



# PC222 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

|                                           |           |
|-------------------------------------------|-----------|
| <b>1. About this Manual .....</b>         | <b>3</b>  |
| <b>2. Product Overview .....</b>          | <b>3</b>  |
| <b>3. Introduction .....</b>              | <b>3</b>  |
| 3.1 Ports and Buttons .....               | 3         |
| 3.2 LED Definition .....                  | 4         |
| <b>4. Introduction to the WebUI .....</b> | <b>4</b>  |
| 4.1 Login .....                           | 5         |
| 4.2 Dashboard .....                       | 5         |
| 4.3 Status .....                          | 6         |
| 4.3.1 WAN Status .....                    | 7         |
| 4.3.2 WiFi Status .....                   | 7         |
| 4.3.3 Software .....                      | 8         |
| 4.3.4 Device List .....                   | 8         |
| 4.3.5 Statistics .....                    | 9         |
| 4.4 Settings .....                        | 9         |
| 4.4.1 Basic Settings .....                | 10        |
| 4.4.2 Security Settings .....             | 12        |
| 4.4.3 Advanced Settings .....             | 22        |
| 4.4.4 Log Management .....                | 26        |
| 4.5 FXS .....                             | 27        |
| 4.5.1 VoIP Settings .....                 | 28        |
| 4.5.2 VoIP Phone Settings .....           | 32        |
| 4.6 Network .....                         | 33        |
| 4.6.1 WAN Settings .....                  | 34        |
| 4.6.2 LTE Settings .....                  | 35        |
| 4.6.3 WiFi Settings .....                 | 37        |
| 4.6.4 LAN Settings .....                  | 46        |
| <b>5. Revision History .....</b>          | <b>50</b> |

# 1. About this Manual

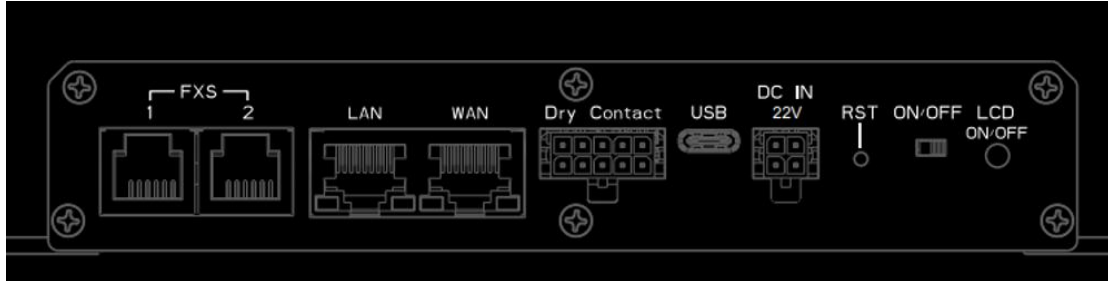
The content of this User Manual has been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice.

## 2. Product Overview

Connect the PC to router using the CAT-6 Ethernet cable, use Ethernet port 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. It is advised to read this manual at leisure to make best use of the router.

## 3. Introduction

### 3.1 Ports 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 2 ports     |
|            | 2. LAN Port: *1 Gigabit port |
|            | 3. WAN Port: *2 Gigabit port |
|            | 4. Dry connector connector   |
|            | 5. USB: Type-C               |
|            | 6. DC IN: for DC 22V input   |
|            | 7. Reset button              |
|            | 8. ON/OFF key                |

## 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 |                                          |
|-----|------------------------------------------|
|     | <a href="#">1.FXS 1(VoIP line 1) LED</a> |
|     | <a href="#">2.FXS 2(VoIP line 2) LED</a> |
|     | <a href="#">3.WWANLED</a>                |
|     | <a href="#">4.WAN LED</a>                |
|     | <a href="#">5.Battery LED</a>            |
|     | <a href="#">6.Power LED</a>              |

## 4. Introduction to the WebUI

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

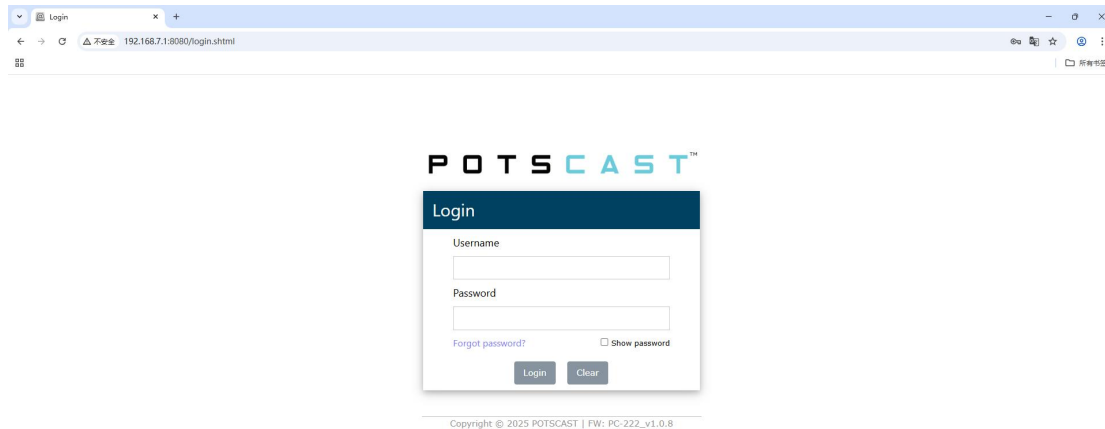
In the following sections, we will introduce you the main functions and the method of how to configure them.

## 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 five main menus on the top bar of the WebGUI.

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

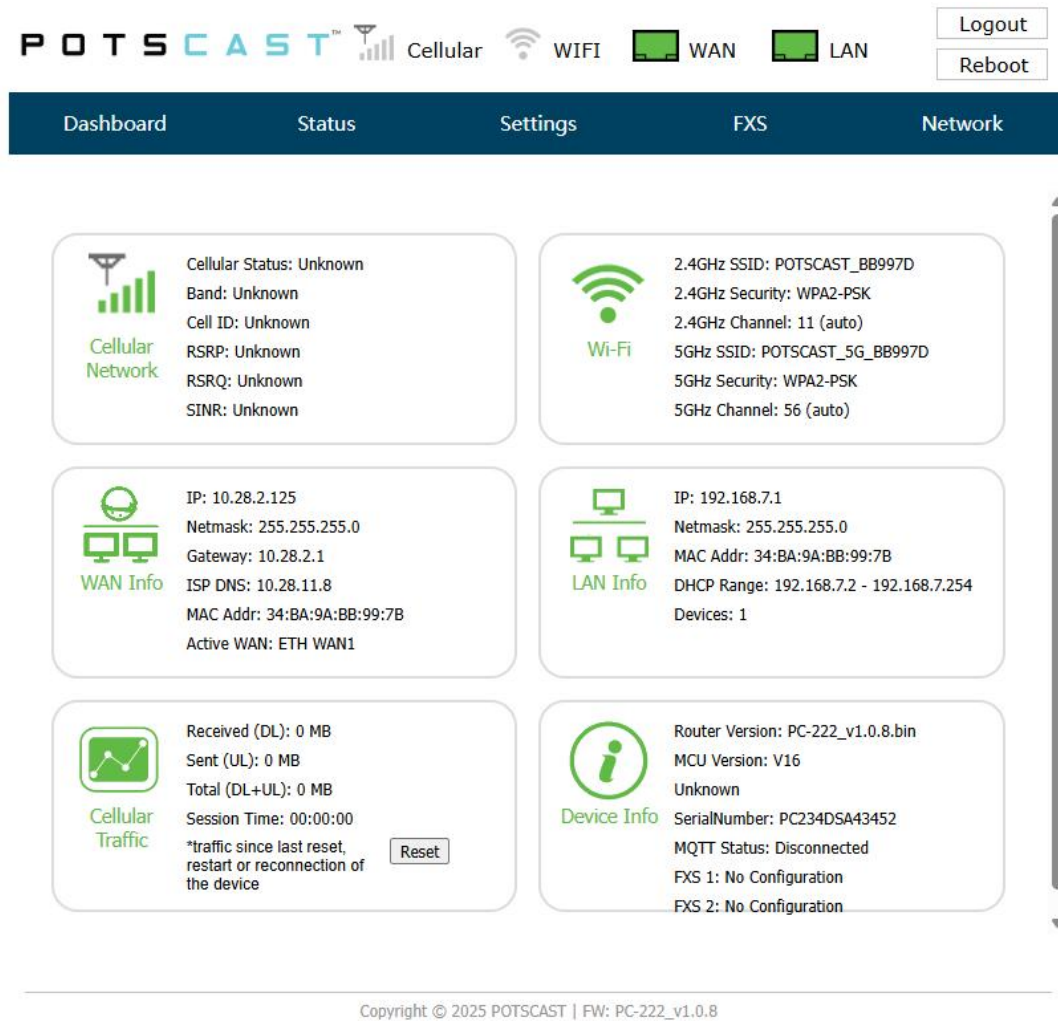


Figure 2 Dashboard

## 4.3 Status

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

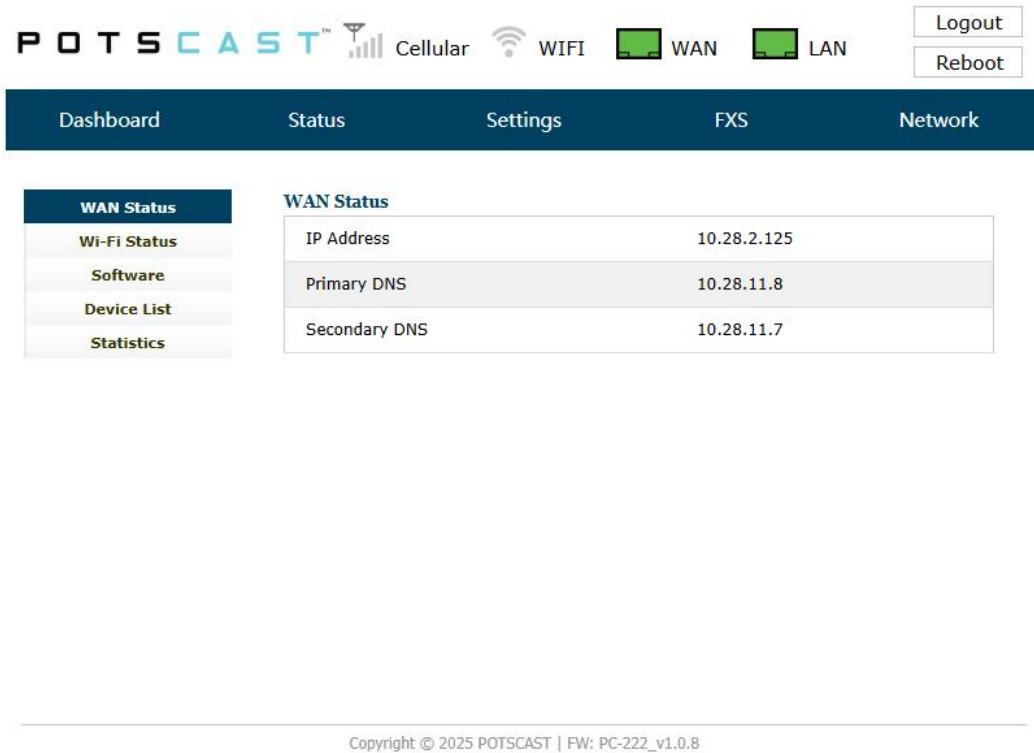


Figure 3 Status

### 4.3.1 WAN Status

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



Figure 4 WAN Status

### 4.3.2 WiFi Status

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

|              |                                        |
|--------------|----------------------------------------|
| WAN Status   | 2.4 GHz Wi-Fi Status                   |
| Wi-Fi Status | Wi-Fi Status Enabled                   |
| Software     | Network Name (SSID) POTSCAST_BB997D    |
| Device List  | Frequency (Channel) Auto (Channel 11)  |
| Statistics   | Security Mode WPA2PSK                  |
|              | 5 GHz Wi-Fi Status                     |
|              | Wi-Fi Status Enabled                   |
|              | Network Name (SSID) POTSCAST_5G_BB997D |
|              | Frequency (Channel) Auto (Channel 56)  |
|              | Security Mode WPA2PSK                  |

Figure 5 WiFi Status

### 4.3.3 Software

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

| Dashboard    | Status                                | Settings | FXS | Network |
|--------------|---------------------------------------|----------|-----|---------|
| WAN Status   | Software                              |          |     |         |
| Wi-Fi Status | Router Software Version PC-222_v1.0.8 |          |     |         |
| Software     | Modem Software Version Unknown        |          |     |         |
| Device List  | MCU Version V16                       |          |     |         |
| Statistics   |                                       |          |     |         |

Figure 6 Software

### 4.3.4 Device List

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

|              |                   |
|--------------|-------------------|
| WAN Status   | Device List       |
| Wi-Fi Status | Hostname          |
| Software     | MAC Address       |
| Device List  | IP Address        |
| Statistics   | Type              |
|              | xppan-pc          |
|              | 6C:1F:F7:08:E5:F4 |
|              | 192.168.7.239     |
|              | Ethernet          |

Figure 7 Device List

## 4.3.5 Statistics

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

|                   |                   |  |  |  |
|-------------------|-------------------|--|--|--|
| WAN Status        | <b>Statistics</b> |  |  |  |
| Wi-Fi Status      |                   |  |  |  |
| Software          |                   |  |  |  |
| Device List       |                   |  |  |  |
| <b>Statistics</b> |                   |  |  |  |

| Download       |        | Upload |  |
|----------------|--------|--------|--|
| Cellular Speed | 0 Kb/s | 0 Kb/s |  |

|      | Downloaded | Uploaded | Total |
|------|------------|----------|-------|
| SIM1 | 0 MB       | 0 MB     | 0 MB  |
| SIM2 | 0 MB       | 0 MB     | 0 MB  |

| Cellular        | Duration | Downloaded | Uploaded | Total Used Data |
|-----------------|----------|------------|----------|-----------------|
| Current Session | 00:00:00 | 0 MB       | 0 MB     | 0 MB            |
| Total           | 00:00:00 | 0 MB       | 0 MB     | 0 MB            |

The amounts of data is approximate. For more information please contact your network operator.

[Clear Session](#)

**Figure 8** Statistics

## 4.4 Settings

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

|           |        |          |     |         |
|-----------|--------|----------|-----|---------|
| Dashboard | Status | Settings | FXS | Network |
|-----------|--------|----------|-----|---------|

|                   |                                                                                                                    |
|-------------------|--------------------------------------------------------------------------------------------------------------------|
| Basic Settings    | UI Access Settings                                                                                                 |
| Management        | Username <input type="text" value="admin"/>                                                                        |
| Software Upgrade  | Current Admin Access Password <input type="password"/> <input type="checkbox"/> Show password (32 characters max.) |
| Remote Upgrade    | New Admin Access Password <input type="password"/> <input type="checkbox"/> Show password (32 characters max.)     |
| Security Settings | Repeat Admin Access Password <input type="password"/> <input type="checkbox"/> Show password (32 characters max.)  |
| Advanced Settings | <input type="button" value="Apply"/> <input type="button" value="Clear"/>                                          |
| Log Management    | UI Control Settings                                                                                                |
|                   | Allow Concurrent Logins <input type="button" value="Enabled"/>                                                     |
|                   | WebUI Timeout <input type="text" value="5"/> Minutes                                                               |
|                   | <input type="button" value="Apply"/>                                                                               |
|                   | Factory Reset                                                                                                      |
|                   | Click button to restore default settings <input type="button" value="Restore"/>                                    |
|                   | Device Reboot                                                                                                      |
|                   | Click button to reboot the device <input type="button" value="Reboot"/>                                            |

**Figure 9** Settings

## 4.4.1 Basic Settings

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

**Basic Settings**

**Management**

**Software Upgrade**

**Remote Upgrade**

**Security Settings**

**Advanced Settings**

**Log Management**

**UI Access Settings**

Username admin

Current Admin Access Password  ☐ Show password (32 characters max.)

New Admin Access Password  ☐ Show password (32 characters max.)

Repeat Admin Access Password  ☐ Show password (32 characters max.)

**UI Control Settings**

Allow Concurrent Logins

WebUI Timeout  Minutes

**Factory Reset**

Click button to restore default settings

**Device Reboot**

Click button to reboot the device

**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.

The screenshot displays the 'Management' section of the PC222 web interface. On the left is a sidebar menu with options: Basic Settings, Management (highlighted), Software Upgrade, Remote Upgrade, Security Settings, Advanced Settings, Remote Management, and Log Management. The main content area is divided into four sections: 1. 'UI Access Settings' with fields for Username (admin), Current Admin Access Password, New Admin Access Password, and Repeat Admin Access Password, each with a 'Show password' checkbox and a 32-character limit. 2. 'UI Control Settings' with 'Allow Concurrent Logins' set to 'Enabled' and 'WebUI Timeout' set to 5 minutes. 3. 'Factory Reset' with a 'Restore' button. 4. 'Device Reboot' with a 'Reboot' button. 'Apply' and 'Clear' buttons are located below the password fields.

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.

The screenshot shows the 'Software Upgrade' page in the PC222 web interface. The sidebar menu is identical to Figure 11, with 'Software Upgrade' highlighted. The main content area has two sections: 1. 'Device Software Upgrade' with a 'Router Upgrade' field containing a file selection button (选择文件) and the text '未选择文件', and an 'Apply' button. 2. 'MCU Software Upgrade' with an 'MCU Upgrade' field containing a file selection button (选择文件) and the text '未选择文件', and an 'Apply' button.

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

## 4.4.2 Security Settings

From this page, you can see MAC Filtering, IP/Port Filtering, Content Filtering, Port Forwarding, Virtual Server, DMZ, UPnP, Dynamic DNS, VPN Passthrough and Network Management.

Figure 14 Security Settings

### 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.

#### MAC Filtering Settings

MAC Filtering Disabled ▼

Default policy - the device that don't match any rule would be: Allow ▼

Apply

**Figure 15** 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.

#### MAC Filtering Settings

MAC Filtering Enabled ▼

Default policy - the device that don't match any rule would be: Allow ▼

#### MAC Address Rule Table

| ID                       | MAC Address | Action |
|--------------------------|-------------|--------|
| Others would be accepted |             | -      |

Delete Add New (Note: maximum rule count is 10)

#### Mac Filtering Schedule

Schedule Disabled ▼

Apply

**Figure 16** Enable MAC Filtering Function

**Add Rule**

MAC Address

Action  ▼

**Figure 17** Add Rule**MAC Filtering Settings**

MAC Filtering  ▼

Default policy - the device that don't match any rule would be:  ▼

**MAC Address Rule Table**

| ID                         | MAC Address       | Action |
|----------------------------|-------------------|--------|
| 1 <input type="checkbox"/> | 82:CE:B8:51:68:16 | Drop   |
| Others would be accepted   |                   | -      |

(Note: maximum rule count is 10)

**Mac Filtering Schedule**

Schedule  ▼

**Figure 18** 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 “Accepted”. Otherwise, the action turns to be “Drop” and the packet that don't match with any rules would be accepted.

**IP/Port Filtering Settings**

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| IP/Port Filtering                                               | Enabled ▼ |
| Default policy - the device that don't match any rule would be: | Dropped ▼ |
| <input type="button" value="Apply"/>                            |           |

**Time Rule table**

| ID                                                                                                                                                 | Dest IP Address | Source IP Address | Protocol | Dest Port Range | Source Port Range | Action |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|----------|-----------------|-------------------|--------|
| Others would be dropped                                                                                                                            |                 |                   |          |                 |                   |        |
| <input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> (Note: maximum rule count is 10) |                 |                   |          |                 |                   |        |

**Figure 19** IP/Port filtering page**IP/Port Filtering Settings**

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| IP/Port Filtering                                               | Enabled ▼ |
| Default policy - the device that don't match any rule would be: | Dropped ▼ |
| <input type="button" value="Apply"/>                            |           |

Time Rule table

| ID                                                                                                                                                 | Dest IP Address | Source IP Address | Protocol | Dest Port Range | Source Port Range | Action |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|----------|-----------------|-------------------|--------|
| Others would be dropped                                                                                                                            |                 |                   |          |                 |                   |        |
| <input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> (Note: maximum rule count is 10) |                 |                   |          |                 |                   |        |

**Figure 20** 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.

**Add Rule**

|                                                                          |                                             |
|--------------------------------------------------------------------------|---------------------------------------------|
| Dest IP Address                                                          | <input type="text" value="8.8.8.8"/>        |
| Source IP Address                                                        | <input type="text" value="192.168.1.2"/>    |
| Protocol                                                                 | <input type="text" value="All"/>            |
| Dest Port Range                                                          | <input type="text"/> - <input type="text"/> |
| Source Port Range                                                        | <input type="text"/> - <input type="text"/> |
| Action                                                                   | <input type="text" value="Accept"/>         |
| <input type="button" value="Apply"/> <input type="button" value="Back"/> |                                             |

**Figure 21** Add New Rule**IP/Port Filtering Settings**

|                                                                 |                                      |
|-----------------------------------------------------------------|--------------------------------------|
| IP/Port Filtering                                               | <input type="text" value="Enabled"/> |
| Default policy - the device that don't match any rule would be: | <input type="text" value="Dropped"/> |

**Time Rule table**

| ID                                                                                                                                                 | Dest IP Address | Source IP Address | Protocol | Dest Port Range | Source Port Range | Action |
|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|-------------------|----------|-----------------|-------------------|--------|
| 1 <input type="checkbox"/>                                                                                                                         | 8.8.8.8         | 192.168.1.2       | All      | -               | -                 | Accept |
| Others would be dropped                                                                                                                            |                 |                   |          |                 |                   |        |
| <input type="button" value="Apply"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> (Note: maximum rule count is 10) |                 |                   |          |                 |                   |        |

**Figure 22** 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.

**Content Filtering Rule Table**

| ID | URL Address or Keyword | Select |
|----|------------------------|--------|
|----|------------------------|--------|

Note: maximum rule count is 8

**Content Filtering Schedule**

Schedule

**Figure 23** Content Filtering**Content Filtering Rule Table**

| ID | URL Address or Keyword | Select |
|----|------------------------|--------|
|----|------------------------|--------|

Note: maximum rule count is 8

**Content Filtering Schedule**

Schedule  ☐ Every day

Time ☒ Every time

|                              |                              |                              |                              |
|------------------------------|------------------------------|------------------------------|------------------------------|
| <input type="checkbox"/> Mon | <input type="checkbox"/> Tue | <input type="checkbox"/> Wed | <input type="checkbox"/> Thu |
| <input type="checkbox"/> Fri | <input type="checkbox"/> Sat | <input type="checkbox"/> Sun |                              |

☐ At a defined time From  h  min. To  h  min.

**Figure 24** 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.

**Port Forwarding Rule Table**

| ID                                                                                                               | IP Address | Port Range | Protocol | Comment |
|------------------------------------------------------------------------------------------------------------------|------------|------------|----------|---------|
| <input type="checkbox"/> Select All (Note: maximum rule count is 20)                                             |            |            |          |         |
| <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> |            |            |          |         |

**Figure 25** Port Forwarding page**Port Forwarding Settings**

Port Forwarding

IP Address

Port Range  -

Protocol

Comment

**Figure 26** 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.

**Port Forwarding Rule Table**

| ID                                                                                                               | IP Address    | Port Range  | Protocol  | Comment |
|------------------------------------------------------------------------------------------------------------------|---------------|-------------|-----------|---------|
| 1 <input type="checkbox"/>                                                                                       | 192.168.7.120 | 5000 - 6000 | TCP + UDP |         |
| <input type="checkbox"/> Select All (Note: maximum rule count is 20)                                             |               |             |           |         |
| <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> |               |             |           |         |

**Figure 27** Rule Table**4.4.2.5 Virtual Server**

Virtual Server 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.

**Virtual Server Rule Table**

| ID                                                                                                               | IP Address | Public Port | Private Port | Protocol |
|------------------------------------------------------------------------------------------------------------------|------------|-------------|--------------|----------|
| <input type="checkbox"/> Select All (Note: maximum rule count is 20)                                             |            |             |              |          |
| <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> |            |             |              |          |

**Figure 28** Virtual Server page**Virtual Server Settings**

|                                                                          |                                              |
|--------------------------------------------------------------------------|----------------------------------------------|
| IP Address                                                               | <input type="text"/>                         |
| Public Port                                                              | <input type="text"/>                         |
| Private Port                                                             | <input type="text"/>                         |
| Protocol                                                                 | <input type="button" value="TCP&amp;UDP ▼"/> |
| <input type="button" value="Apply"/> <input type="button" value="Back"/> |                                              |

**Figure 29** 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.

**Virtual Server Rule Table**

| ID                                                                                                               | IP Address    | Public Port | Private Port | Protocol  |
|------------------------------------------------------------------------------------------------------------------|---------------|-------------|--------------|-----------|
| 1 <input type="checkbox"/>                                                                                       | 192.168.7.120 | 5000        | 6000         | TCP + UDP |
| <input type="checkbox"/> Select All (Note: maximum rule count is 20)                                             |               |             |              |           |
| <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Add New"/> |               |             |              |           |

**Figure 30** 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).

#### DMZ Settings

|                                      |                      |
|--------------------------------------|----------------------|
| DMZ                                  | Disabled ▼           |
| DMZ IP Address                       | <input type="text"/> |
| <input type="button" value="Apply"/> |                      |

Figure 31 DMZ page

#### DMZ Settings

|                                      |               |
|--------------------------------------|---------------|
| DMZ                                  | Enabled ▼     |
| DMZ IP Address                       | 192.168.7.178 |
| <input type="button" value="Apply"/> |               |

Figure 32 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.

#### UPnP Settings

|                                      |                                      |
|--------------------------------------|--------------------------------------|
| UPnP                                 | Disabled ▼                           |
| <input type="button" value="Apply"/> | <input type="button" value="Reset"/> |

Figure 33 UPnP page

### 4.4.2.8 Dynamic DNS

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

**DDNS Settings**

|                                      |                          |
|--------------------------------------|--------------------------|
| DDNS Status                          | Disabled                 |
| Dynamic DNS Provider                 | Disabled ▼               |
| User Name                            | <input type="text"/>     |
| Password                             | <input type="password"/> |
| Domain Name                          | <input type="text"/>     |
| <input type="button" value="Apply"/> |                          |

**Figure 34** 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.

**VPN Passthrough**

|                                      |           |
|--------------------------------------|-----------|
| L2TP Passthrough                     | Enabled ▼ |
| IPSec Passthrough                    | Enabled ▼ |
| PPTP Passthrough                     | Enabled ▼ |
| <input type="button" value="Apply"/> |           |

**Figure 35** 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.

### Network Management

|                                      |            |
|--------------------------------------|------------|
| Remote management (http)             | Disabled ▼ |
| HTTP Login (WebUI Management)        | Enabled ▼  |
| HTTPS Login (WebUI Management)       | Disabled ▼ |
| Respond to PING on WAN               | Disabled ▼ |
| Respond to PING on LAN               | Disabled ▼ |
| <input type="button" value="Apply"/> |            |

Figure 36 Network Management

## 4.4.3 Advanced Settings

From this page, you can see Routing, NTP, Backup & Restore, Diagnostic, USB PD, Scheduled Reboot and Log Management.

Basic Settings

Security Settings

Advanced Settings

Routing

NTP

Backup & Restore

Diagnostic

USB PD

Scheduled Reboot

Log Management

Rule table

| No. | Destination     | Netmask         | Gateway   | Interface    |
|-----|-----------------|-----------------|-----------|--------------|
| 1   | 0.0.0.0         | 0.0.0.0         | 10.28.2.1 | WAN1(eth2.2) |
| 2   | 10.28.2.0       | 255.255.255.0   | 0.0.0.0   | WAN1(eth2.2) |
| 3   | 192.168.7.0     | 255.255.255.0   | 0.0.0.0   | LAN(br0)     |
| 4   | 239.255.255.250 | 255.255.255.255 | 0.0.0.0   | LAN(br0)     |

(maximum alert10)

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.

Rule table

| No. | Destination     | Netmask         | Gateway   | Interface    |
|-----|-----------------|-----------------|-----------|--------------|
| 1   | 0.0.0.0         | 0.0.0.0         | 10.28.2.1 | WAN1(eth2.2) |
| 2   | 10.28.2.0       | 255.255.255.0   | 0.0.0.0   | WAN1(eth2.2) |
| 3   | 192.168.7.0     | 255.255.255.0   | 0.0.0.0   | LAN(br0)     |
| 4   | 239.255.255.250 | 255.255.255.255 | 0.0.0.0   | LAN(br0)     |

(maximum alert10)

Figure 38 Routing table

#### Static Routing Settings

|                                      |                                   |
|--------------------------------------|-----------------------------------|
| Destination                          | <input type="text"/>              |
| Range                                | <input type="text" value="Host"/> |
| Gateway                              | <input type="text"/>              |
| Interface                            | <input type="text" value="LAN"/>  |
| <input type="button" value="Apply"/> |                                   |

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 Interval synchronization. When the device obtains the WAN IP, the current time will synchronize with the NTP server automatically.

### NTP Settings

|                                                      |                                                                                    |                |
|------------------------------------------------------|------------------------------------------------------------------------------------|----------------|
| Current Time                                         | Wed Jan 01 21:13:11 UTC                                                            | Sync with host |
| Time Zone:                                           | (GMT-08:00) Pacific Time ▼                                                         |                |
| NTP Server                                           | sn.pool.ntp.org<br>e.g.:time.stdtime.gov.tw<br>time.nist.gov<br>ntp0.broad.mit.edu |                |
| Interval synchronization<br>(hours of range 1 - 300) | 24                                                                                 |                |
| <div>Apply</div> <div>Cancel</div>                   |                                                                                    |                |

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.

#### Backup & Restore Settings

|                                                   |                                        |
|---------------------------------------------------|----------------------------------------|
| <input type="checkbox"/> Need password to backup  | <div></div> <div>(32 characters)</div> |
| Backup device configuration                       | <div>Backup</div>                      |
| <input type="checkbox"/> Need password to restore | <div></div> <div>(32 characters)</div> |
| Restore device configuration from file            | <div>选择文件</div> 未选择文件                  |
| <div>Restore</div>                                |                                        |

Figure 41 Backup & Restore

### 4.4.3.4 Diagnostic

There are 2 function on this page. Ping and Traceroute

**Diagnostic Tool**

Choose Operation :

☒ Ping ☐ Traceroute

Host :

**Figure 42** Diagnostic

### 4.4.3.5 USB PD

From this page, you can choose direction Power-in or Power-out.

**USB PD Power Direction**

Direction

**Figure 43** USB PD

### 4.4.3.6 Scheduled Reboot Settings

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.

**Scheduled Reboot Settings**

Status

Date

☐ Every day ☐ Every week ☒ Every monthDay of month 

Time

At a defined time  h  min.**Figure 44** Enable Scheduled Reboot Setting

## 4.4.4 Log Management

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

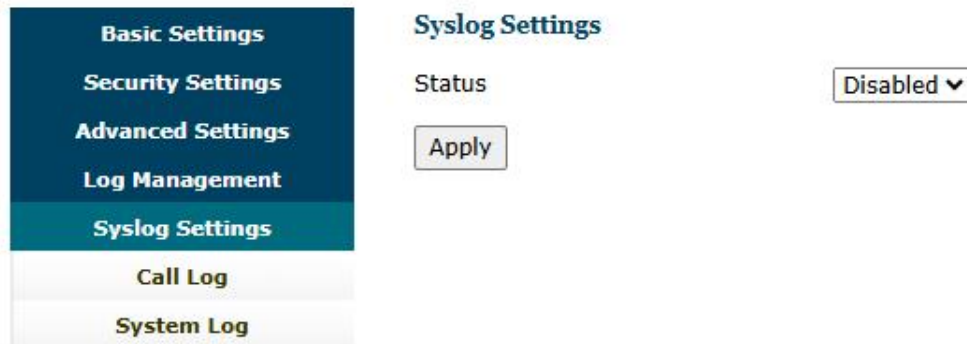


Figure 45 Log Management

### 4.4.4.1 Syslog Settings

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

**Syslog Settings**

|                                      |                      |
|--------------------------------------|----------------------|
| Status                               | Enabled ▼            |
| Log Type                             | ALL ▼                |
| Remote Server Address (IP or URL)    | <input type="text"/> |
| Remote Server Port                   | 514                  |
| Proto                                | UDP ▼                |
| <input type="button" value="Apply"/> |                      |

Figure 46 Syslog Settings

### 4.4.4.2 Call Log

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

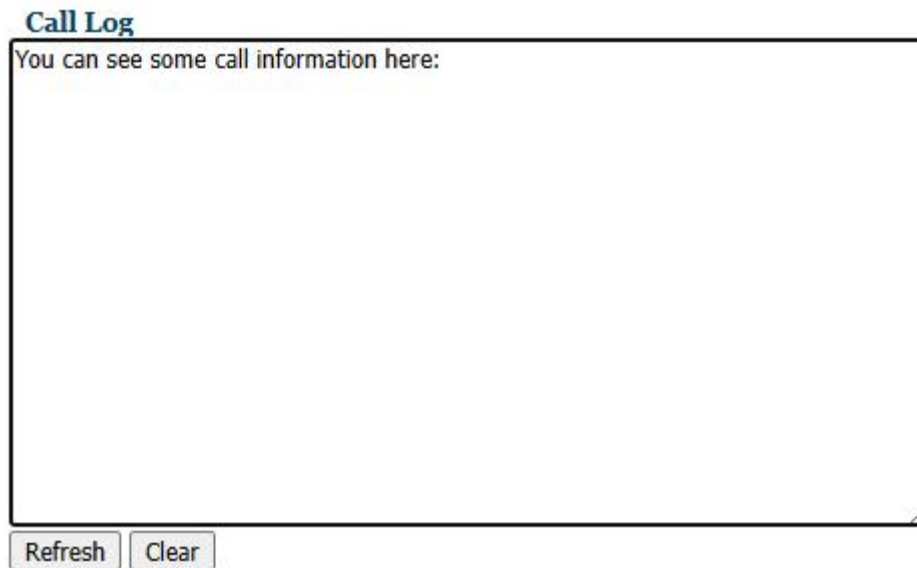


Figure 47 Call Log

#### 4.4.4.3 System Log

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

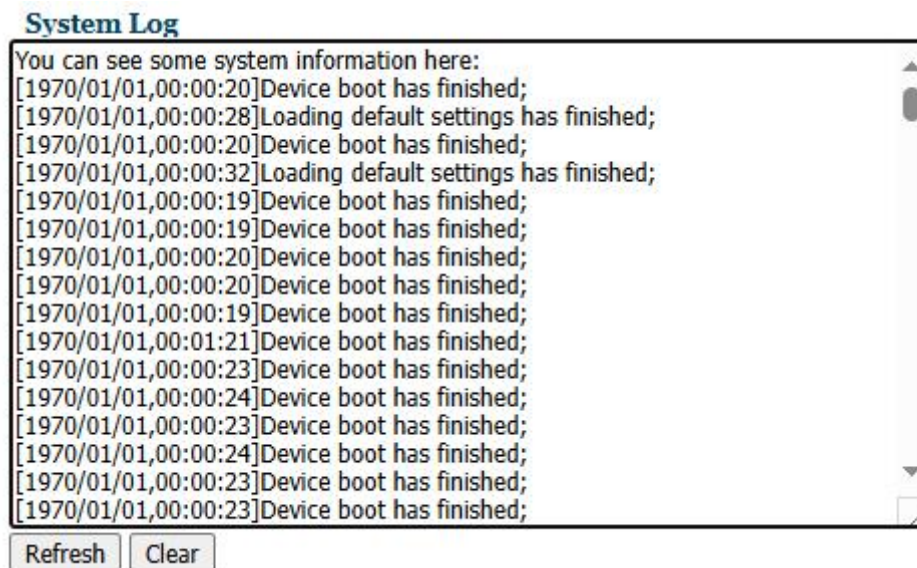


Figure 48 System Log

## 4.5 FXS

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

| Dashboard | Status | Settings | FXS | Network |
|-----------|--------|----------|-----|---------|
|-----------|--------|----------|-----|---------|

|                            |                                                                       |
|----------------------------|-----------------------------------------------------------------------|
| <b>VoIP Settings</b>       | <b>Account</b>                                                        |
| <b>Account Settings</b>    | <a href="#">Automatic Configuration</a>                               |
| FXS Basic Settings         | Start Port Num <input type="text"/> End Port Num <input type="text"/> |
| FXS Advance Settings       | Display Name <input type="text"/> Phone Number <input type="text"/>   |
| SIP Settings               | Account <input type="text"/> Password <input type="text"/>            |
| VoIP QoS                   |                                                                       |
| Port Group                 |                                                                       |
| <b>VoIP Phone Settings</b> |                                                                       |

| Port  | Display Name         | Phone Number         | Account              | Password             | Enable                   |
|-------|----------------------|----------------------|----------------------|----------------------|--------------------------|
| FXS 1 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 2 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 3 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 4 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 5 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 6 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 7 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 8 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

Figure 49 FXS

## 4.5.1 VoIP Settings

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

|                            |                                                                       |
|----------------------------|-----------------------------------------------------------------------|
| <b>VoIP Settings</b>       | <b>Account</b>                                                        |
| <b>Account Settings</b>    | <a href="#">Automatic Configuration</a>                               |
| FXS Basic Settings         | Start Port Num <input type="text"/> End Port Num <input type="text"/> |
| FXS Advance Settings       | Display Name <input type="text"/> Phone Number <input type="text"/>   |
| SIP Settings               | Account <input type="text"/> Password <input type="text"/>            |
| VoIP QoS                   | <input type="button" value="Set"/>                                    |
| Alarm Settings             | Start Port Num <input type="text"/> End Port Num <input type="text"/> |
| <b>VoIP Phone Settings</b> | <input type="button" value="Clear"/>                                  |

[Manual Configuration](#)

| Port  | Display Name         | Phone Number         | Account              | Password             | Enable                   |
|-------|----------------------|----------------------|----------------------|----------------------|--------------------------|
| FXS 1 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 2 | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |

Figure 50 VoIP Settings

### 4.5.1.1 Account Settings

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

#### Account

##### Automatic Configuration

|                                      |                      |              |                      |
|--------------------------------------|----------------------|--------------|----------------------|
| Start Port Num                       | <input type="text"/> | End Port Num | <input type="text"/> |
| Display Name                         | <input type="text"/> | Phone Number | <input type="text"/> |
| Account                              | <input type="text"/> | Password     | <input type="text"/> |
| <input type="button" value="Set"/>   |                      |              |                      |
| Start Port Num                       | <input type="text"/> | End Port Num | <input type="text"/> |
| <input type="button" value="Clear"/> |                      |              |                      |

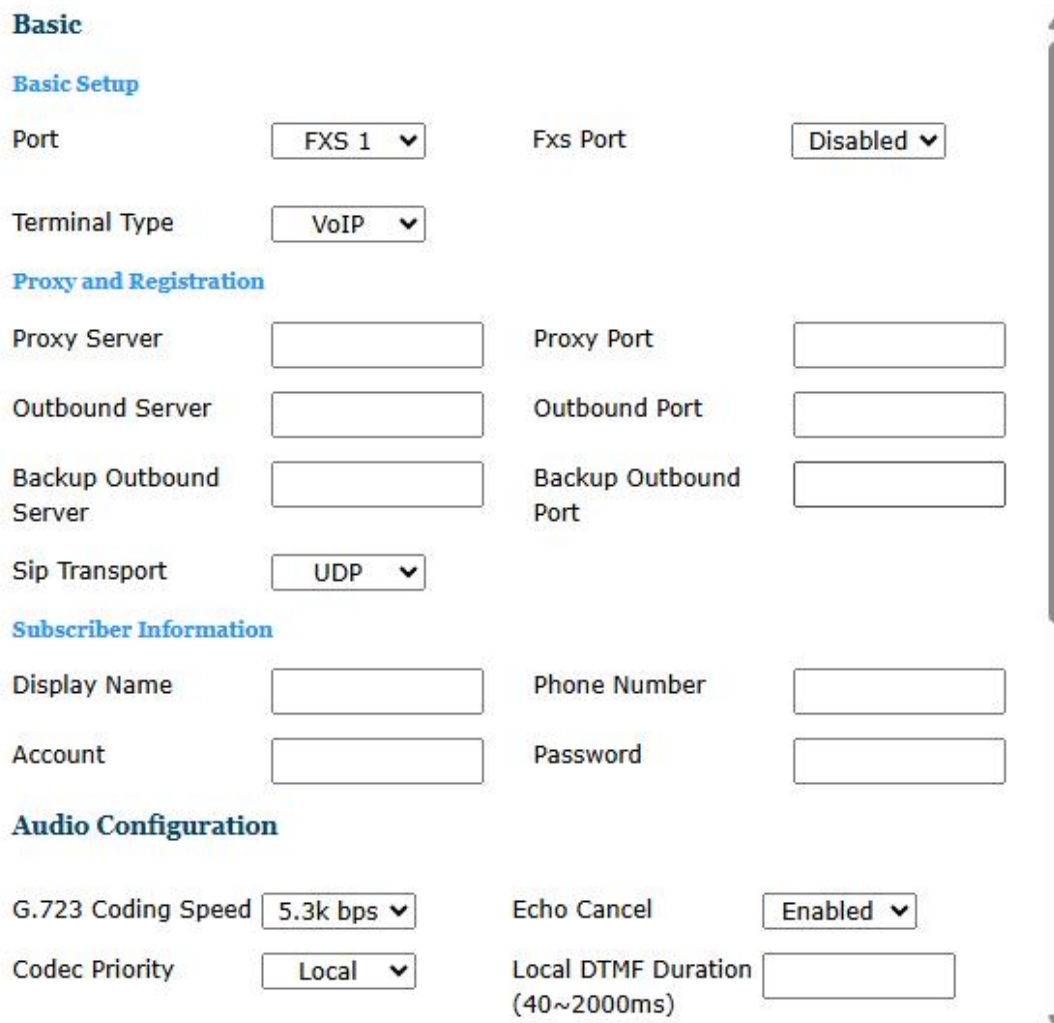
##### Manual Configuration

| Port                                 | Display Name                          | Phone Number         | Account              | Password             | Enable                   |
|--------------------------------------|---------------------------------------|----------------------|----------------------|----------------------|--------------------------|
| FXS 1                                | <input type="text"/>                  | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| FXS 2                                | <input type="text"/>                  | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="checkbox"/> |
| <input type="button" value="Apply"/> | <input type="button" value="Cancel"/> |                      |                      |                      |                          |

**Figure 51** Account Settings

### 4.5.1.2 FXS Basic Settings

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



**Basic**

**Basic Setup**

Port  Fxs Port

Terminal Type

**Proxy and Registration**

Proxy Server  Proxy Port

Outbound Server  Outbound Port

Backup Outbound Server  Backup Outbound Port

Sip Transport

**Subscriber Information**

Display Name  Phone Number

Account  Password

**Audio Configuration**

G.723 Coding Speed  Echo Cancel

Codec Priority  Local DTMF Duration (40~2000ms)

Figure 52 FXS Basic Settings

### 4.5.1.3 FXS Advance Settings

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

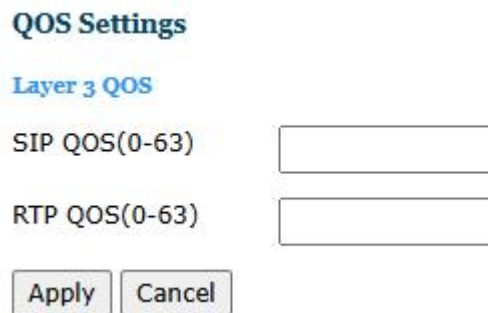
**Advanced****Select Port**Port **SIP Advanced Setup**Carry Port Information DTMF Type RFC2833 Payload(>=96) Call Waiting Caller ID Session Refresh Time(sec) Refresher Initial Reg With Authorization Primary Server Detect Interval NAT Keep-alive Interval(10-60s) Proxy DNS Type Signal Port Register Refresh Interval(sec) Remove Last Reg Min Session Timer(sec) Enable SIP OPTIONS Reply 182 On Call Waiting Max Detect Fail Count **Figure 53** FXS Advance Settings**4.5.1.4 SIP Settings**

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

**SIP Parameters**SIP T1(ms)  SIP User Agent Name Max Auth  Reg Retry Intvl (sec) **NAT Traversal**NAT Traversal  STUN Server Address NAT Refresh Interval (sec)  STUN Server Port  **Figure 54** SIP Settings

### 4.5.1.5 VoIP QoS

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



**QOS Settings**

**Layer 3 QOS**

SIP QOS(0-63)

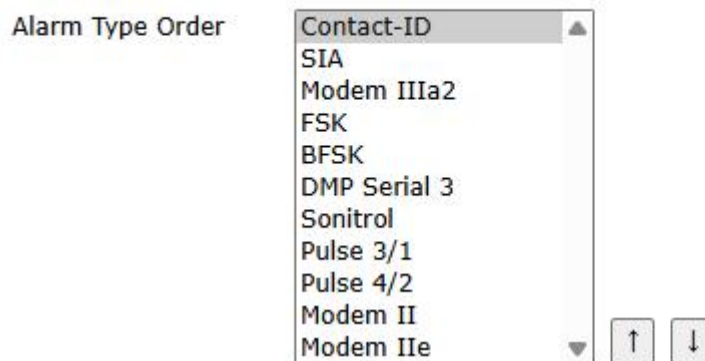
RTP QOS(0-63)

Figure 55 VoIP QoS

### 4.5.1.6 Alarm Settings

On this page, you can set alarm settings.

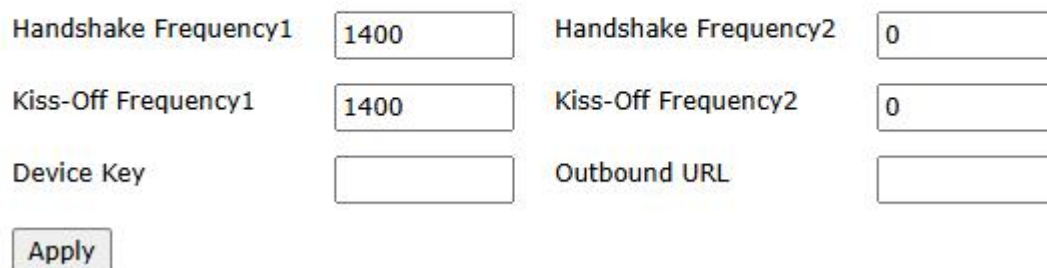
#### Alarm Settings



Alarm Type Order

- Contact-ID
- SIA
- Modem IIIa2
- FSK
- BFSK
- DMP Serial 3
- Sonitrol
- Pulse 3/1
- Pulse 4/2
- Modem II
- Modem IIe

#### Common Parameters



Handshake Frequency1  Handshake Frequency2

Kiss-Off Frequency1  Kiss-Off Frequency2

Device Key  Outbound URL

Figure 56 Alarm Settings

## 4.5.2 VoIP Phone Settings

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

**VoIP Settings**  
VoIP Phone Settings  
Phone Preferences Settings

**Preferences**

**Volume Settings**

Handset Input Gain

Port Volume Controls(Input 20~-40db)

Port Volume Controls(Output 20~-40db)

DTMF Volume Level(0~-20dbm)

DTMF Volume Twist(1~3dbm)

**Regional**

Tone Type

Dial Tone

Busy Tone

Ring Back Tone

Call Waiting Tone

Ringing Cadence

Min Jitter Delay (0~120ms)  Max Jitter Delay (0~120ms)

Figure 57 VoIP Phone Settings

## 4.6 Network

From this page, you can see WAN Settings, LTE Settings WiFi Settings and LAN Settings.

**Dashboard** **Status** **Settings** **FXS** **Network**

**WAN Settings**  
WAN Setting  
POE Output Voltage  
LTE Settings  
WiFi Settings  
LAN Settings

**WAN Setting**

WAN Mode

Main WAN

Back up WAN

ICMP DETECTION SERVER

ICMP DETECTION BACKUP SERVER

ICMP Detection Interval  Seconds

ICMP Detection Timeout  Seconds

ICMP Detection Retries

Figure 58 Network

## 4.6.1 WAN Settings

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

|                                      |                |
|--------------------------------------|----------------|
| <b>WAN Setting</b>                   |                |
| WAN Mode                             | Hot Failover ▼ |
| Main WAN                             | ETH WAN1 ▼     |
| Back up WAN                          | ETH WAN2 ▼     |
| ICMP DETECTION SERVER                | 8.8.8.8        |
| ICMP DETECTION BACKUP SERVER         | 1.1.1.1        |
| ICMP Detection Interval              | 60 Seconds     |
| ICMP Detection Timeout               | 10 Seconds     |
| ICMP Detection Retries               | 2              |
| <input type="button" value="Apply"/> |                |

Figure 59 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.

|                                      |                |
|--------------------------------------|----------------|
| <b>WAN Setting</b>                   |                |
| WAN Mode                             | Hot Failover ▼ |
| Main WAN                             | ETH WAN1 ▼     |
| Back up WAN                          | ETH WAN2 ▼     |
| ICMP DETECTION SERVER                | 8.8.8.8        |
| ICMP DETECTION BACKUP SERVER         | 1.1.1.1        |
| ICMP Detection Interval              | 60 Seconds     |
| ICMP Detection Timeout               | 10 Seconds     |
| ICMP Detection Retries               | 2              |
| <input type="button" value="Apply"/> |                |

Figure 60 WAN Setting

### 4.6.1.2 POE Output Voltage

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

**POE Output Voltage**

WAN1 PoE Voltage Disabled ▾

WAN2 PoE Voltage Disabled ▾

WAN1 Cycle Time 12V (0 ~ 3600)

WAN2 Cycle Time 24V (0 ~ 3600)

Apply

Figure 61 POE Output Voltage

## 4.6.2LTE Settings

From this page, you can see SIM Switch, APN Settings.

**WAN Settings**

**LTE Settings**

**SIM Switch**

**APN Settings**

**PIN Management**

**WiFi Settings**

**LAN Settings**

**Switch SIM Card**

SIM Auto Switch Enable ▾

SIM Card mode SIM1 ▾

Current SIM Card

**Internet Check**

URL or IP address to ping no.1 8.8.8.8

URL or IP address to ping no.2 1.1.1.1

Wait time between ping groups(sec) 60

Apply

Figure 62 LTE Settings

### 4.6.2.1 SIM Switch

From this page, you can switch SIM1 or SIM2.

**Switch SIM Card**

SIM Auto Switch Enable ▾

SIM Card mode SIM1 ▾

Current SIM Card SIM1  
SIM2

**Internet Check**

URL or IP address to ping no.1 8.8.8.8

URL or IP address to ping no.2 1.1.1.1

Wait time between ping groups(sec) 60

Apply

Figure 63 SIM Switch

#### 4.6.2.2 APN Settings

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

**Switch SIM Card**

Switch SIM Card SIM1 ▾

**SIM APN Settings**

Mode ☒ Auto ☐ Manual

Host Name ▾

Profile Name Auto

APN Auto

Authentication None ▾

User Name

Password

Set as default

Figure 64 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.

**Switch SIM Card**

Switch SIM Card SIM1 ▾

**SIM APN Settings**Mode ☐ Auto ☒ Manual

Host Name ▾ Add New

Profile Name internet

APN

Authentication None ▾

User Name

Password

Set as default

**Figure 65** Add New Configuration

## 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.

WAN Settings

LTE Settings

WiFi Settings

Wi-Fi 2.4GHz

Wi-Fi 5GHz

Wireless Block Users

Wi-Fi Guest

WWAN Hotspot

LAN Settings

Wi-Fi 2.4GHz Settings

Wi-Fi Status

Enabled

Wi-Fi Standard

11b/g/n mixed mode

Network Name (SSID)

POTSCAST\_BB99C6

Frequency (Channel)

Auto (Channel 6)

Broadcast SSID

☒Enabled ☐Disabled

Bandwidth

☐20 MHz ☒20/40 MHz

Wi-Fi 2.4GHz Security

Security Mode

WPA2-PSK

WPA Algorithms

☐TKIP ☒AES ☐TKIP/AES

Password

RHYpQHb9

Key Renewal Interval

3600

 Seconds (0 ~ 4194302)

Wi-Fi 2.4GHz QR Code



Apply

Clear

Figure 66 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.

**Wi-Fi 2.4GHz Settings**

Wi-Fi Status

Wi-Fi Standard

Network Name (SSID)

Frequency (Channel)

Broadcast SSID ☒ Enabled ☐ Disabled

Bandwidth ☐ 20 MHz ☒ 20/40 MHz

**Wi-Fi 2.4GHz Security**

Security Mode

WPA Algorithms ☐ TKIP ☒ AES ☐ TKIP/AES

Password

Key Renewal Interval  Seconds (0 ~ 4194302)

**Wi-Fi 2.4GHz QR Code**



Figure 67 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".

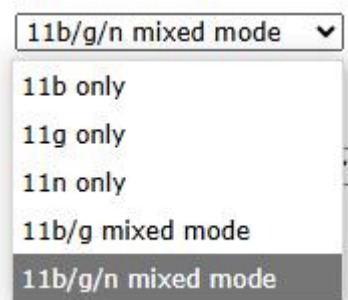


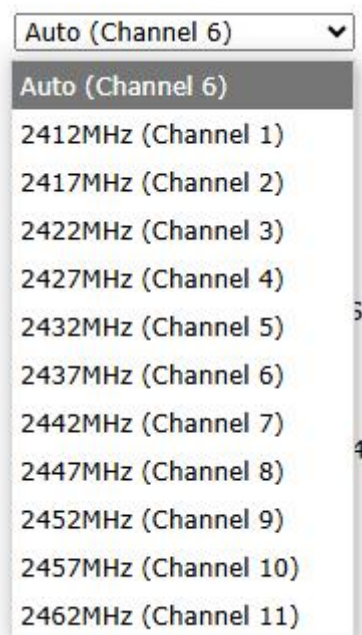
Figure 68 WiFi 2.4G Standard

- **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 69** 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.

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

**Wi-Fi 2.4GHz Security**

Security Mode

WPA Algorithms ☐ TKIP ☒ AES ☐ TKIP/AES

Password

Key Renewal Interval  Seconds (0 ~ 4194302)

**Wi-Fi 2.4GHz QR Code**



**Figure 70** 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 165, configure broadcast SSID and bandwidth.

**Wi-Fi 5GHz Settings**

|                     |                                                                                                            |
|---------------------|------------------------------------------------------------------------------------------------------------|
| Wi-Fi Status        | <input type="button" value="Enabled"/>                                                                     |
| Wi-Fi Standard      | <input type="button" value="11n/ac mixed mode"/>                                                           |
| Network Name (SSID) | <input type="text" value="POTSCAST_5G_BB99C6"/>                                                            |
| Frequency (Channel) | <input type="button" value="Auto (Channel 52)"/>                                                           |
| Broadcast SSID      | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled                                    |
| Bandwidth           | <input type="radio"/> 20 MHz <input type="radio"/> 20/40 MHz <input checked="" type="radio"/> 20/40/80 MHz |

**Wi-Fi 5GHz Security**

|                      |                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------|
| Security Mode        | <input type="button" value="WPA2-PSK"/>                                                        |
| WPA Algorithms       | <input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES |
| Password             | <input type="text" value="RHYpQHb9"/>                                                          |
| Key Renewal Interval | <input type="text" value="3600"/> Seconds(0 ~ 4194302)                                         |

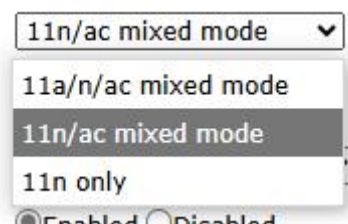
**Wi-Fi 5GHz QR Code****Figure 71** WiFi 5GHz Settings

- **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".

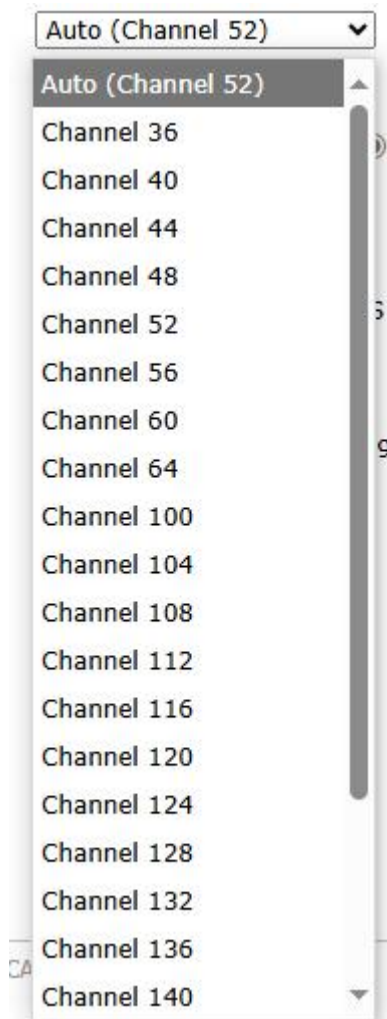
**Figure 72** WiFi 5GHz standard

- **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 73** 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.

**Wi-Fi 5GHz Security**

Security Mode: WPA2-PSK

WPA Algorithms: ☐ TKIP ☒ AES ☐ TKIP/AES

Password: RHYpQHb9

Key Renewal Interval: 3600 Seconds(0 ~ 4194302)

**Wi-Fi 5GHz QR Code**

Apply Clear

**Figure 74** 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.

**Connected Wireless Users**

| ID                                     | Hostname | IP Address | MAC Address | MCS | RSSI0 | RSSI1 | Select                               |
|----------------------------------------|----------|------------|-------------|-----|-------|-------|--------------------------------------|
| <input type="button" value="Refresh"/> |          |            |             |     |       |       | <input type="button" value="Block"/> |

**Block Wireless Users**

Please select MAC Address of Wi-Fi client device to restore:

| ID | MAC Address | Select                                 |
|----|-------------|----------------------------------------|
|    |             | <input type="button" value="Restore"/> |

**Figure 75** WirelessBlock Users

#### 4.6.3.4 Wi-Fi Guest

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

**Wi-Fi Guest 2.4GHz Settings**  
Wi-Fi Status

**Wi-Fi Guest 5GHz Settings**  
Wi-Fi Status

**Figure 76** 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.

**Selected Hotspot**

SSID

Password

Status

Disconnected

Connect

**Wi-Fi Scan Results**

| No. | SSID                 | AuthMode      | EncryptType | Signal | Select                |
|-----|----------------------|---------------|-------------|--------|-----------------------|
| 1   | Guest_192477         | WPA2PSK       | AES         | Good   | <input type="radio"/> |
| 2   | TP-LINK_F438         | WPAPSKWPA2PSK | AES         | Good   | <input type="radio"/> |
| 3   | Atel_Guest           | OPEN          | NONE        | Poor   | <input type="radio"/> |
| 4   | GM200_3B97           | OPEN          | NONE        | Poor   | <input type="radio"/> |
| 5   | Atel_Staff           | WPA2          | AES         | Poor   | <input type="radio"/> |
| 6   | Atel_Guest           | OPEN          | NONE        | Poor   | <input type="radio"/> |
| 7   | Atel_Staff           | WPA2          | AES         | Poor   | <input type="radio"/> |
| 8   | Atel_Guest           | OPEN          | NONE        | Poor   | <input type="radio"/> |
| 9   | Atel_Staff           | WPA2          | AES         | Poor   | <input type="radio"/> |
| 10  | PW550_195407         | WPA2PSK       | AES         | Middle | <input type="radio"/> |
| 11  | MD310-880_MTN_9336CD | WPA2PSK       | AES         | Middle | <input type="radio"/> |
| 12  | LEGO                 | WPAPSKWPA2PSK | AES         | Good   | <input type="radio"/> |
| 13  | Wireless-N-2.4G-test | WPAPSKWPA2PSK | AES         | Good   | <input type="radio"/> |
| 14  | Atel_Staff           | WPA2          | AES         | Poor   | <input type="radio"/> |
| 15  | Atel_Guest           | OPEN          | NONE        | Poor   | <input type="radio"/> |

Figure 77 WWAN Hostport

## 4.6.4 LAN Settings

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

**LAN Settings**

|                  |                                            |                          |
|------------------|--------------------------------------------|--------------------------|
| IP Address       | <input type="text" value="192.168.7.1"/>   |                          |
| Subnet Mask      | <input type="text" value="255.255.255.0"/> |                          |
| DHCP             | <input type="text" value="Enabled"/>       |                          |
| Start IP Address | <input type="text" value="192.168.7.2"/>   |                          |
| End IP Address   | <input type="text" value="192.168.7.254"/> |                          |
| Lease Time       | <input type="text" value="86400"/>         |                          |
| Static IP 1      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 2      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 3      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 4      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 5      | MAC: <input type="text"/>                  | IP: <input type="text"/> |

**Figure 78** 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.

**LAN Settings**

|                  |                                            |                          |
|------------------|--------------------------------------------|--------------------------|
| IP Address       | <input type="text" value="192.168.7.1"/>   |                          |
| Subnet Mask      | <input type="text" value="255.255.255.0"/> |                          |
| DHCP             | <input type="button" value="Enabled"/> ▼   |                          |
| Start IP Address | <input type="text" value="192.168.7.2"/>   |                          |
| End IP Address   | <input type="text" value="192.168.7.254"/> |                          |
| Lease Time       | <input type="text" value="86400"/>         |                          |
| Static IP 1      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 2      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 3      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 4      | MAC: <input type="text"/>                  | IP: <input type="text"/> |
| Static IP 5      | MAC: <input type="text"/>                  | IP: <input type="text"/> |

Figure 79 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.

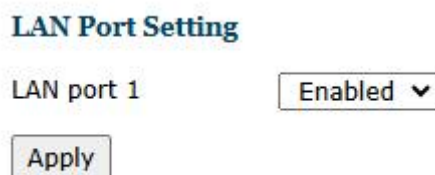
 **Note:**

- 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.



**Figure 80** 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       |
|--------|----------|---------------|------------|
| XPPan  | V1.0     | Initial Draft | 2025-05-09 |
|        |          |               |            |
|        |          |               |            |