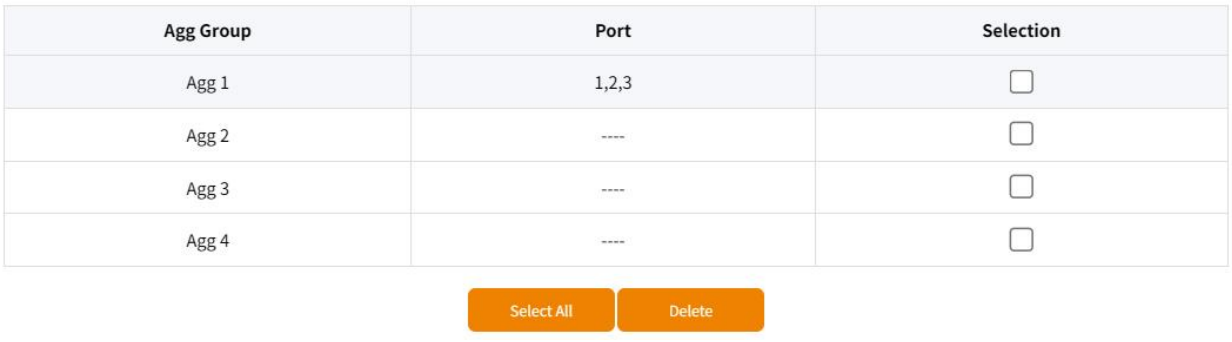



Figure 6-5

To delete an aggregation group, select Select and click Delete.

Parameter Description

| Parameter items | illustrate |
| --- | --- |
| Aggregation Group | Aggregation group name |
| Forwarding ports | Aggregation group forwarding member port |

**Attention：**

- (1) The system supports adding 4 aggregation groups, and each aggregation group supports up to 8 member ports .
- (2) Port attribute configuration includes: requiring the port rate, duplex mode, and link type to be consistent.

## 6.3 Port Mirroring Configuration

### 6.3.1 Overview

The mirroring function allows users to copy packets from a device port and send them through another port. Connecting this port to a tester or other packet collection device allows users to capture and analyze the original packets. The mirroring function does not affect the original network traffic on the switch.

### 6.3.2 Entering the port mirroring configuration interface

Select "Port Mirroring" under "System Configuration" in the menu bar to enter the port mirroring page (as shown in Figure 6 - 6 ).

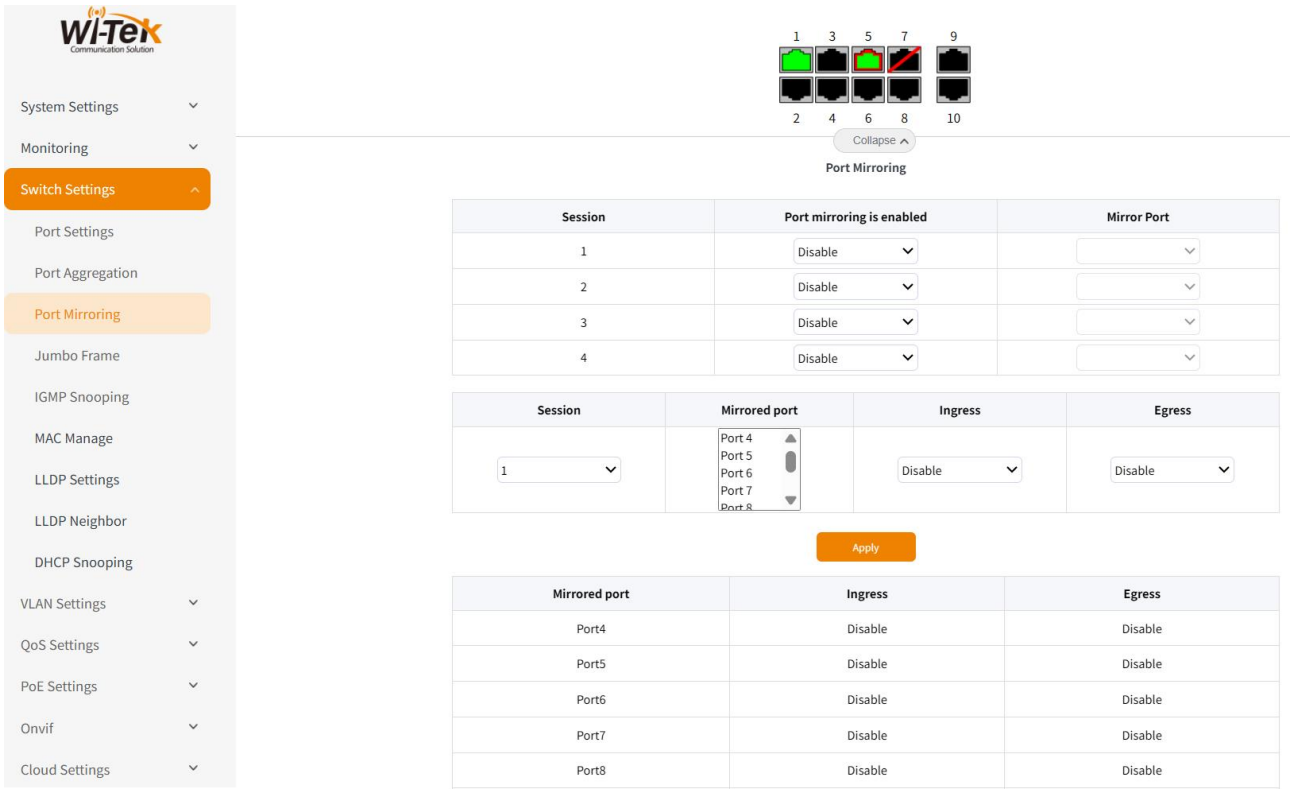



Figure 6 - 6

### 6.3.3 Configuring Port Mirroring

Select Port Mirroring Enable as Enable, select Port 4 as the mirror destination port and Mirror Session 1, Port 5 as the mirrored port , and Enable as Ingress/Egress. Click Apply (as shown in Figure 6-7 ) .

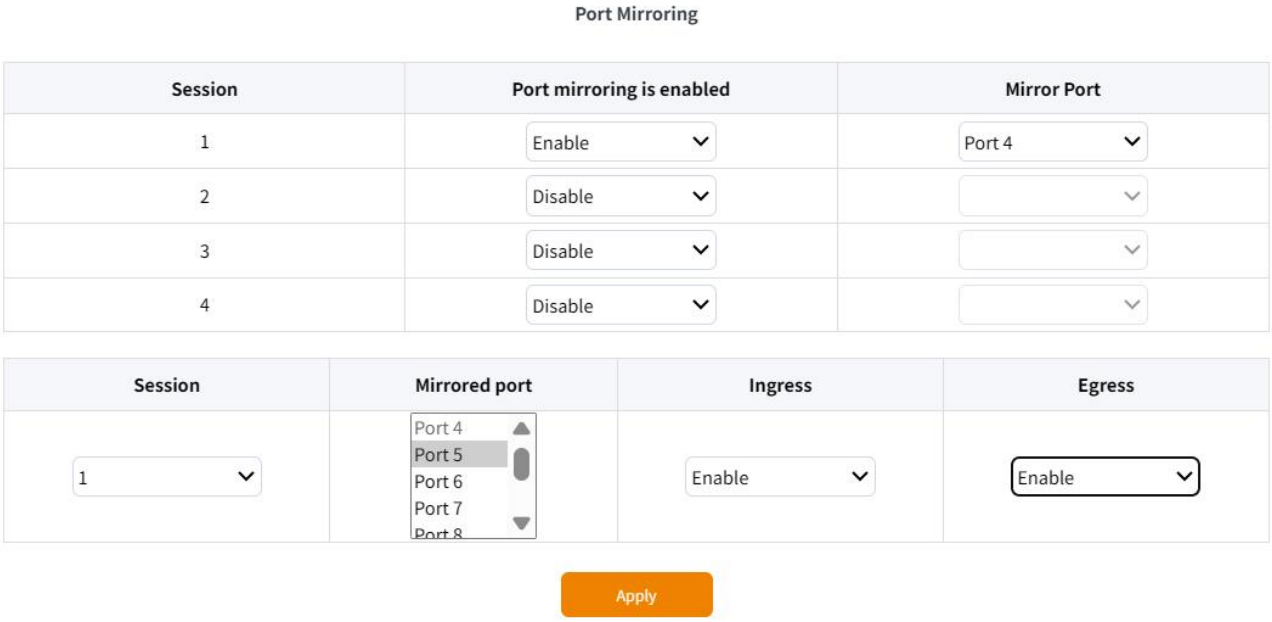



Figure 6-7

The mirroring table entry displays the mirroring group and the mirrored port (as shown in Figure 6-8 ).

| Mirrored port | Ingress | Egress |
|---|---|---|
| Port4 | Disable | Disable |
| Port5 | 1 | 1 |
| Port6 | Disable | Disable |
| Port7 | Disable | Disable |
| Port8 | Disable | Disable |
| Port9 | Disable | Disable |
| Port10 | Disable | Disable |
| Agg1 | Disable | Disable |

Figure 6-8

Select " Disable " from the drop-down box to delete the configuration. (See Figure 6 - 9 )


Figure 6-9

Parameter Description

| Parameter items | illustrate |
|---|---|
| Mirror Session | The mirroring session name. |
| Enable port mirroring | There are two states: disabled and enabled. |
| Mirror port | Destination port for mirroring. |
| Mirrored port | Mirrored source port. |
| Entrance | Mirrors the ingress traffic of the source port. |
| exit | Mirrors the egress traffic of the source port. |

**Attention：**

- The destination port cannot be configured the same as the source port

# 6.4 Jumbo Frames

## 6.4.1 Overview

Jumbo frames reduce the number of network packet processing by increasing the frame size, thereby improving network bandwidth and throughput.

## 6.4.2 Entering the Jumbo Frame Interface

Select "Jumbo Frame" under "System Configuration" in the menu bar to enter the jumbo frame configuration page (as shown in Figure 6-10 ).

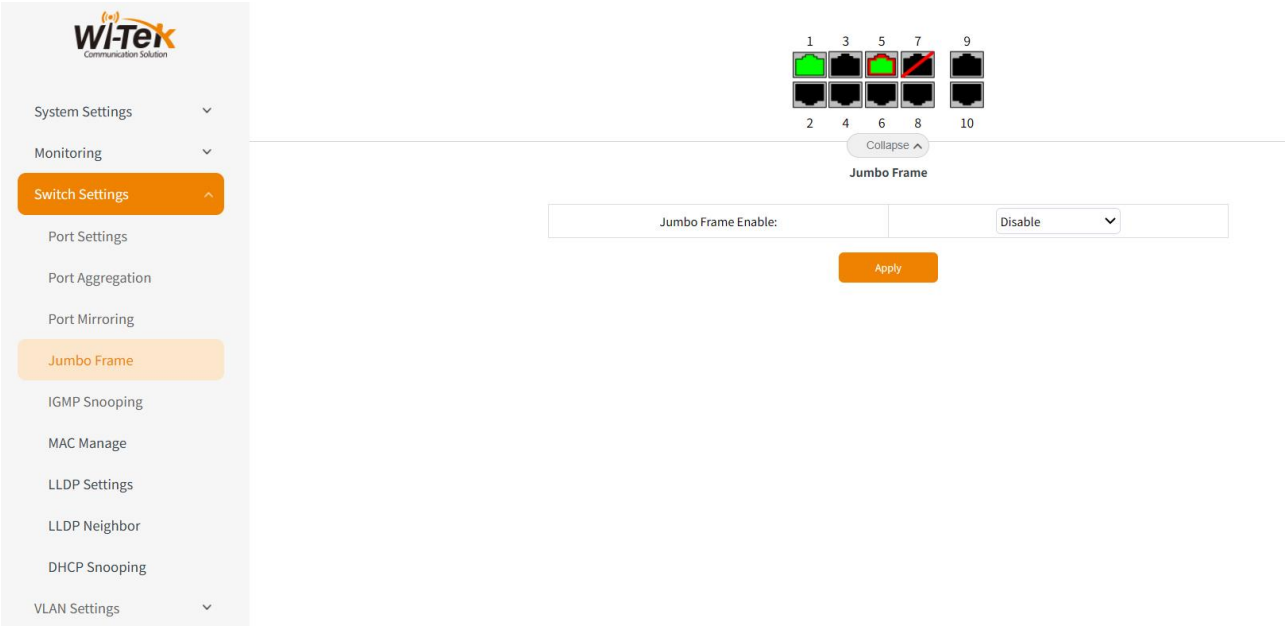



Figure 6-10

## 6.4.3 Configuring Jumbo Frames

Enable jumbo frames on the jumbo frame configuration page, set the MTU size to 4k, and click "Apply" (as shown in Figure 6 - 11 ).


Figure 6-11

# 6.5 IGMP Snooping

Cloud Easy Smart PoE Switch use IGMP Snooping to control the flooding of multicast traffic, ensuring that it is

forwarded only to interfaces associated with IP multicast devices. As the name suggests, IGMP Snooping (Internet Group Management Protocol Snooping) requires the LAN switch to snoop on IGMP transmissions between hosts and routers and track multicast group member ports. Click System Configuration > IGMP Snooping to access the page (see Figure 6-12 ).

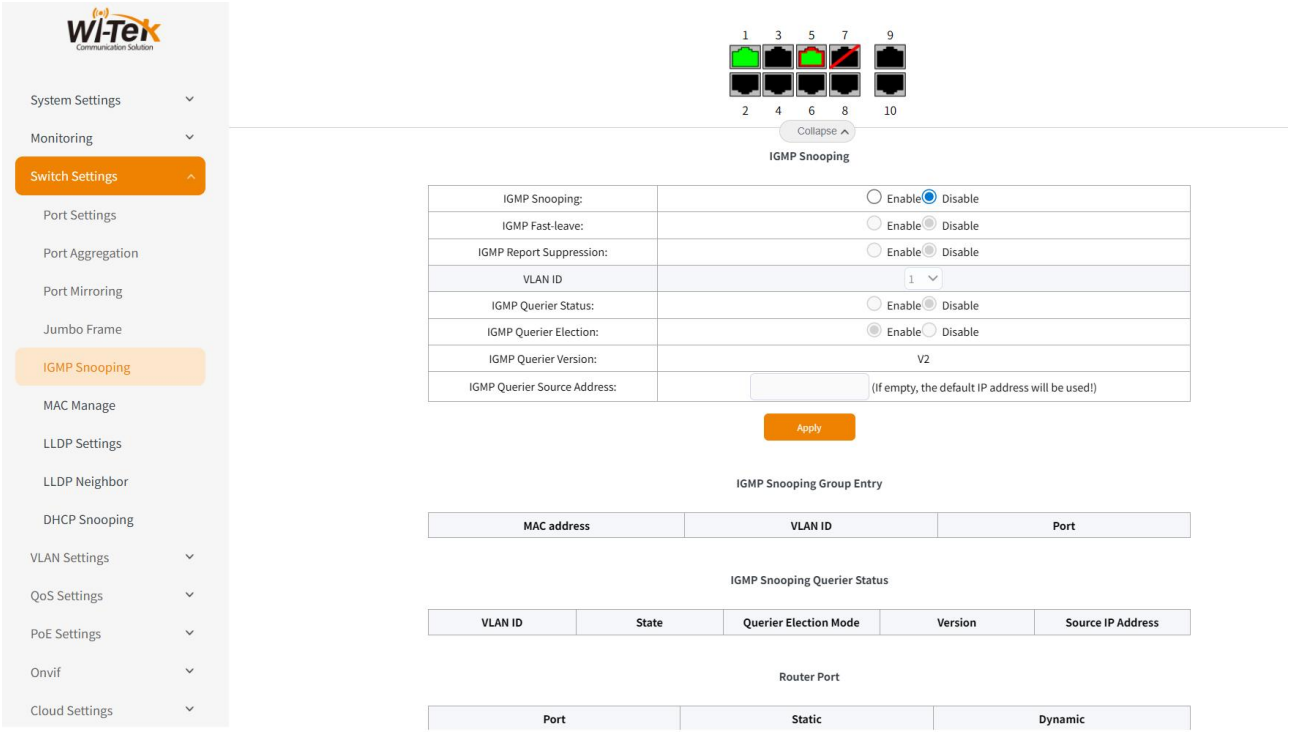



Figure 6-12

## 6.5.1 IGMP Snooping Settings

IGMP Snooping configuration must be enabled globally. When IGMP Snooping is disabled globally, other configuration options are unavailable. When IGMP Snooping is enabled, you can enable IGMP Snooping for certain VLANs and enable the IGMP Snooping querier. (See Figure 6-13 for examples.) This section describes how to enable IGMP Snooping for VLAN 1 and the querier function.

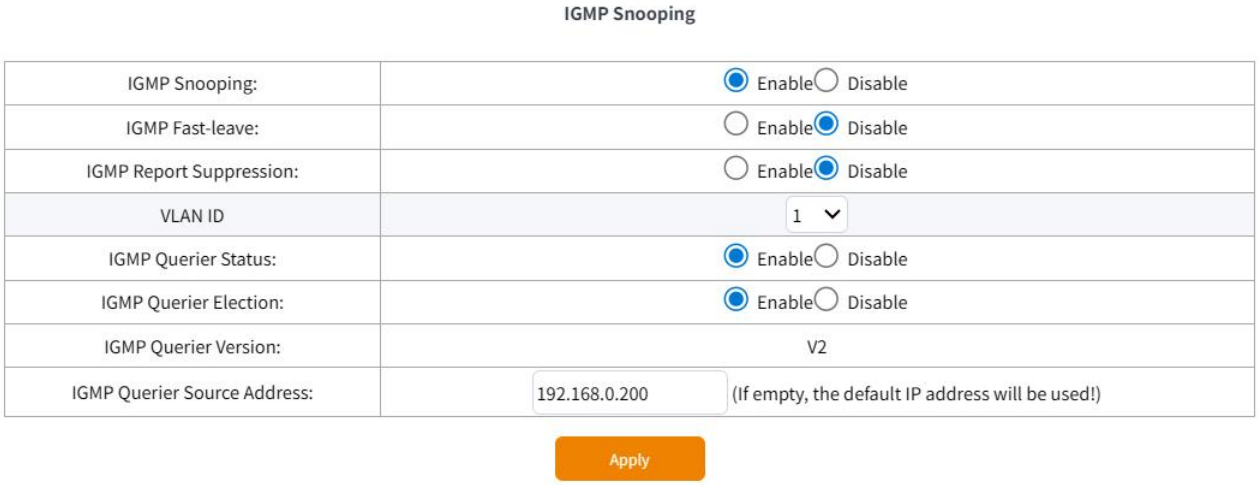



Figure 6-13

Parameter Description

| Parameter items | illustrate |
|---|---|

| | |
|---|---|
| IGMP Snooping switch | IGMP Snooping switch, on or off |
| IGMP Fast Leave | IGMP fast leave function is disabled by default, provided that IGMP Snooping is enabled |
| IGMP Report Suppression | Select VLAN to enable message suppression function, provided that the VLAN exists and IGMP Snooping is enabled |
| VLAN ID | Select VLAN to enable IGMP snooping, provided that the VLAN exists and IGMP Snooping is enabled |
| IGMP querier status | IGMP querier function switch, disabled by default |
| IGMP Querier Election | IGMP querier election switch |
| IGMP querier version | IGMP querier version is V2 |
| IGMP querier global address | Configure the source IP address of the IGMP querier, provided that IGMP Snooping and IGMP querier are enabled. |

### 6.5.2 IGMP Snooping Group

Used to record dynamic multicast entries, it supports IGMP Versions 1 and 2 ( see Figure 6-14 ), with a maximum of 64 entries . To prevent the use of protocol multicast addresses, the reserved addresses 224.0.0.1-224.0.0.255 are restricted from learning the dynamic multicast table.


Figure 6-14

Parameter Description

| Parameter items | illustrate |
|---|---|
| MAC address | Multicast group address |
| VLAN ID | Multicast entry VLAN number |
| port | Multicast member port |

### 6.5.3 IGMP Snooping Querier Status

Used to record the querier status , fixed at version V2 (as shown in Figure 6-15 ) . Enable the IGMP querier,

with the default source IP address being 192.168.0.200 .

IGMP Snooping Querier Status

| VLAN ID | State | Querier Election Mode | Version | Source IP Address |
|---|---|---|---|---|
| 1 | Querier | Enable | V2 | 192.168.0.200 |

Figure 6-15

Parameter Description

| Parameter items | illustrate |
|---|---|
| VLAN ID | Multicast entry VLAN number |
| state | Querier Status |
| Querier election mode | Querier election mode status |
| Version | Query engine version number |
| Source Address | Querier source IP address |

### 6.5.4 Routing port

Used to configure static routing ports and learn dynamic routing ports (as shown in Figure 6-16).

Router Port

| Port | Static | Dynamic |
|---|---|---|
| Port 4 | ☐ | ☐ |
| Port 5 | ☐ | ☐ |
| Port 6 | ☐ | ☐ |
| Port 7 | ☐ | ☐ |
| Port 8 | ☐ | ☐ |
| Port 9 | ☐ | ☐ |
| Port 10 | ☐ | ☐ |
| Agg1 | ☐ | ☐ |

Apply

Figure 6-16

Parameter Description

| Parameter items | illustrate |
|---|---|

| | |
|---|---|
| port | Port number |
| Static routing | Static routing port |
| Dynamic Routing | Dynamic routing port, the prerequisite is to enable IGMP querier |

## 6.6 MAC Management

The MAC address table contains the address information for forwarding traffic between switch ports. The address table includes the following address types:

Dynamic address: The interface learns the source MAC address in the message, and the entry can be aged.

Static address: manually configured by the user. The table entry cannot be aged and the configuration will not be lost after a restart.

Click the menu bar - " System Configuration " - "MAC Management " to enter. (As shown in Figure 6-17 )

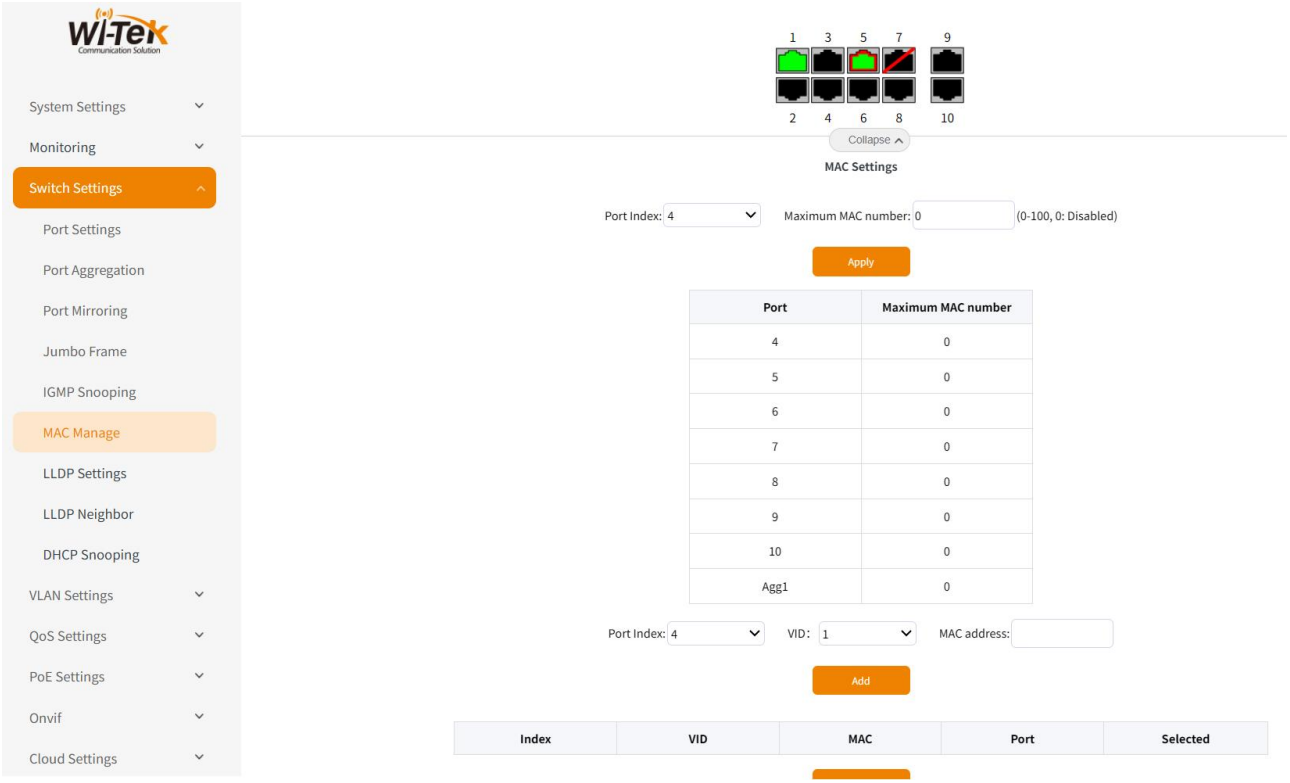



Figure 6-17

### 6.6.1 MAC Restriction

Used to limit the number of MAC addresses learned on the port. The default state is Disable. A learning number of 0 means no limit. (As shown in Figure 6-18 )

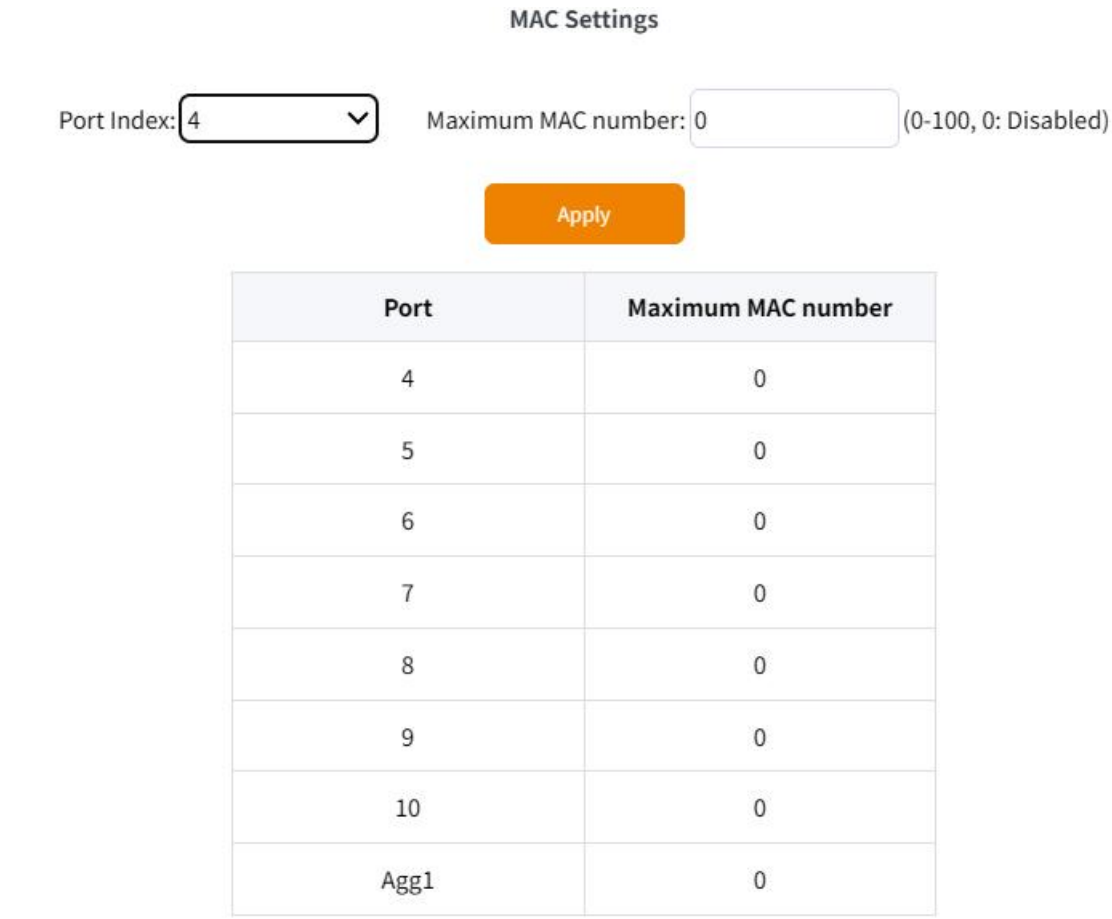



Figure 6-18

Configure the maximum MAC number of port 4 to 100, select 4 as the port number, configure the maximum MAC number to 100, and click " Apply " (as shown in Figure 6-19 ) . Port 4 can only learn 100 MAC addresses.

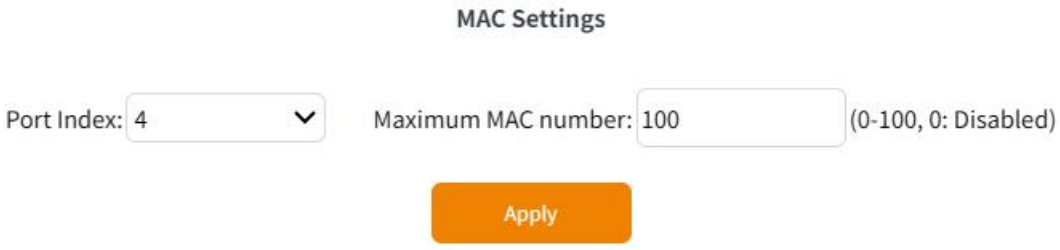



Figure 6-19

Parameter Description

| Parameter items | illustrate |
|---|---|
| port | Physical port |
| Maximum number of MAC addresses | Maximum number of MAC addresses learned by a port |

## 6.6.2 Static MAC Address Table

Used to manually add static MAC address entries (as shown in Figure 6-20 ) . The specification supports configuring 32 entries.

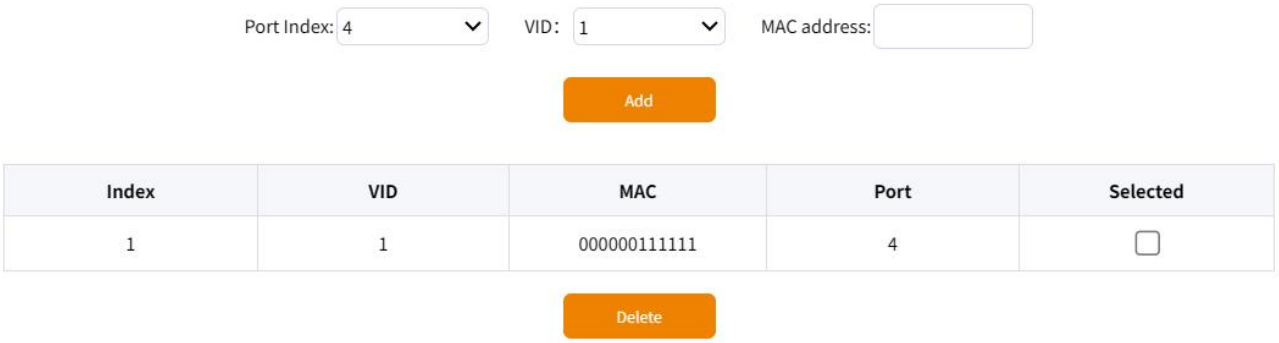



Figure 6-20

Parameter Description

| Parameter items | illustrate |
|---|---|
| Port number | Port information corresponding to static MAC entries |
| VID | VLAN ID corresponding to the static MAC entry |
| MAC address | The MAC address corresponding to the static MAC table entry only supports the configuration of unicast addresses |
| Serial number | Arrangement number |

## 6.6.3 MAC Address Table

Used to view the MAC address entries learned by the current device . The specification supports 8k entries . ( As shown in Figure 6-21 )

| Index | VID | MAC | Port | Aging time(in seconds) |
|---|---|---|---|---|
| 1 | 1 | 6C1FF7208712 | Agg1 | 301 |

Figure 6-21

## 6.6.4 MAC Address Query

Used to query whether a certain MAC address table entry learned by the current device exists (as shown in Figure 6-22 ) . Click " Search " to query. After the query is completed, if the MAC address exists, only the MAC address will be displayed in the MAC address table .

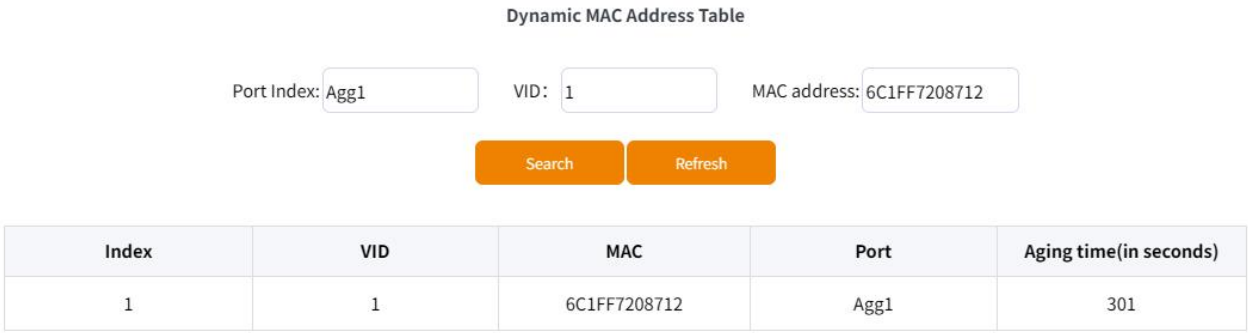



Figure 6-22

Parameter Description

| Parameter items | illustrate |
|---|---|
| Serial number | MAC address sequence number |
| VID | VLAN ID corresponding to the FDB table |
| MAC | MAC address corresponding to the FDB table |
| port | Port information corresponding to the MAC entry |
| Aging time | MAC address aging time, default 300s |

# 6.7 LLDP Configuration

## 6.7.1 Overview

LLDP (Link Layer Discovery Protocol) is a Layer 2 discovery protocol defined in IEEE 802.1AB. By using LLDP, network management systems can quickly monitor Layer 2 network topology information and topology changes as networks rapidly expand.

## 6.7.2 Entering the LLDP Configuration Interface

Select "LLDP Configuration" under "System Configuration" in the menu bar to enter the LLDP configuration interface (as shown in Figure 6-23 ) .

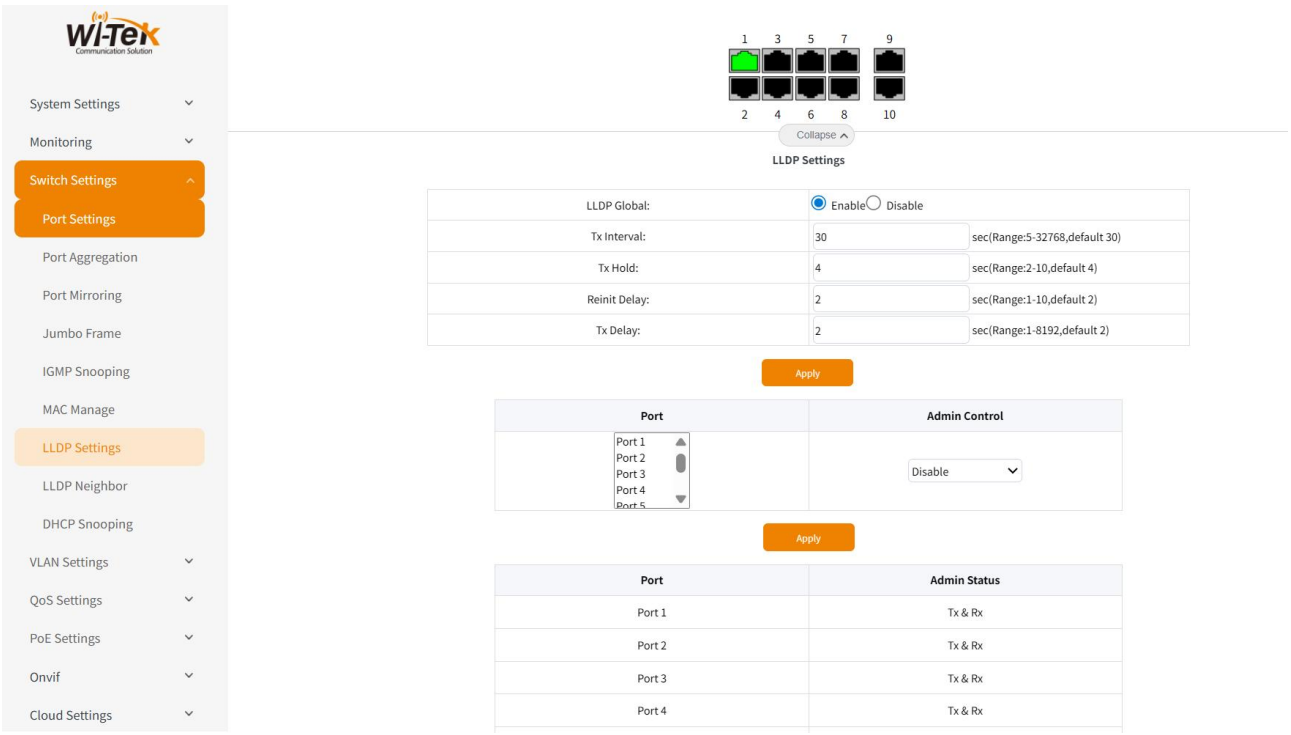



Figure 6-23

## 6.7.3 Configuring LLDP

You can configure the LLDP global status, send interval , send hold, reinitialization delay, and send delay ( as shown in Figure 6-24 ) . Click "Apply" to complete the configuration .

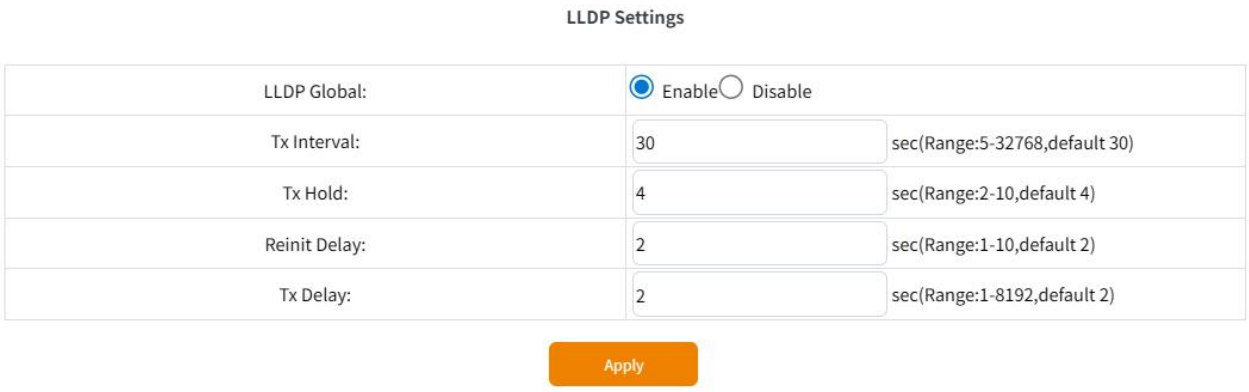



Figure 6-24

For LLDP port configuration, press the ctrl key to select the corresponding port, select Tx&Rx in the Management Control drop-down box, and click "Apply" (as shown in Figure 6-25) .

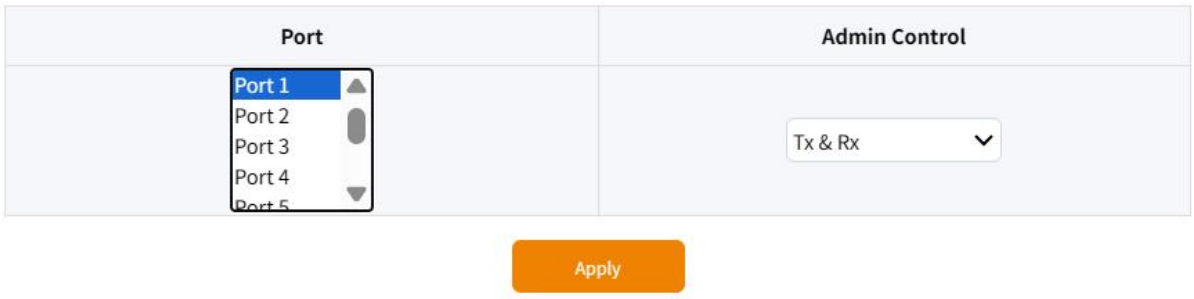



Figure 6-25

Port status display . ( Figure 6-26 )

| Port | Admin Status |
|---|---|
| Port 1 | Tx & Rx |
| Port 2 | Tx & Rx |
| Port 3 | Tx & Rx |
| Port 4 | Tx & Rx |
| Port 5 | Tx & Rx |
| Port 6 | Tx & Rx |
| Port 7 | Tx & Rx |
| Port 8 | Tx & Rx |
| Port 9 | Tx & Rx |
| Port 10 | Tx & Rx |

Figure 6-26

Parameter Description

| Parameter items | illustrate |
|---|---|
| LLDP Global | LLDP global function switch |
| Sending interval | Interval for sending LLDP packets |
| Send Hold | Neighbor aging factor for LLDP messages |
| Reinitialization Delay | Message resending delay |
| Sending Delay | Message sending delay |
| port | Port name |
| Management Control | LLDP operating mode of a port:<br>Disable<br>send<br>take over<br>Send & Receive |

# 6.8 LLDP Neighbors

## 6.8.1 LLDP Neighbor Table

The LLDP neighbor table records information about neighbor devices discovered by a device through the LLDP protocol. This information includes the neighbor device's interface, status, and duration.

Click the menu bar - " System Configuration " - " LLDP Neighbor " to enter. (As shown in Figure 6-27 )


Figure 6-27

# 6.9 DHCP Snooping

DHCP Snooping is mainly used to ensure that DHCP clients obtain IP addresses from legitimate DHCP servers and record the correspondence between DHCP client IP addresses and parameters such as MAC addresses, thereby defending against various attacks against DHCP in the network and providing a more secure network environment and more stable network services.

Click on the menu bar - " System Configuration " - " DHCP Snooping " to enter. (As shown in Figure 6-28 )

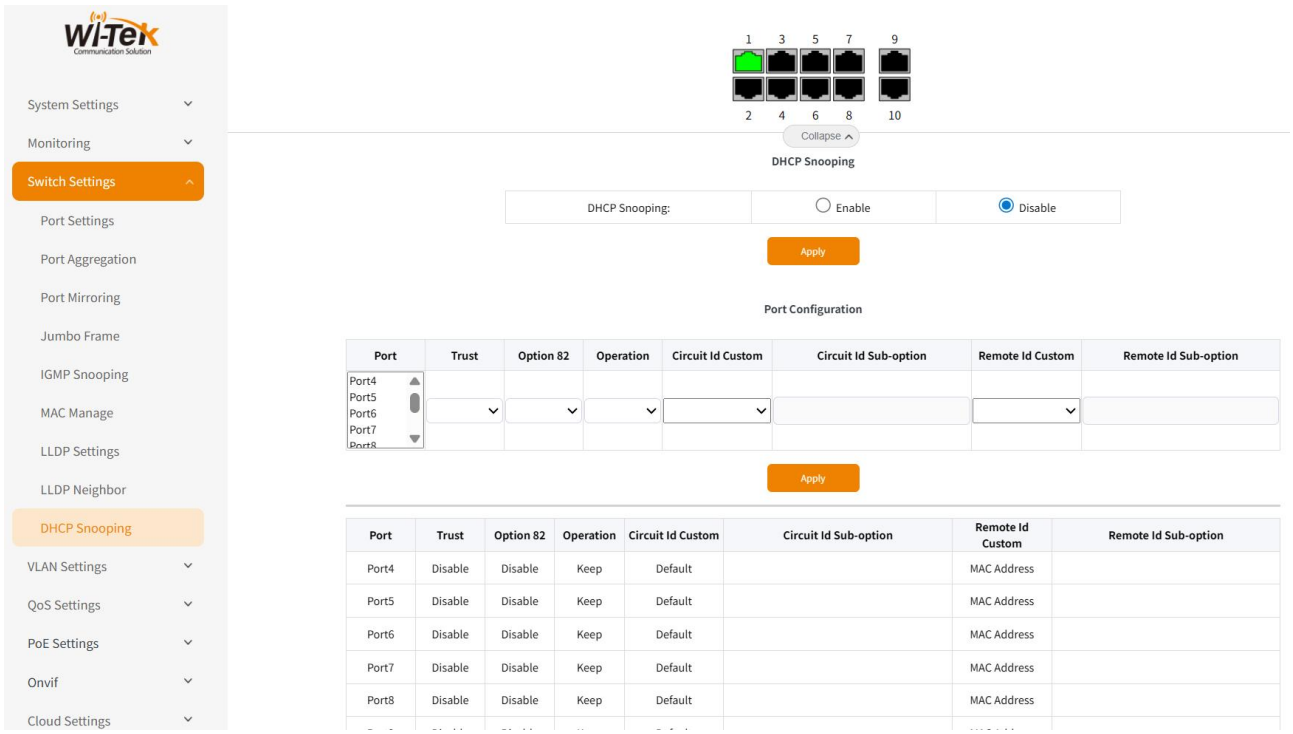



Figure 6-28

## 6.9.1 DHCP Snooping

Used to enable the DHCP-snooping function. The default status is enable. (See Figure 6-29 )

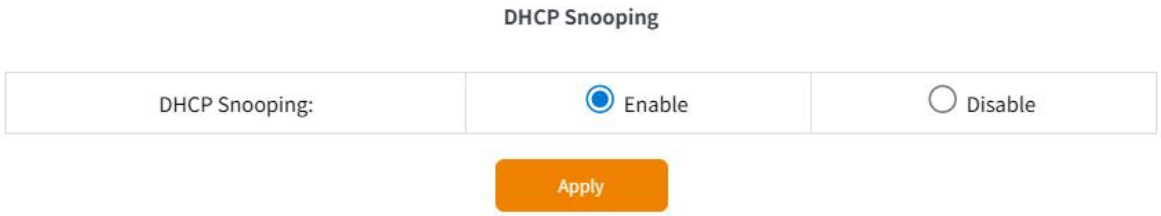



Figure 6-29

Select the port and configure the following settings: Enable Trust, Enable Option 82, Action Mode to Replace, Customize Circuit ID, and Customize Remote ID (as shown in Figure 6-30) .

| Port | Trust | Option 82 | Operation | Circuit Id Custom | Circuit Id Sub-option | Remote Id Custom | Remote Id Sub-option |
|---|---|---|---|---|---|---|---|
| Port4 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |
| Port5 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |
| Port6 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |
| Port7 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |
| Port8 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |
| Port9 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |
| Port10 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |
| Agg1 | Enable | Enable | Replace | User Config | aaaaaaa | User Config | CCCCCCC----- |

Figure 6-30

Parameter Description

| Parameter items | illustrate |
| --- | --- |
| port | Physical port |
| trust | Configure the port as a trust port |
| Option82 | Enable/disable option 82 function |
| model | Message processing policy, the default is to retain |
| Circuit ID customization | Circuit Id |
| Remote ID customization | Remote Id |

# 7 VLAN

## 7.1 MTU VLAN

MTU VLAN ( Multi-Tenant Unit VLAN ) is to divide the port occupied by each user and the uplink port into a separate VLAN . Ordinary ports can only communicate with the pre-set uplink port, and cannot communicate with each other. Users on different ports cannot communicate directly to ensure network security . By default, port 1 is the uplink port and the rest of the ports are downlink ports ( as shown in the Figure 7 - 1 ).

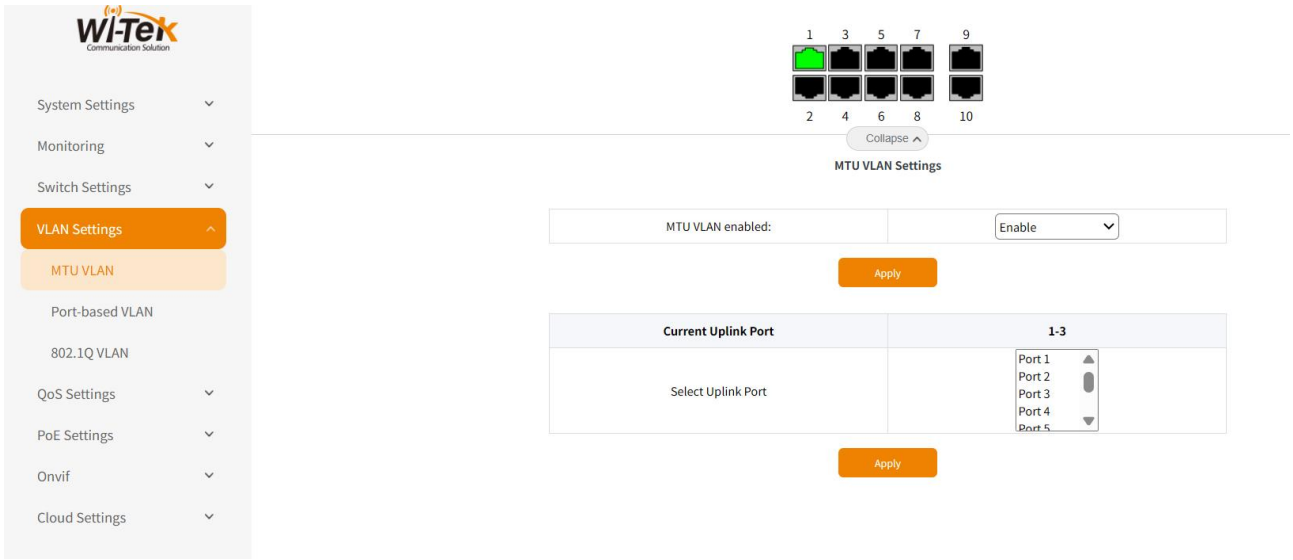



Figure 7-1

### 7.1.1 MTU VLAN settings

Click vlan-mtu vlan, select enable mtu vlan , select port 2 and click apply to set it as an uplink port. At this time, other ports cannot communicate with each other and can only communicate with port 2; conversely, the uplink port can communicate with all ports ( as shown in Figure 7-2 ) .

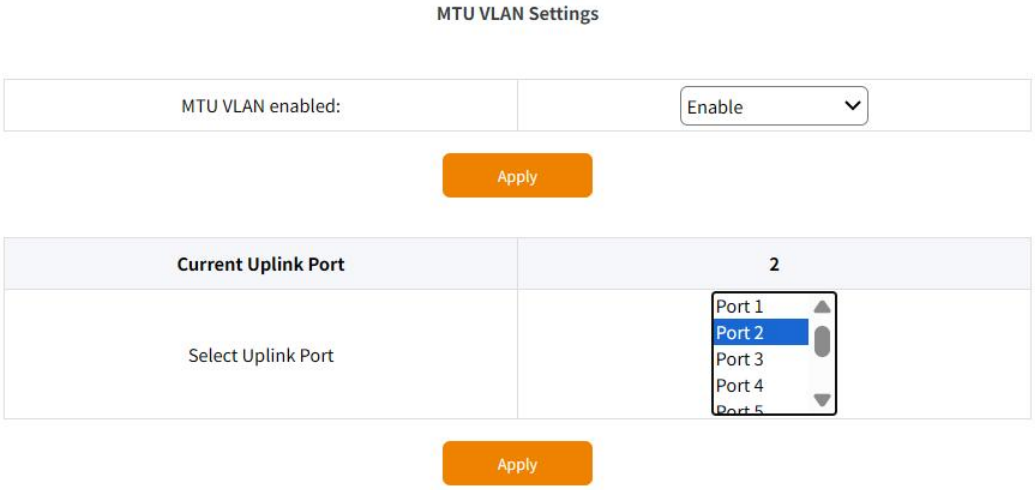



Figure 7-2

**Attention：**

- Only one of MTU VLAN, port VLAN, and 802.1Q VLAN can be enabled. When one is enabled, the other two are disabled.

## 7.2 Port VLAN

Port VLAN is similar to port isolation function, which divides ports into different VLANs. Ports in the same VLAN can communicate with each other, but ports in different VLANs cannot communicate . All ports are in VLAN 1 by default ( as shown in the Figure 7-3 )

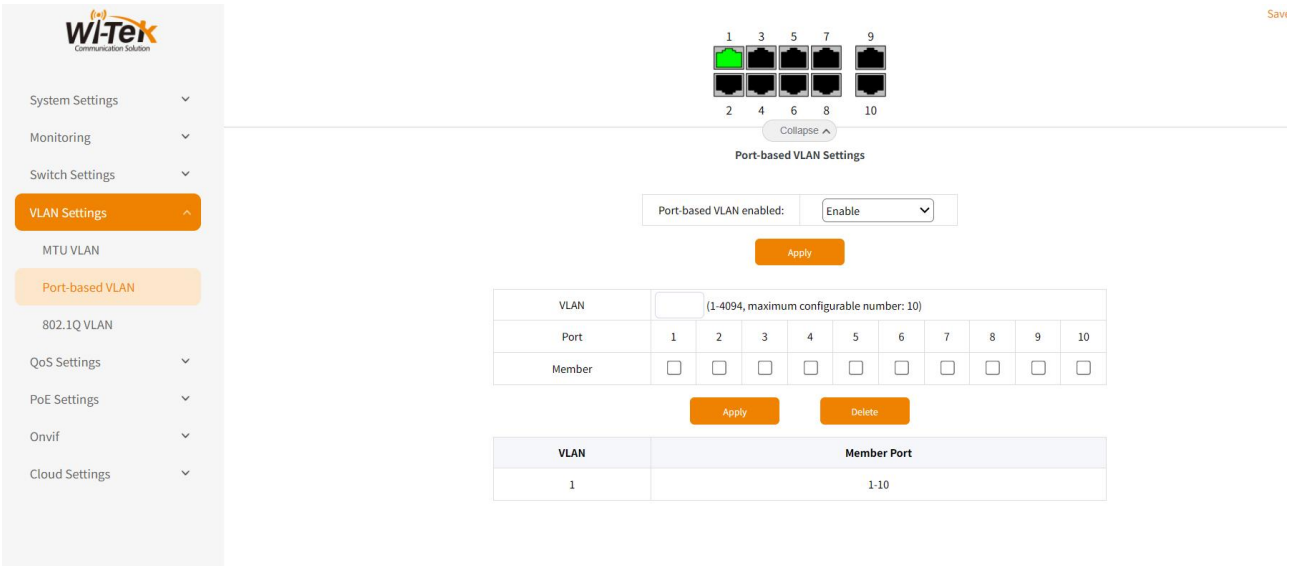



Figure 7-3

### 7.2.1 Port VLAN Settings

Click VLAN > Port VLAN, select Enable MTU VLAN, add VLAN 2 including ports 2 and 4; then select VLAN 1 to exclude ports 2 and 4. Now ports 2 and 4 can communicate with each other, but cannot communicate with other ports ( as shown in Figure 7-4 ) .

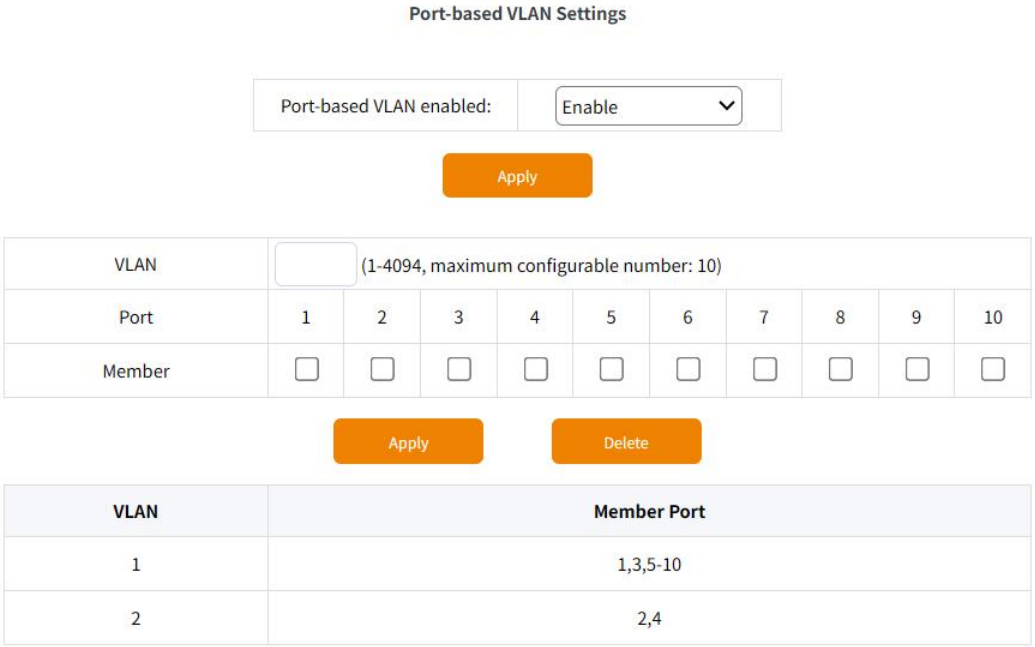



Figure 7-4

**Attention：**

- Only one of MTU VLAN, port VLAN, and 802.1Q VLAN can be enabled. When one is enabled, the other two are disabled.

## 7.3 802.1Q VLAN

A VLAN (Virtual Local Area Network) is a network that is logically divided into different broadcast domains, so that data packets can only be exchanged between ports designated as the same VLAN. Each VLAN is considered a logical network, and data packets destined for different VLANs must be forwarded through routing.

VLANs are described according to the following terms:

VID: VLAN identifier

LAN: Local Area Network

VLAN: Virtual Local Area Network

PVID: Port Vlan ID, which is the virtual local area network ID number of the port, related to the VLAN TAG tag when the port sends and receives data frames

Tagged Frame: It carries a 4-byte VLAN tag, as shown in Figure 7-5 below :

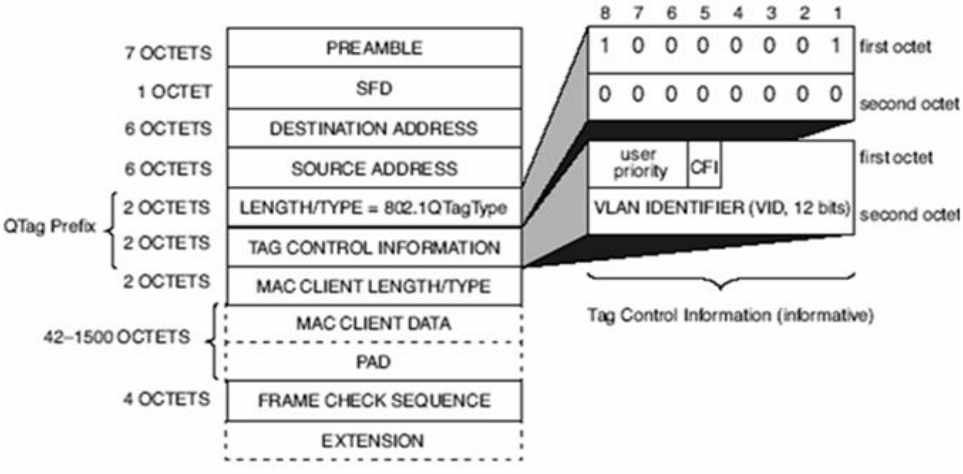



Figure 7-5 Tagged Frame

### 7.3.1 VLAN Creation

Click vlan > 802.1Q VLAN and select Enable 802.1Q VLAN. This is used to add a new VLAN. The specification supports 32 VLANs , and you can add one at a time. When creating a VLAN, you can also select the port tag attribute and VLAN description.

Configuration: Add VLAN 2 including ports 1-8, with ports 1-4 as untagged, ports 2-8 as tagged, and ports 9-10 as non-VLAN 2 member ports. The VLAN description is Aatest_123 ( as shown in Figure 7-6 ) .

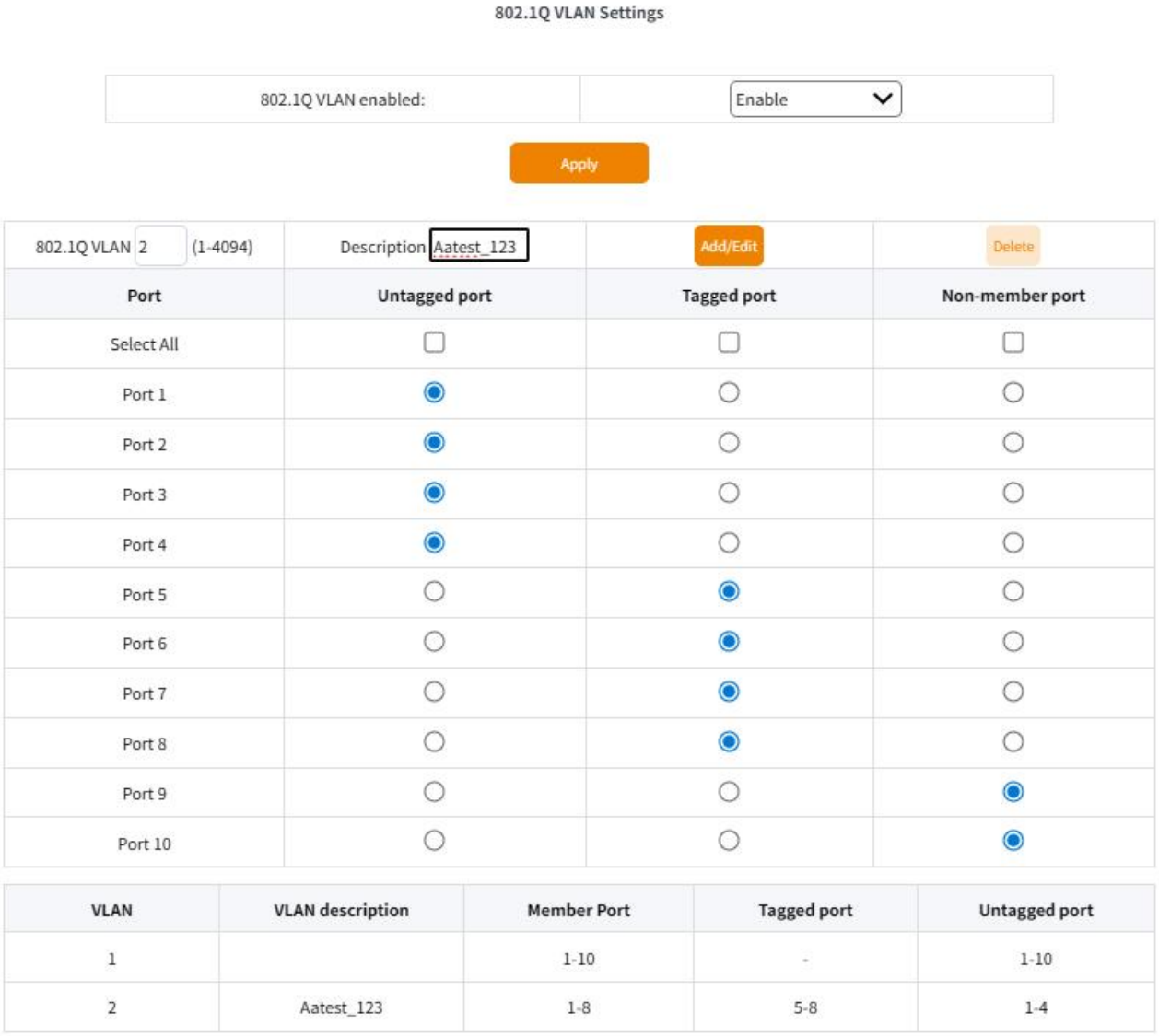



Figure 7-6

By default, VLAN 1 is created, including all ports, and the port attribute is untagged.

# 8 QoS

## 8.1 Port Speed Limit

### 8.1.1 Overview

It mainly implements port speed limit at the exit or entrance; it limits the total rate of messages entering or sending from the port.

### 8.1.2 Entering the port speed limit interface

Select "Port Speed Limit" under "Qos" in the menu bar to enter the port speed limit page (as shown in Figure 8-1 ).

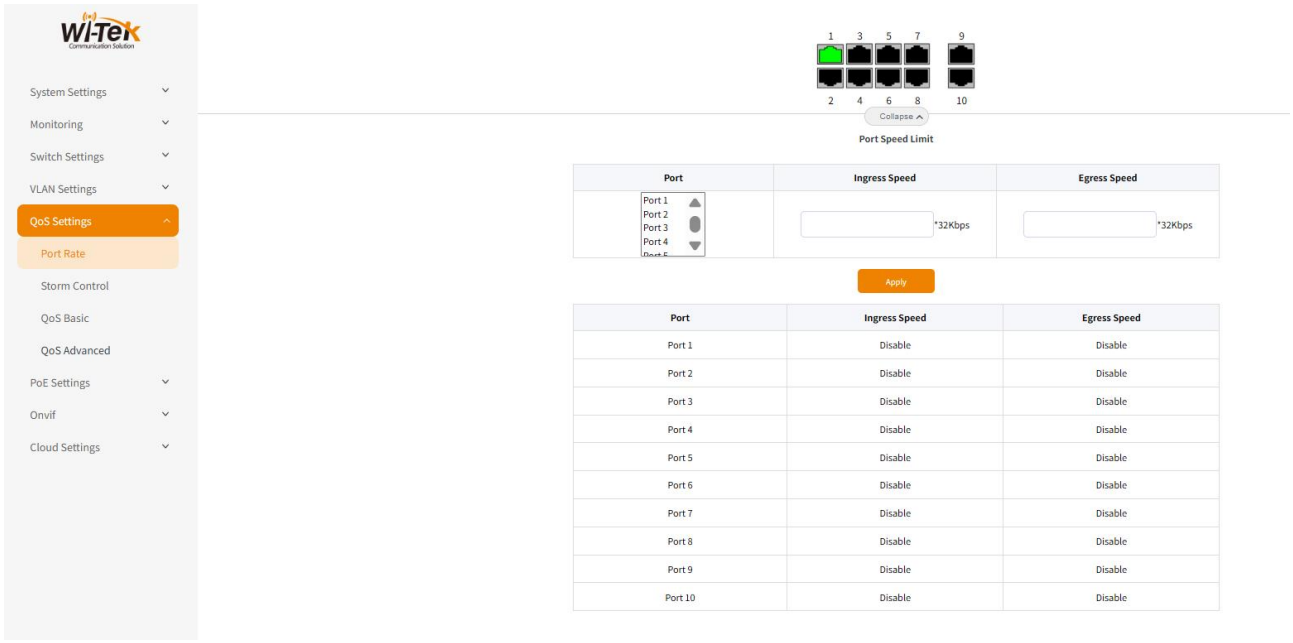



Figure 8-1

### 8.1.3 Configuring Port Rate Limit

On the port speed limit page, press the ctrl key to select the port to be configured, configure the speed limit value in the inlet/outlet speed input box, and click "Apply" (as shown in Figure 8-2 ) .

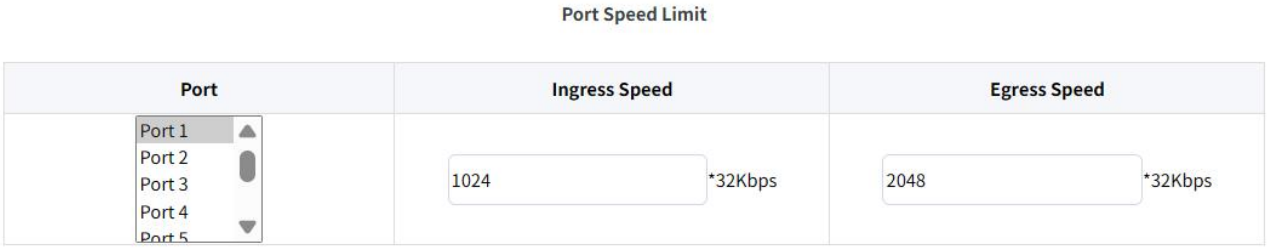



Figure 8-2

The port display page is displayed (as shown in Figure 8-3 ).

| Port | Ingress Speed | Egress Speed |
|---|---|---|
| Port 1 | 32768 Kbps | 65536 Kbps |
| Port 2 | Disable | Disable |
| Port 3 | Disable | Disable |
| Port 4 | Disable | Disable |
| Port 5 | Disable | Disable |
| Port 6 | Disable | Disable |
| Port 7 | Disable | Disable |
| Port 8 | Disable | Disable |
| Port 9 | Disable | Disable |
| Port 10 | Disable | Disable |

Figure 8-3

Parameter Description

| Parameter items | illustrate |
|---|---|
| port | Port number |
| Inlet velocity | Port ingress rate limit |
| Exit speed | Port egress rate limit |

# 8.2 Storm Suppression

## 8.2.1 Overview

Storm suppression limits the maximum amount of broadcast, unknown unicast, and multicast traffic received on a specified interface to prevent flooding from consuming excessive switch resources and ensure normal service operation.

Storm control can be performed in one of two ways:

Bit rate mode (Kbps)

Packet rate mode (pps)

Kpbs: The acronym for Kilo bit per second, which means the number of kilo bits transmitted per second, that is, kilo bit rate.

Pps: The abbreviation of Packets per second, the number of packets transmitted per second, that is, the packet rate.

## 8.2.2 Entering the Storm Suppression Interface

Select "Storm Suppression" under "Qos" in the menu bar to enter the storm suppression interface (as shown

in Figure 8-4 ) .

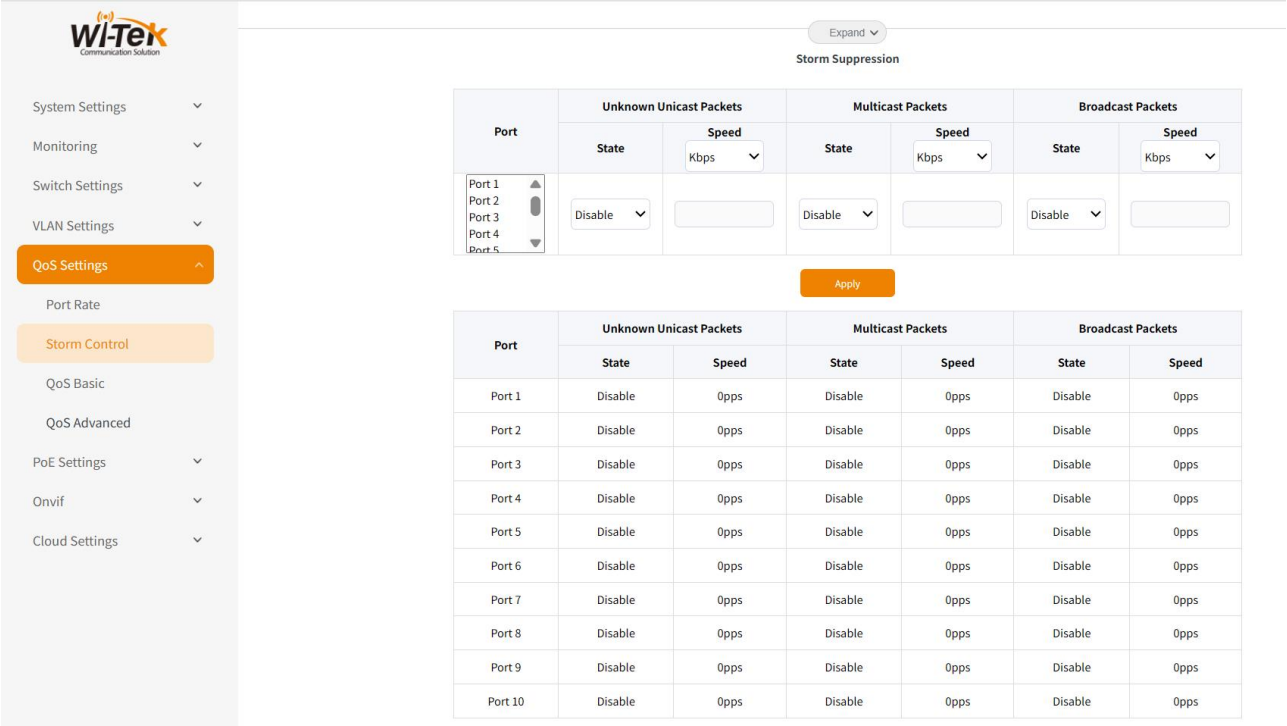



Figure 8-4

## 8.2.3 Configuring Storm Suppression

On the Storm Suppression page, press the Ctrl key to select the port to be configured, configure the unknown unicast packet rate to 512Kbps , multicast packet rate to 1024Kbps , and broadcast packet rate to 2048Kbps . The status can be selected as Kbps or PPS (as shown in Figure 8-5 ).

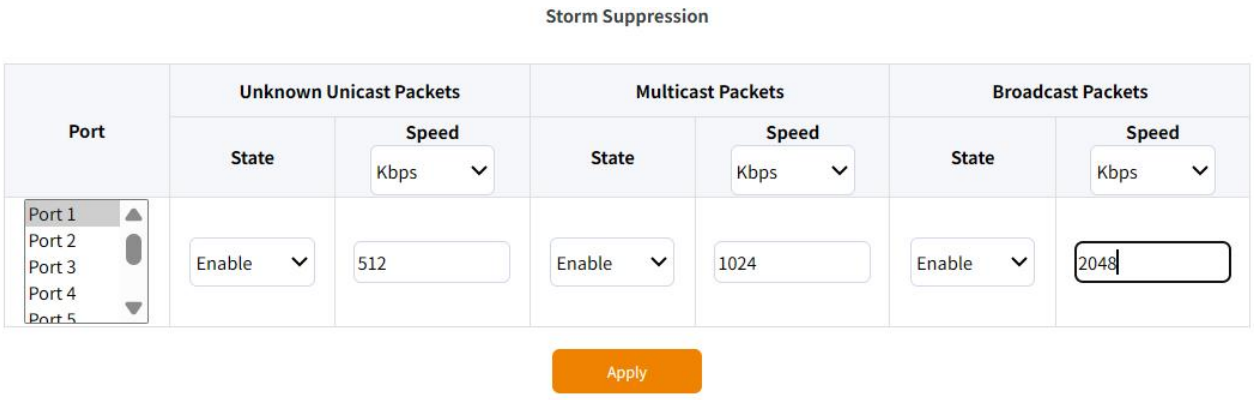



Figure 8-5

It is displayed on the port storm suppression rate display page (as shown in Figure 8-6 ).

| Port | Unknown Unicast Packets | | Multicast Packets | | Broadcast Packets | |
|---|---|---|---|---|---|---|
| | State | Speed | State | Speed | State | Speed |
| Port 1 | Enable | 512Kbps | Enable | 1024Kbps | Enable | 2048Kbps |
| Port 2 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 3 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 4 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 5 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 6 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 7 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 8 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 9 | Disable | 0pps | Disable | 0pps | Disable | 0pps |
| Port 10 | Disable | 0pps | Disable | 0pps | Disable | 0pps |

Figure 8-6

Parameter Description

| Parameter items | illustrate |
|---|---|
| port | Port Name |
| Unknown unicast packet | The destination address is not in the FDB table entry |
| Multicast packets | The destination address is a multicast address |
| Broadcast Packet | The destination address is FF-FF-FF-FF-FF-FF |
| state | Contains two states: disabled and enabled |
| rate | Based on Kpbs and pps modes, 0 is the default value, no limit |

# 8.3 Basic QoS Configuration

## 8.3.1 Overview

The QoS basic configuration page is used to configure queue scheduling, which solves the problem of multiple packets competing for resources when the network is congested.

## 8.3.2 Entering the QoS basic configuration interface

“QoS Basic" under "QoS Settings" in the menu bar to enter the QoS basic configuration interface (as shown in

Figure 8-7 ) .

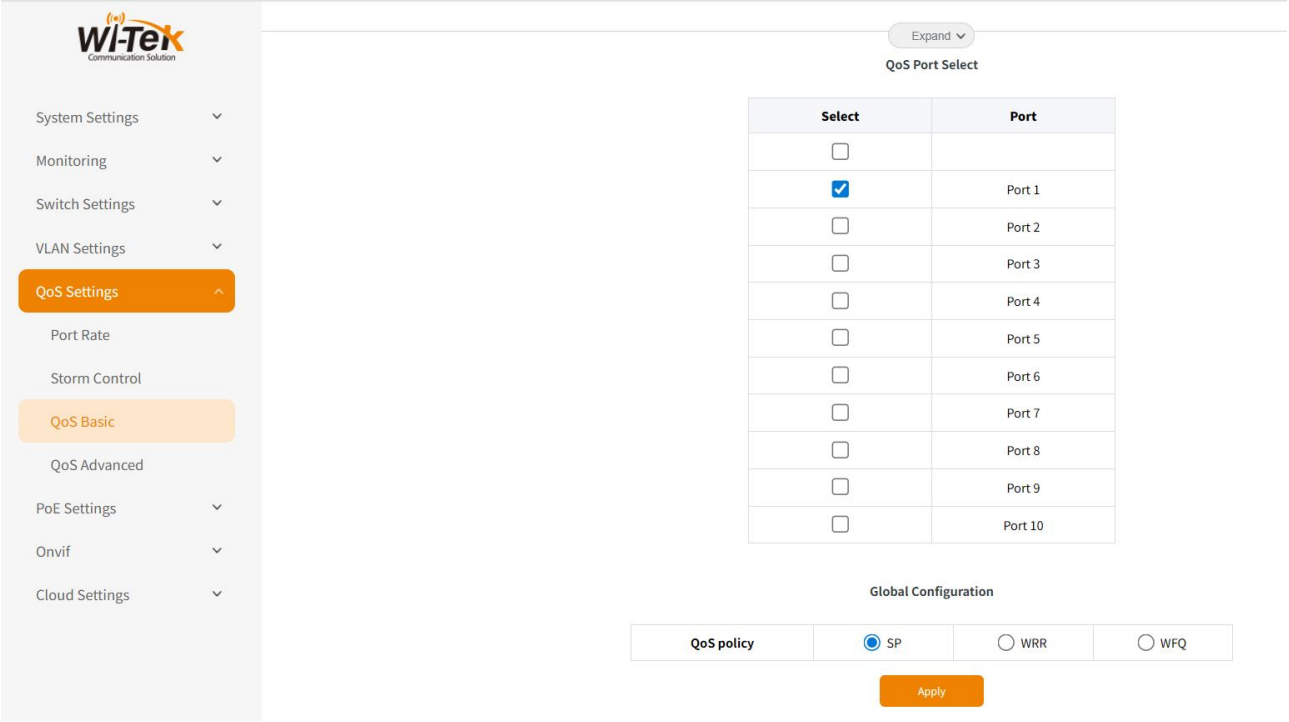



Figure 8-7

## 8.3.3 Basic QoS Configuration

In the QoS basic configuration interface, you can select QoS ports and QoS policies . By default, each port has the same priority (as shown in Figure 8-8 ).

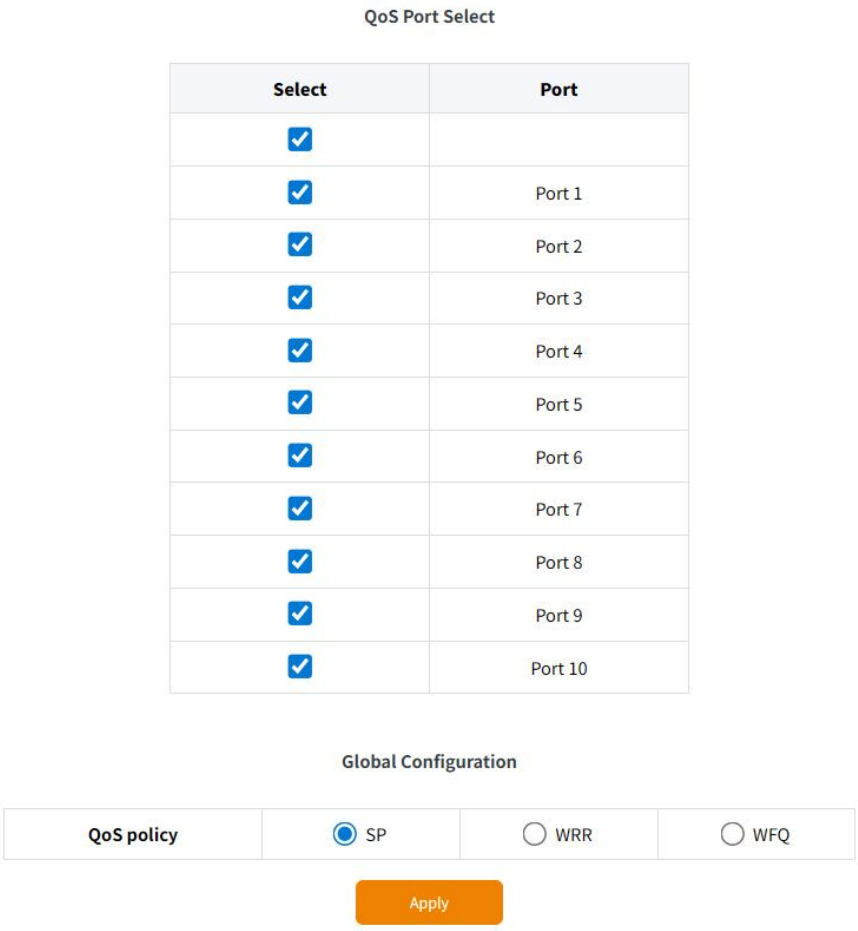



Figure 8-8

Parameter Description

| Parameter items | illustrate |
|---|---|
| port | Device port number |
| QoS strategy | There are three strategies:<br>SP, demands priority service when congestion occurs ;<br>WRR, weighted round-robin scheduling based on user-defined parameters;<br>WFQ schedules the queues in the SP group first using the SP method, and then performs round-robin scheduling based on the scheduling weight of each queue in the WFQ group. |

## 8.4 QoS Advanced Configuration

Select "QoS Advanced Configuration" under "QoS" in the menu bar to enter the QoS advanced configuration interface (as shown in Figure 8-9).

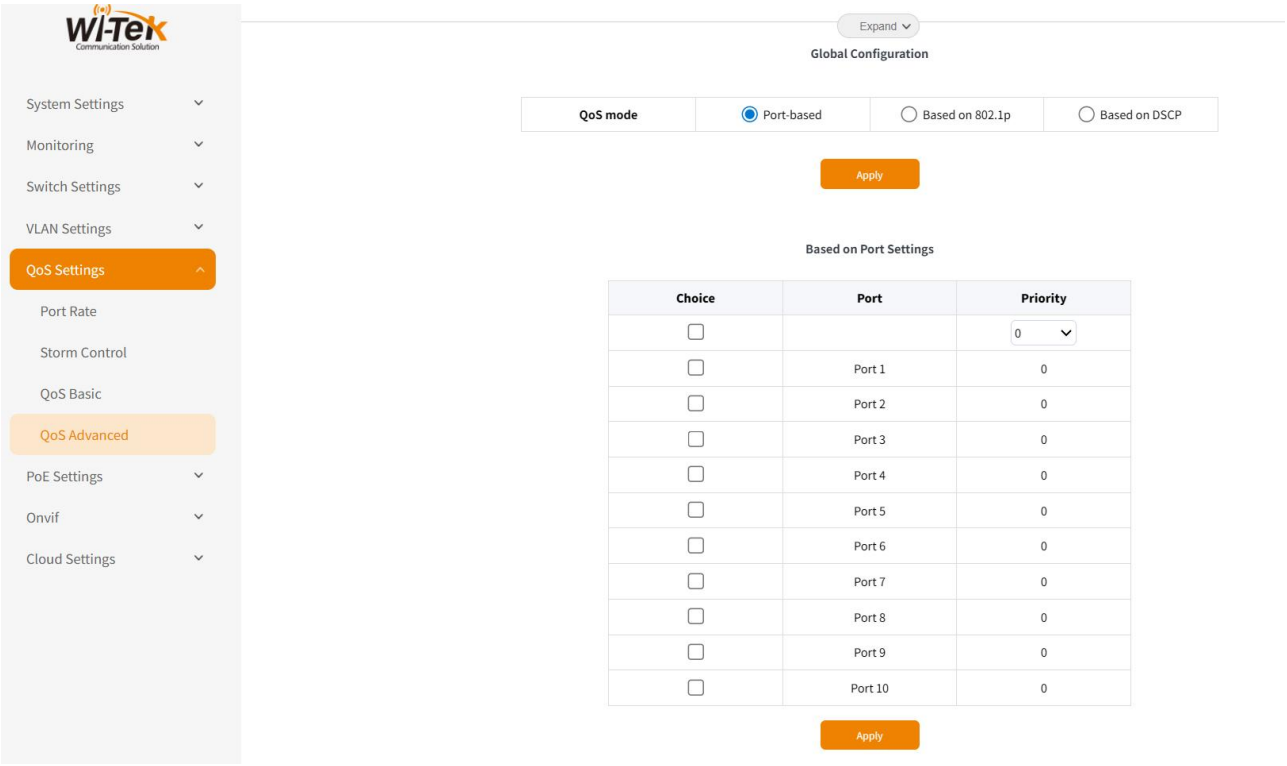



Figure 8-9

## 8.4.1 Perform advanced QoS configuration

This page allows users to modify the QoS mode, port priority, and port priority mapping queue. The default QoS mode is port-based. Select the port to be configured, select the value to be configured from the priority drop-down box, and click Apply to successfully configure (as shown in Figure 8-10) .

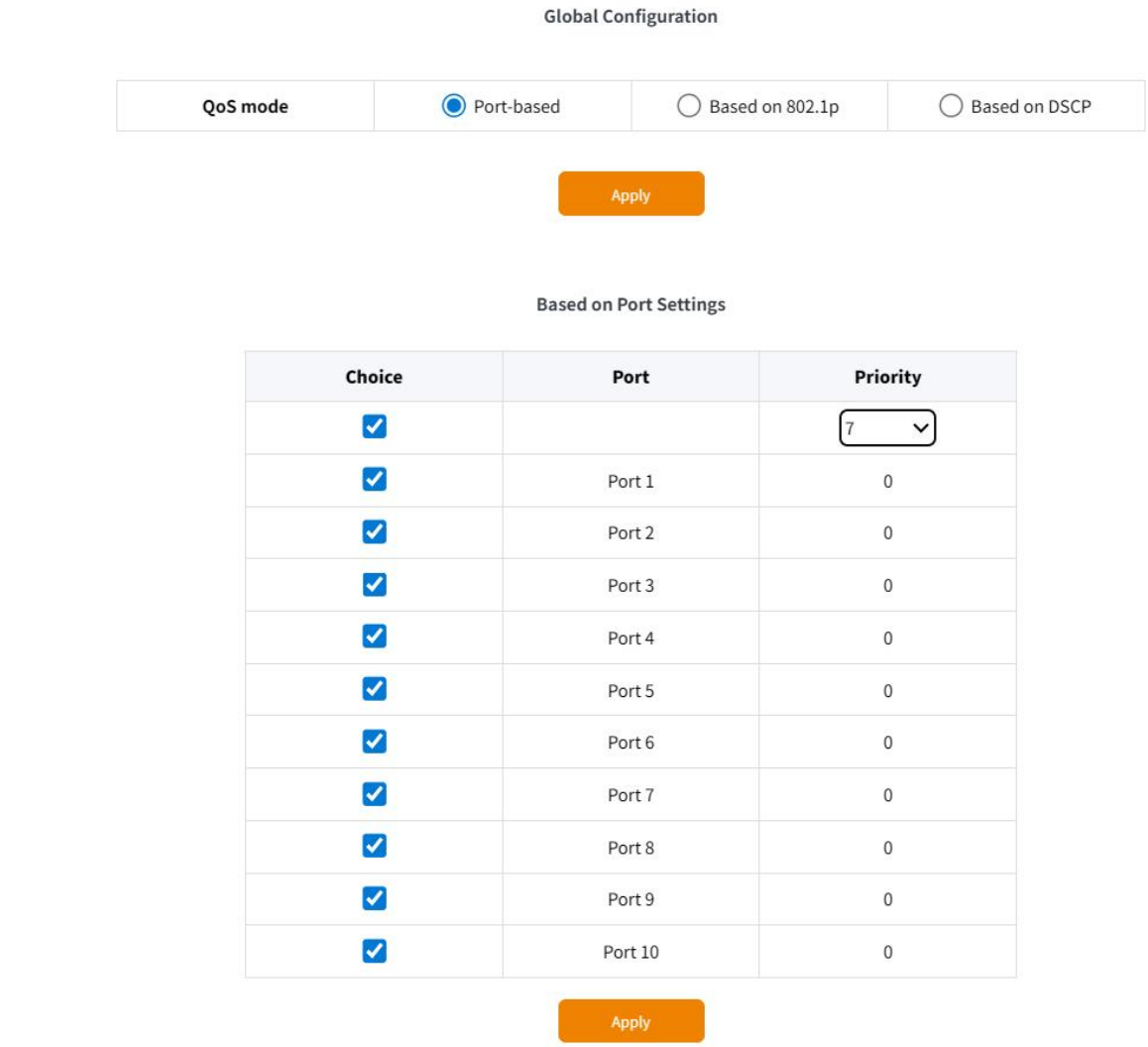



Figure 8 - 10

Select the priority you want to modify, select the mapped queue from the Queue drop-down box, and click Apply to successfully configure it (as shown in Figure 8-11) .

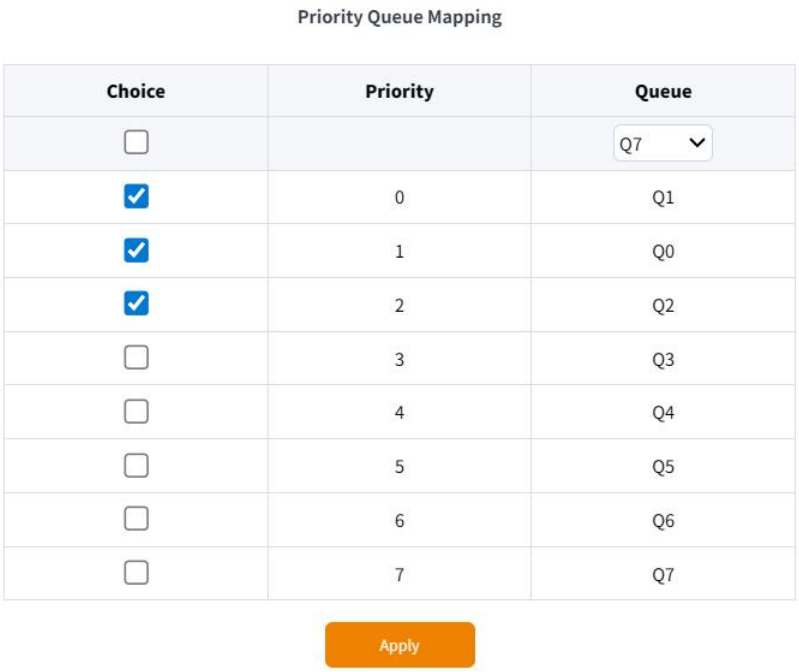



Figure 8 - 11

Parameter Description

| Parameter items | illustrate |
|---|---|
| Qos mode | There are three QoS modes:<br>● Port-based, port priority.<br>● Based on the value of the pri field in 802.1P and 802.1Q VLAN frames.<br>● Based on DSCP, the value corresponding to the DSCP in the TOS byte in the IPv4 packet header. |
| port | Port name. |
| Priority | 802.1P priority, ranging from 0 to 7.<br>DSCP priority, ranging from 0 to 63. |
| queue | Hardware priority queue. |

# 9 POE

Power over Ethernet (PoE) refers to power supply over an Ethernet network. It is also known as a local area network (LAN)-based power supply system (PoL) or active Ethernet.

PoE, a wired Power over Ethernet (PoE) technology, is currently the most widely used technology in local area networks (LANs). PoE allows power to be transmitted to terminal devices via data transmission lines or idle lines. Powered by 10BASE-T, 100BASE-TX, 1000BASE-T, and 2.5GE BASE-T Ethernet networks, PoE reliably provides power up to 100 meters. This effectively solves the problem of centralized power supply for terminals such as IP phones, wireless access points (APs), portable device chargers, card readers, cameras, and data acquisition systems. These terminals no longer need to worry about indoor power system cabling; they can be powered the moment they connect to the network.

Advantages of PoE:

•Reliable: Centralized power supply and easy backup.

• Simple connection: The network terminal does not require an external power supply, only a network cable.

•Standard: Complies with IEEE 802.3bt, IEEE 802.3af, and IEEE 802.3at standards, and uses a globally unified power interface.

Currently, this series of switches supports the IEEE 802.3af/at standard based on Power over Ethernet (PoE) .

Click on the menu bar - " POE " to enter ( as shown in the Figure 9 -1 ).

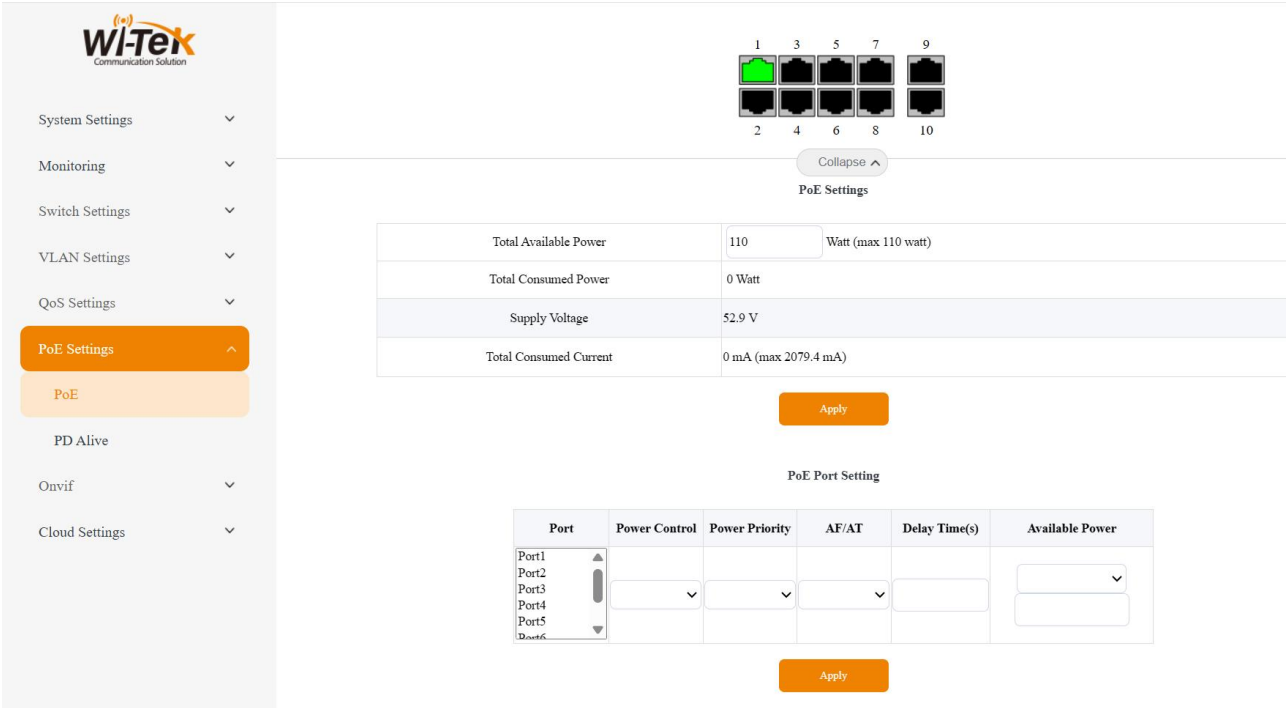



Figure 9-1

## 9.1 POE Settings

On this page, you can configure the maximum power supply of PoE (power range 0-110w, default is 110w), and view the power supply status of PoE ( as shown in Figure 9-2 )

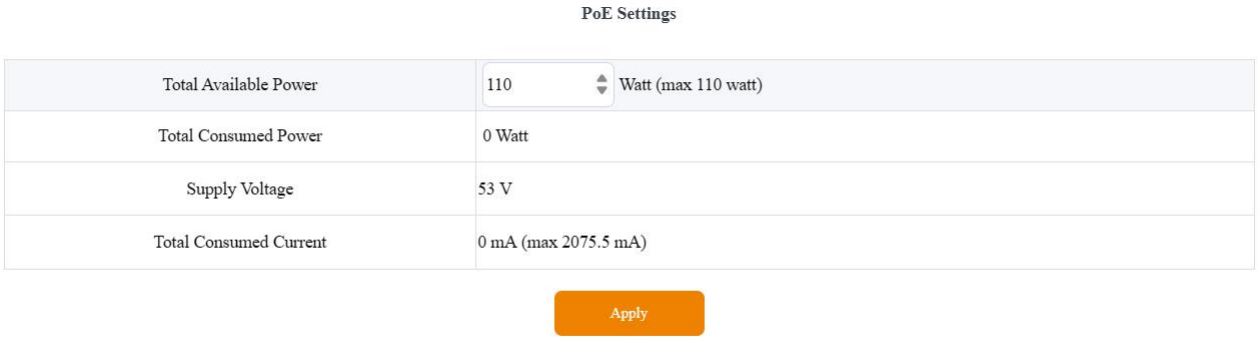
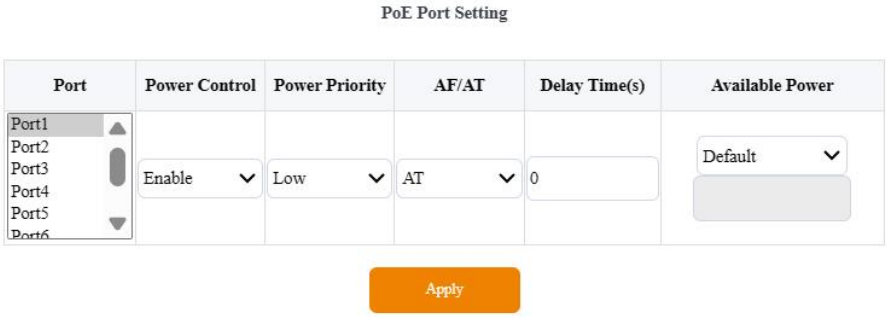



Figure 9-2

## 9.2 POE port settings

On the POE port settings page, you can select the switch port's POE status, priority, protocol type, power-on delay (configuration range 0-10S), and available power. By default, all POE ports are enabled, low priority, use the AF protocol, have a power-on delay of 0, and a port power limit of 30W. Ports 9 and 10 do not support POE configuration. ( See Figure 9-3 )




| Port | Power Control | Power Priority | AF/AT | Delay Time(s) | Power Status | PD Class | Power(watt) | | Voltage(V) | Current(mA) | Power Event |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Available | Consumed | | | |
| Port1 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port2 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port3 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port4 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port5 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port6 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 52.8 | 0 | N/A |
| Port7 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 52.8 | 0 | N/A |
| Port8 | Enable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |

Figure 9-3

Configuration: Turn off the PoE power supply of ports 1-4, set the priority of ports 5-8 to high, the power supply protocol to AF, the power-on delay to 5 seconds, and the available power to 10W ( as shown in Figure 9-4 ).

| Port | Power Control | Power Priority | AF/AT | Delay Time(s) | Power Status | PD Class | Power(watt) | | Voltage(V) | Current(mA) | Power Event |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | Available | Consumed | | | |
| Port1 | Disable | Low | AT | 0 | Off | N/A | Default | 0 | 53.1 | 0 | N/A |
| Port2 | Disable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port3 | Disable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port4 | Disable | Low | AT | 0 | Off | N/A | Default | 0 | 53 | 0 | N/A |
| Port5 | Enable | High | AF | 5 | Off | N/A | 10 | 0 | 53 | 0 | N/A |
| Port6 | Enable | High | AF | 5 | Off | N/A | 10 | 0 | 53 | 0 | N/A |
| Port7 | Enable | High | AF | 5 | Off | N/A | 10 | 0 | 53 | 0 | N/A |
| Port8 | Enable | High | AF | 5 | Off | N/A | 10 | 0 | 53 | 0 | N/A |

Figure 9-4

Parameter Description

| Parameter items | illustrate |
|---|---|
| Power Control | of the port is on by default |
| Power supply priority | Port power supply priority, there are three levels: highest, high, and low |
| AF/AT | The power supply protocol selected for the corresponding port |
| Power-on delay time (S) | Port power-on delay time, in seconds |
| Power supply status | Distinguish whether the port is powered normally, with two modes: on and off |
| PD classification | Identify the PD level of the powered device according to the power supply, there are five levels from 0 to 4 |
| Power ( W ) | In the power supply state, it displays the actual power consumed by the port |
| Current ( mA ) | In the power supply state, the actual output current of the display port is in milliamperes |
| Voltage ( V ) | In the power supply state, the actual output voltage of the display port is in volts |
| Available power | The available power setting needs to be |

| | |
|---|---|
| | compared with the reference power supply protocol. The power range of the AF protocol is 0-15.4W, and the power range of the AT protocol is 0-30W. |

## 9.3 PD Alive Settings

Click the menu bar - " POE " - "PD Alive" to enter . This interface can enable the PD Alive function on the port and configure the waiting time of this function. The configuration range is 90-300S. By default, this function is disabled on all ports ( as shown in Figure 9-5 ).

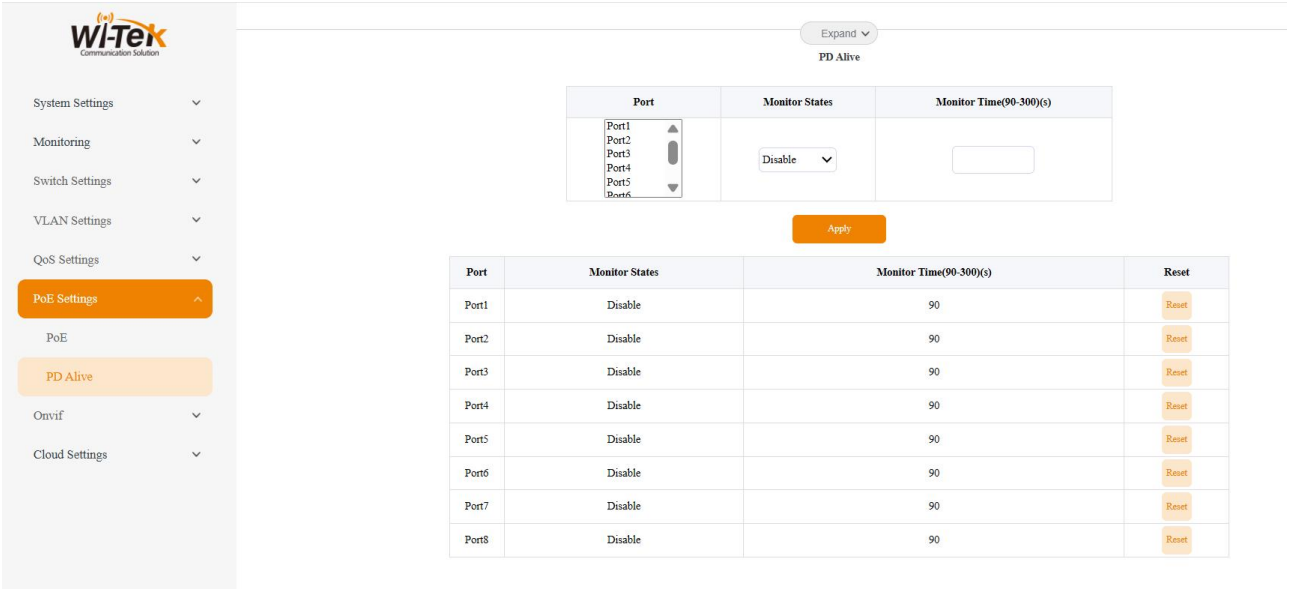



Figure 9-5

Configuration: Enable PD Alive on ports 1-4 and set the wait time to 100S ( see Figure 9-6 ).

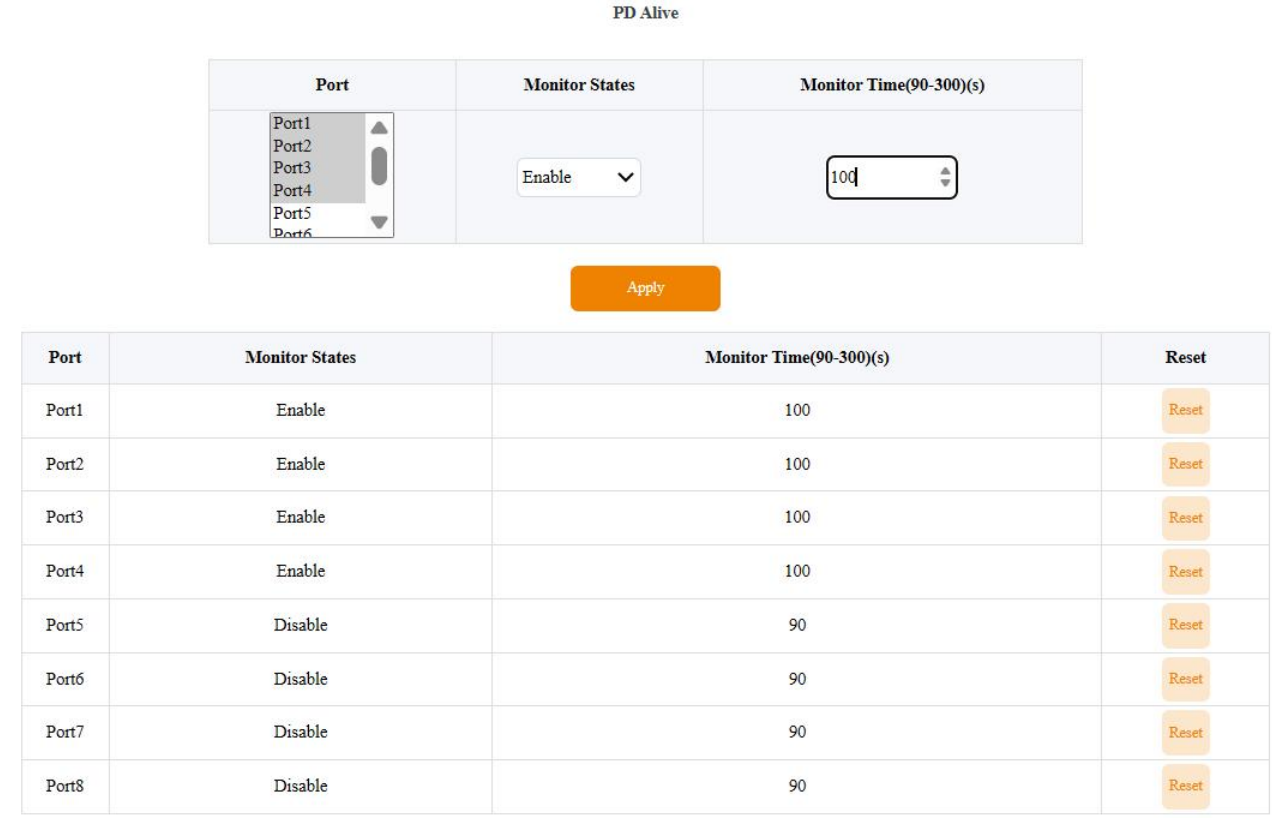



Figure 9-6

# 10 Onvif

## 10.1 Onvif detection

### 10.1.1 Overview

The ONVIF protocol (Open Network Video Interface Forum) is a global, open industry standard designed to promote interoperability among network video products (such as cameras and video recorders) across multiple brands. The ONVIF protocol defines a set of common interfaces that enable network video products from different manufacturers to be compatible and interconnected within surveillance systems.

### 10.1.2 Entering the Onvif detection interface

Onvif detection is used to identify connected cameras . Select "Onvif" -- " Onvif detection " to enter the interface . (As shown in Figure 10-1 )

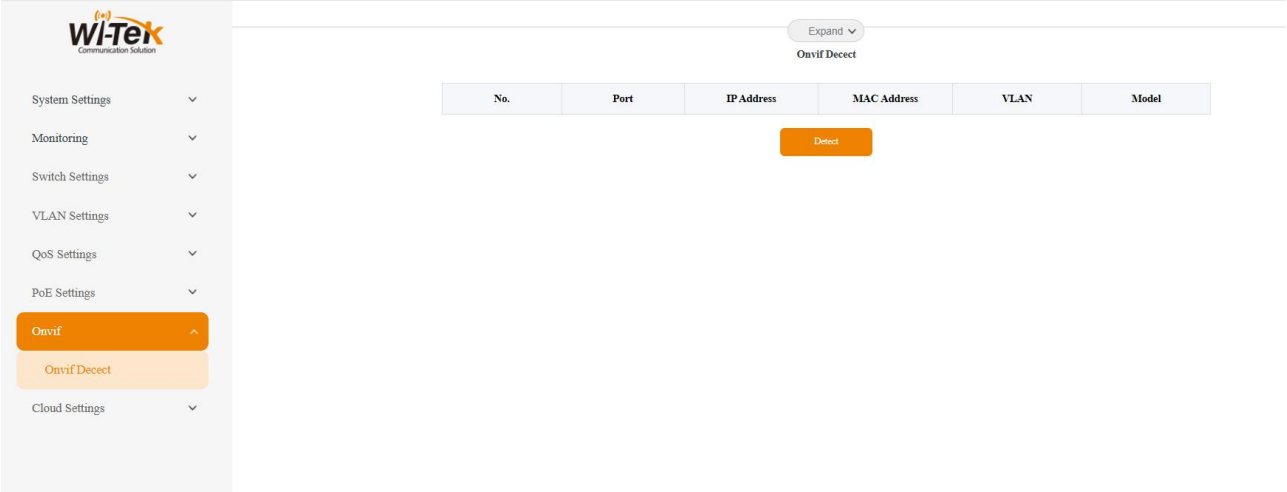



Figure 10-1

Parameter Description

| Parameter items | illustrate |
|---|---|
| No. | Serial number |
| port | Access camera connection port |
| IP address | Access camera IP address |
| MAC address | MAC address of the connected camera |
| VLAN | VLAN ID |
| model | Connected camera model |

# 11 Cloud Configuration

## 11.1 Cloud Configuration

To configure the parameters for connecting the device to the cloud platform, you must first ensure that the device and the cloud platform server can communicate. The default status is Enable.

(As shown in Figure 10-2 ). Click the menu bar--" Cloud Configuration" to enter.

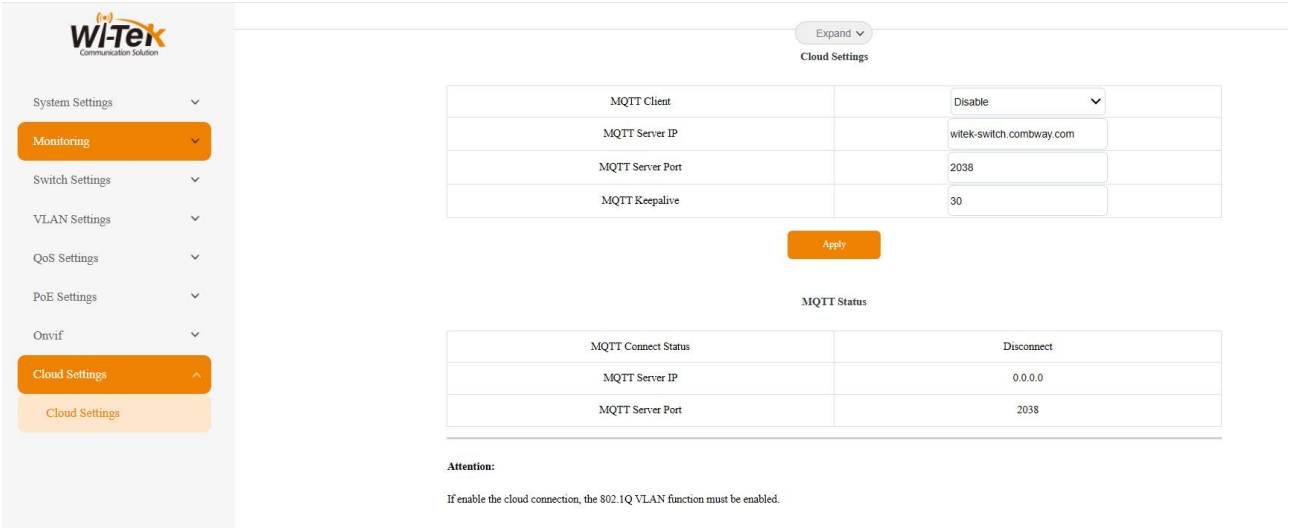



Figure 10-2

Parameter Description

| Parameter items | illustrate |
|---|---|
| MQTT Client | Enabling and disabling functions |
| MQTT server address | Cloud server address, which is the domain name |
| MQTT server port | MQTT server port number |
| MQTT server lifetime | MQTT heartbeat packet sending cycle |