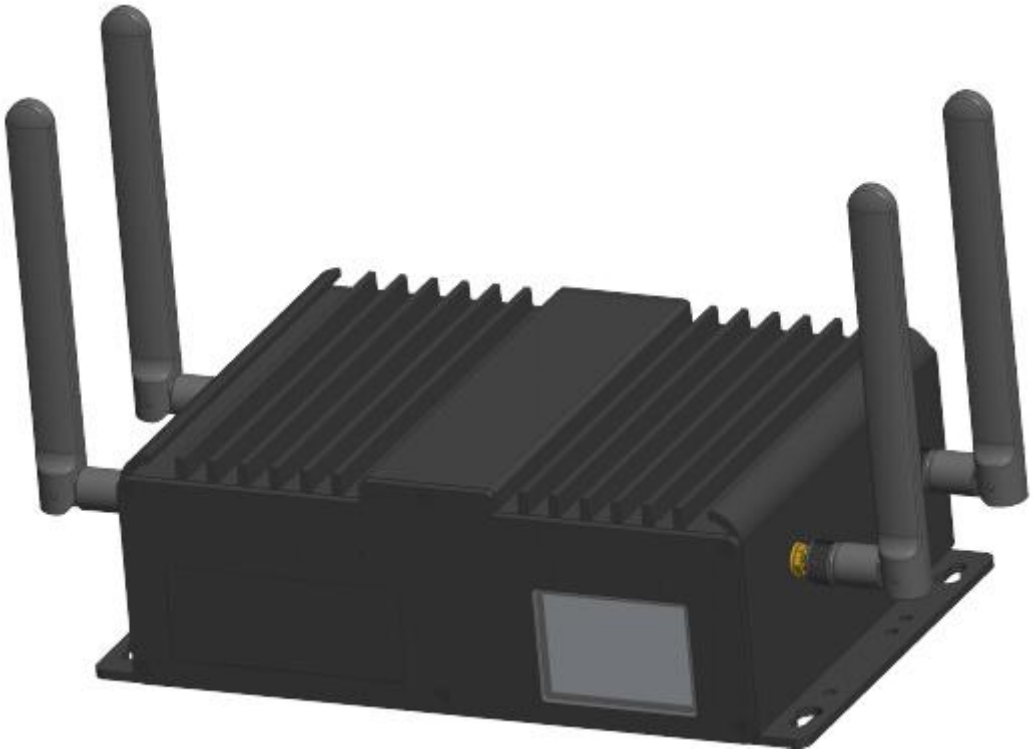


TC100 User's Manual

Rev-1.0

*The content of this User Manual has been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice.

Index

1. About this Manual

The content of this User Manual has been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice.

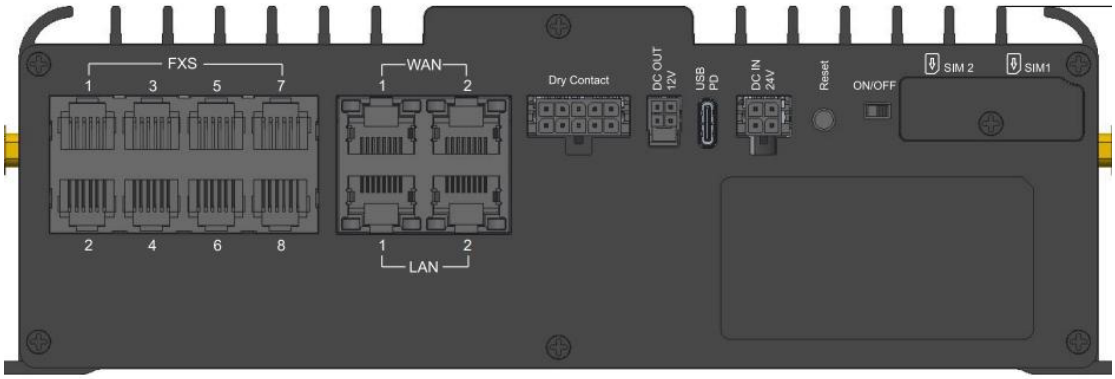
2. Product Overview

The LTE frequency band supported by this Router depends on the configuration of the ODU module and supports popular operating systems such as Windows, Linux, and Mac.

Connect the PC to router using the CAT-6 Ethernet cable. Use any one of the two Ethernet ports on the router. plug in the adapter in the AC socket and DC in the power port of router and waiting for about 40 seconds until the device finished initializing. You can also connect the PC to router by Wi-Fi, choose the correct Wi-Fi SSID and input the accurate password as the label shows. The default Wi-Fi SSID is ALR-LTE-XXXXXX, XXXXXX denotes the last six digits of the Router's MAC address. It is advised to read this manual at leisure to make best use of the router.

3. Introduction

3.1Ports and Buttons

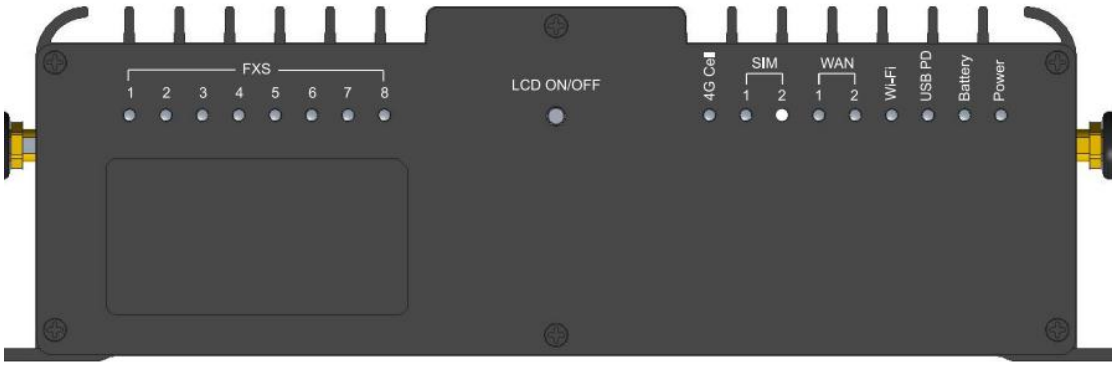


The following ports are located on the rear panel (refer above image from left to right)

Interfaces	One side：

	1. FXS Port：Max 8 ports (2/4/6/8 ports is optional) 2. WAN Port: *2 Gigabit port with Passive PoE 3. LAN Port:*2 Gigabit port 4. USB: Type-C 5. SIM: Nano/4FF SIM card*2 (Physical SIM Port) 6. Battery: Internal (Replaceable) 7. 4 Pin UPS Power Out, 12V 3A Power Output 8. DC Jack: for DC input 9. LEDs indicator (see below and LED Indicator Definition） 10. Reset button 11. SMA: *5 (2/3/5 optional, default *2 for LTE ANT) 12. ON/OFF key 13. Dry connector connector

3.2 LED Definition



LEDs are located on the front panel.

You might see difference with Led behavior as described below due to continue development to meet customer requirements.

LED	14. FXS 1(VoIP line 1) LED

	15. FXS 2(VoIP line 2) LED 16. FXS 3(VoIP line 3) LED 17. FXS 4(VoIP line 4) LED 18. FXS 5(VoIP line 5) LED 19. FXS 6(VoIP line 6) LED 20. FXS 7(VoIP line 7) LED 21. FXS 8(VoIP line 8) LED 22. 4G LTE Signal indicator: Tri-color LED 23. WAN 1 LED 24. WAN 2 LED 25. WiFi LED 26. SIM 1 LED 27. SIM 2 LED 28. Battery LED: Tri-color LED 29. Power LED 30. EXT Power LED

4. Introduction to the WebUI

The basic settings in WebGUI consist of four main parts named Dashboard, Status, Settings, SMS. You can login to WebGUI as follows, and configure the settings according to your requirements.

In the following sections, we will introduce you the main functions and the method of how to configure them.

4.1 Login

Open your Web browser and enter 192.168.7.1:8080 in the address bar; Login window will popup;

When prompted for User name and password, enter the following username and password.

Username/Password: admin/P9cocWo3

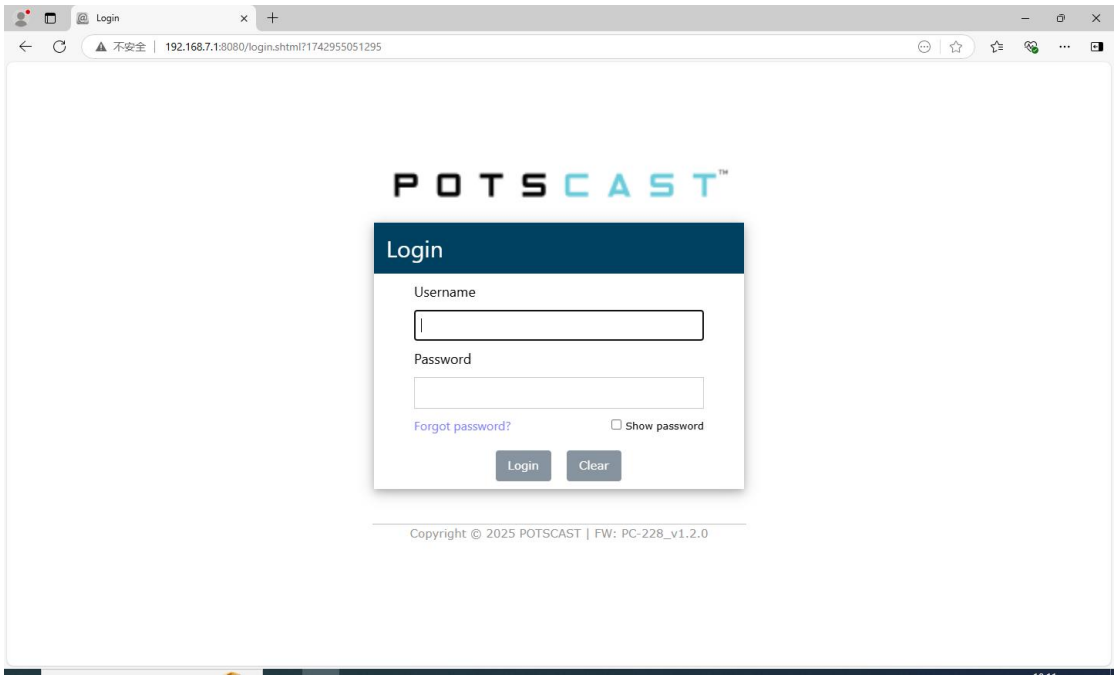


Figure 1 Login Page

4.2 Dashboard

After successful login, the following screen will appear and you will see four main menus on the top bar of the WebGUI.

The bars in the middle indicate the received signal level and USIM icon displays the status of USIM.

From this page, you can also know the Cellular network status and the LTE data transmission.

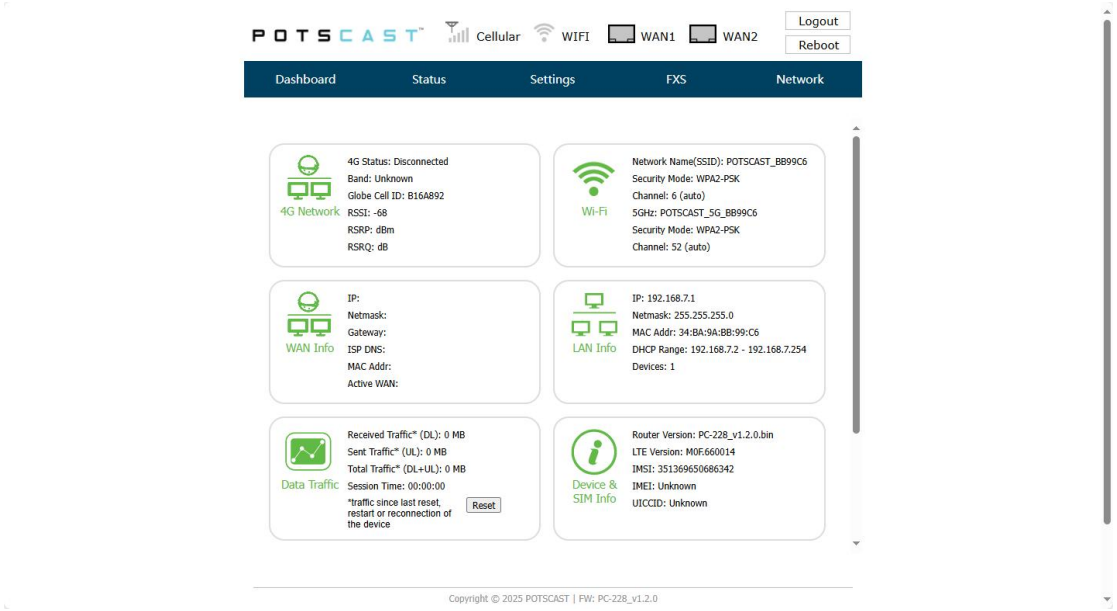


Figure 2 Dashboard

4.3 Status

On this page, you can see WAN Status, WiFi Status, Software, Device List and Statistics.

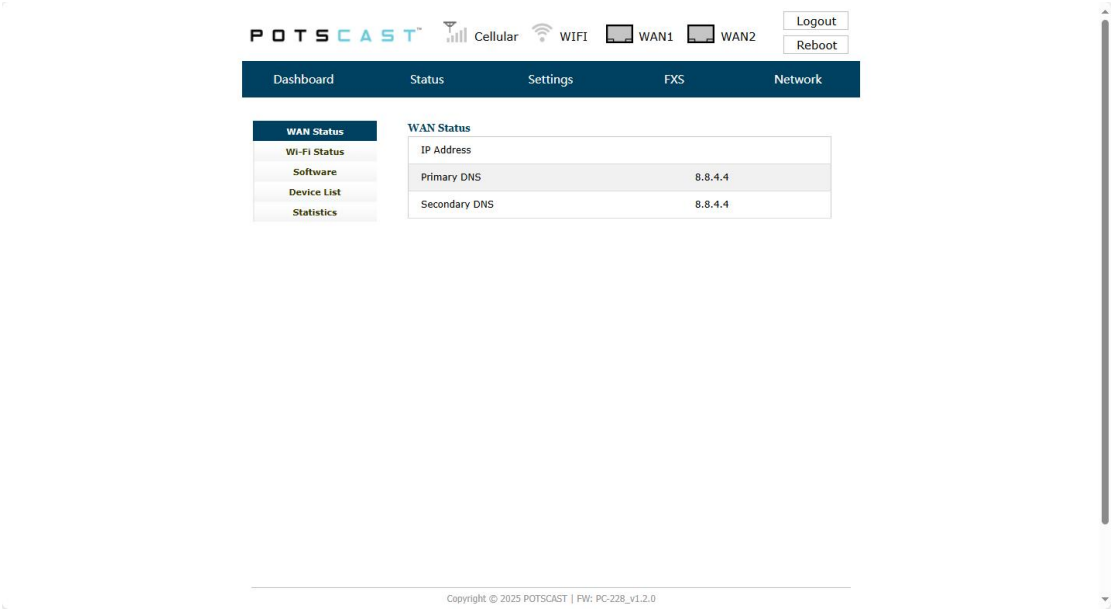


Figure 3 Status

4.3.1WAN Status

From the WAN Status, you can see IP Address, Primary DNS and Secondary DNS.

Figure 4 WAN Status

4.3.2WiFi Status

From this page, you can know the WiFi Status such as SSID, Channel, Security Mode, and so on.

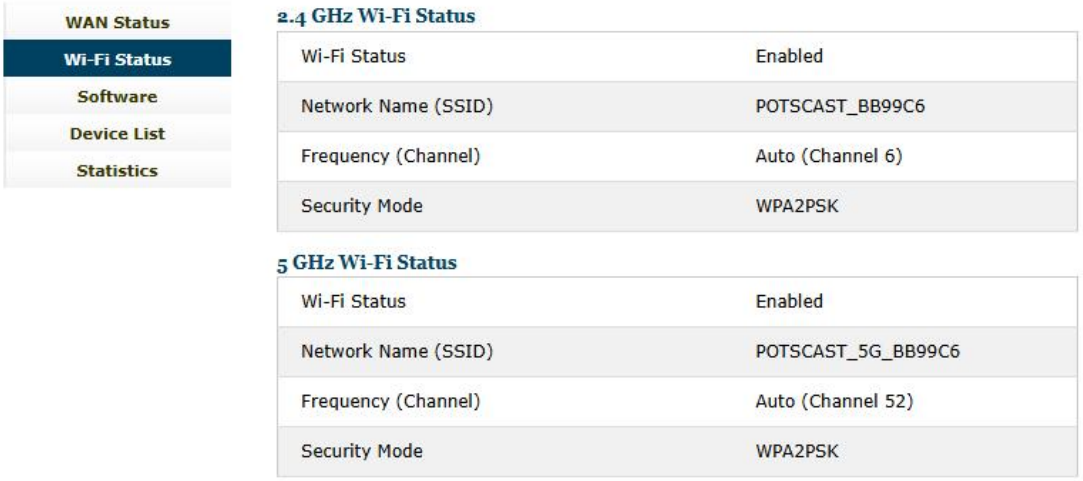


Figure 5 WiFi Status

4.3.3Software

From this page, you can know the software version and the Module version.

Figure 6 Software

4.3.4Device List

From the device list, you can know the users' information, include hostname, MAC address, IP address and expires time.

Figure 7 Device List

4.3.5Statistics

From the device list, you can know the users' speed and Current Session.

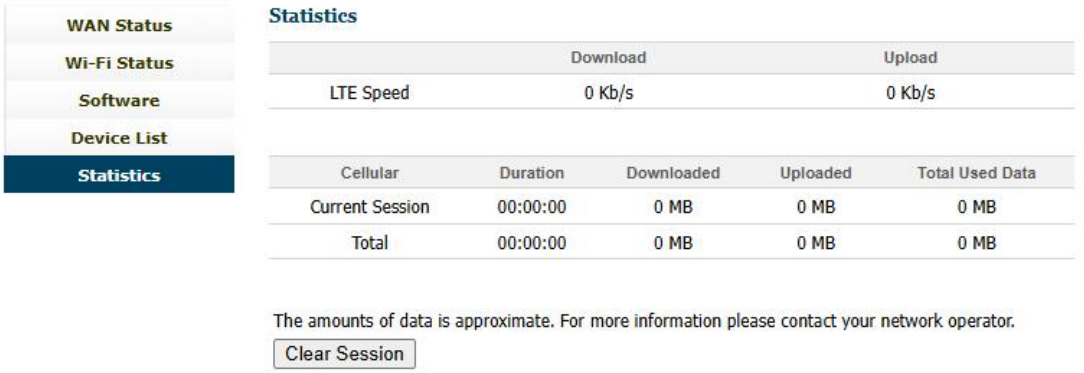


Figure 8 Statistics

4.4 Settings

The settings menu consists of two main menus named Basic Settings, Security Settings, Advanced Settings, Remote Management and Log Management.

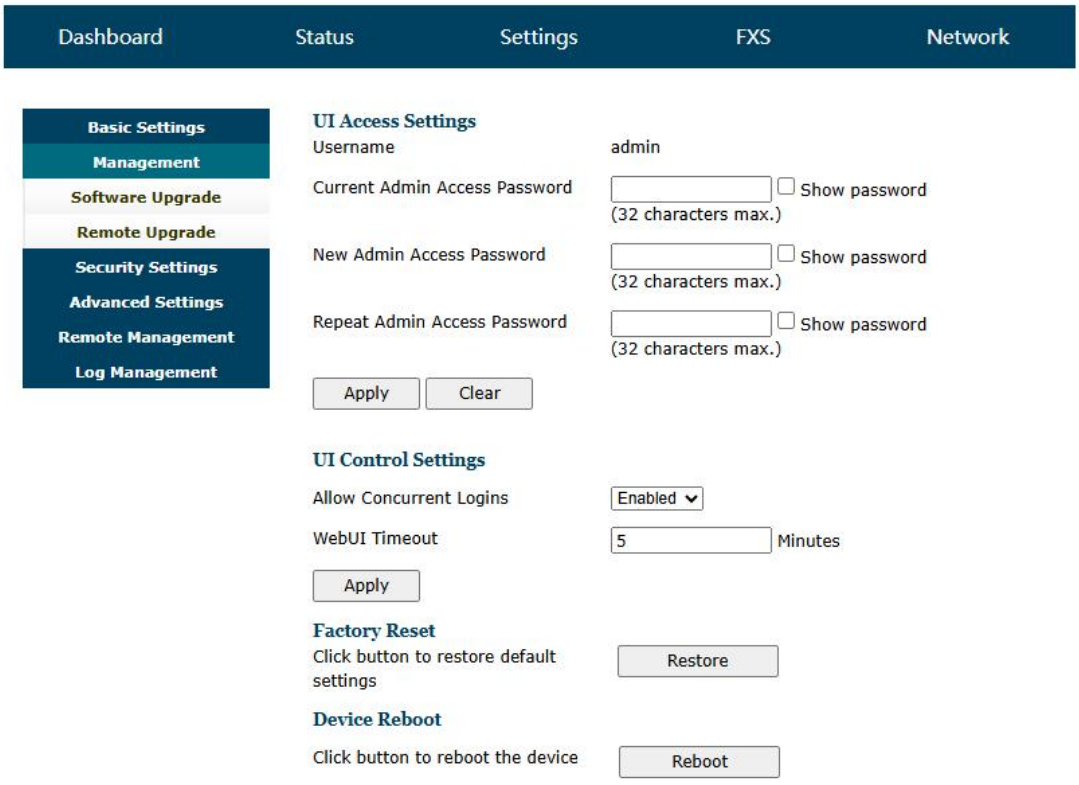


Figure 9 Settings

4.4.1Basic

From this page, you can see Management, Software Upgrade and Remote Upgrade.

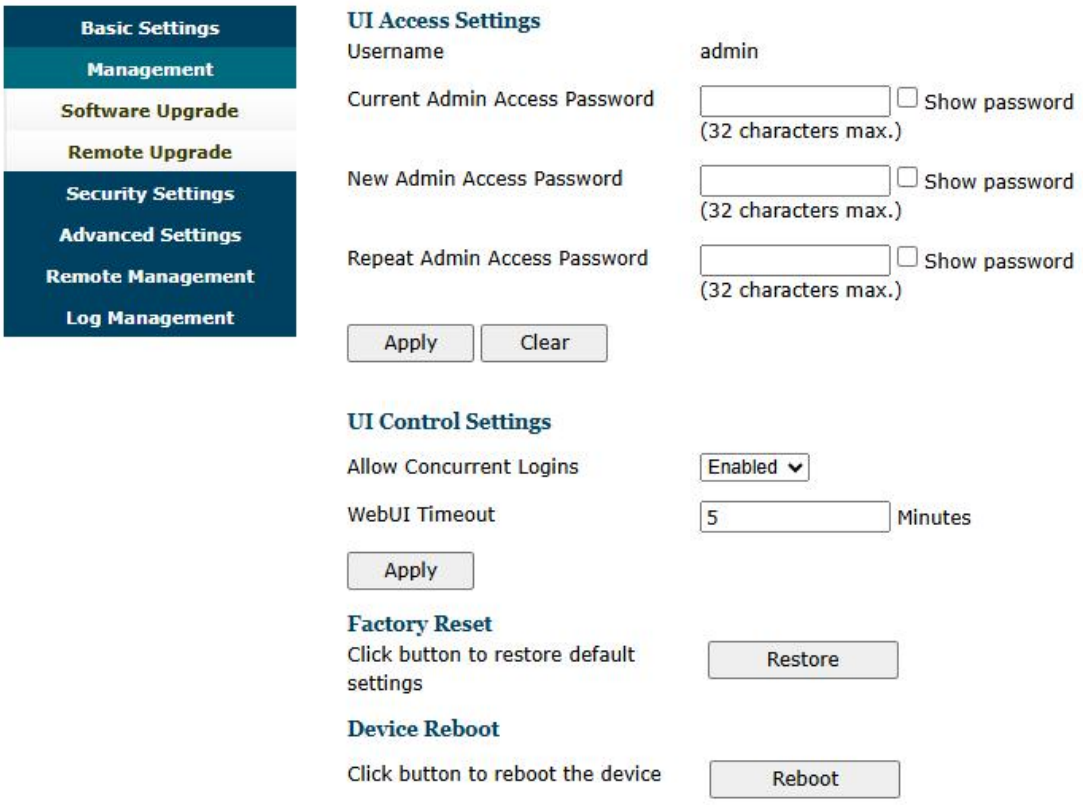


Figure 10 Basic Settings

4.4.1.1 Management

The default password is admin, you can enter 1~32 characters for 2 times as your new password. Then you would logout automatically and you should login to the system by the new password.

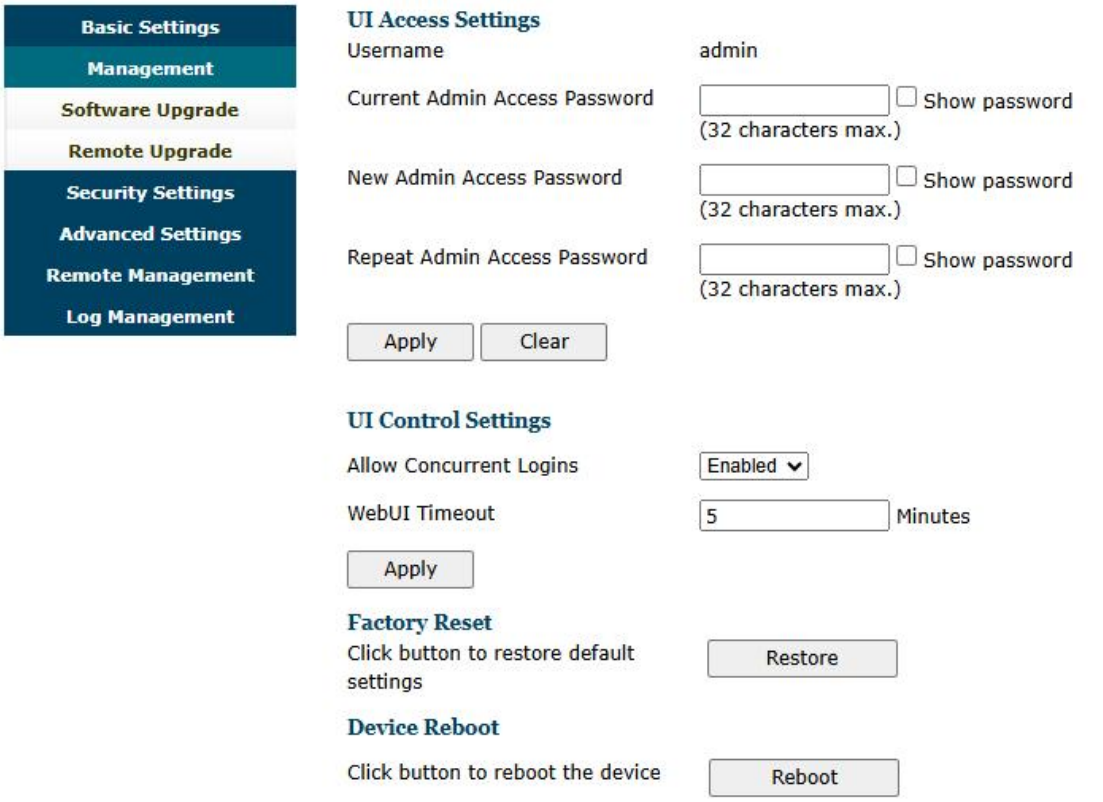


Figure 11 Management

- **Restore:** You can click the “Restore” button to load default to the factory setting.
- **Reboot:** You can click the “Reboot” button to restart the device.

4.4.1.2 Software Upgrade

On this page, you can upgrade the Device version and MCU Version from the local PC. About 100s is needed to complete the whole upgrade process, and then the device will reboot automatically.

Figure 12 Software Upgrade

Note:

- The firmware version must be suitable for the corresponding hardware;
- Please make sure the adequate and stable power supply while upgrading.

4.4.1.3 Remote Upgrade

After the device detects the new router version from Web server, the device will upgrade the new version automatically, or the device will upgrade the new version after you click the “Apple” button.

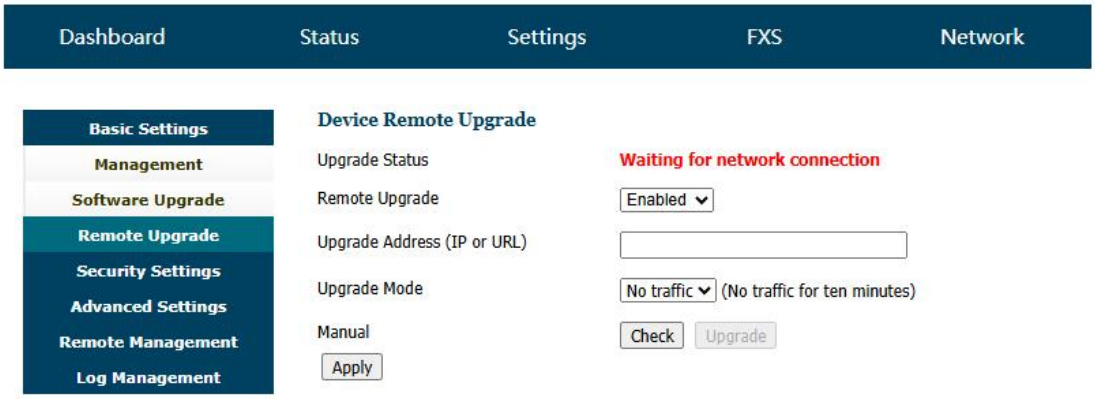


Figure 13 Remote Upgrade

4.4.2Security

4.4.2.1 MAC Filtering

This function is a powerful security feature that allows you to specify which wireless client users are not allowed to surf the Internet.

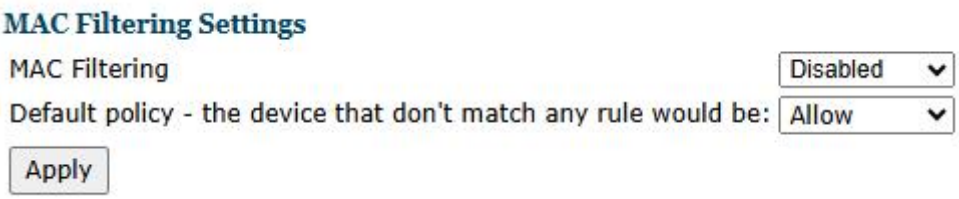


Figure 14 MAC Filtering page

The default MAC filtering setting is disabled, so you should enable it before you begin to configure the filter. Then click the “Add New” button, you can configure the rules you like

- **Default Policy**
  - The packets that don’t match with any rules would be “Allow/Deny”. If you choose the “Allow” button here, the MAC address that you add would be dropped. Otherwise, only the MAC addresses on the rule table can be accepted.
  - The new rules will be shown on the rule table, here you can delete the rules that you have selected and add new rules sequentially. The maximum rule count is

10.

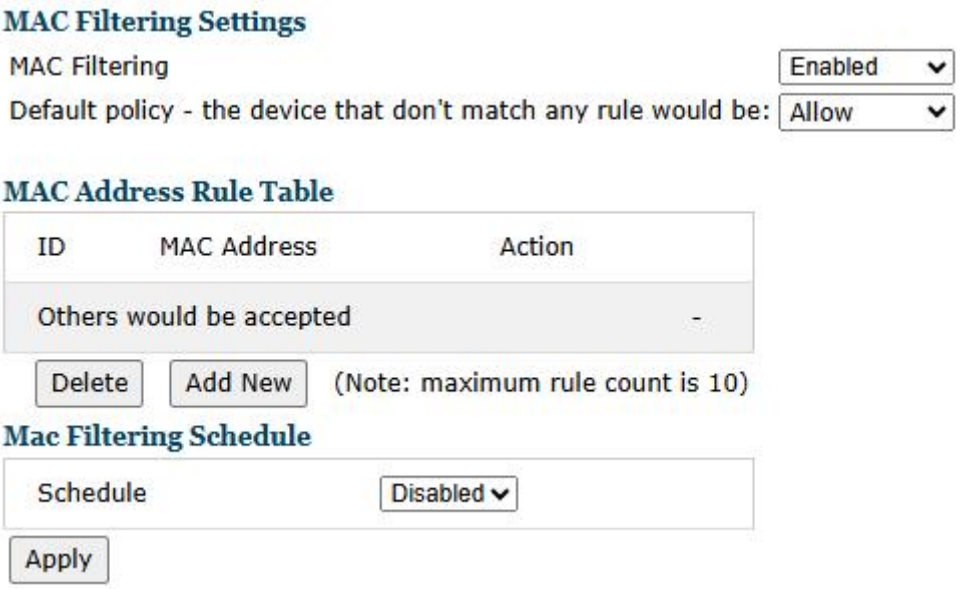


Figure 15 Enable MAC Filtering Function

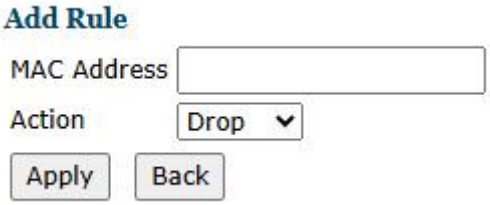


Figure 16 Add Rule

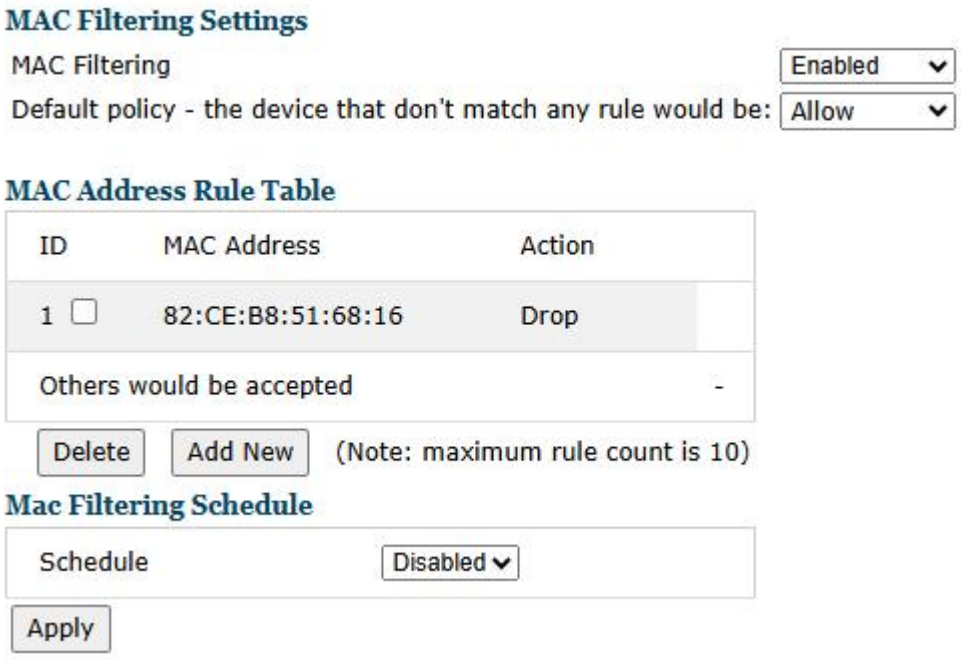


Figure 17 Rule Table

4.4.2.2 IP/Port Filtering

From this page, you can configure the IP/Port filter to forbid relevant users to login the router device.

The default IP/Port filter setting is disabled, so you should enable it before you begin to configure the filter. Then clicking the “Add New” button, you can configure the settings you like .

- **Default Policy:** The packets that don’t match with any rules would be “Dropped/Accepted”. If you choose “Dropped” here, the action of the new rule would be “Accept”. Otherwise, the action turns to be “Drop” and the packet that don’t match with any rules would be accepted.

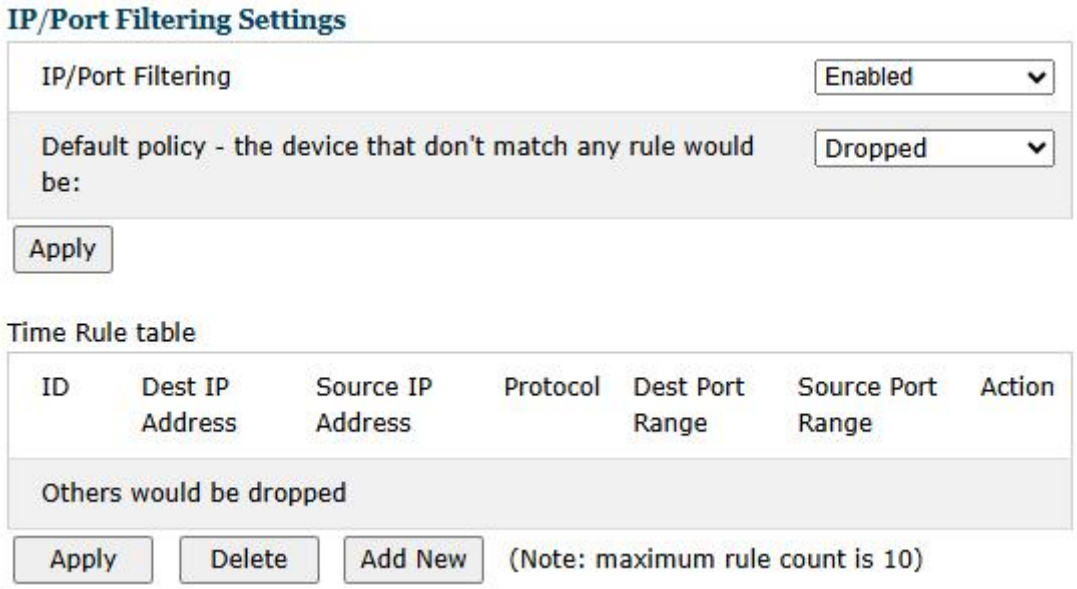


Figure 18 IP/Port filtering page

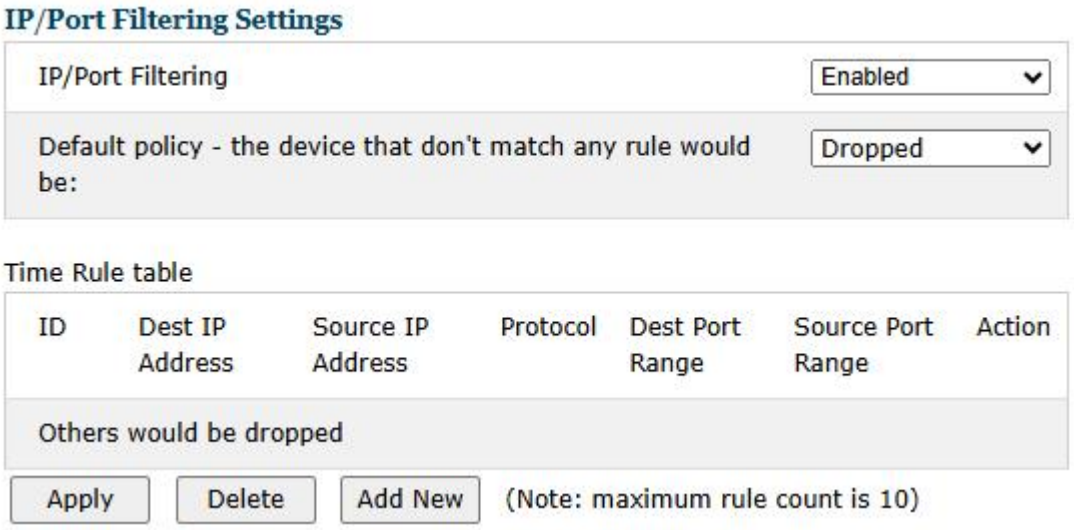


Figure 19 Enable IP/Port Filtering function

- **Dest IP Address:** The IP address of a website that you want to filter (Such as google 74.125.128.106).
- **Source IP Address:** The IP address of PC. (Such as 192.168.1.2).
- **Protocol:** TCP, UDP, ICMP.
- **Dest Port Range:** To restrict Internet access to the single user, you can set a fixed value, such as 21-21.
- **Source Port Range:** 1~65535
- **Action:** Accept, Drop

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 10.

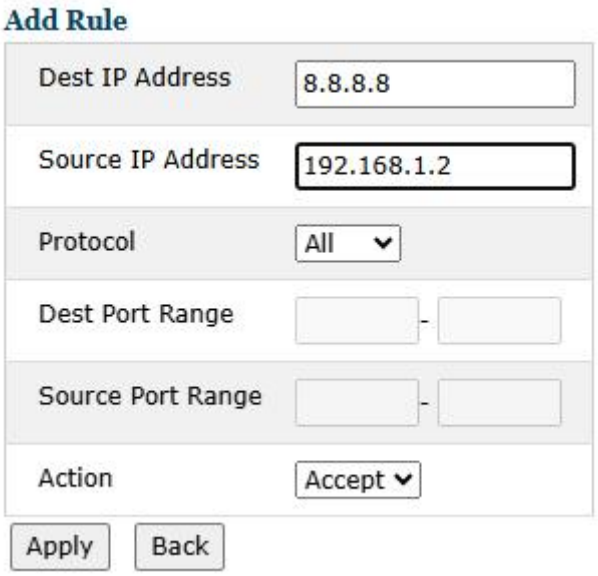


Figure 20 Add New Rule

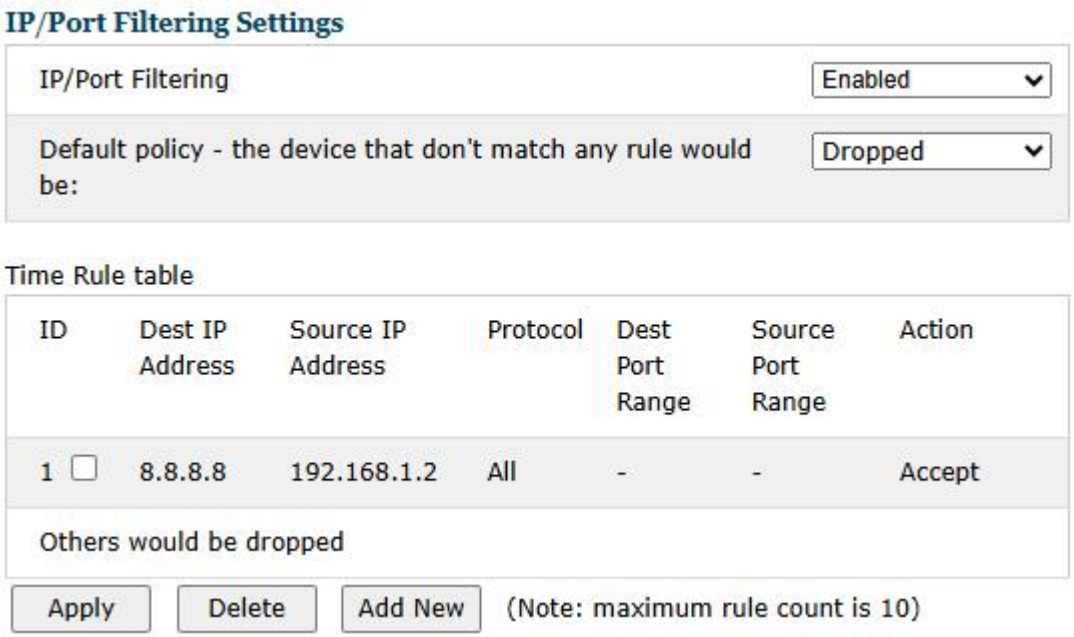


Figure 21 Rule Table

4.4.2.3 Content Filtering

It is a function that forbids users to login the URL or keyword on the rule table. You can configure the settings you like by clicking the "Add New" button.

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 8.

Figure 22 Content Filtering

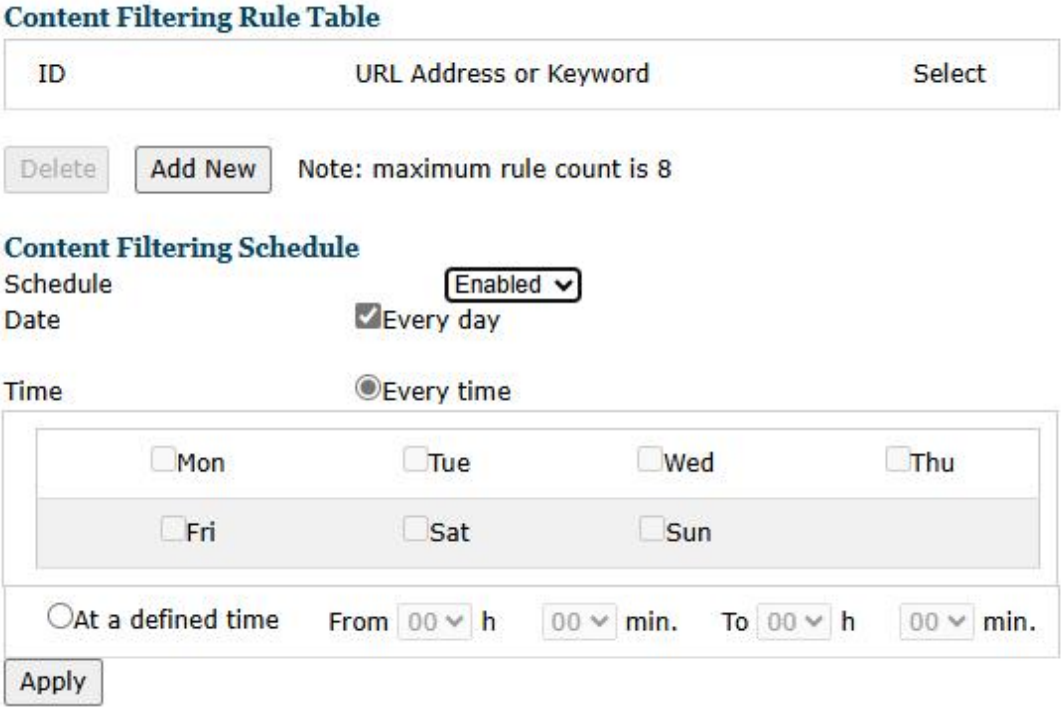


Figure 23 Configure Filtering Schedule

- Content Filtering Schedule

Here you can configure the schedule to define when the rules take effect. This feature is disabled in default, you should enable it first and then configure the date and time, such as working time. Click the “Apply” button, you can see the new rule on the content filtering page.

4.4.2.4 Port Forwarding

Clicking on the header of the “Port Forwarding” button will take you to the “Port Forwarding” header page. Clicking on the “Add New” button, you can configure IP address, port range to achieve the port forwarding purpose.

Figure 24 Port Forwarding page

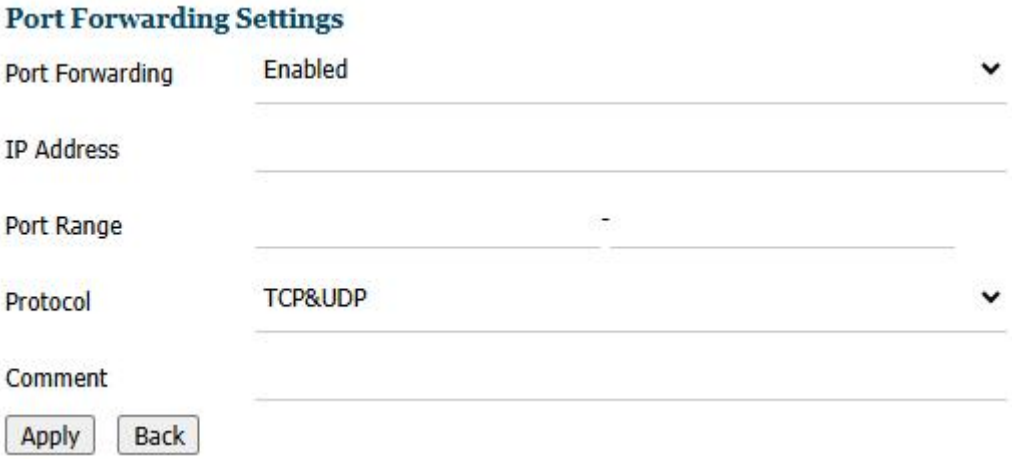


Figure 25 Port Forwarding Setting

- **IP Address:** The IP address of the PC running the service application;
- **Port Range:** You can enter a range of service port or set a fixed value;
- **Protocol:** UDP, TCP, TCP&UDP.

The new rules will be shown on the rule table, you can delete the items that you have selected or add new rules by clicking the “Add New” button here. The maximum rule count is 20.

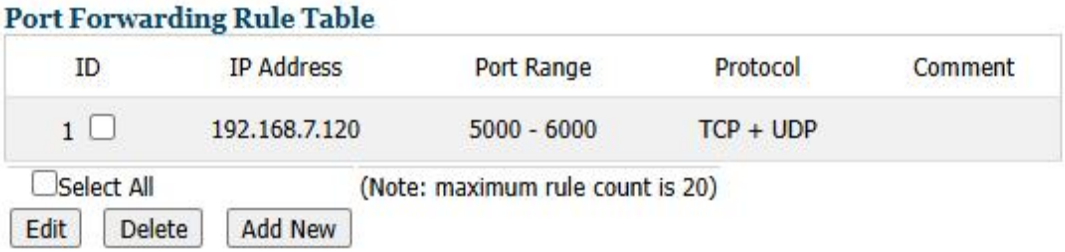


Figure 26 Rule Table

4.4.2.5 Virtual Server

Clicking on the header of the “Virtual Server” button will take you to the “Virtual Server” header page (Figure 41). It is a feature that similar to port forwarding, clicking on the “Add New” button, you can configure IP address, public port, private port and protocol to achieve the virtual server function.

Figure 27 Virtual Server page

Figure 28 Virtual Server Setting

- **IP Address:** The IP address of the PC running the service application;
- **Public Port:** The port of server-side;
- **Private Port:** The port of client-side, it can be same with the public port;
- **Protocol:** UDP, TCP, TCP&UDP.

The new rules will be shown on the rule table, you can delete the items that you have selected or add new rules by clicking the “Add New” button here. The maximum rule count is 20.

Figure 29 Rule Table

4.4.2.6 DMZ

From this page, you can configure a De-militarized Zone (DMZ) to separate internal

network and Internet.

- **DMZ IP Address:** The IP address of your PC. (such as 192.168.7.178).

Figure 30 DMZ page

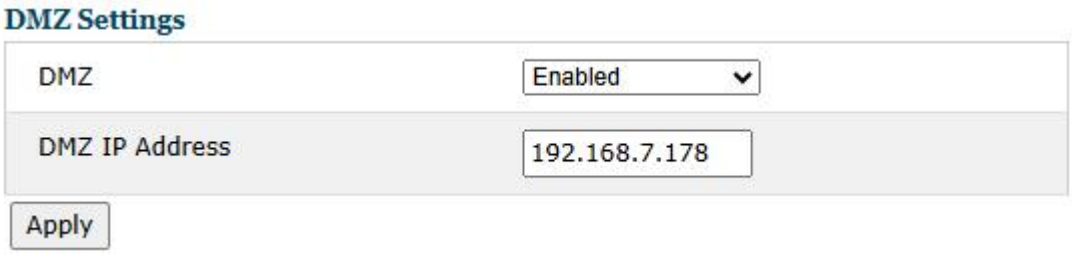


Figure 31 DMZ Setting

4.4.2.7 UPnP

The UPnP function is disabled in default, you should enable it on the system security page before using it. The new rules that you added will be shown on this page.

Figure 32 UPnP page

4.4.2.8 Dynamic DNS

Your CPE automatically selects a Domain Name Server (DNS) or you can manually set one.

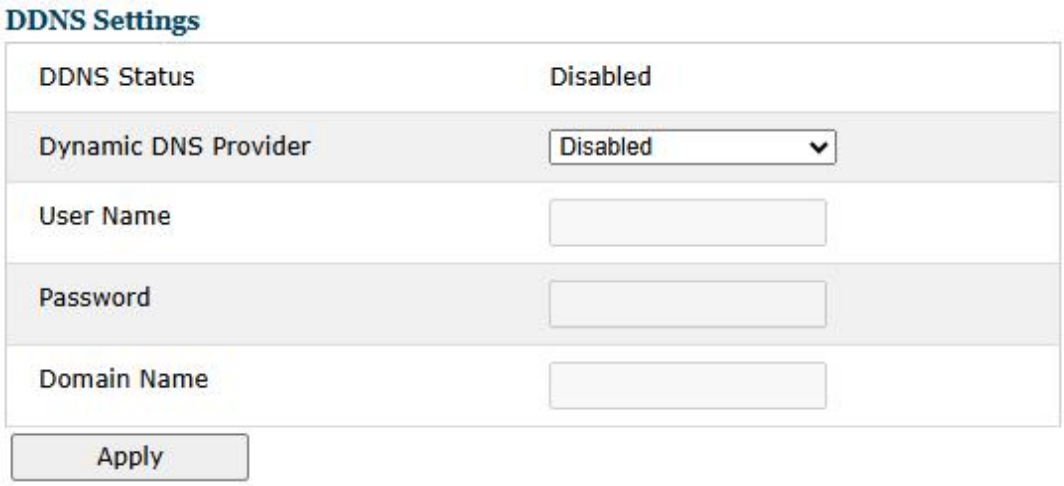


Figure 33 DNS page

4.4.2.9 VPN Passthrough

A virtual private network (VPN) is a point-to-point connection across a private or public network (Internet).

VPN Passthrough allows the VPN traffic to pass through the router. Thereby we can establish VPN connections to remote network. For example, VPNs allow you to securely access your company's intranet at home. There are three main kinds of the VPN tunneling protocol, PPTP, L2TP and IPSec.

Figure 34 VPN Passthrough

Note:

- VPN Passthrough does not mean the router can create a VPN endpoint. VPN Passthrough is a feature that allows VPN traffic created by other endpoints to "pass through" the router.

4.4.2.10 Network Management

Clicking on the header of the “System Settings” tab will take you to the “System Security Settings” page. From this page, you can configure the system security settings to protect the device itself from the external attacking.

Figure 35 Network Management

4.4.2.11 Parental Control

The rules added to the list are to configure when the Mac ADDRESS will be ALLOWED to access the Internet.

The Mac ADDRESS will automatically to denied access in any period outside the defined rules

Figure 36 Parent Control

4.4.3Advanced

From this page, you can see Routing, NTP, Backup & Restore, Diagnostic, L2TP VPN, GRE VPN, Dynamic Routing, SNMP and POE Output Voltage.

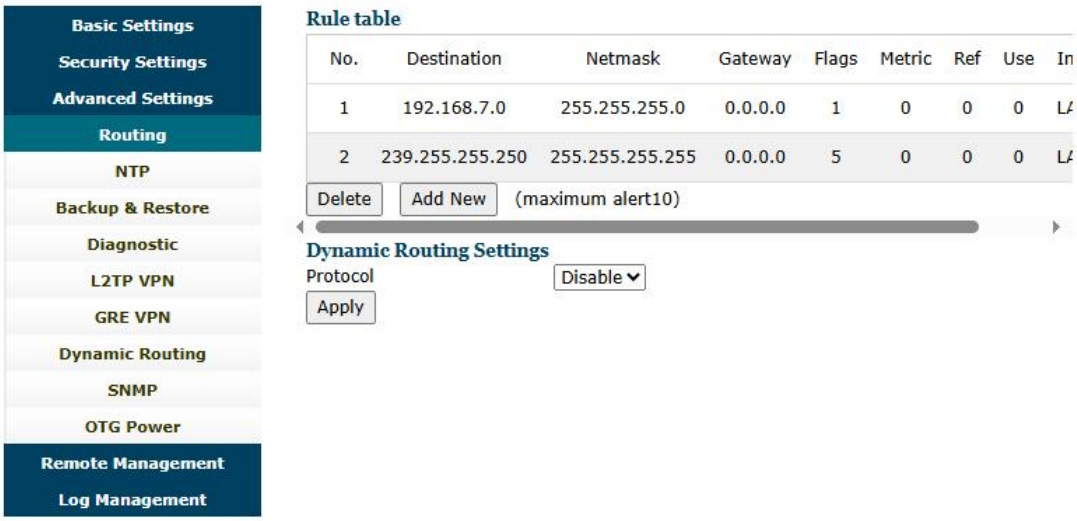


Figure 37 Advanced Settings

4.4.3.1 Routing

From the rule table, you can see the default route information. Clicking on the "Add New" button, you can configure the static routing setting. The new rules will be shown on the rule table, here you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 10.

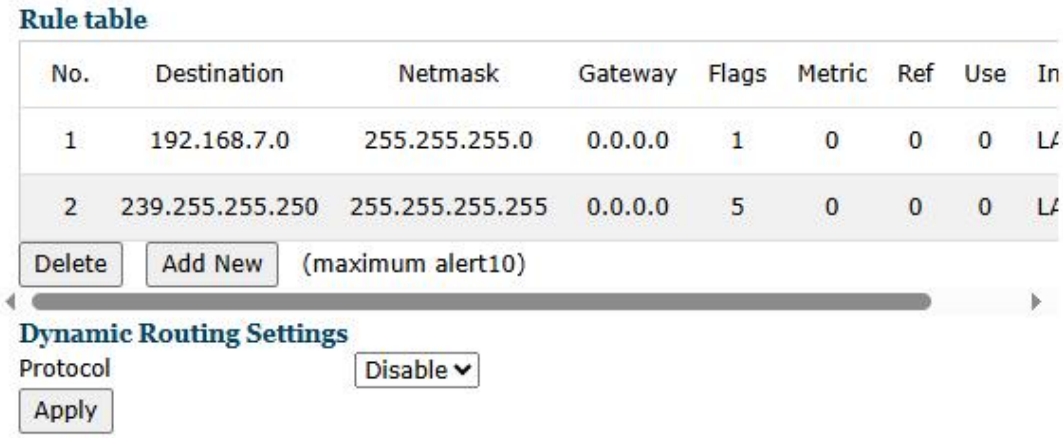


Figure 38 Routing

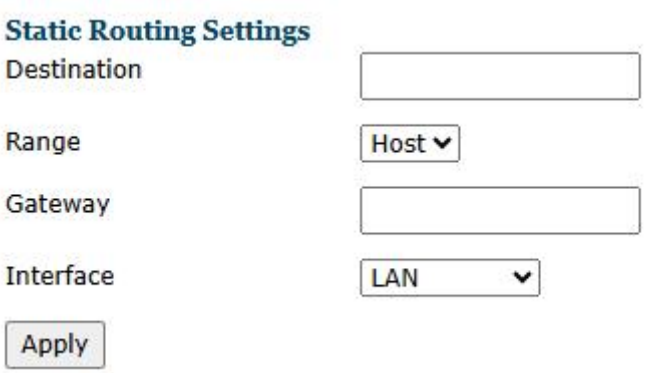


Figure 39 Configure the static routing settings

- **Destination:** The address of the network or host that assigned by the static route;
- **Range:** Host/Net;
- **Gateway:** This is the IP address of the gateway device that is used to contact between the router and the network or host;
- **Interface:** LAN/WAN;

4.4.3.2 NTP

From this page, you can set the Current Time, Time Zone, NTP Server and NTP synchronization. When the device obtains the WAN IP, the current time will synchronize with the NTP server automatically.

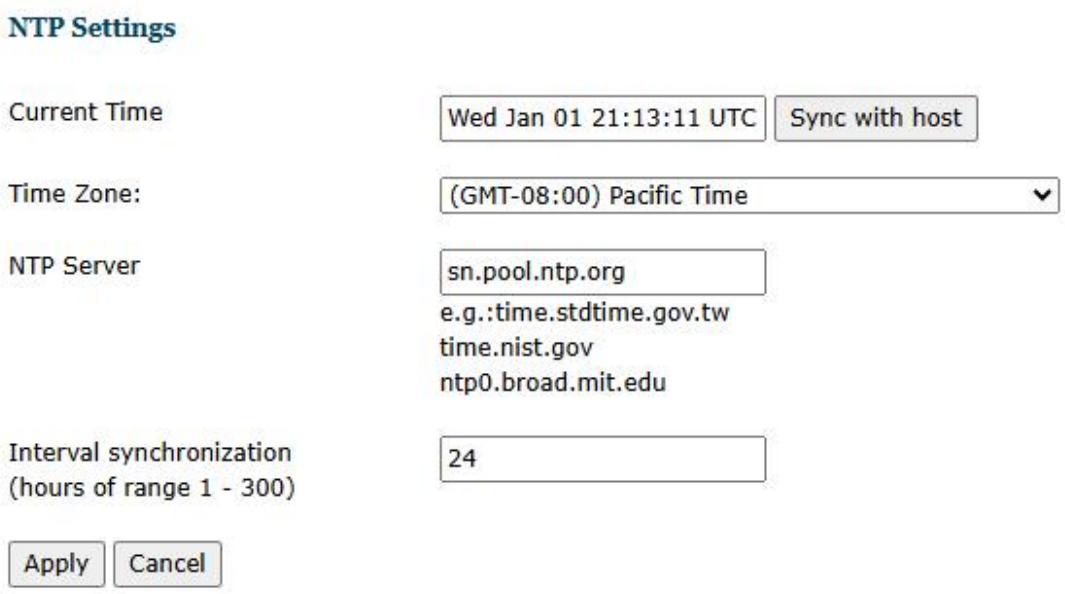


Figure 40 NTP

4.4.3.3 Backup & Restore

Clicking the “Backup &Restore” button, the current settings will be saved as a data file to the local PC. You can restore the device configuration from the files that you saved.

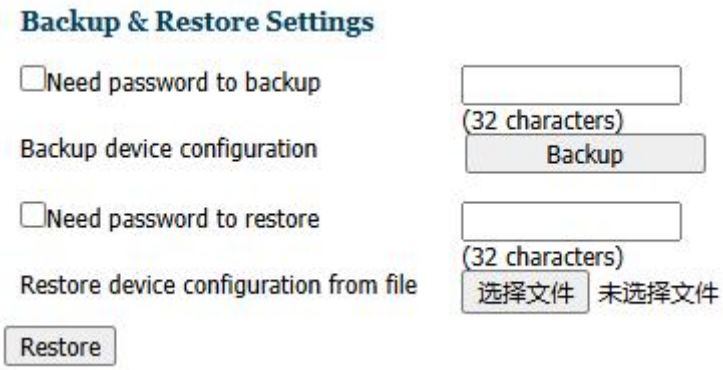


Figure 41 Backup & Restore

4.4.3.4 Diagnostic

There are 2 function on this page. Ping and Traceroute

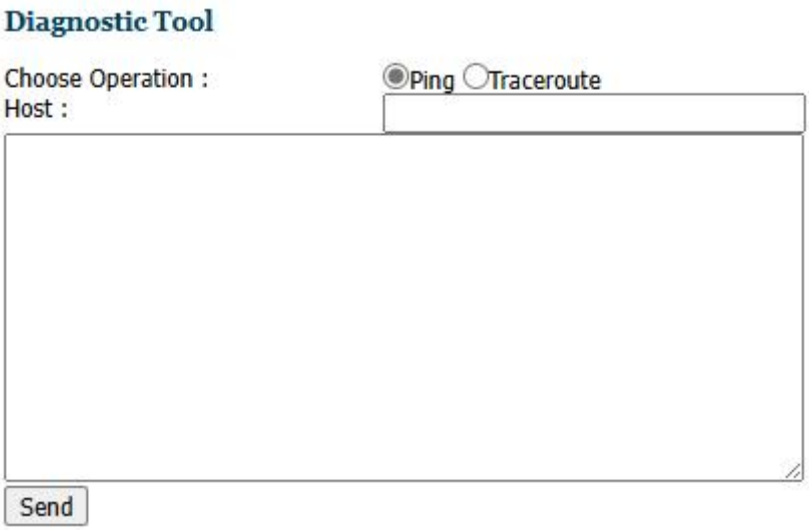


Figure 42 Diagnostic

4.4.3.5 L2TP VPN

From this page, you can Enable and Disable L2TP VPN.

Figure 43 L2TP VPN

4.4.3.6 GRE VPN

From this page, you can Enable and Disable GRE VPN.

Figure 44 GRE VPN

4.4.3.7 Dynamic Routing

From this page, you can Enable and Disable Dynamic Routing.

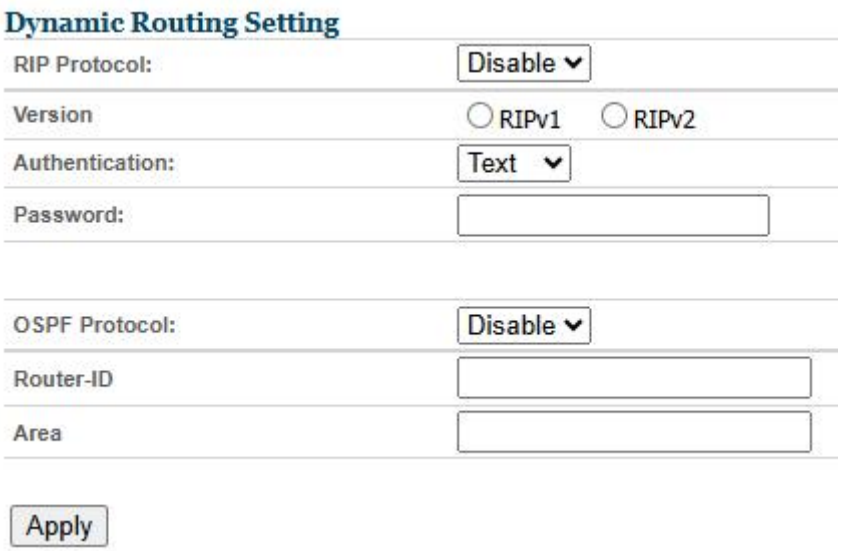


Figure 45 Dynamic Routing

4.4.3.8 SNMP

From this page, you can Enable and Disable SNMP.

Figure 46 SNMP

4.4.3.9 Output Voltage

From this page, you can set the poe output voltage as Power-in or Power-out.

Figure 47 WAN Mode Select

4.4.4Remote Management

From this page, you can see Reboot by SMS and Scheduled Reboot.

Figure 48 Remote Management

4.4.4.1 Scheduled Reboot

From this page, you can Enable/Disable Scheduled Reboot, Set the status to enabled, you can configure reboot data and time that the device reboots.

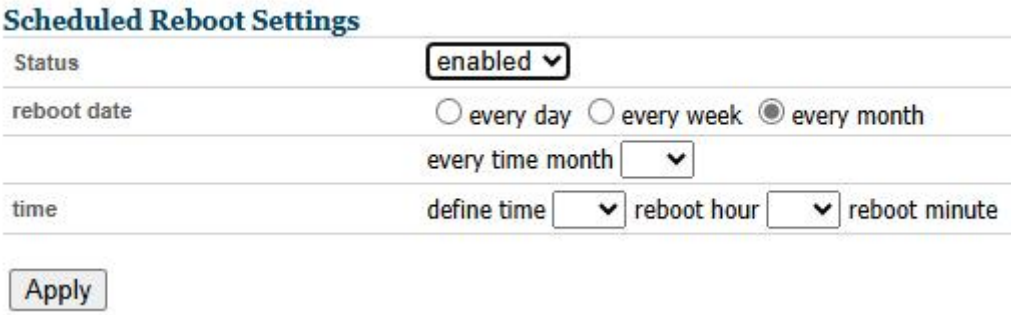


Figure 49 Enable Scheduled Reboot Setting

4.4.4.2 Reboot by SMS

From this page, you can Enable/Disable SMS reboot, Set the status to enabled, you can input keyword then click “apply” .

Figure 50 Reboot by SMS

4.4.5Log Management

From this page, you can see Syslog Settings, Call Log and System Log.

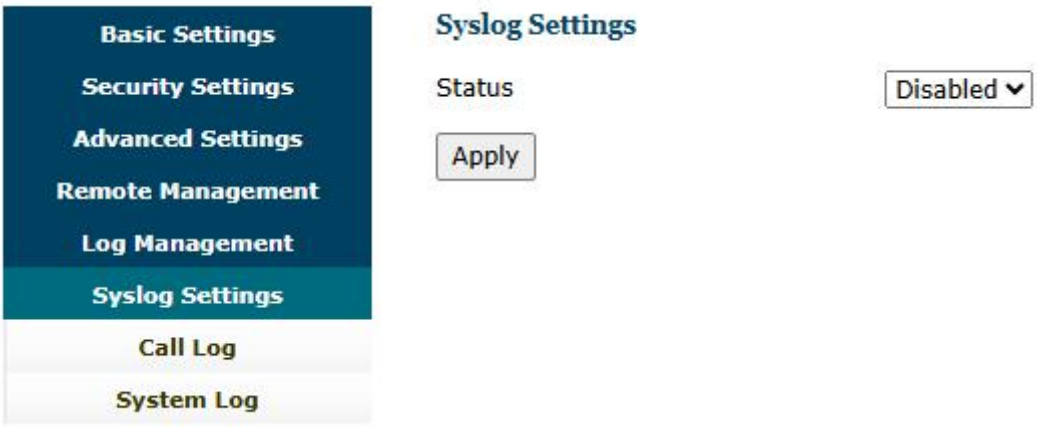


Figure 51 Log Management

4.4.5.1 Syslog Settings

From this page, you can Enable/Disable Syslog Settings.

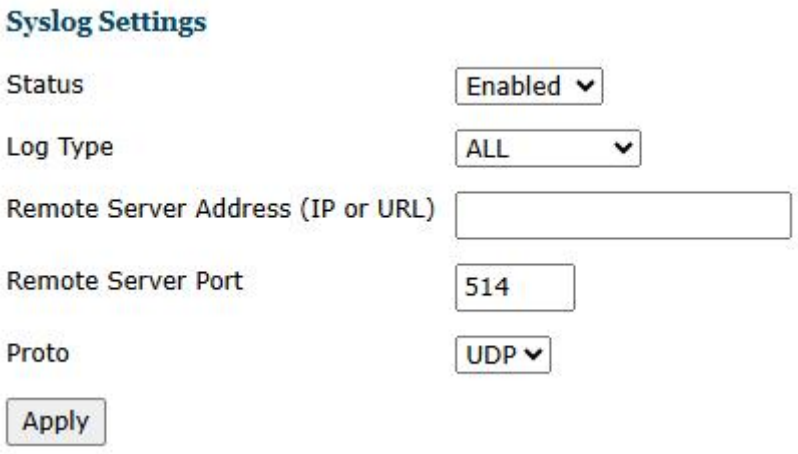


Figure 52 Syslog Settings

4.4.5.2 Call Log

From this page, you can Enable/Disable Call Log.

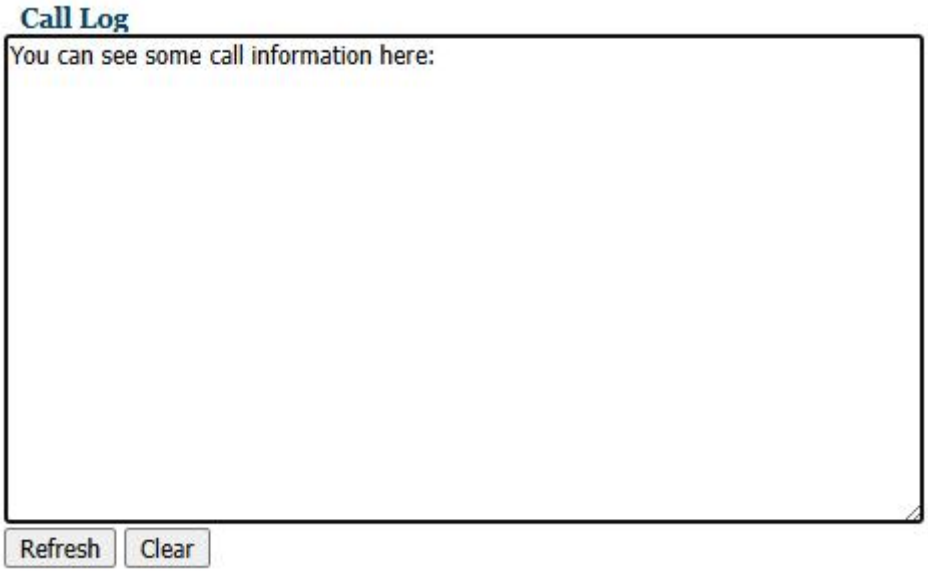


Figure 53 Call Log

4.4.5.3 System Log

From this page, you can Enable/Disable System Log.

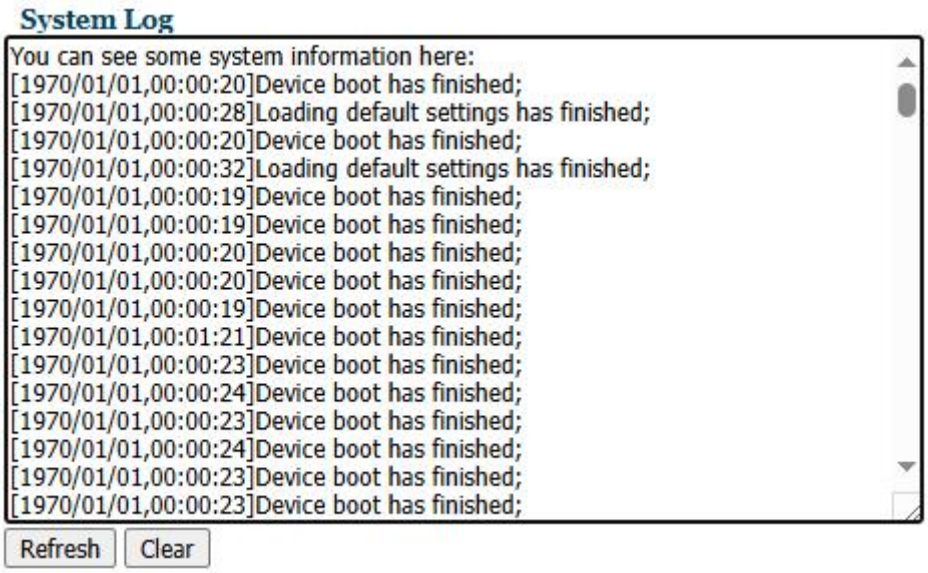


Figure 54 System Log

4.5 FXS

The settings menu consists of two main menus named VoIP Settings and VoIP Phone Settings.

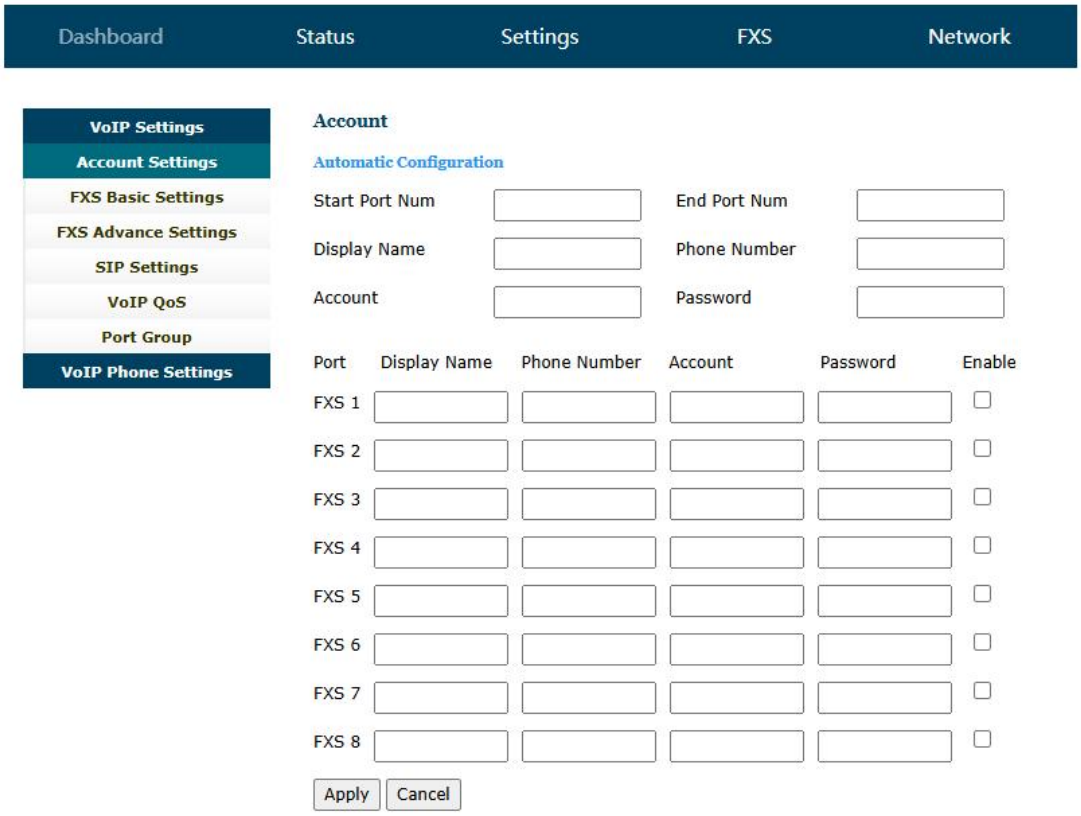


Figure 55 SMS

4.5.1Voip Settings

From this page, you can see Account Settings, FXS Basic Settings, FXS Advance Settings, SIP Settings, VoIP QoS and Port Group.

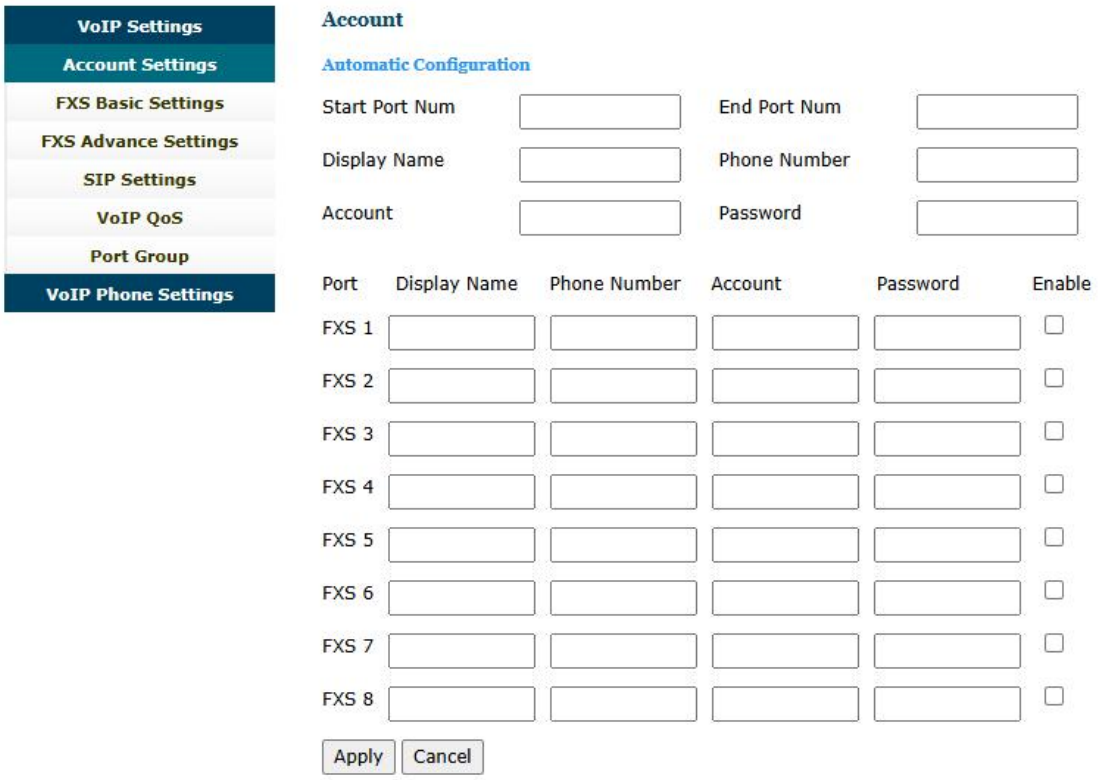


Figure 56 VoIP Settings

4.5.1.1 Account Settings

On this page, you can enter FXS to enable the phone to make outside calls.

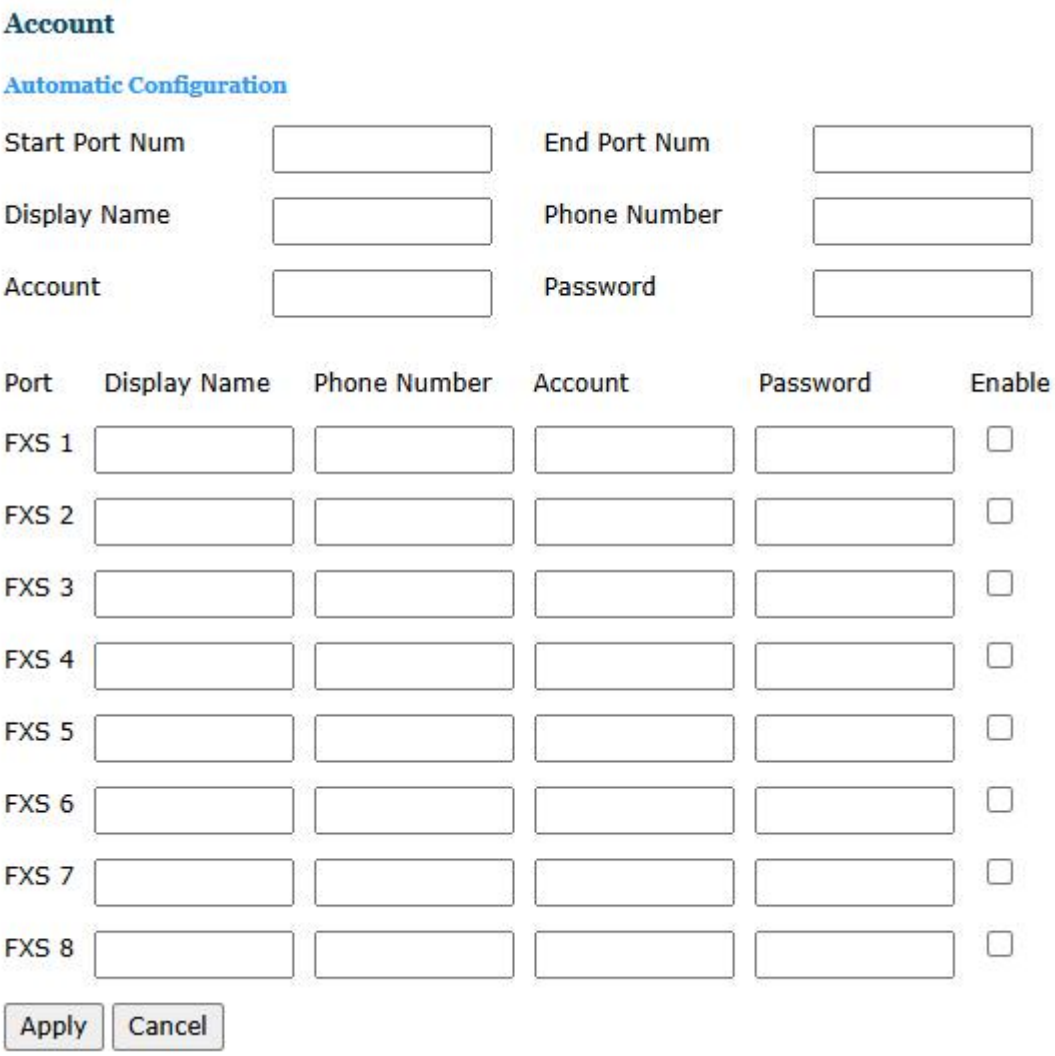


Figure 57 Account Settings

4.5.1.2 FXS Basic Settings

On this page, you can set the basic information of FXS.

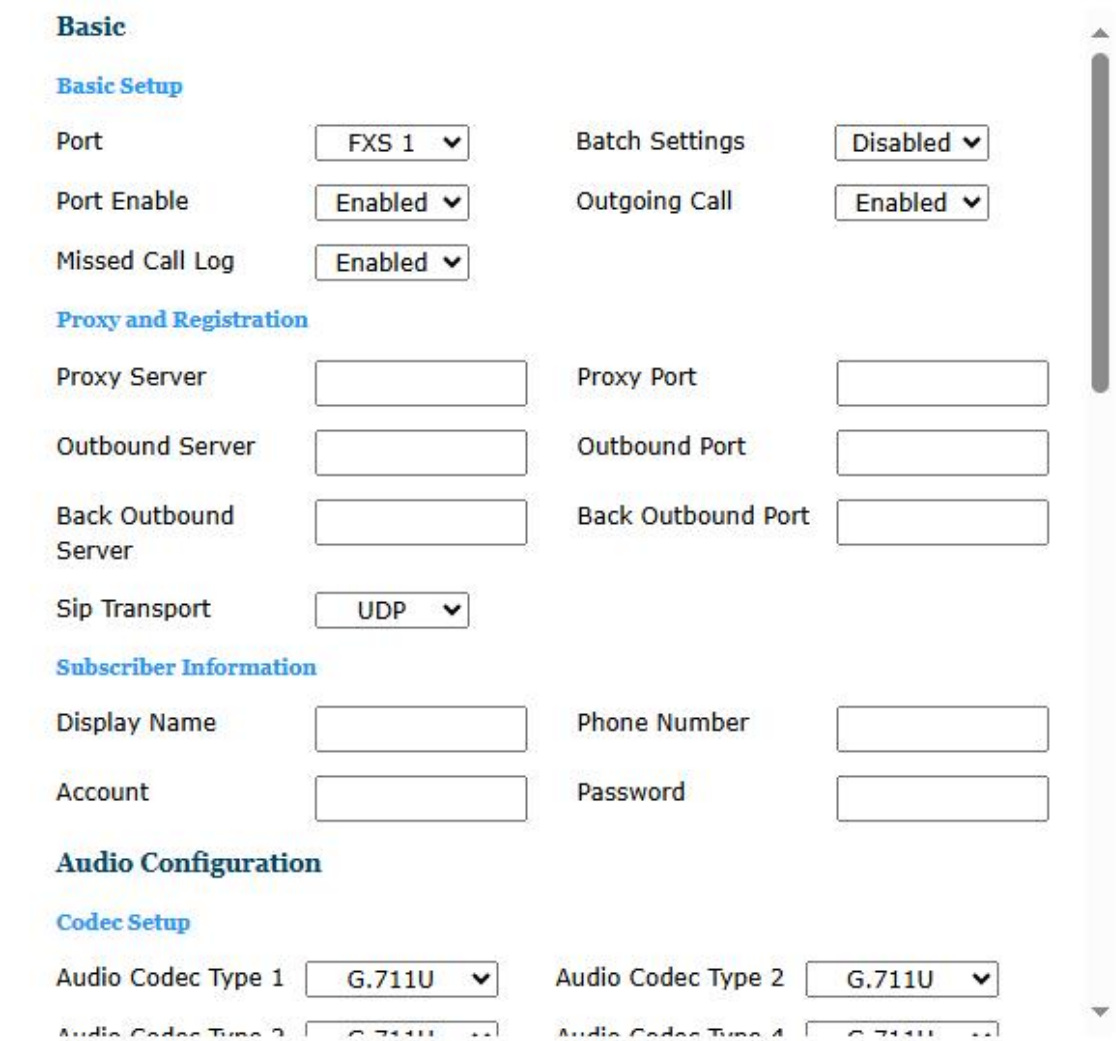


Figure 58 FXS Basic Settings

4.5.1.3 FXS Advance Settings

On this page, you can set the advance information of FXS.

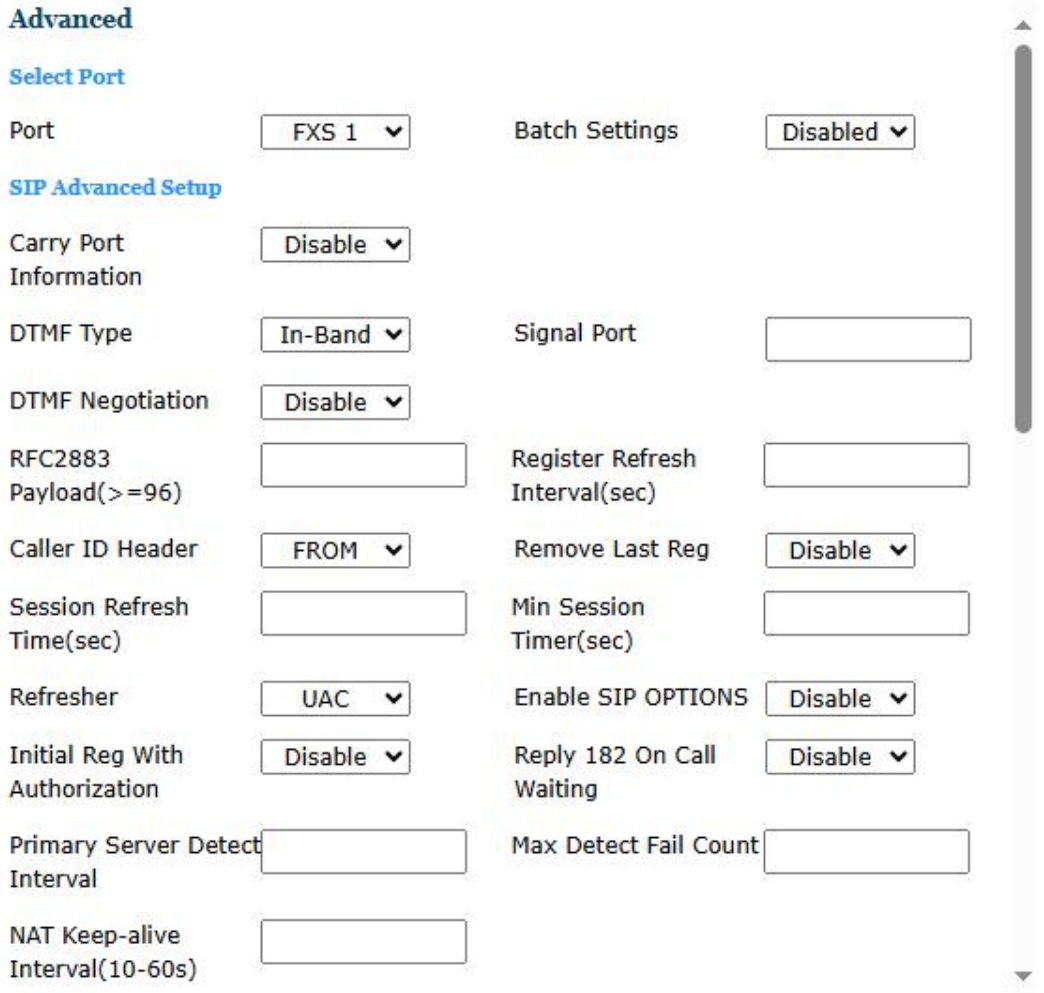


Figure 59 FXS Advance Settings

4.5.1.4 SIP Settings

On this page, you can set SIP Parameters and NAT Traversal.

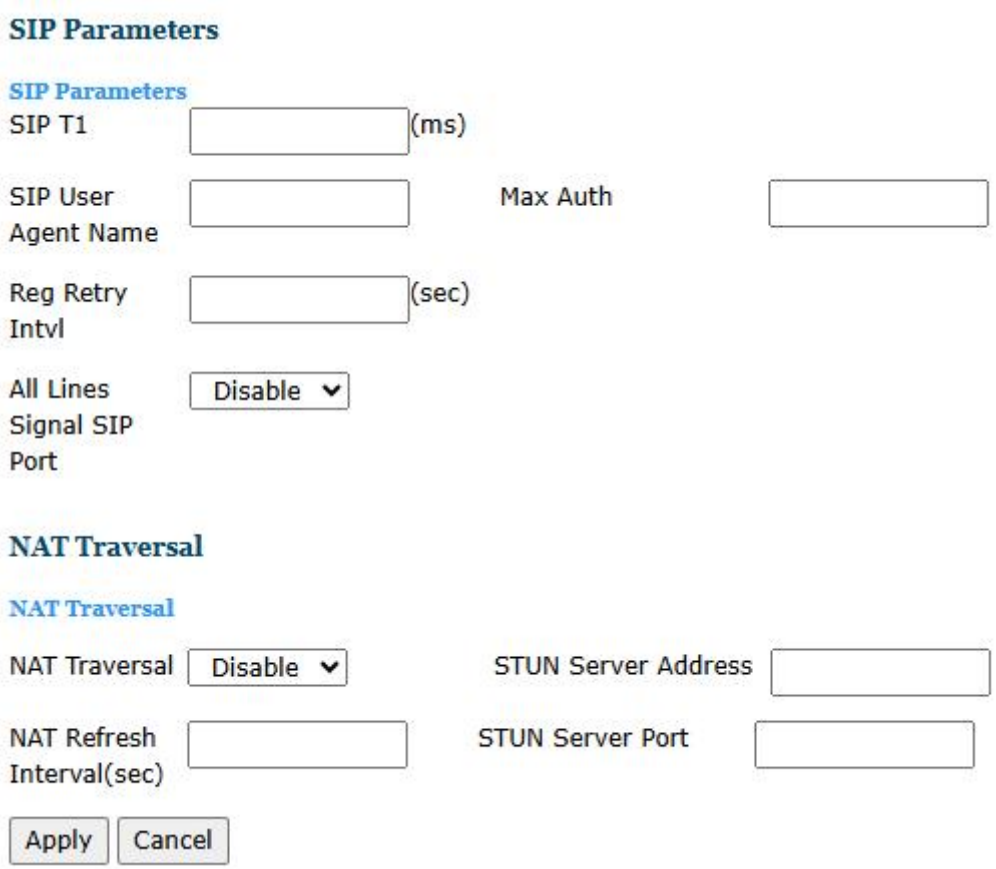


Figure 60 SIP Settings

4.5.1.5 VoIP QoS

On this page, you can set SIP QOS and RTP QOS.

Figure 61 VoIP QoS

4.5.1.6 Port Group

On this page, you can set Port Group.

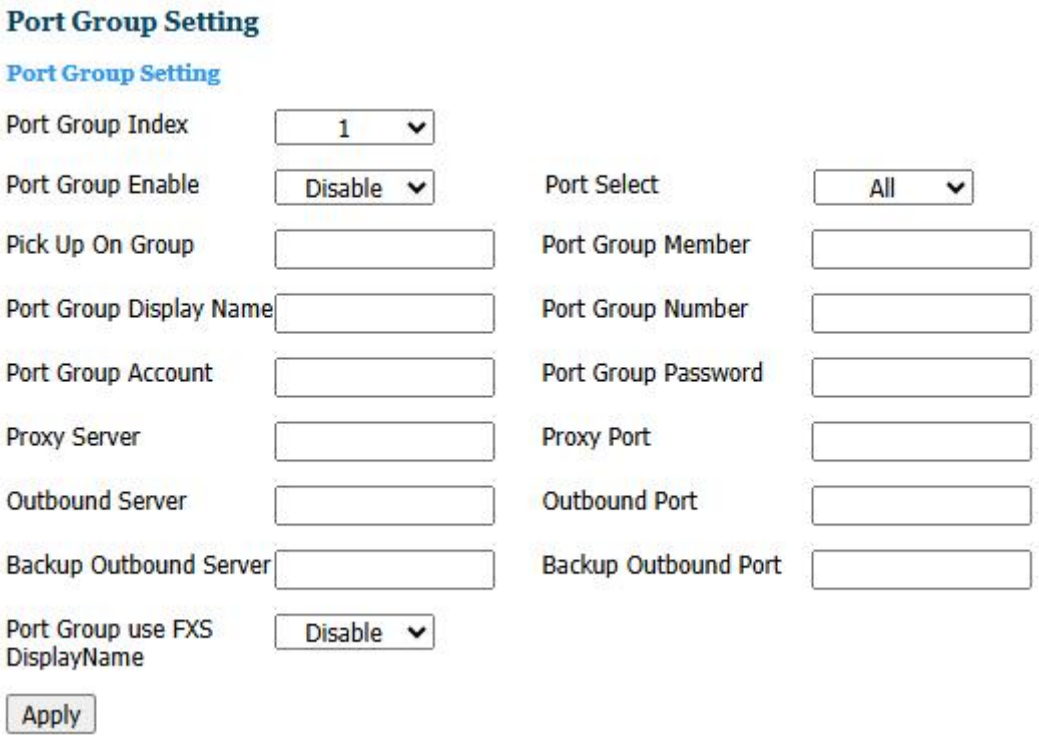


Figure 62 Port Group

4.5.2VoIP Phone Settings

From this page, you can see Phone Preferences Settings and Dial Plan.

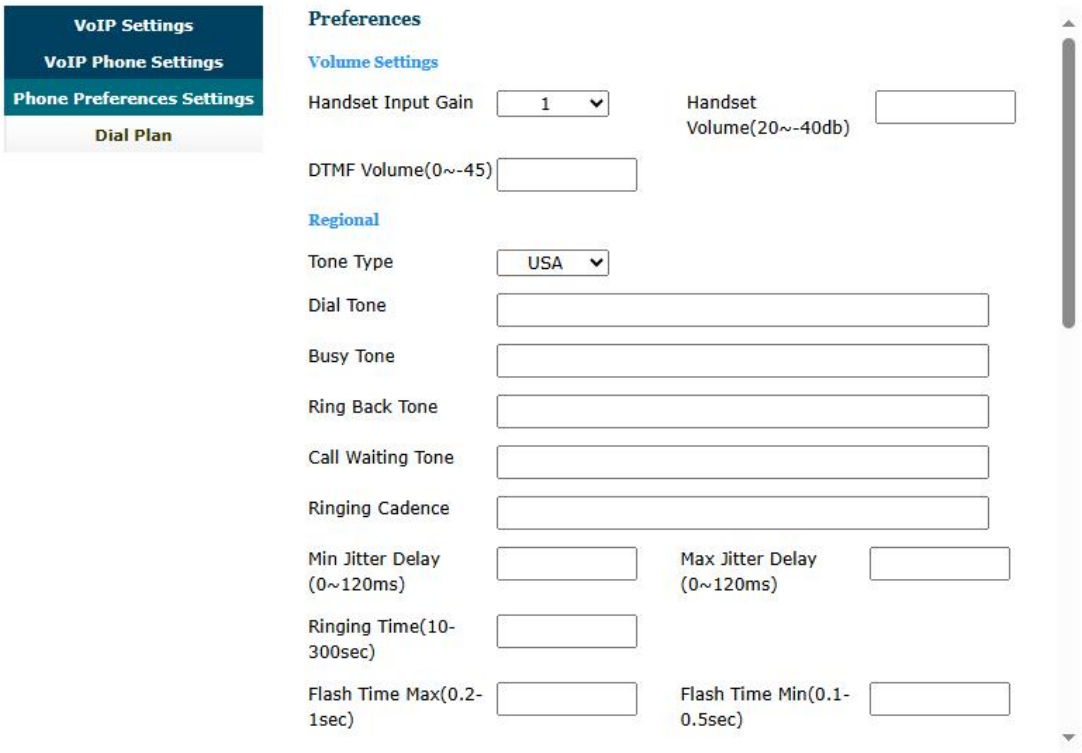


Figure 63 VoIP Phone Settings

4.5.2.1 Phone Preferences Settings

On this page, you can set Volume Settings and Regional.

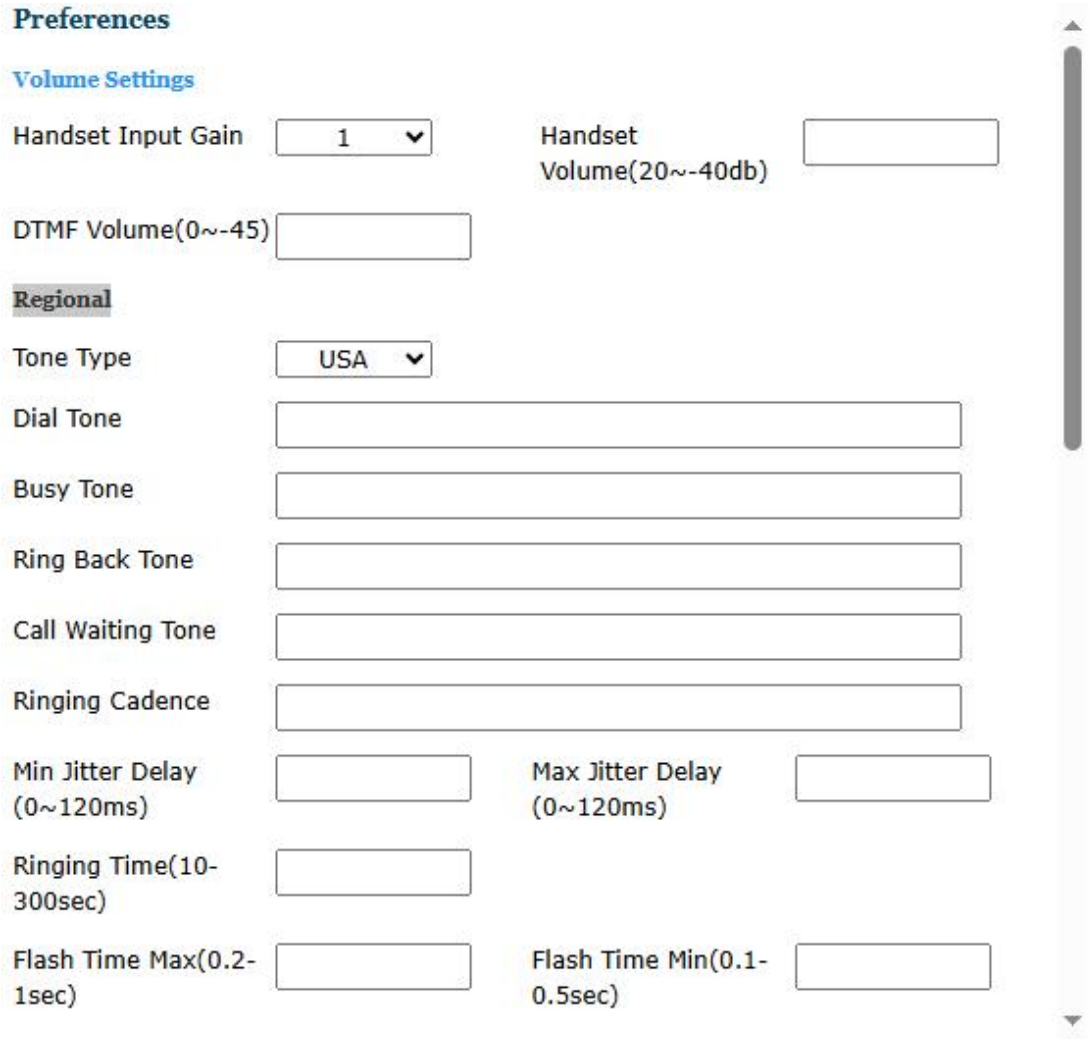


Figure 64 Phone Preferences Settings

4.5.2.2 Dial Plan

On this page, you can set General and Dial Plan Config.

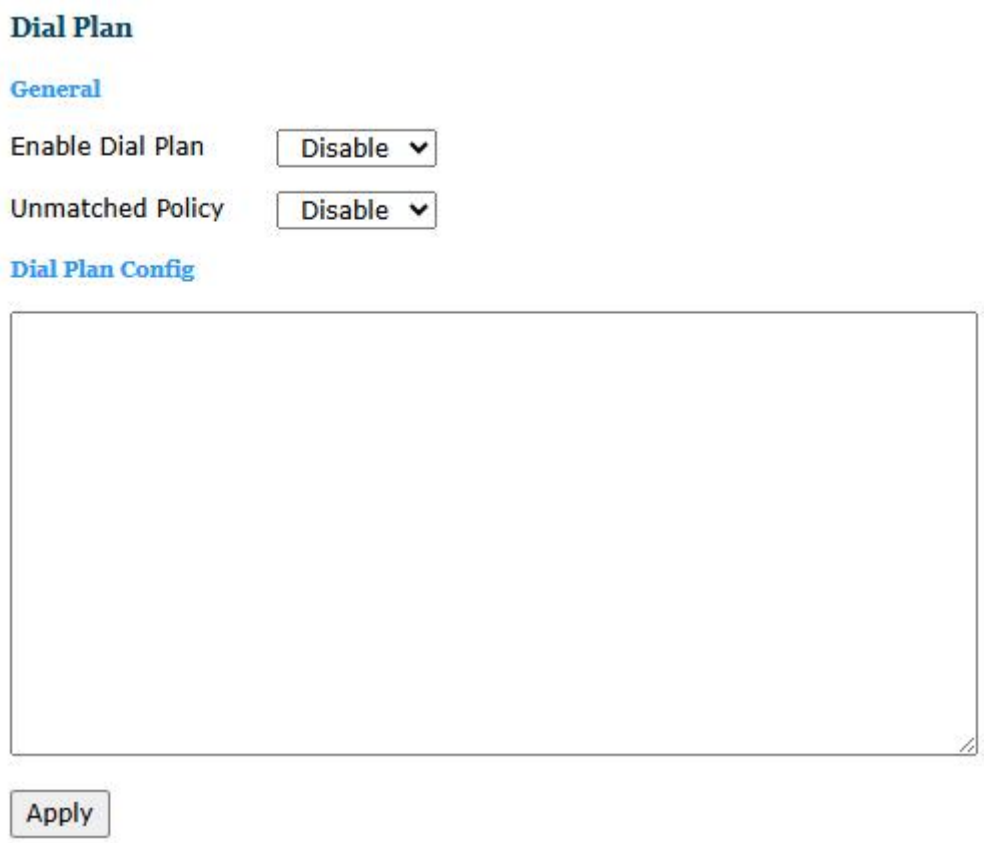


Figure 65 Dial Plan

4.6 Network

From this page, you can see WAN Settings, LTE Settings and Remote Upgrade.

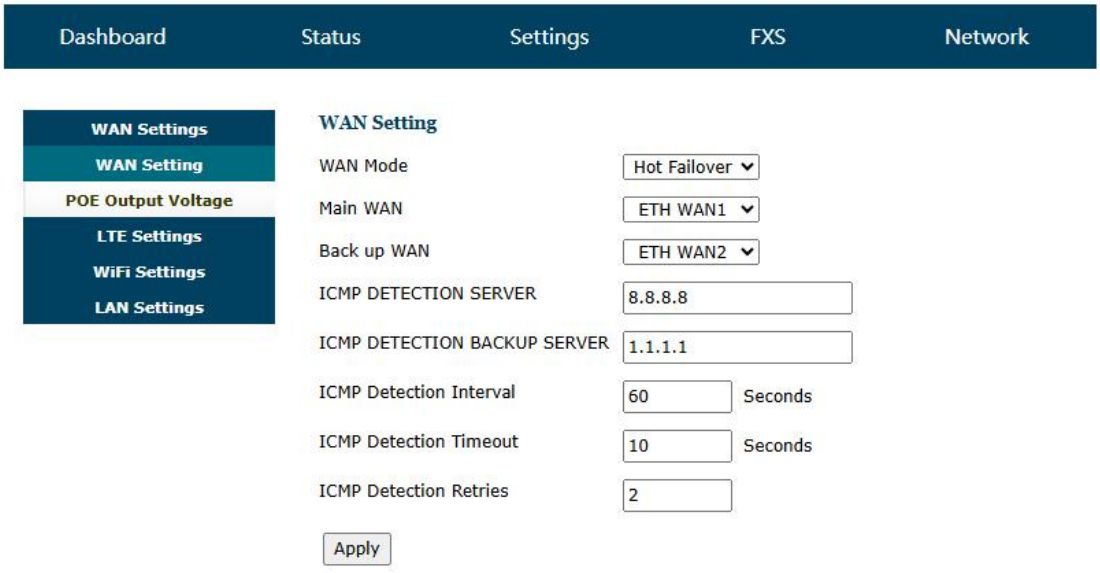


Figure 66 Network

4.6.1WAN Settings

From this page, you can see WAN Setting and POE Output Voltage.

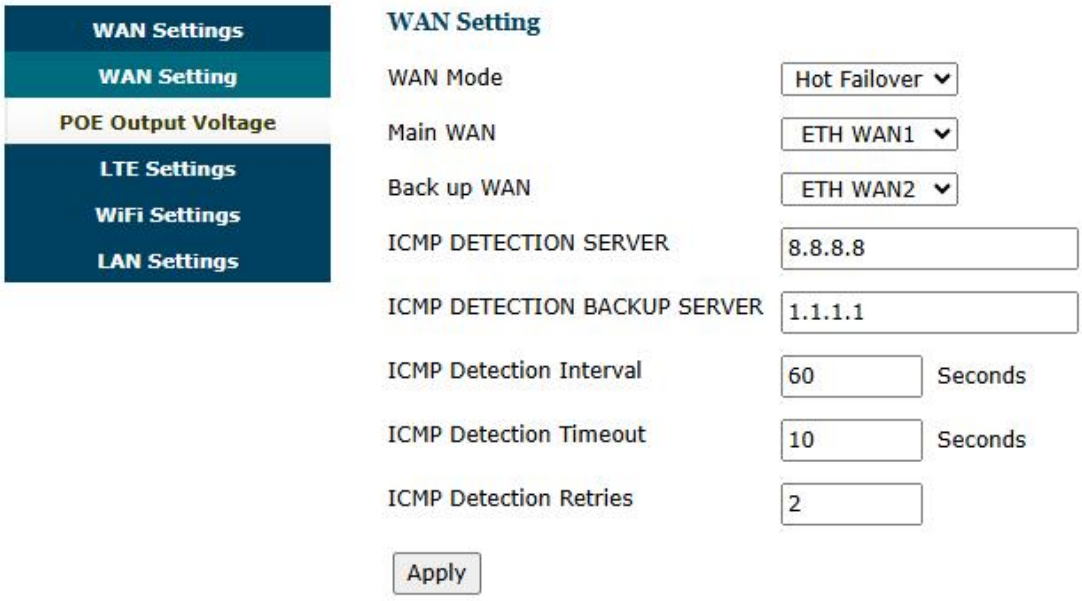


Figure 67 Network

4.6.1.1 WAN Setting

From this page, you can set the wan's connection mode such as ETH WAN1, ETH WAN2, Cellular WAN or WiFi WAN.

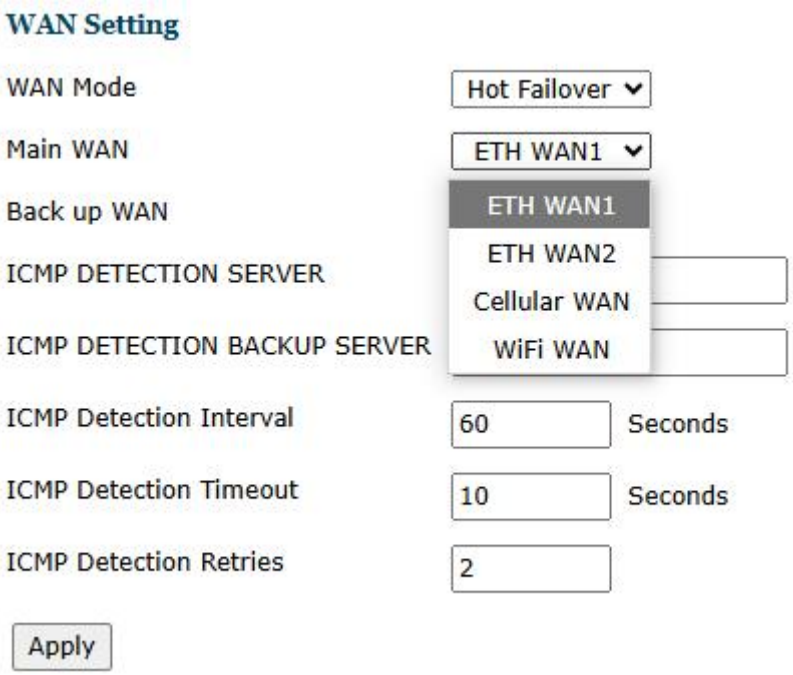


Figure 68 WAN Setting

4.6.1.2 POE Output Voltage

From this page, you can set the poe output voltage as 12V, 24V or 48V.

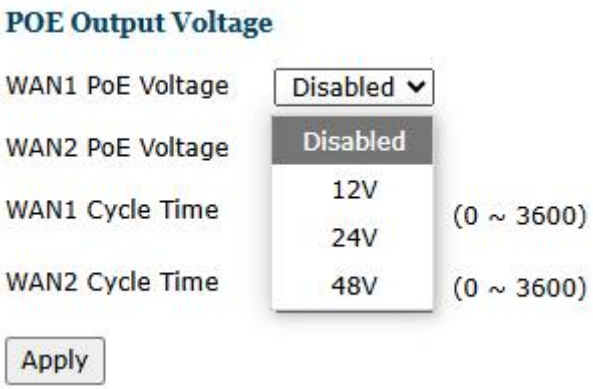


Figure 69 POE Output Voltage

4.6.2LTE Settings

From this page, you can see Data Roaming, SIM Switch , APN Settings and PIN Management.

Figure 70 LTE Settings

4.6.2.1 Data Roaming

From this page ,you can Enable/Disable SIM1/SIM2 Data Roaming.

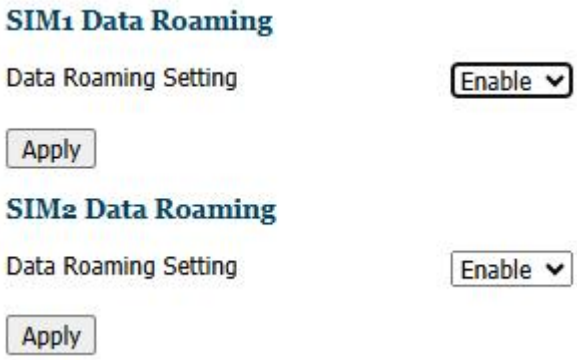


Figure 71 Data Roaming

4.6.2.2 SIM Switch

From this page ,you can switch SIM1or SIM2.

Figure 72 SIM Switch

4.6.2.3 APN Settings

The default APN configured, you can configure the APN settings by clicking on the “Add New” button.

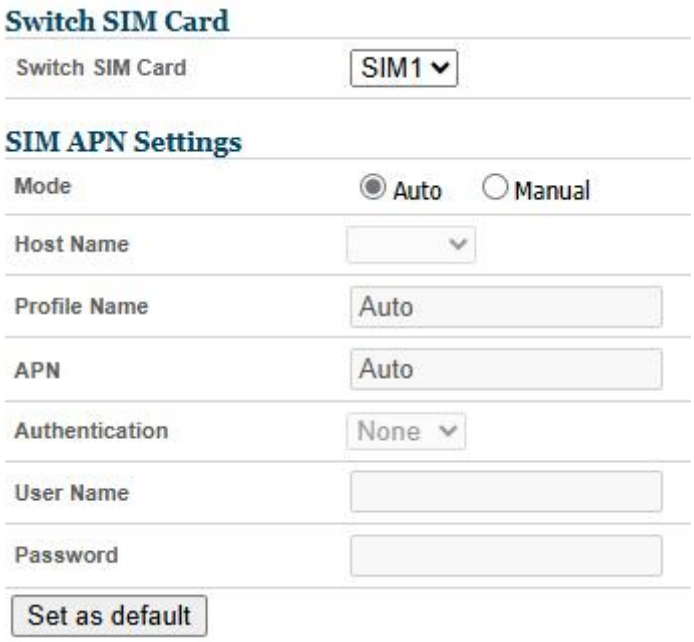


Figure 72 APN Settings

From the “Host Name” option, you can choose the APN that you had configured, then click “Set as default” to make it take effect.

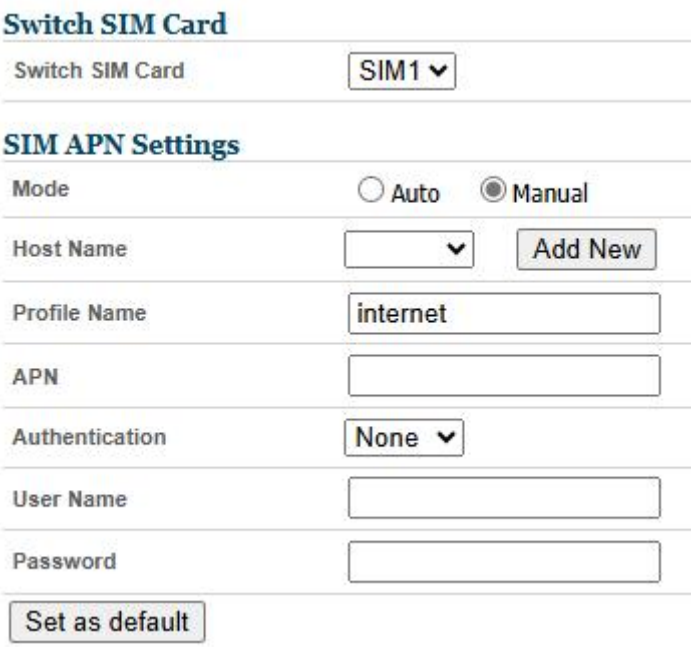


Figure 73 Add New Configuration

4.6.2.4 PIN Management

From this page, you can see SIM1/SIM2 cards status and PIN status.

The default PIN status is disabled, you can input the correct PIN to enable the PIN function. The maximum PIN attempts are 3, otherwise you must enter PUK to reset the PIN code. The USIM will be invalid after the unsuccessful attempts for 10 times.

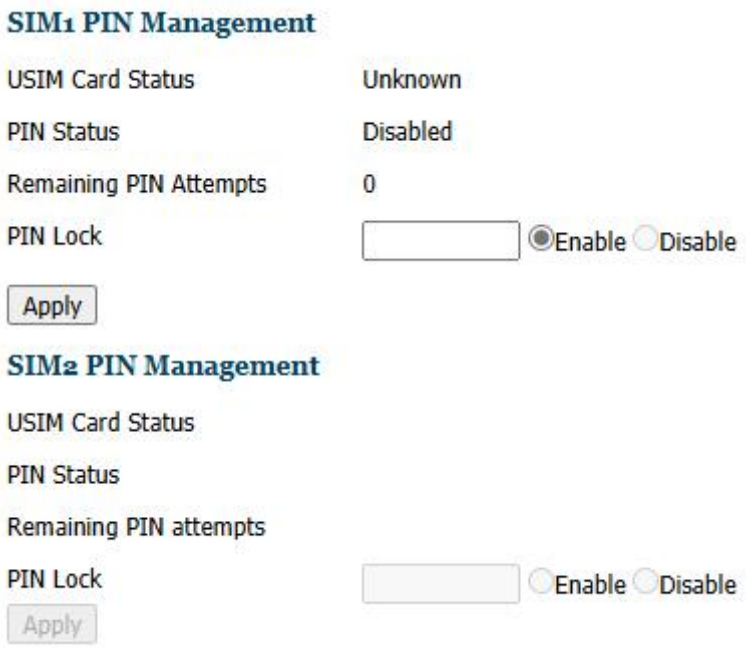


Figure 74 PIN Management

4.6.3WiFi Settings

On this page, you can see Wi-Fi 2.4GHz, Wi-Fi 5GHz, Wireless Block Users, Wi-Fi Guest, and WWAN Hotspot.

Figure 75 WiFi Page

4.6.3.1 Wi-Fi 2.4GHz

You can set the Wi-Fi status, configure the Wi-Fi standard, configure the network name, select the Wi-Fi channel from 1 to 11, configure broadcast SSID and bandwidth.

Figure 76 WiFi 2.4G Settings

- **WiFi Status:** Enabled(default)/Disabled

The wifi status is enabled in default, you can only connect to the device by CAT-6 Ethernet cable if it is disabled.

- **WiFi Standard**

The router can be operated in five different wireless modes: “11b only”, “11g only”, “11n only”, ”11b/g mixed mode” and ”11b/g /n mixed mode”.

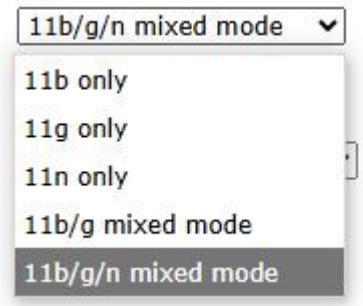


Figure 77 WiFi 2.4G Standard

- **Network Name(SSID)**

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. You can set it to anything you like and you should make sure that your SSID is unique if there are other wireless networks operating in your area.

- **Frequency (Channel)**

This field determines which operating frequency will be used for WiFi. It is not necessary to change the wireless channel unless you noticed the interference problems with other access points nearby.

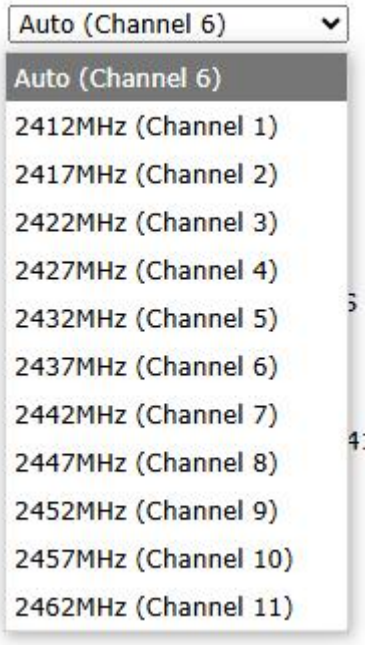


Figure 78 WIFI 2.4G Frequency (Channel)

- **Broadcast SSID:** Enabled(default)/Disabled

When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disabled this feature, the wifi of the router is invisible.

- **Channel BandWidth:** 20MHz and 20/40MHz.

- **WiFi 2.4GHz Security**

Setting the wireless security and encryption to prevent the router from unauthorized access and monitoring. Default security mode is WPA2-PSK and the default password is unique (Figure 22), you can modify the security mode and password you like from this page.

- **Security Mode:** Disabled, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK ,

WPA3-SAE.

- **WPA Algorithms: T**KIP, AES, TKIP/AES.
- **Password:** 8~63 characters.
- **Key Renewal Interval:** 0~4194302s.

Figure 79 Default WiFi Security

4.6.3.2 Wi-Fi 5GHz

You can set the Wi-Fi status, configure the Wi-Fi standard, configure the network name and select the Wi-Fi channel from 36 to 48, configure broadcast SSID and bandwidth.

Figure 80 WiFi 5GHz Settings

- **WiFi Status:** Enabled(default)/Disabled

The wifi status is enabled in default, you can only connect to the device by CAT-5 Ethernet cable if it is disabled.

- **WiFi Standard**

The router can be operated in 3 different wireless modes: ”11a/n/ac mixed mode”, ”11n/ac mixed mode”, “11n only”.

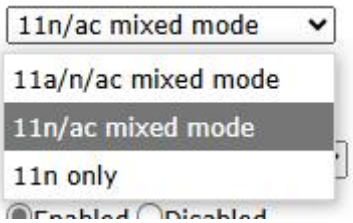


Figure 81 WiFi 5GHz standard

- **Network Name (SSID)**

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. You can set it to anything you like and you should make sure that your SSID is unique if there are other wireless networks operating in your area.

- **Frequency (Channel)**

This field determines which operating frequency will be used for WiFi. It is not necessary to change the wireless channel unless you noticed the interference problems with other access points nearby.

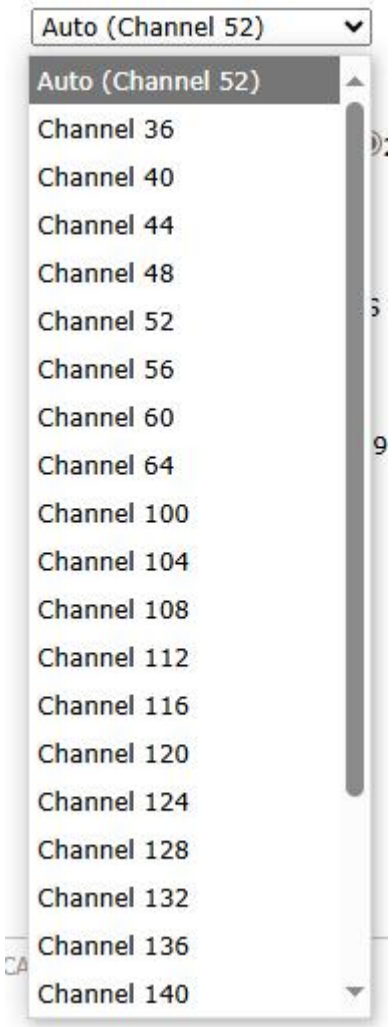


Figure 82 5GHz Frequency (Channel)

- **Broadcast SSID:** Enabled(default)/Disabled

When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disabled this feature, the wifi of the router is invisible.

- **BandWidth:** 20MHz, 20/40MHz, 20/40/80MHz.

- **WiFi 5GHz Security**

Setting the wireless security and encryption to prevent the router from unauthorized access and monitoring. Default security mode is WPA2-PSK and the default password is unique (Figure 21), you can modify the security mode and password you like from this page.

- **Security Mode:** Disabled, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK, WPA3-SAE.
- **WPA Algorithms:** TKIP, AES, TKIP/AES.
- **Password:** 8~63 characters.
- **Key Renewal Interval:** 0~4194302s.

Figure 83 Default WiFi Security

4.6.3.3 Wireless Block Users

You can see all Wi-Fi Device on this page, and you can user more function, they are Block, Refresh and so on.

Figure 84 WirelessBlock Users

4.6.3.4 Wi-Fi Guest

From this page, you can Enable/Disable Wi-Fi Guest 2.4GHz and 5GHz.

Figure 85 Wi-Fi Guest

4.6.3.5 WWAN Hotspot

From this page, you can Enable/Disable Wi-Fi WAN, Scan Wi-Fi and connect the Hotspot.

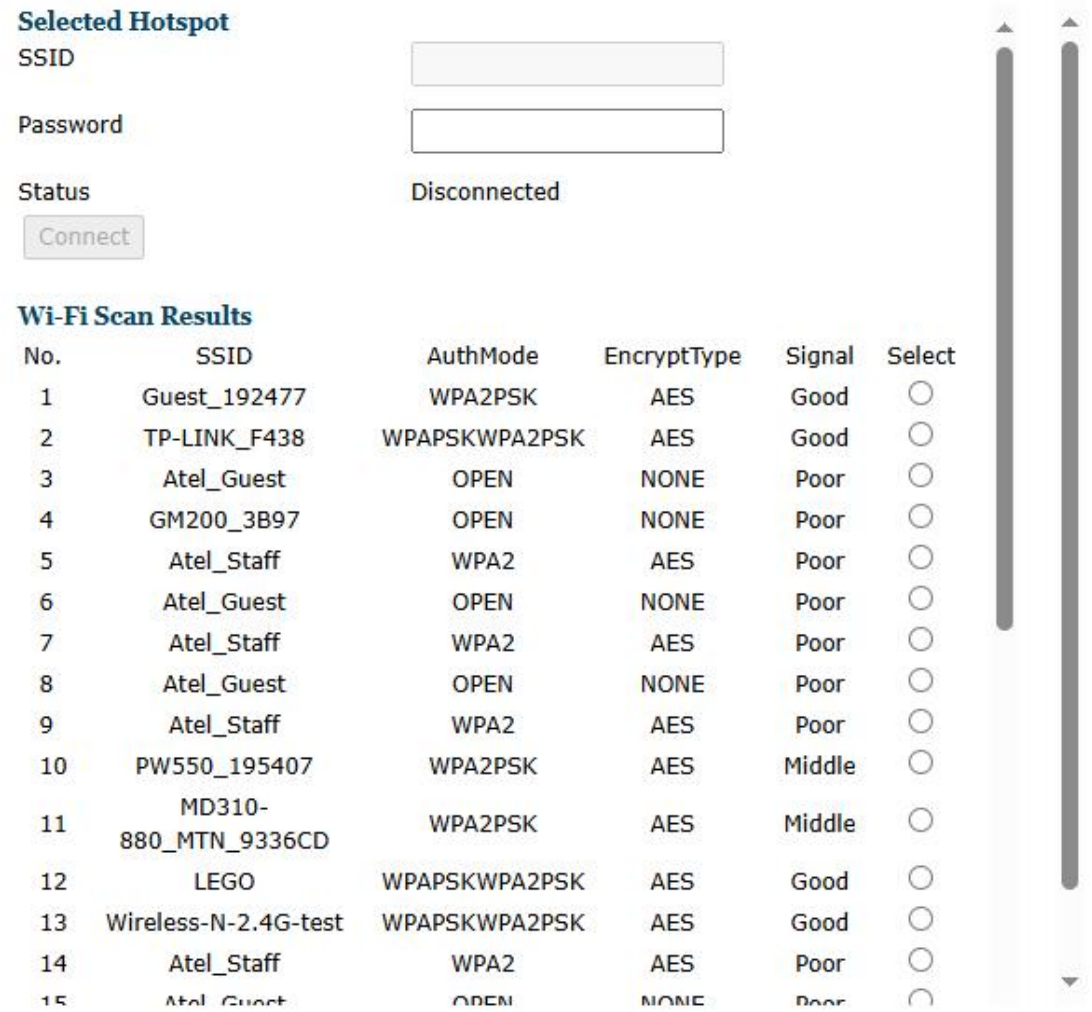


Figure 86 WWAN Hostport

4.6.4LAN Settings

On this page, you can see LAN Setting and LAN Port Setting.

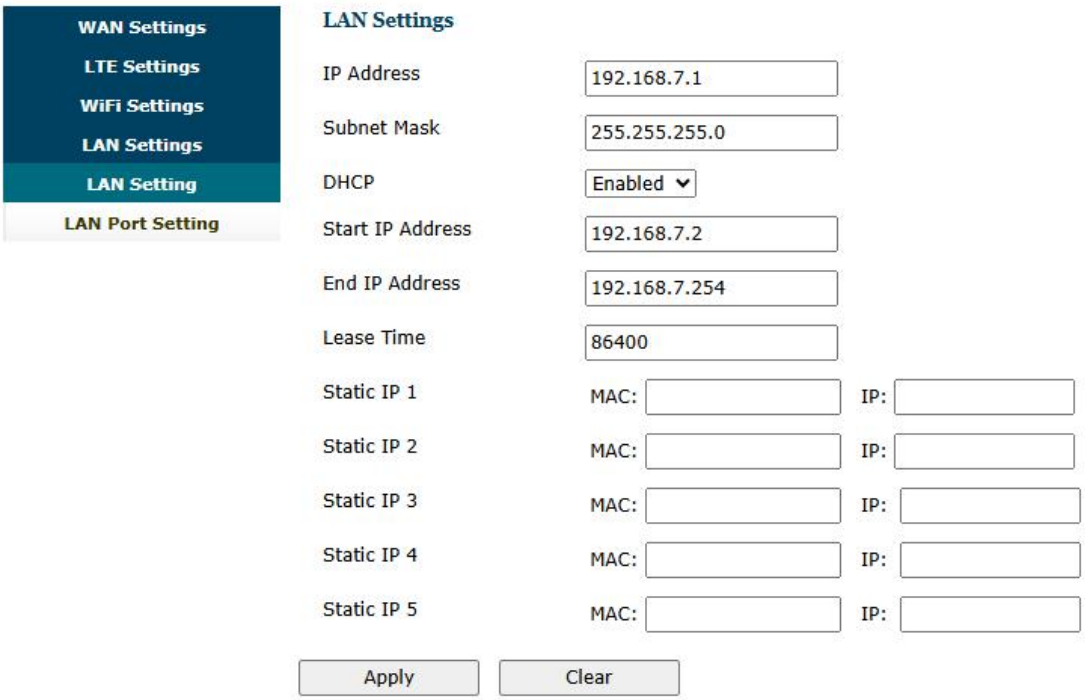


Figure 87 LAN Settings

4.6.4.1 LAN Setting

Clicking on the “LAN Setting” tab will take you to the “LAN Setting” header page. On this page, all settings for the internal LAN setup of the CPE router can be viewed and changed.

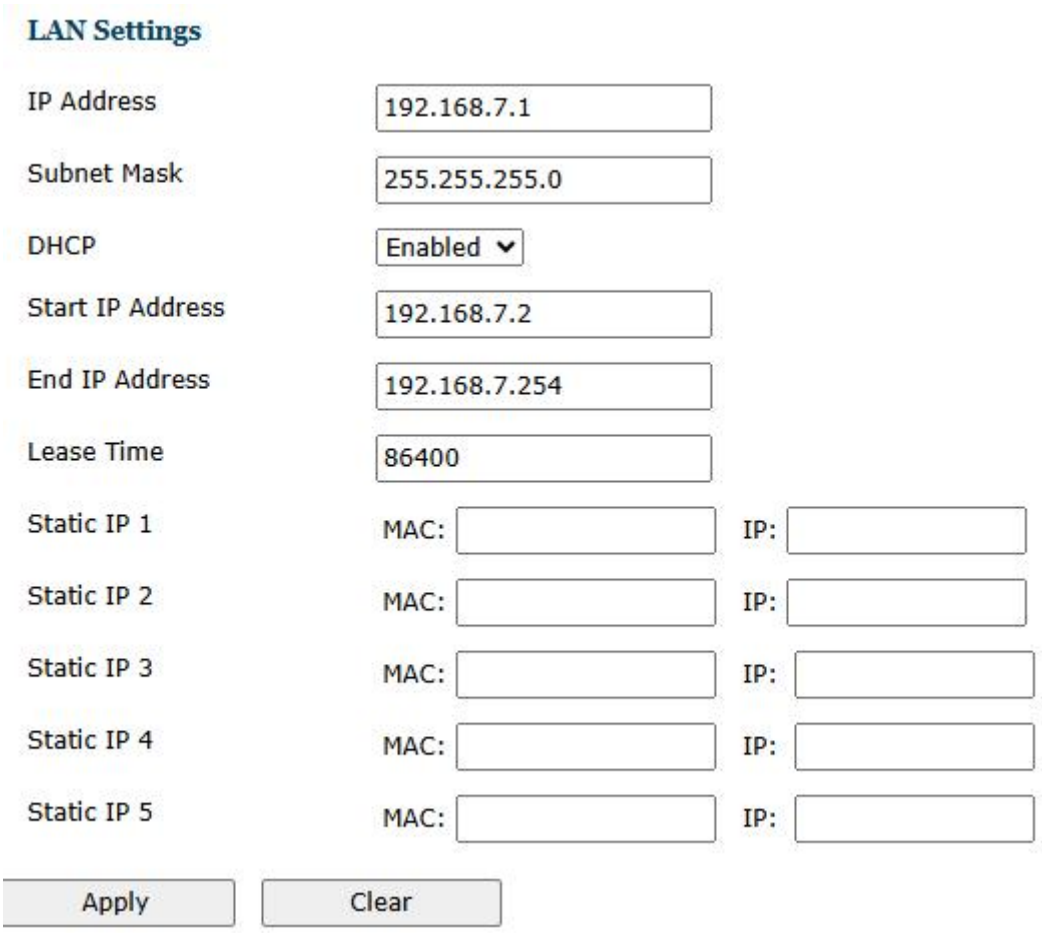


Figure 88 LAN Setting

- **IP Address :** Enter the IP address of your router (factory default: 192.168.7.1).
- **Subnet Mask:** An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **DHCP:** Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the address of your PC manually.
- **Start IP Address:** Specify an IP address for the DHCP server to start with when assigning IP address. The default start address is 192.168.7.2.
- **End IP Address:** Specify an IP address for the DHCP Server to end with when assigning IP address. The default end address is 192.168. 7.254.
- **Lease Time:** The Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP address. After the time is up, the user will be assigned a new dynamic IP address automatically.
- **Static IP1~ Static IP5:** IP/MAC binding function, the system will assign a fixed IP address to the MAC according to the rules.

Note:

- If you change the IP Address of LAN, you must use the new IP address to login to the CPE router.

If the new LAN IP address you set is not in the same subnet, the IP address pool of the DHCP server will

change at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

4.6.4.2 LAN Port Setting

From this page, you can set LAN port 1 and LAN port 1.

Figure 89 LAN Port Setting

4.6.4.3 FCC Rule

FCC Regulations:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2)this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with FCC RF Exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for the transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co - located or operating in conjunction with any other antenna or transmitter.

5. Revision History

Author	Revision	Changes	Date
ZhFei	V1.0	Initial Draft	2025-01-03
ZhFei	V1.1	Replace the silkscreen	2025-01-06
ZhFei	V1.2	Modify some functions	2025-03-26