XikeStor

Catalogs

**I. Initial Login to the Switch Web Management Interface** ..... **2**
**II. System Config** ..... **3**
1. System Homepage ..... **3**
**2. Device Info** ..... **4**
**3. IP Config** ..... **4**
3.1 IPv4 Config ..... 4
3.2 IPv6 Config ..... 5
**4. Web Config** ..... **6**
4.1 Web Timeout ..... 6
4.2 HTTP ..... 6
4.3 HTTPS ..... 6
4.4 Security IP ..... 7
4.5 ACL(Access Control) ..... 7
**5. User Management** ..... **7**
5.1 User Management ..... 7
5.2 Authentication Method ..... 8
**6. Firmware Upgrade** ..... **8**
6.1 HTTP Upgrade ..... 8
6.2 TFTP Service ..... 9
6.3 FTP Service ..... 9
**7. Management Config** ..... **9**
7.1 TFTP ..... 9
7.2 HTTP ..... 9
**8. NTP** ..... **10**
8.1 NTP Config ..... 10
8.2 NTP Authentication Config ..... 10
**9. SNTP** ..... **10**
9.1 Server Config ..... 10
9.2 Time Zone Config ..... 10
**10. Device Management** ..... **11**
10.1 Device Reboot/Reset ..... 11
10.2 System Utilization ..... 11
10.3 View System Config ..... 11
**III. Switch Config** ..... **12**
**1. Port Config** ..... **12**
1.1 Port Config ..... 12
1.2 Port 10G Mode ..... 13

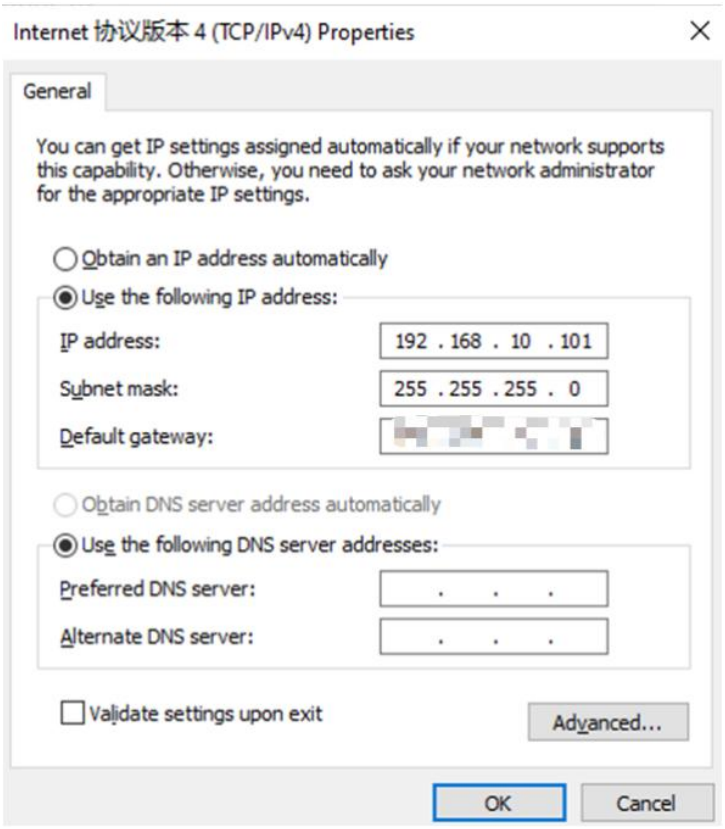
XikeStor

# I. Initial Login to the Switch Web Management Interface

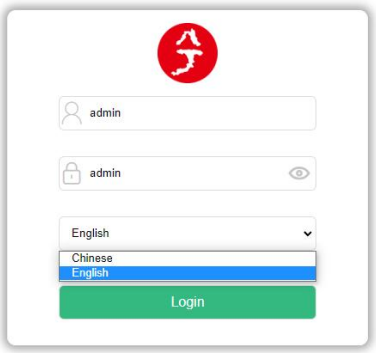
1. The default management ip of SKS8300-8X/SKS8300-12X is 192.168.10.12, with the default login account admin and the default login password admin.

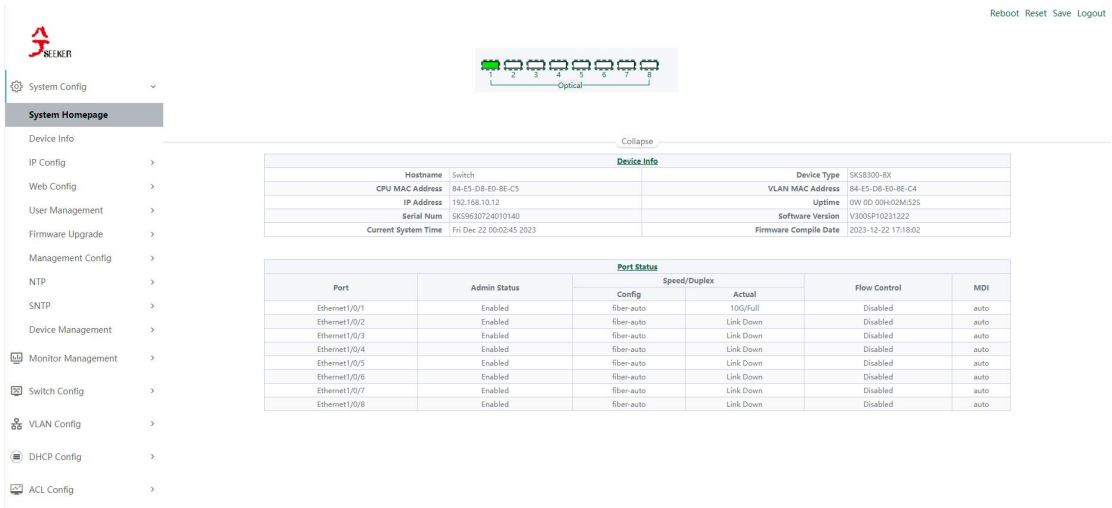
2. First, we use a network cable to connect from the network port of the computer to any port of the switch (this switch requires a MODULE), which defaults in a vlan 1. If the connected port signal light flashes normally, go to step 3. If the port signal light is not on, force the port rate (see SKS8300-8X/SKS8300-12X forced port rate tutorial for details), and proceed to step 3.

3. The ip of the computer is static ip, the ip address is 192.168.10.100, and the subnet mask is 255.255.255.0. (Of course, the computer network card ip as long as 192.168.10.X, the range of X from 1-254, I only take 192.168.10.100 as an example).




4. We open a web page, enter 192.168.10.12 in the url, and enter the default account number and password admin / admin. Enter into the interface of

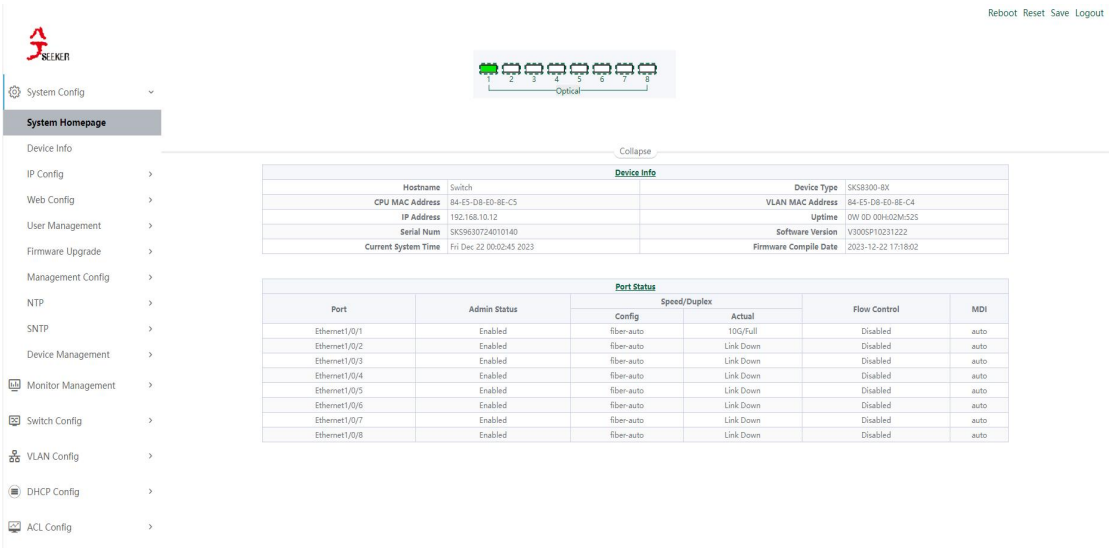



## II. System Config

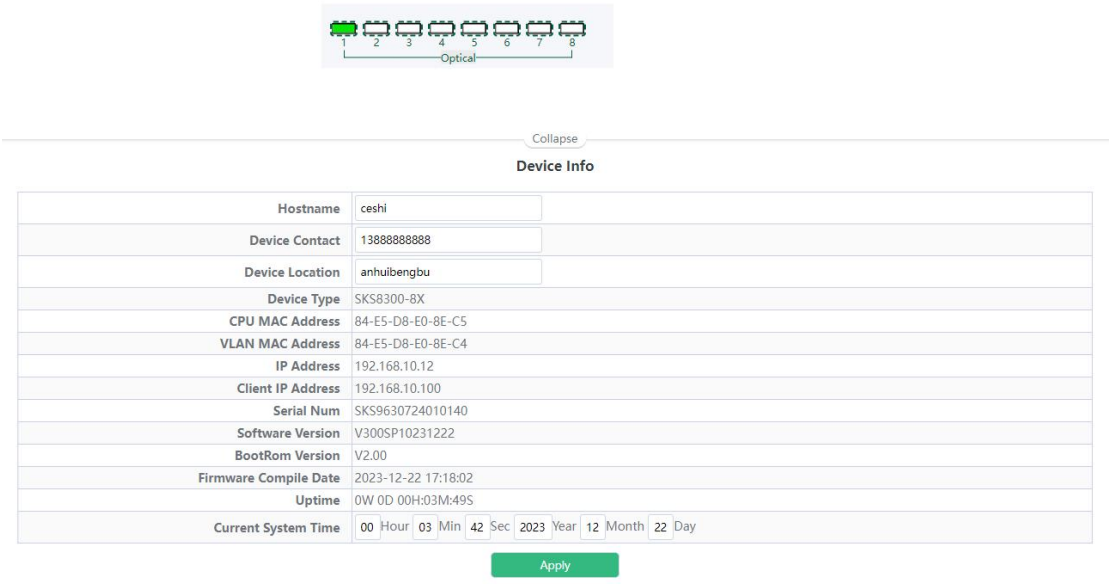
1. System Homepage

You can see the basic information of the device and the port information (only viewing)




2. Device Info

In the equipment information can view the information parameters of the equipment, and can modify the equipment name, equipment contact and the location of the equipment, do not support Chinese input, for example, we modify the equipment name to ceshi, equipment contact to 138888888888, the equipment location of the anhuibengbu, click application, and save.

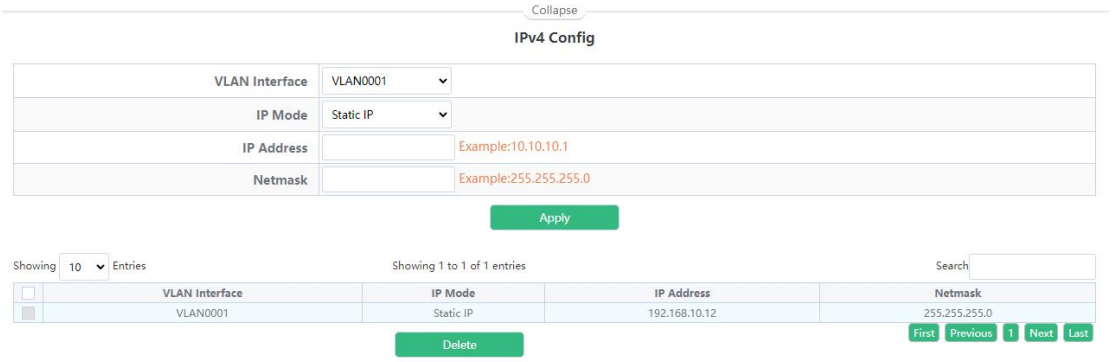



3. IP Config

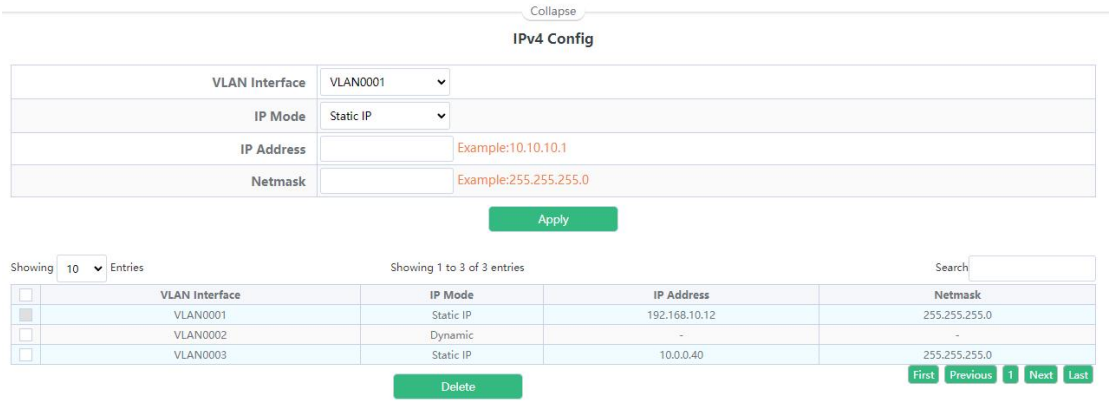
3.1 IPv4 Config

The default VLAN001 is static IP and the address is 192.168.10.12

To change or add IP, you need to choose the VLAN interface name (the default is only VLAN001, and other ports need to be added by yourself), obtain the IP in static IP or dynamic acquisition, add the corresponding IP and subnet mask, add, click application, and save (top right corner of the page). Delete IP as the corresponding row, click delete. Note: The IP addresses of a different VLAN cannot be changed to the same network segment.



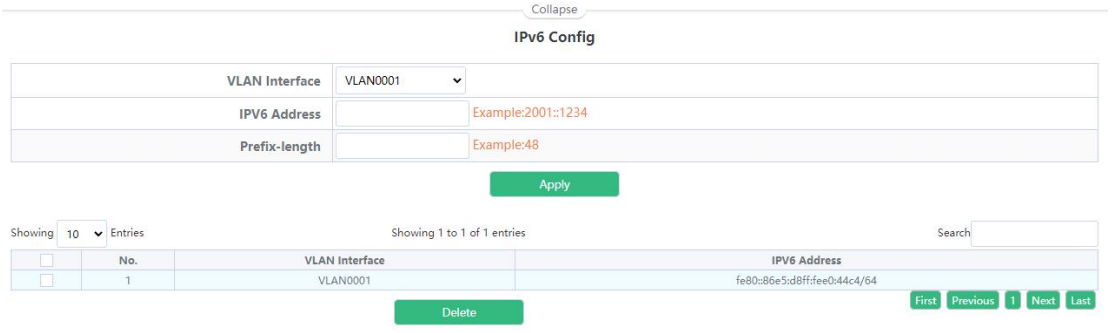

For example, the IP of VLAN002 is set to be dynamic acquisition, the IP of VLAN003 is set to be 10.0.0.40, and the subnet mask is 255.255.255.0



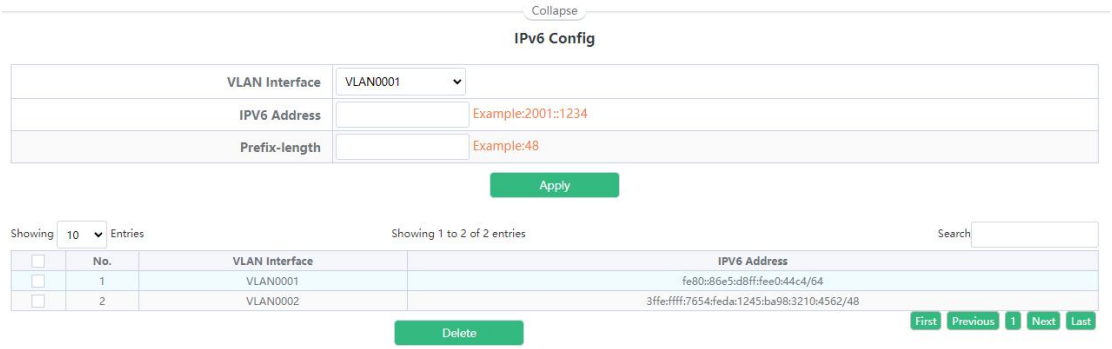

## 3.2 IPv6 Config

The IPv6 address of the system default VLAN001 is fe80::86e5:d8ff:fee0:44c4/64.

To change or add an IP, you need to choose the VLAN interface name (only VLAN001 by default, other ports need to be added by themselves), and then the IPv6 address, and prefix length, click Apply, and save. Delete IP as the corresponding row, click delete.



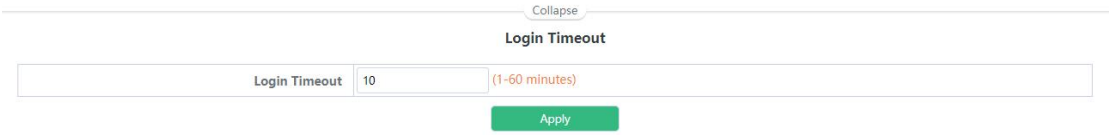

For example, set the VLAN002 with an IPv6 address to 3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562/48



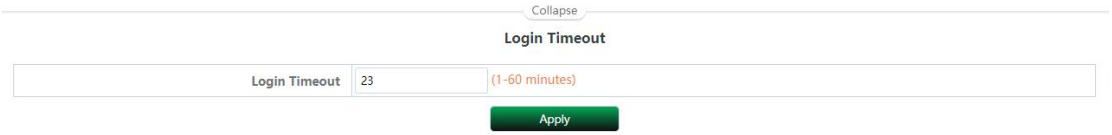

4. Web Config

4.1 Web Timeout

web login timeout time, the system default time is 10 minutes, can be modified to 1-60 minutes, modify and click apply, and save.



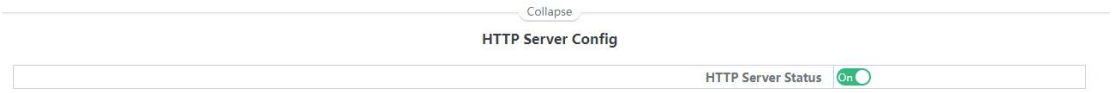

For example, the modified login timeout is 23 minutes




4.2 HTTP

The HTTP server configuration module that can be used to start or stop the HTTP service for the switch. The default is On, which can be modified according to the requirements.

Note that the HTTP service cannot be closed when logging in through HTTP mode. It can only be closed in other login modes. For example, when logging in through HTTPS mode, the HTTP service can be closed and saved. The default login mode of this manual is HTTP service. After the switch is directly closed, however, it is not saved, it can be directly cut off power, and then re-access the power supply, you can log in the background of the switch again through HTTP.

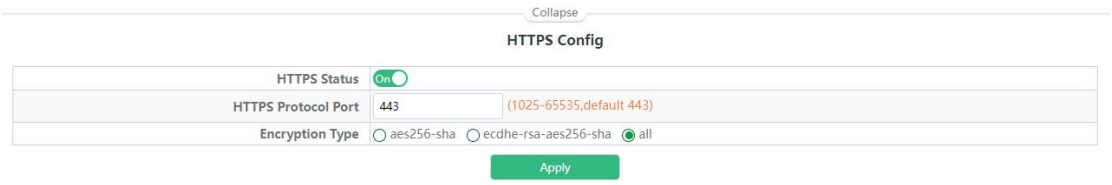



4.3 HTTPS

HTTPS Server configuration module which to start or stop the HTTPS service of the switch. The default is On, which can be modified according to the requirements. Note that HTTPS service cannot be closed when logging in through HTTPS mode. It can only be closed in other login modes. For example, when logging in through HTTP mode, HTTPS service can be closed and saved.

When HTTPS status is on, you can configure HTTPS, save the protocol port number (1025-65535,

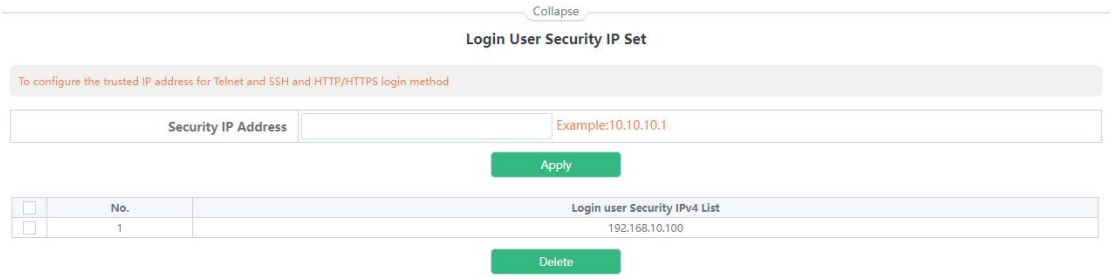
the default is 443), and select the encryption type aes256-sha or ecdhe-rsa-aes256-sha.




4.4 Security IP

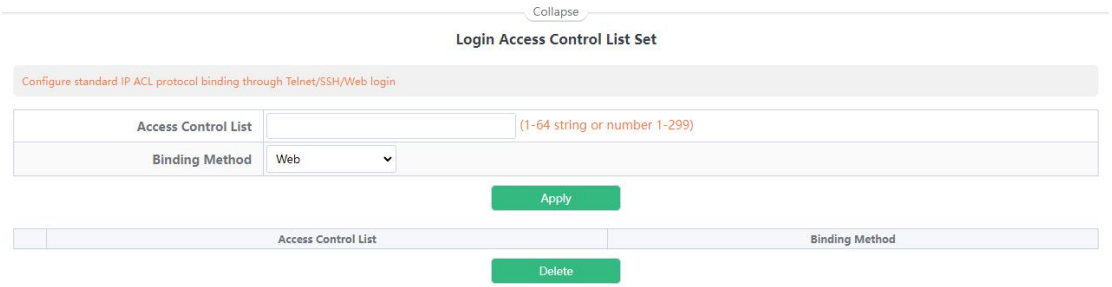
Set the secure IP address, and the IPv4 address outside the list cannot access the web interface.

For example, set the security IP address 192.168.10.100 (the computer IP address we originally modified)




4.5 ACL(Access Control)

Control the access control list (configured in ACL), which can be added or deleted.

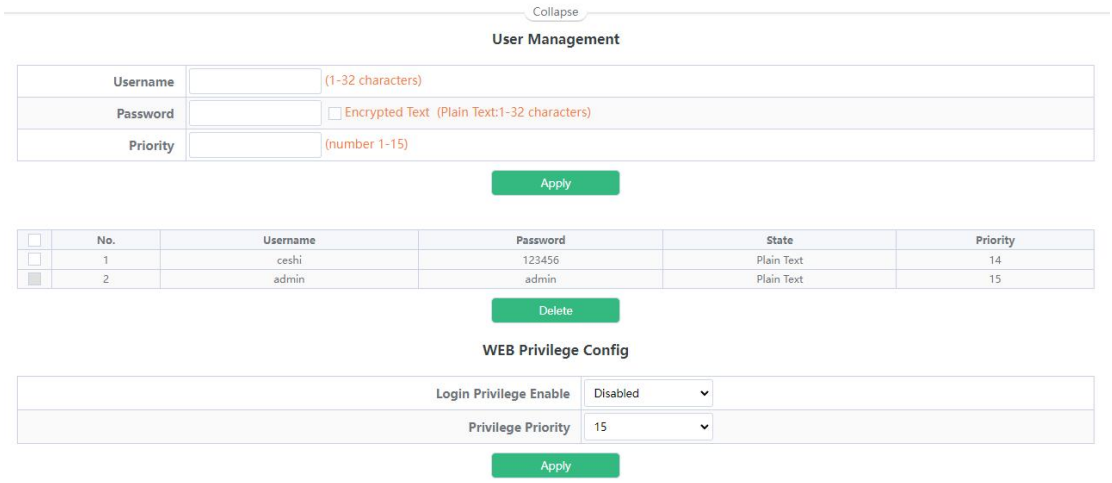



5. User Management

5.1 User Management

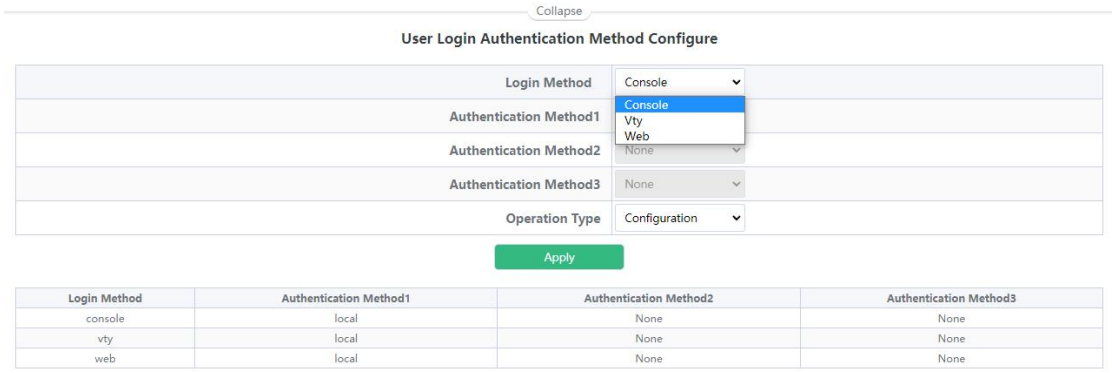
Add the user can edit the user name (1-32 characters) and set the user password (check the hidden text if necessary)

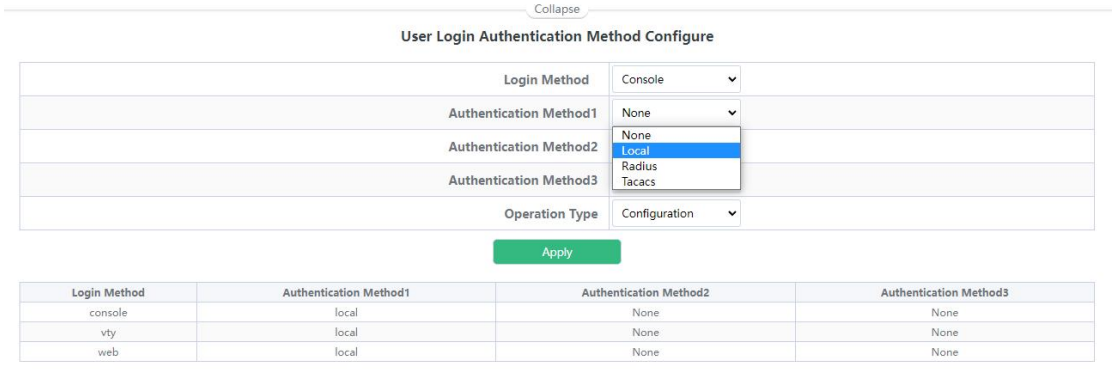
For example, add user ceshi, password 123456, priority 14




## 5.2 Authentication Method

Three login methods can be configured: console (management port) / vty (virtual machine) / web (web page). The authentication method can be either or combination of Local (local), radius (remote dial) and tacacs (terminal access control access control system). Local is generally local account and password login authentication method. radius and tacacs authentication method can only be used after corresponding configuration. The default login authentication method of the system is local.

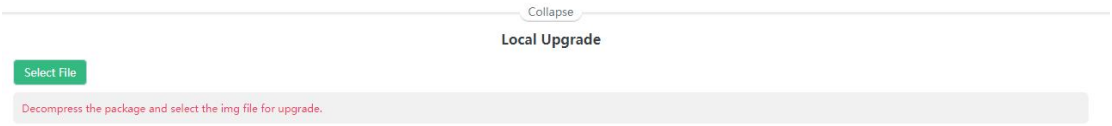



# 6. Firmware Upgrade

## 6.1 HTTP Upgrade

Through the upgrade package locally, select the corresponding img file for firmware upgrade.

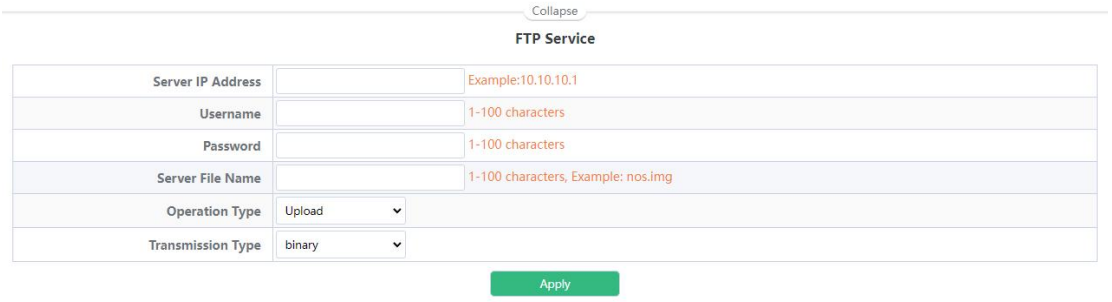



## 6.2 TFTP Service

Here, files can be uploaded or downloaded through TFTP, and the firmware of the switch can be upgraded in this way.

## 6.3 FTP Service

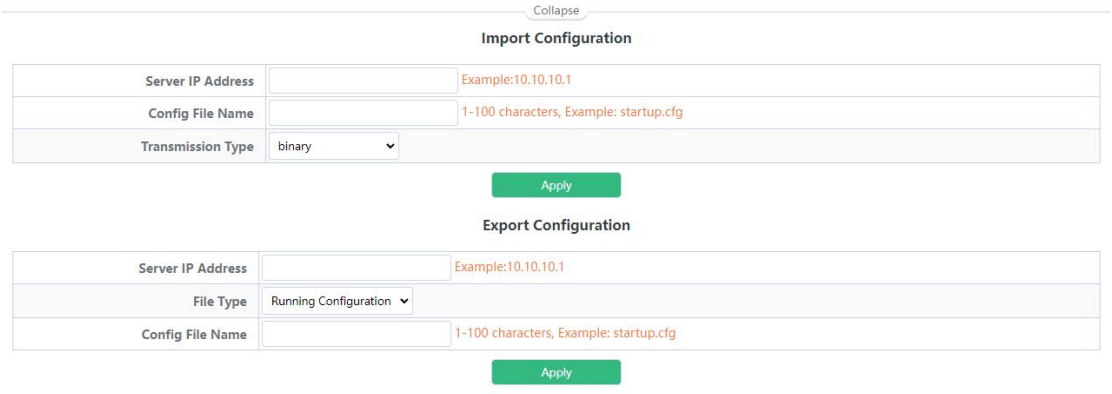
Here you can upload or download files through FTP, and the firmware of the switch can be upgraded in this way.




# 7. Management Config

## 7.1 TFTP

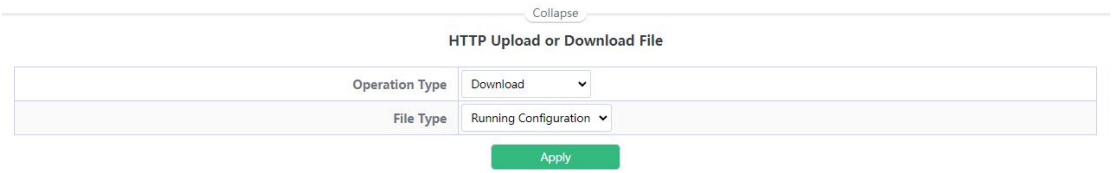
Here, you can import or export the system configuration through the TFTP mode, and operate according to the prompts.




## 7.2 HTTP

Here, you can import or export the system configuration through the HTTP mode, and operate

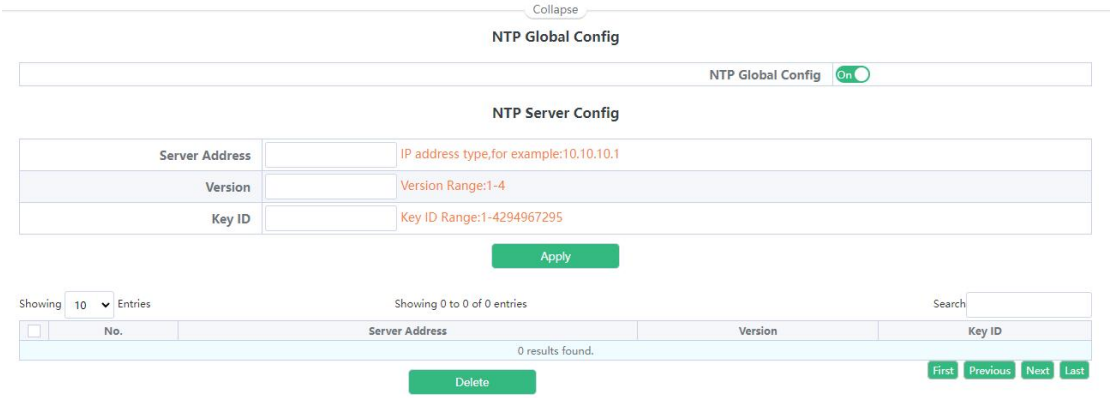
according to the prompts.




8. NTP

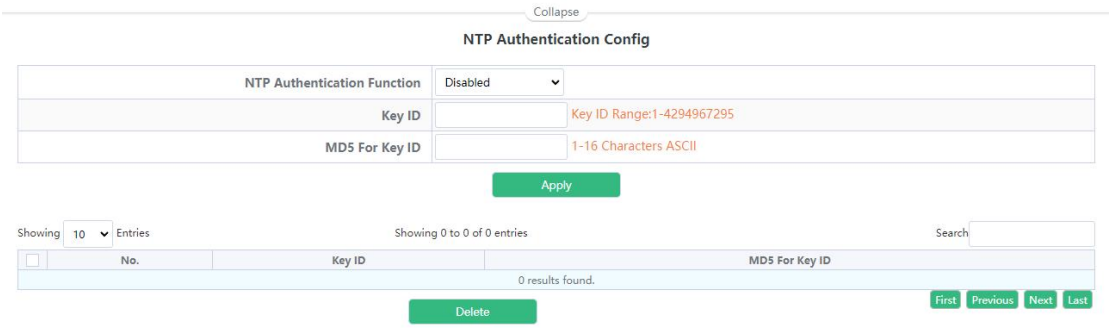
8.1 NTP Config

Here, you can configure the NTP server accordingly, and follow the prompts.




8.2 NTP Authentication Config

Here, you can configure the NTP authentication accordingly, and follow the prompts.



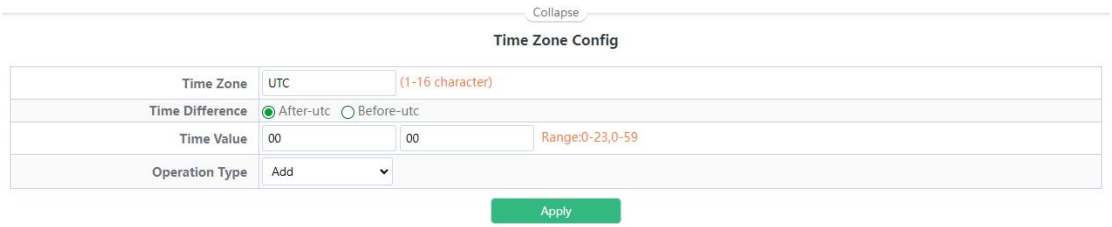

9. SNTP

9.1 Server Config

Here, the SNTP server can be configured accordingly, and then follow the prompts.

9.2 Time Zone Config

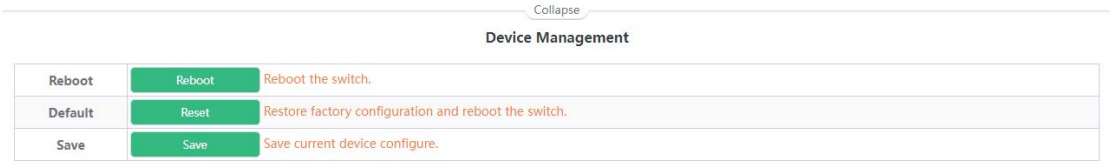
You can increase or reduce time here to make time more accurate.




10. Device Management

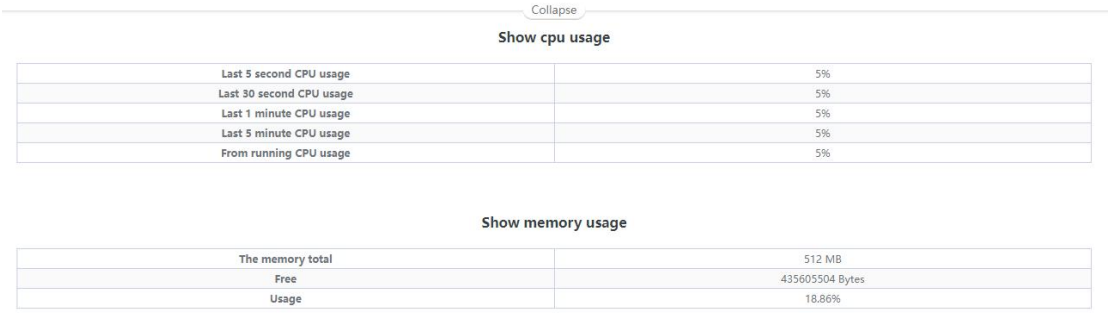
10.1 Device Reboot/Reset

You can restart, restore factory settings and save switches.



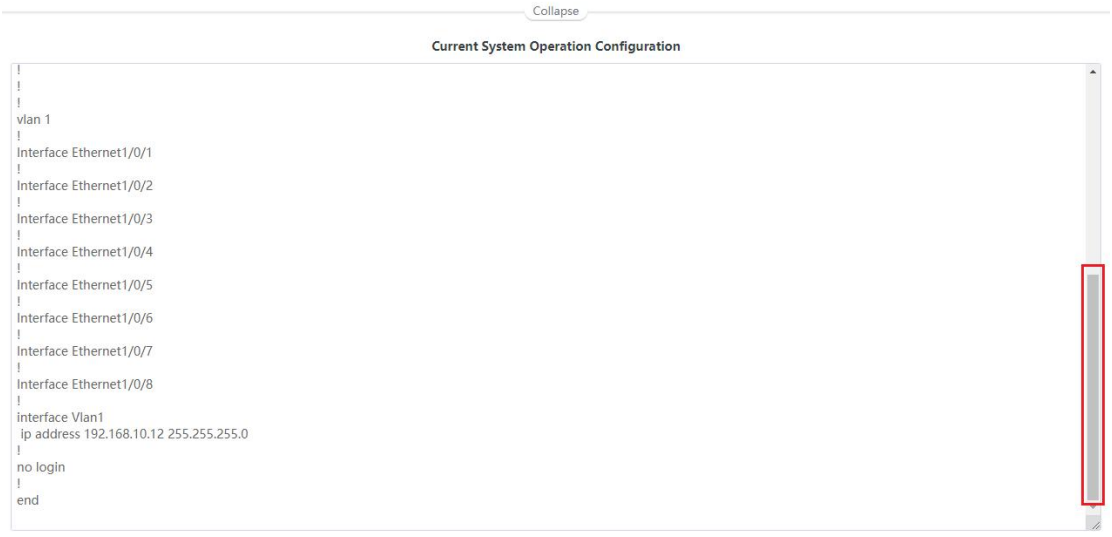

10.2 System Utilization

Here you can see the CPU usage, and the memory usage.

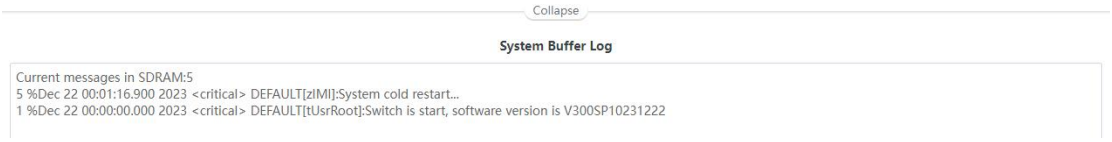



10.3 View System Config

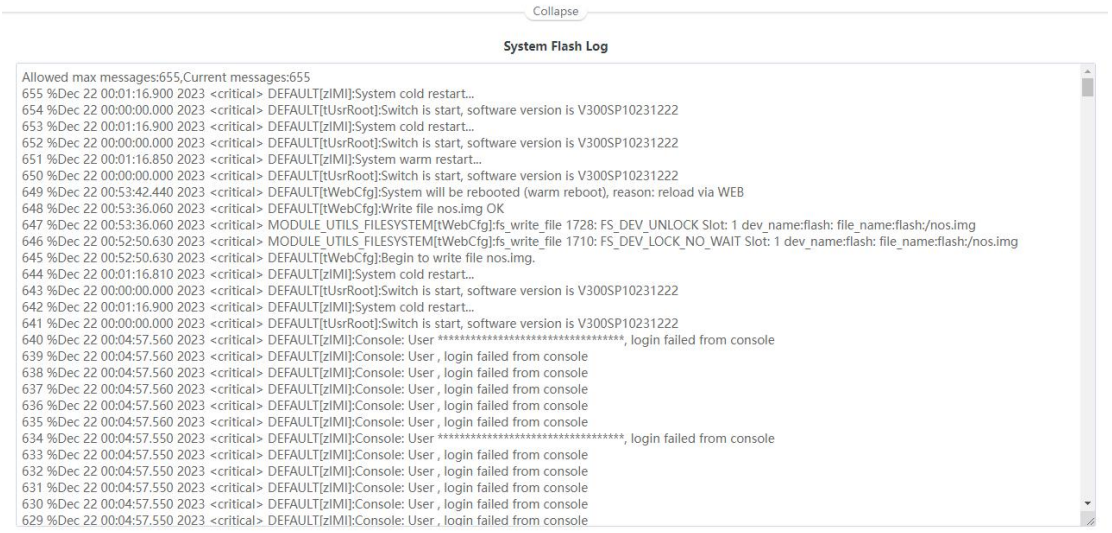
Here, you can view the relevant configuration of the system




10.4 View Logging Buffer




10.5 View Logging Flash

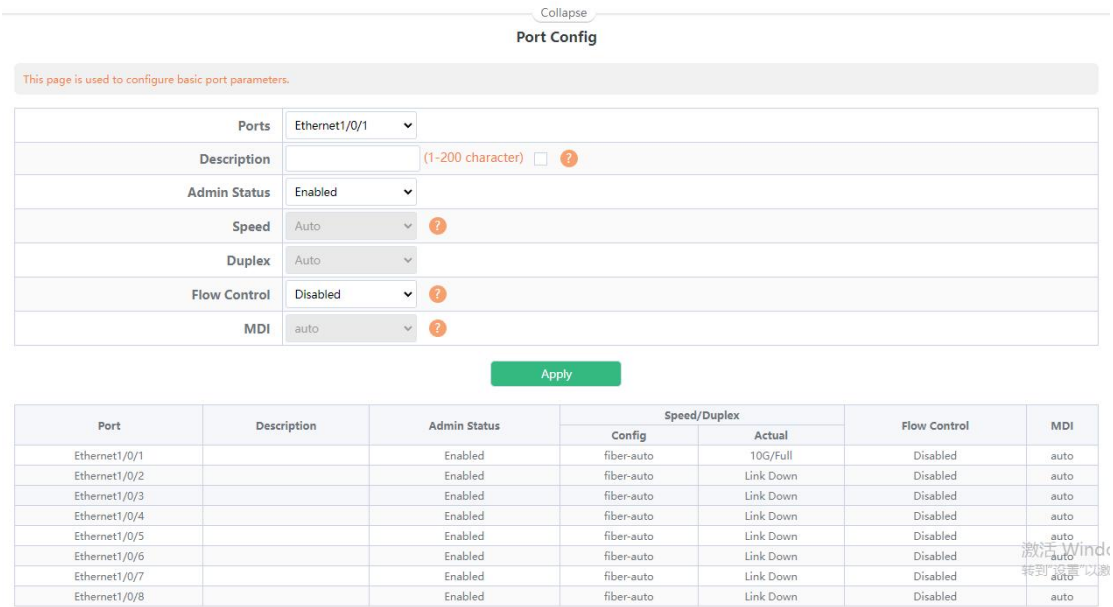



# III. Switch Config

1. Port Config

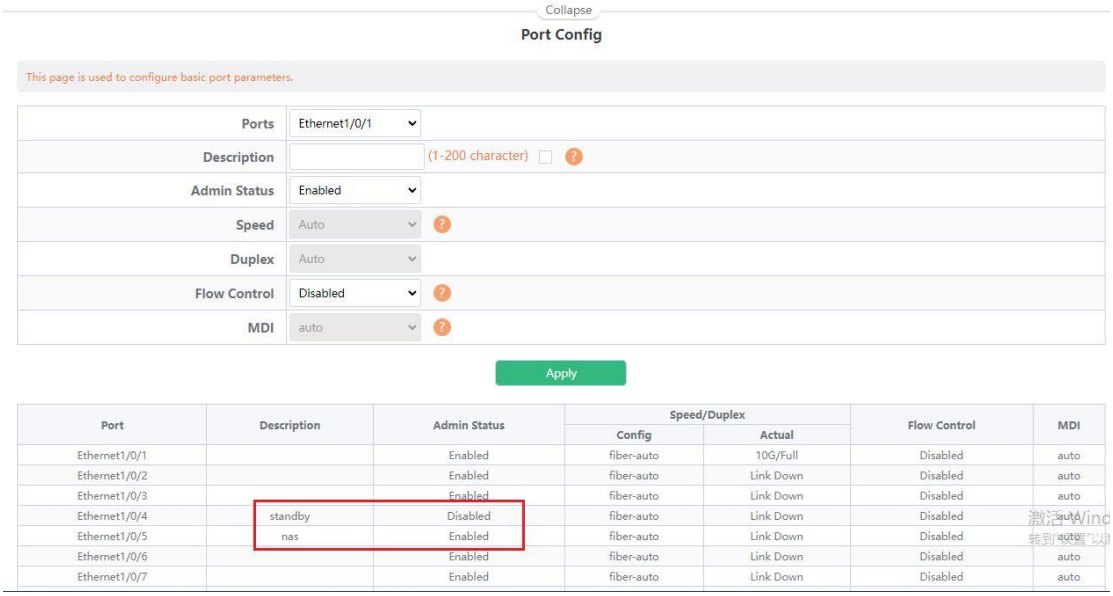
1.1 Port Config

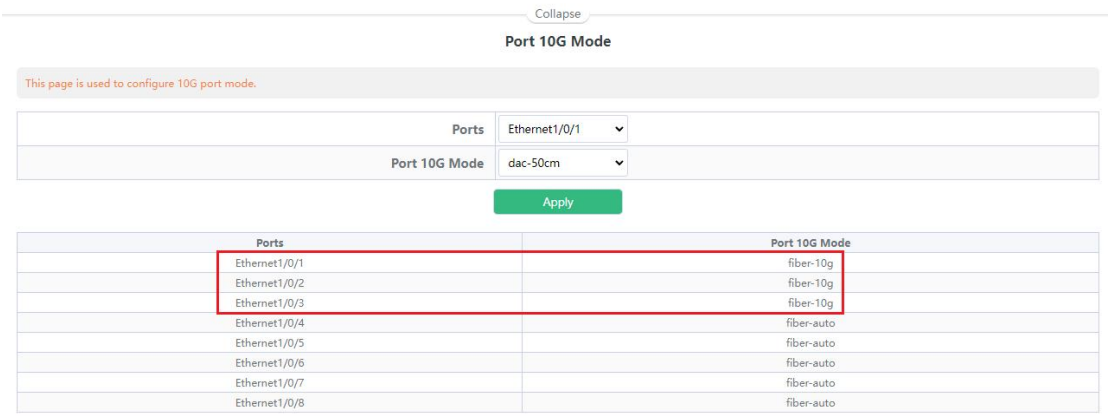
Here, you can configure the basic parameters of port alias, management status, flow control and so on, and then applied and saved. The yellow question mark is the illustration of the project.




For example, we set the Description of port 4 (Ethernet1 / 0 / 4) as standby, and the Admin Status is Disabled; the Description of port 5 (Ethernet1 / 0 / 5) is nas, and the management Admin

Status is Enabled.




## 1.2 Port 10G Mode

Here, a 10G mode (adaptive or forced rate) can be set. Generally, when the connection module is not communicating, the corresponding rate can be forced to the corresponding. For example, we force port 1-3, with a rate of 10G.