

# 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

<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>5</b>
4.1    Login .....	5
4.2    Dashboard .....	6
4.3    Status .....	7
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 .....	10
4.4.2    Security .....	12
4.4.3    Advanced .....	22
4.4.4    Remote Management .....	28
4.4.5    Log Management .....	29
4.5    FXS .....	31
4.5.1    Voip Settings .....	31
4.5.2    VoIP Phone Settings .....	37
4.6    Network .....	39
4.6.1    WAN Settings .....	40
4.6.2    LTE Settings .....	41
4.6.3    WiFi Settings .....	44
4.6.4    LAN Settings .....	53
<b>5. Revision History .....</b>	<b>57</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.

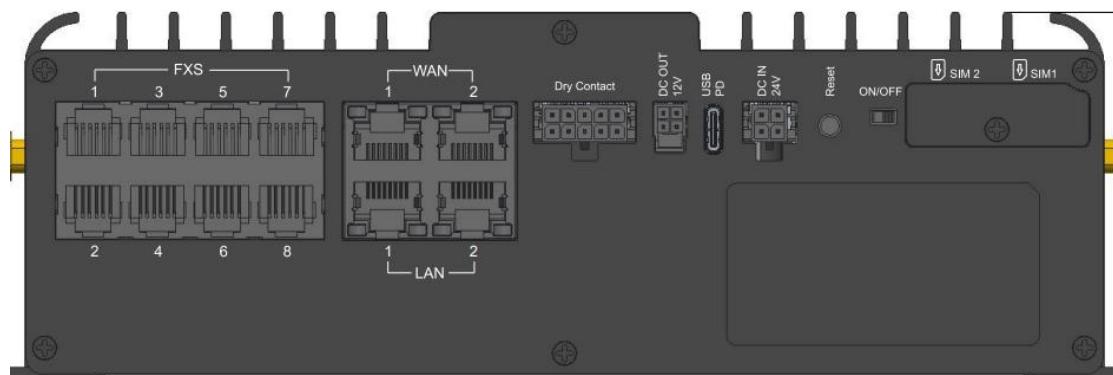
# 2. Product Overview

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

## 3.1 Ports and Buttons

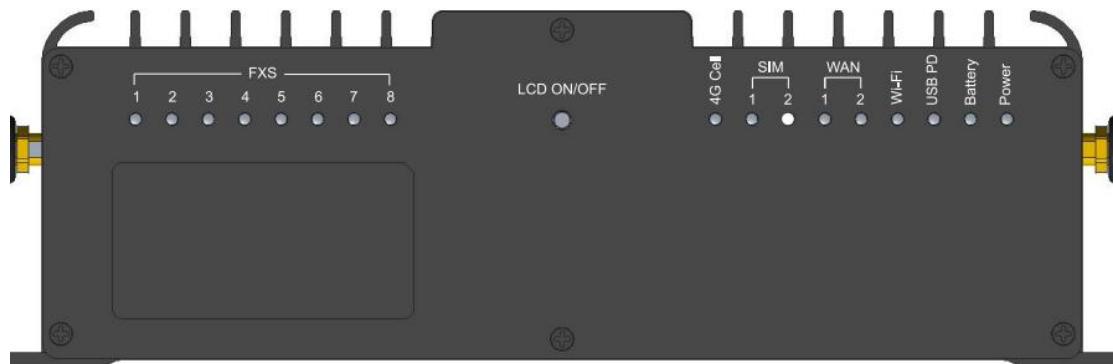


The following ports are located on the rear panel (refer above image from left to right)

Interfaces	One side:

	<ol style="list-style-type: none"> <li>1. FXS Port: Max 8 ports (2/4/6/8 ports is optional)</li> <li>2. WAN Port: *2 Gigabit port with Passive PoE</li> <li>3. LAN Port: *2 Gigabit port</li> <li>4. USB: Type-C</li> <li>5. SIM: Nano/4FF SIM card*2 (Physical SIM Port)</li> <li>6. Battery: Internal (Replaceable)</li> <li>7. 4 Pin UPS Power Out, 12V 3A Power Output</li> <li>8. DC Jack: for DC input</li> <li>9. LEDs indicator (see below and LED Indicator Definition)</li> <li>10. Reset button</li> <li>11. SMA: *5 (2/3/5 optional, default *2 for LTE ANT)</li> <li>12. ON/OFF key</li> <li>13. Dry connector connector</li> </ol>
--	--

### 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.

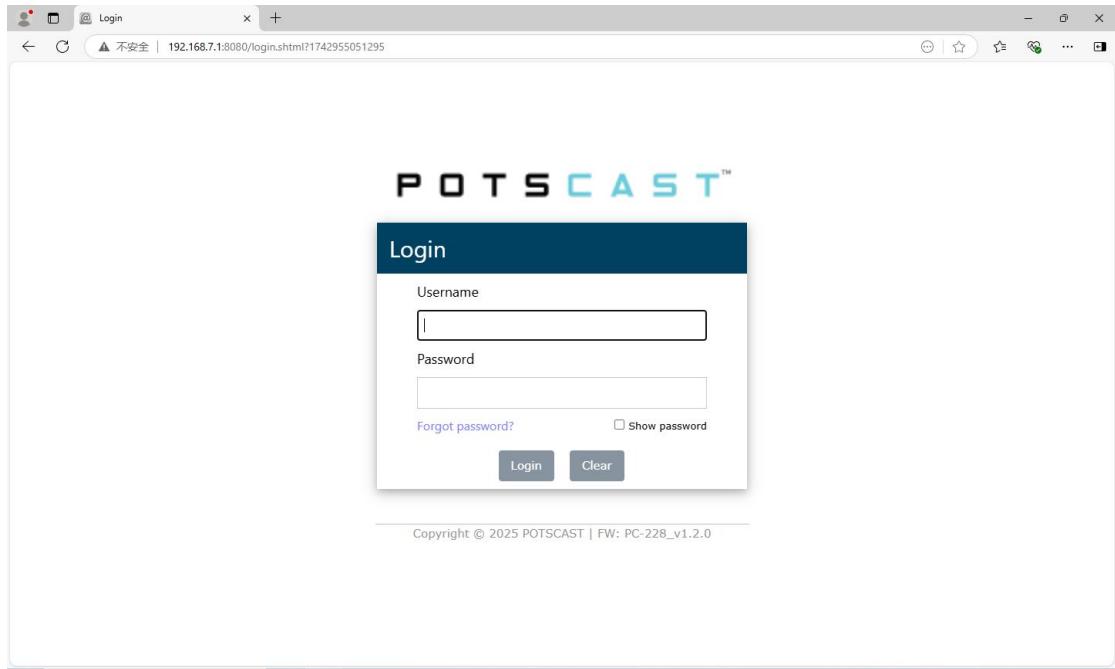
In the following sections, we will introduce you the main functions and the method of how to configure them.

### 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**



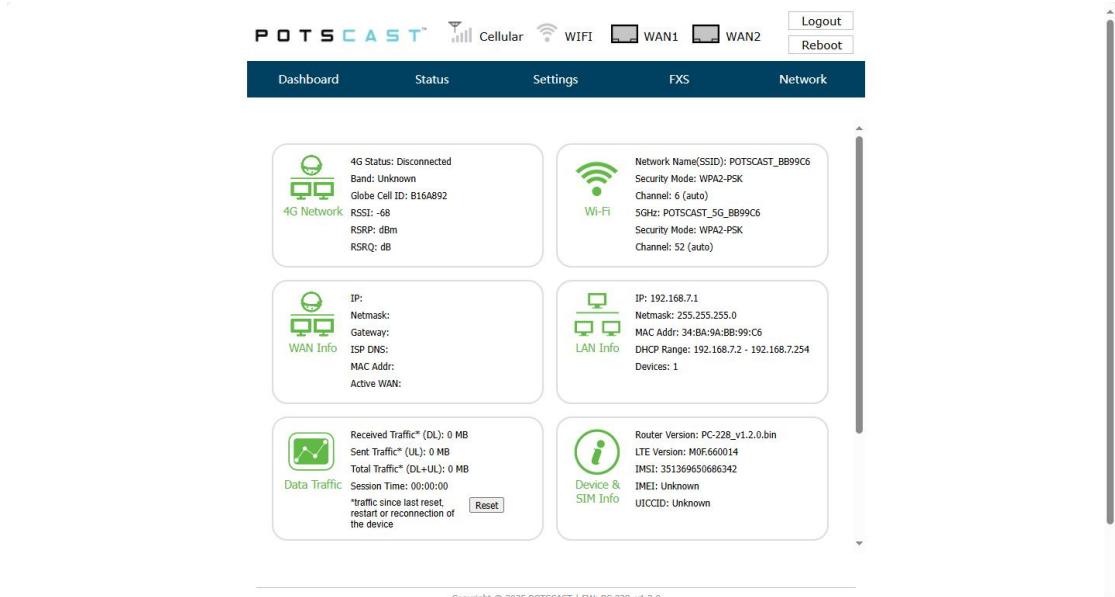
**Figure 1** Login Page

## 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.

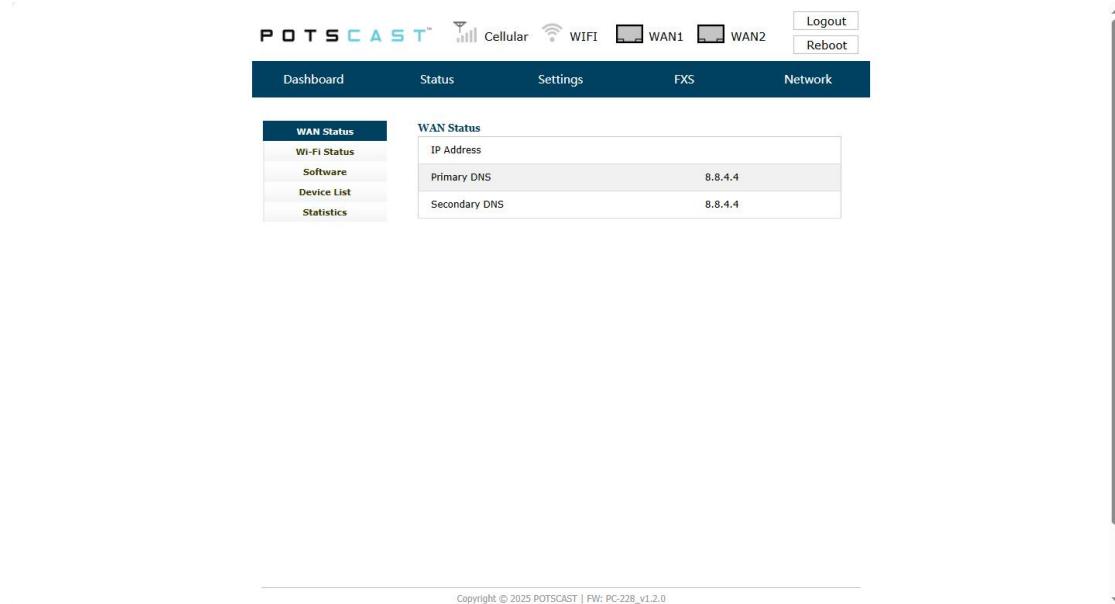
From this page, you can also know the Cellular network status and the LTE data transmission.



**Figure 2** Dashboard

## 4.3 Status

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

**Figure 3** Status

### 4.3.1 WAN Status

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

WAN Status	
Wi-Fi Status	
Software	
Device List	
Statistics	
WAN Status	
IP Address	
Primary DNS	8.8.4.4
Secondary DNS	8.8.4.4

**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_BB99C6
Device List	Frequency (Channel)	Auto (Channel 6)
Statistics	Security Mode	WPA2PSK
5 GHz Wi-Fi Status		
	Wi-Fi Status	Enabled
	Network Name (SSID)	POTSCAST_5G_BB99C6
	Frequency (Channel)	Auto (Channel 52)
	Security Mode	WPA2PSK

**Figure 5 WiFi Status**

### 4.3.3 Software

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

Dashboard	Status	Settings	FXS	Network
WAN Status	Software			
Wi-Fi Status	Router Software Version	PC-228_v1.2.0		
Software	Modem Software Version	M0F.660014		
Device List	MCU Version	V2012452432		
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 expires time.

WAN Status	Device List			
Wi-Fi Status	Hostname	MAC Address	IP Address	Type
Software	zhfei-pc2024	2C:16:DB:AB:DA:13	192.168.7.152	Ethernet
Device List				
Statistics				

**Figure 7 Device List**

## 4.3.5 Statistics

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

WAN Status	Statistics							
Wi-Fi Status	Download		Upload					
Software	LTE Speed	0 Kb/s						
Device List								
Statistics	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, Remote Management and Log Management.

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

**Figure 9** Settings

## 4.4.1 Basic

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

Basic Settings  
 Management  
 Software Upgrade  
 Remote Upgrade  
 Security Settings  
 Advanced Settings  
 Remote Management  
 Log Management

**UI Access Settings**

Username	admin
Current Admin Access Password	<input type="password"/> <input type="checkbox"/> Show password (32 characters max.)
New Admin Access Password	<input type="password"/> <input type="checkbox"/> Show password (32 characters max.)
Repeat Admin Access Password	<input type="password"/> <input type="checkbox"/> Show password (32 characters max.)

Apply

Clear

**UI Control Settings**

Allow Concurrent Logins	<input type="button" value="Enabled ▾"/>
WebUI Timeout	<input type="text" value="5"/> Minutes

Apply

**Factory Reset**

Click button to restore default settings	<input type="button" value="Restore"/>
--	--

Click button to reboot the device

Reboot

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.

Basic Settings

Management

Software Upgrade

Remote Upgrade

Security Settings

Advanced Settings

Remote Management

Log Management

**UI Access Settings**

Username	admin
Current Admin Access Password	<input type="password"/> <input type="checkbox"/> Show password (32 characters max.)
New Admin Access Password	<input type="password"/> <input type="checkbox"/> Show password (32 characters max.)
Repeat Admin Access Password	<input type="password"/> <input type="checkbox"/> Show password (32 characters max.)

Apply

Clear

**UI Control Settings**

Allow Concurrent Logins	<input type="button" value="Enabled ▾"/>
WebUI Timeout	<input type="text" value="5"/> Minutes

Apply

**Factory Reset**

Click button to restore default settings

Restore

**Device Reboot**

Click button to reboot the device

Reboot

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.

Dashboard

Status

Settings

FXS

Network

Basic Settings

Management

Software Upgrade

Remote Upgrade

Security Settings

Advanced Settings

Remote Management

Log Management

**Device Software Upgrade**

Router Upgrade:	<input type="file"/> 未选择文件
-----------------	----------------------------

Apply

**MCU Software Upgrade**

MCU Upgrade	<input type="file"/> 未选择文件
-------------	----------------------------

Apply

Figure 12 Software Upgrade

**Note:**

25/03/26

11

- 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.

Basic Settings		Device Remote Upgrade	
Management	Upgrade Status	Waiting for network connection	
Software Upgrade	Remote Upgrade	Enabled	
Remote Upgrade	Upgrade Address (IP or URL)		
Security Settings	Upgrade Mode	No traffic (No traffic for ten minutes)	
Advanced Settings	Manual	Check	Upgrade
Remote Management	Apply		
Log Management			

Figure 13 Remote Upgrade

#### 4.4.2 Security

##### 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 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.

**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	-

(Note: maximum rule count is 10)

**Mac Filtering Schedule**

Schedule

Disabled **Figure 15** Enable MAC Filtering Function**Add Rule**MAC Address 

Action

Drop **Figure 16** Add Rule**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
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

Disabled

**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.

**IP/Port Filtering Settings**

IP/Port Filtering	Enabled
Default policy - the device that don't match any rule would be:	Dropped
<b>Apply</b>	

**Time Rule table**

ID	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action
Others would be dropped						

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

**Figure 18** IP/Port filtering page

**IP/Port Filtering Settings**

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

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

**Figure 20** Add New Rule

**IP/Port Filtering Settings**

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

**Content Filtering Rule Table**

ID	URL Address or Keyword	Select
<input type="button" value="Delete"/>	<input type="button" value="Add New"/>	Note: maximum rule count is 8

**Content Filtering Schedule**

Schedule	<input type="button" value="Disabled ▼"/>
<input type="button" value="Apply"/>	

**Figure 22 Content Filtering**

**Content Filtering Rule Table**

ID	URL Address or Keyword	Select
<input type="button" value="Delete"/> <input type="button" value="Add New"/> Note: maximum rule count is 8		

**Content Filtering Schedule**

Schedule	<input type="button" value="Enabled"/>
Date	<input checked="" type="checkbox"/> Every day
Time	<input checked="" type="radio"/> 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	
<input type="radio"/> At a defined time    From <input type="button" value="00"/> h <input type="button" value="00"/> min.    To <input type="button" value="00"/> h <input type="button" value="00"/> min.	
<input type="button" value="Apply"/>	

**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.

**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 24** Port Forwarding page

**Port Forwarding Settings**

Port Forwarding	Enabled	▼
IP Address		
Port Range	-	
Protocol	TCP&UDP	
Comment		
<input type="button" value="Apply"/> <input type="button" value="Back"/>		

**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.

**Port Forwarding Rule Table**

ID	IP Address	Port Range	Protocol	Comment
1 <input type="checkbox"/>	192.168.7.120	5000 - 6000	TCP + UDP	

Select All (Note: 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.

Virtual Server Rule Table				
ID	IP Address	Public Port	Private Port	Protocol
1	192.168.1.100	80	8080	HTTP
<input type="checkbox"/> Select All	(Note: maximum rule count is 20)			
<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Add New</a>		

## Figure 27 Virtual Server page

**Virtual Server Settings**

IP Address	<input type="text"/>
Public Port	<input type="text"/>
Private Port	<input type="text"/>
Protocol	TCP&UDP

**Buttons**

**Apply** **Back**

**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.

Virtual Server Rule Table				
ID	IP Address	Public Port	Private Port	Protocol
1	192.168.7.120	5000	6000	TCP + UDP
<input type="checkbox"/> Select All	(Note: maximum rule count is 20)			
<a href="#">Edit</a>		<a href="#">Delete</a>	<a href="#">Add New</a>	

**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).

#### DMZ Settings

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

**Figure 30** DMZ page

#### DMZ Settings

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

**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.

#### UPnP Settings

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

**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.

**DDNS Settings**

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

**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.

**VPN Passthrough**

L2TP Passthrough	<input type="button" value="Enabled ▾"/>
IPSec Passthrough	<input type="button" value="Enabled ▾"/>
PPTP Passthrough	<input type="button" value="Enabled ▾"/>
<input type="button" value="Apply"/>	

**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.

**Network Management**

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

**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

**Parental Control**

Parental Control	<input type="button" value="Disable ▾"/>
------------------	--

**Figure 36** Parent Control**4.4.3 Advanced**

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

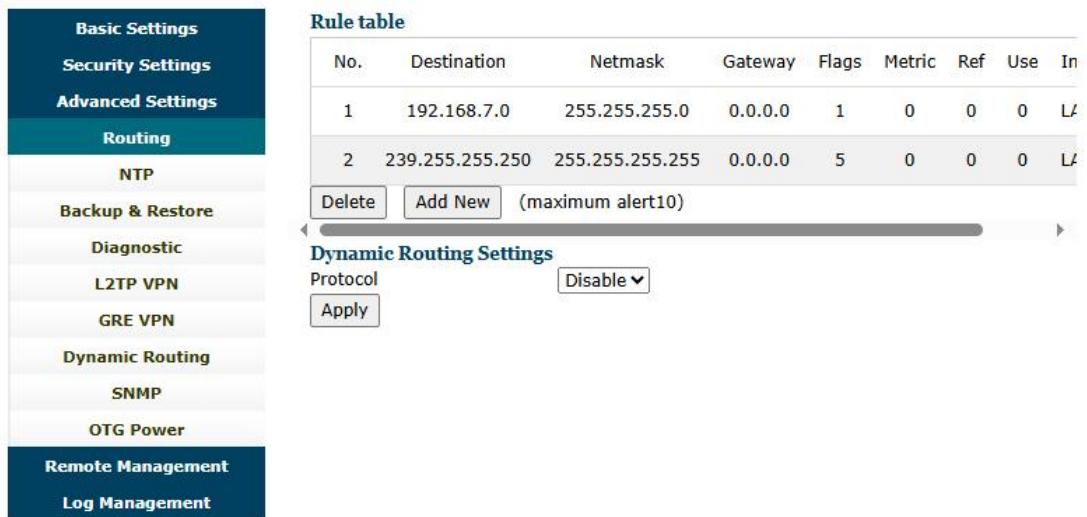


Figure 37 Advanced Settings

#### 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.

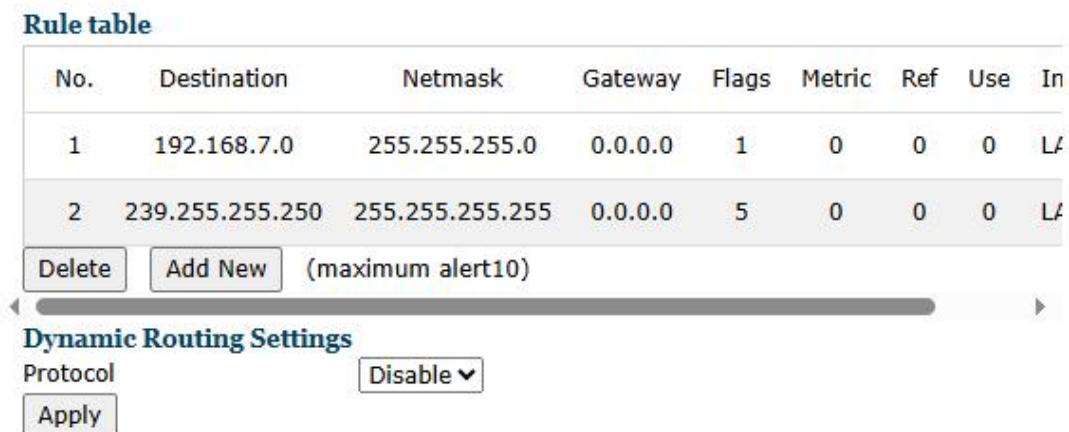


Figure 38 Routing

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

##### NTP Settings

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

**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**

Need password to backup   
(32 characters)

Backup device configuration

Need password to restore   
(32 characters)

Restore device configuration from file  未选择文件

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 L2TP VPN

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

**L2TP VPN**

Enable	<input type="button" value="Enable ▾"/>
Type	<input type="button" value="L2TPV2 ▾"/>
Mode	<input type="button" value="Client ▾"/>
Server Address	<input type="text"/>
Account	<input type="text"/>
Password	<input type="text"/>
Gateway	<input type="button" value="None ▾"/>
Client Connection Status	<input type="text"/>
<input type="button" value="Apply"/>	

**Figure 43** L2TP VPN

#### 4.4.3.6 GRE VPN

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

**GRE VPN**

GRE Status	<input type="button" value="Disabled ▾"/>
<input type="button" value="Apply"/>	

**Figure 44** GRE VPN

#### 4.4.3.7 Dynamic Routing

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

**Dynamic Routing Setting**

RIP Protocol:	<input type="button" value="Disable ▾"/>
Version	<input type="radio"/> RIPv1 <input type="radio"/> RIPv2
Authentication:	<input type="button" value="Text ▾"/>
Password:	<input type="text"/>
OSPF Protocol:	<input type="button" value="Disable ▾"/>
Router-ID	<input type="text"/>
Area	<input type="text"/>
<input type="button" value="Apply"/>	

**Figure 45** Dynamic Routing

#### 4.4.3.8 SNMP

From this page, you can Enable and Disable SNMP.

**SNMP Settings**

SNMP Service	<input type="button" value="Disable ▾"/>
<input type="button" value="Apply"/>	

**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.

**OTG Power Direction**

Direction	<input type="button" value="Power-in ▾"/>
<input type="button" value="Apply"/> <div style="border: 1px solid black; padding: 2px; display: inline-block; margin-left: 10px;"> <input style="background-color: #666; color: white; border: none; padding: 2px 10px; margin-bottom: 2px;" type="button" value="Power-in"/> <input style="border: none; padding: 2px 10px;" type="button" value="Power-out"/> </div>	

**Figure 47** WAN Mode Select

## 4.4.4 Remote Management

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

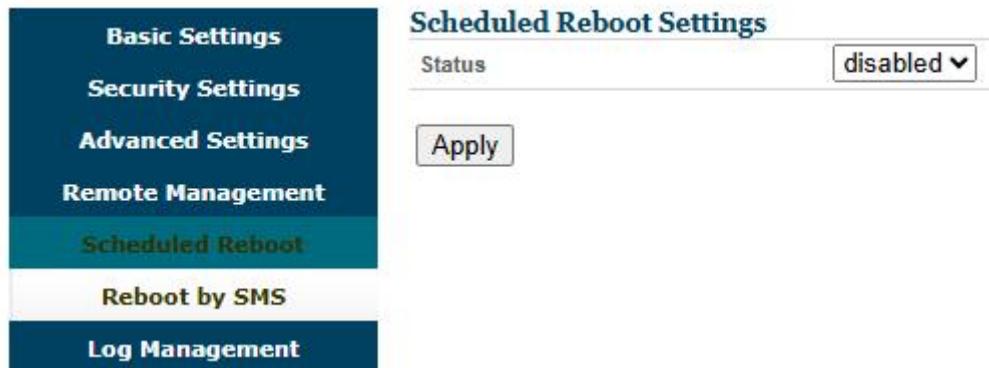


Figure 48 Remote Management

### 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.

The image shows the 'Scheduled Reboot Settings' configuration page. It includes fields for 'Status' (set to 'enabled'), 'reboot date' (set to 'every month'), and 'time' (with dropdowns for 'define time', 'reboot hour', and 'reboot minute'). An 'Apply' button is located at the bottom.

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” .

**SMS Reboot Setting**

Status	Enable <input type="button" value="▼"/>
Keyword	<input type="text"/>
<input type="button" value="Apply"/>	

**Figure 50** Reboot by SMS

## 4.4.5 Log Management

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

<a href="#">Basic Settings</a> <a href="#">Security Settings</a> <a href="#">Advanced Settings</a> <a href="#">Remote Management</a> <a href="#">Log Management</a> <b><a href="#">Syslog Settings</a></b>	<p><b>Syslog Settings</b></p> <table border="1"> <tr> <td>Status</td> <td>Disabled <input type="button" value="▼"/></td> </tr> <tr> <td colspan="2"><input type="button" value="Apply"/></td> </tr> </table>	Status	Disabled <input type="button" value="▼"/>	<input type="button" value="Apply"/>	
Status	Disabled <input type="button" value="▼"/>				
<input type="button" value="Apply"/>					
<a href="#">Call Log</a> <a href="#">System Log</a>					

**Figure 51** Log Management

### 4.4.5.1 Syslog Settings

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

**Syslog Settings**

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

**Figure 52** Syslog Settings

#### 4.4.5.2 Call Log

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

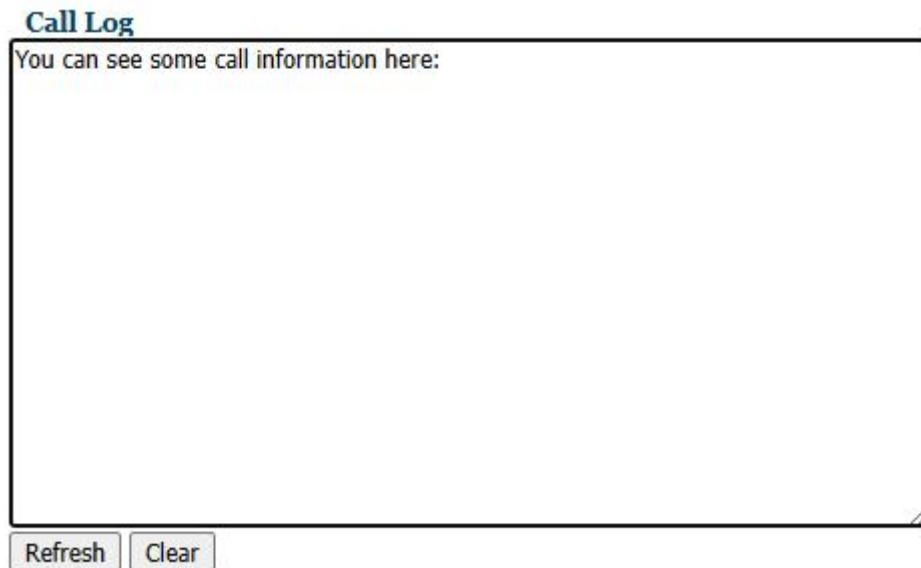


Figure 53 Call Log

#### 4.4.5.3 System Log

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

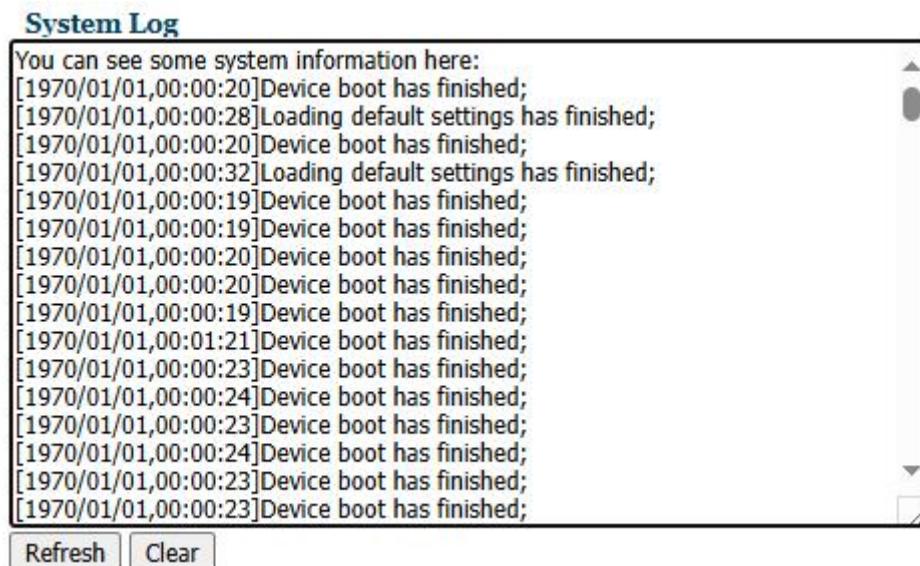


Figure 54 System Log

## 4.5 FXS

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

Dashboard	Status	Settings	FXS	Network																																																												
<b>VoIP Settings</b> <ul style="list-style-type: none"> <li><b>Account Settings</b> <ul style="list-style-type: none"> <li><b>FXS Basic Settings</b></li> <li><b>FXS Advance Settings</b></li> <li><b>SIP Settings</b></li> <li><b>VoIP QoS</b></li> <li><b>Port Group</b></li> </ul> </li> <li><b>VoIP Phone Settings</b></li> </ul>	<b>Account</b> <p><b>Automatic Configuration</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">Start Port Num</td> <td style="width: 20%;"><input type="text"/></td> <td style="width: 30%;">End Port Num</td> <td style="width: 20%;"><input type="text"/></td> </tr> <tr> <td>Display Name</td> <td><input type="text"/></td> <td>Phone Number</td> <td><input type="text"/></td> </tr> <tr> <td>Account</td> <td><input type="text"/></td> <td>Password</td> <td><input type="text"/></td> </tr> </table> <p><b>Port</b> <b>Display Name</b> <b>Phone Number</b> <b>Account</b> <b>Password</b> <b>Enable</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 10%;">FXS 1</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>FXS 2</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>FXS 3</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>FXS 4</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>FXS 5</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>FXS 6</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>FXS 7</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>FXS 8</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="checkbox"/></td> </tr> </table> <p><b>Apply</b> <b>Cancel</b></p>				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"/>	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"/>
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"/>																																																													
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 55** SMS

### 4.5.1 Voip Settings

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

VoIP Settings	<b>Account</b>					
Account Settings	<b>Automatic Configuration</b>					
FXS Basic Settings	Start Port Num		End Port Num			
FXS Advance Settings	Display Name		Phone Number			
SIP Settings	Account		Password			
VoIP QoS	Port	Display Name	Phone Number	Account	Password	Enable
Port Group	FXS 1					<input type="checkbox"/>
VoIP Phone Settings	FXS 2					<input type="checkbox"/>
	FXS 3					<input type="checkbox"/>
	FXS 4					<input type="checkbox"/>
	FXS 5					<input type="checkbox"/>
	FXS 6					<input type="checkbox"/>
	FXS 7					<input type="checkbox"/>
	FXS 8					<input type="checkbox"/>

**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"/>		
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 57** 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 1 <input type="button" value="▼"/>	Batch Settings	Disabled <input type="button" value="▼"/>
Port Enable	Enabled <input type="button" value="▼"/>	Outgoing Call	Enabled <input type="button" value="▼"/>
Missed Call Log	Enabled <input type="button" value="▼"/>		

**Proxy and Registration**

Proxy Server	<input type="text"/>	Proxy Port	<input type="text"/>
Outbound Server	<input type="text"/>	Outbound Port	<input type="text"/>
Back Outbound Server	<input type="text"/>	Back Outbound Port	<input type="text"/>
Sip Transport	UDP <input type="button" value="▼"/>		

**Subscriber Information**

Display Name	<input type="text"/>	Phone Number	<input type="text"/>
Account	<input type="text"/>	Password	<input type="text"/>

**Audio Configuration****Codec Setup**

Audio Codec Type 1	G.711U <input type="button" value="▼"/>	Audio Codec Type 2	G.711U <input type="button" value="▼"/>
Audio Codec Type 3	G.711U <input type="button" value="▼"/>	Audio Codec Type 4	G.711U <input type="button" value="▼"/>

**Figure 58** 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	FXS 1	Batch Settings	Disabled
------	-------	----------------	----------

**SIP Advanced Setup**

Carry Port Information	Disable	Signal Port	
DTMF Type	In-Band	Register Refresh Interval(sec)	
DTMF Negotiation	Disable	Remove Last Reg	Disable
RFC2883 Payload(>=96)		Min Session Timer(sec)	
Caller ID Header	FROM	Enable SIP OPTIONS	Disable
Session Refresh Time(sec)		Reply 182 On Call Waiting	Disable
Refresher	UAC	Max Detect Fail Count	
Initial Reg With Authorization	Disable		
Primary Server Detect Interval			
NAT Keep-alive Interval(10-60s)			

**Figure 59** FXS Advance Settings**4.5.1.4 SIP Settings**

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

**SIP Parameters**

**SIP Parameters**

SIP T1	<input type="text"/> (ms)		
SIP User Agent Name	<input type="text"/>	Max Auth	<input type="text"/>
Reg Retry Intvl	<input type="text"/> (sec)		
All Lines Signal SIP Port	<input type="button" value="Disable ▾"/>		

**NAT Traversal**

**NAT Traversal**

NAT Traversal	<input type="button" value="Disable ▾"/>	STUN Server Address	<input type="text"/>
NAT Refresh Interval(sec)	<input type="text"/>	STUN Server Port	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

**Figure 60** 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 61** VoIP QoS**4.5.1.6 Port Group**

On this page, you can set Port Group.

### Port Group Setting

#### Port Group Setting

Port Group Index	<input type="text" value="1"/>		
Port Group Enable	<input type="text" value="Disable"/>	Port Select	<input type="text" value="All"/>
Pick Up On Group	<input type="text"/>	Port Group Member	<input type="text"/>
Port Group Display Name	<input type="text"/>	Port Group Number	<input type="text"/>
Port Group Account	<input type="text"/>	Port Group Password	<input type="text"/>
Proxy Server	<input type="text"/>	Proxy Port	<input type="text"/>
Outbound Server	<input type="text"/>	Outbound Port	<input type="text"/>
Backup Outbound Server	<input type="text"/>	Backup Outbound Port	<input type="text"/>
Port Group use FXS DisplayName	<input type="text" value="Disable"/>		
<input type="button" value="Apply"/>			

Figure 62 Port Group

### 4.5.2 VoIP Phone Settings

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

VoIP Settings	Preferences		
VoIP Phone Settings	Volume Settings		
Phone Preferences Settings	Handset Input Gain	<input type="text" value="1"/>	Handset Volume(20~40db)
Dial Plan	DTMF Volume(0~45)		
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)	
Ringing Time(10-300sec)			
Flash Time Max(0.2-1sec)		Flash Time Min(0.1-0.5sec)	

Figure 63 VoIP Phone Settings

### 4.5.2.1 Phone Preferences Settings

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

#### Preferences

##### Volume Settings

Handset Input Gain	<input style="width: 50px; height: 20px; border: 1px solid black; border-radius: 5px; padding: 2px 5px;" type="button" value="1"/> <input style="width: 15px; height: 15px; border: 1px solid black; border-radius: 5px; padding: 2px 5px;" type="button"/>	Handset Volume(20~40db)	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>
DTMF Volume(0~45)	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		

##### Regional

Tone Type	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		
Dial Tone	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		
Busy Tone	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		
Ring Back Tone	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		
Call Waiting Tone	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		
Ringing Cadence	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		
Min Jitter Delay (0~120ms)	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>	Max Jitter Delay (0~120ms)	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>
Ringing Time(10- 300sec)	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>		
Flash Time Max(0.2- 1sec)	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>	Flash Time Min(0.1- 0.5sec)	<input style="width: 150px; height: 25px; border: 1px solid black; border-radius: 5px; padding: 5px;" type="button"/>

**Figure 64** Phone Preferences Settings

### 4.5.2.2 Dial Plan

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

**Dial Plan****General**Enable Dial Plan Unmatched Policy **Dial Plan Config****Figure 65** Dial Plan

## 4.6 Network

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

Dashboard	Status	Settings	FXS	Network
<a href="#">WAN Settings</a> <a href="#">WAN Setting</a> <a href="#">POE Output Voltage</a> <a href="#">LTE Settings</a> <a href="#">WiFi Settings</a> <a href="#">LAN Settings</a>	<b>WAN Setting</b> WAN Mode <input type="button" value="Hot Failover ▾"/> Main WAN <input type="button" value="ETH WAN1 ▾"/> Back up WAN <input type="button" value="ETH WAN2 ▾"/> ICMP DETECTION SERVER <input type="text" value="8.8.8.8"/> ICMP DETECTION BACKUP SERVER <input type="text" value="1.1.1.1"/> ICMP Detection Interval <input type="text" value="60"/> Seconds ICMP Detection Timeout <input type="text" value="10"/> Seconds ICMP Detection Retries <input type="text" value="2"/>	<input type="button" value="Apply"/>		

**Figure 66** Network

## 4.6.1 WAN Settings

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

WAN Settings	
<b>WAN Setting</b>	<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
<b>Apply</b>	

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.

WAN Setting	
WAN Mode	Hot Failover
Main WAN	ETH WAN1
Back up WAN	ETH WAN1
ICMP DETECTION SERVER	ETH WAN2
ICMP DETECTION BACKUP SERVER	Cellular WAN
ICMP Detection Interval	60 Seconds
ICMP Detection Timeout	10 Seconds
ICMP Detection Retries	2
<b>Apply</b>	

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.

**POE Output Voltage**

WAN1 PoE Voltage	Disabled
WAN2 PoE Voltage	Disabled
WAN1 Cycle Time	12V 24V (0 ~ 3600)
WAN2 Cycle Time	48V (0 ~ 3600)

**Apply**

Figure 69 POE Output Voltage

### 4.6.2 LTE Settings

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

<b>WAN Settings</b>	<b>SIM1 Data Roaming</b>
<b>LTE Settings</b>	Data Roaming Setting
<b>Data Roaming</b>	Enable
<b>SIM Switch</b>	<b>SIM2 Data Roaming</b>
<b>APN Settings</b>	Data Roaming Setting
<b>PIN Management</b>	Enable
<b>WiFi Settings</b>	<b>Apply</b>
<b>LAN Settings</b>	<b>Apply</b>

Figure 70 LTE Settings

#### 4.6.2.1 Data Roaming

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

**SIM1 Data Roaming**

Data Roaming Setting	Enable <input type="button" value="▼"/>
<input type="button" value="Apply"/>	
Data Roaming Setting	Enable <input type="button" value="▼"/>
<input type="button" value="Apply"/>	

**Figure 71** Data Roaming

#### 4.6.2.2 SIM Switch

From this page ,you can switch SIM1or SIM2.

**SIM Switch Setting**

SIM Card mode	SIM1 <input type="button" value="▼"/>		
<input type="button" value="Apply"/>			
<table><tr><td>SIM1</td></tr><tr><td>SIM2</td></tr></table>		SIM1	SIM2
SIM1			
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.

**Switch SIM Card**

Switch SIM Card	<input type="button" value="SIM1 ▾"/>
-----------------	---------------------------------------

**SIM APN Settings**

Mode	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Host Name	<input type="button" value="▼"/>
Profile Name	<input type="text" value="Auto"/>
APN	<input type="text" value="Auto"/>
Authentication	<input type="button" value="None ▾"/>
User Name	<input type="text"/>
Password	<input type="text"/>

**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.

**Switch SIM Card**

Switch SIM Card	<input type="button" value="SIM1 ▾"/>
-----------------	---------------------------------------

**SIM APN Settings**

Mode	<input type="radio"/> Auto <input checked="" type="radio"/> Manual
Host Name	<input type="button" value="▼"/> <input type="button" value="Add New"/>
Profile Name	<input type="text" value="internet"/>
APN	<input type="text"/>
Authentication	<input type="button" value="None ▾"/>
User Name	<input type="text"/>
Password	<input type="text"/>

**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.

#### **SIM1 PIN Management**

USIM Card Status	Unknown
PIN Status	Disabled
Remaining PIN Attempts	0
PIN Lock	<input type="checkbox"/> <input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Apply</b>	

#### **SIM2 PIN Management**

USIM Card Status	
PIN Status	
Remaining PIN attempts	
PIN Lock	<input type="checkbox"/> <input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Apply</b>	

**Figure 74** PIN Management

### **4.6.3 WiFi Settings**

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

<div style="background-color: #005a7b; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">WAN Settings</div> <div style="background-color: #e0e0e0; color: #005a7b; padding: 2px; font-size: 0.8em;">LTE Settings</div> <div style="background-color: #005a7b; color: white; padding: 2px; font-size: 0.8em;">WiFi Settings</div> <div style="background-color: #005a7b; color: white; padding: 2px; font-size: 0.8em;">Wi-Fi 2.4GHz</div> <div style="background-color: #e0e0e0; color: #005a7b; padding: 2px; font-size: 0.8em;">Wi-Fi 5GHz</div> <div style="background-color: #e0e0e0; color: #005a7b; padding: 2px; font-size: 0.8em;">Wireless Block Users</div> <div style="background-color: #e0e0e0; color: #005a7b; padding: 2px; font-size: 0.8em;">Wi-Fi Guest</div> <div style="background-color: #e0e0e0; color: #005a7b; padding: 2px; font-size: 0.8em;">WWAN Hotspot</div> <div style="background-color: #005a7b; color: white; padding: 2px; font-size: 0.8em;">LAN Settings</div>	<div style="border-bottom: 1px solid #ccc; padding-bottom: 10px;"> <b>Wi-Fi 2.4GHz Settings</b> </div> <table border="0"> <tr> <td>Wi-Fi Status</td> <td style="text-align: right;"><input type="button" value="Enabled ▾"/></td> </tr> <tr> <td>Wi-Fi Standard</td> <td style="text-align: right;"><input type="button" value="11b/g/n mixed mode ▾"/></td> </tr> <tr> <td>Network Name (SSID)</td> <td style="text-align: right;"><input type="text" value="POTSCAST_BB99C6"/></td> </tr> <tr> <td>Frequency (Channel)</td> <td style="text-align: right;"><input type="button" value="Auto (Channel 6) ▾"/></td> </tr> <tr> <td>Broadcast SSID</td> <td style="text-align: right;"><input checked="" type="radio"/> Enabled <input type="radio"/> Disabled</td> </tr> <tr> <td>Bandwidth</td> <td style="text-align: right;"><input type="radio"/> 20 MHz <input checked="" type="radio"/> 20/40 MHz</td> </tr> </table> <div style="border-bottom: 1px solid #ccc; padding-bottom: 10px;"> <b>Wi-Fi 2.4GHz Security</b> </div> <table border="0"> <tr> <td>Security Mode</td> <td style="text-align: right;"><input type="button" value="WPA2-PSK ▾"/></td> </tr> <tr> <td>WPA Algorithms</td> <td style="text-align: right;"><input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES</td> </tr> <tr> <td>Password</td> <td style="text-align: right;"><input type="text" value="RHYpQHb9"/></td> </tr> <tr> <td>Key Renewal Interval</td> <td style="text-align: right;"><input type="text" value="3600"/> Seconds (0 ~ 4194302)</td> </tr> </table> <div style="border-bottom: 1px solid #ccc; padding-bottom: 10px;"> <b>Wi-Fi 2.4GHz QR Code</b> </div> <div style="text-align: center;">  </div> <div style="text-align: center; margin-top: 10px;"> <input type="button" value="Apply"/> <input type="button" value="Clear"/> </div>	Wi-Fi Status	<input type="button" value="Enabled ▾"/>	Wi-Fi Standard	<input type="button" value="11b/g/n mixed mode ▾"/>	Network Name (SSID)	<input type="text" value="POTSCAST_BB99C6"/>	Frequency (Channel)	<input type="button" value="Auto (Channel 6) ▾"/>	Broadcast SSID	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled	Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> 20/40 MHz	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 Status	<input type="button" value="Enabled ▾"/>																				
Wi-Fi Standard	<input type="button" value="11b/g/n mixed mode ▾"/>																				
Network Name (SSID)	<input type="text" value="POTSCAST_BB99C6"/>																				
Frequency (Channel)	<input type="button" value="Auto (Channel 6) ▾"/>																				
Broadcast SSID	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled																				
Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> 20/40 MHz																				
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)																				

**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.

**Wi-Fi 2.4GHz Settings**

Wi-Fi Status	Enabled <input type="button" value="▼"/>
Wi-Fi Standard	11b/g/n mixed mode <input type="button" value="▼"/>
Network Name (SSID)	POTSCAST_BB99C6
Frequency (Channel)	Auto (Channel 6) <input type="button" value="▼"/>
Broadcast SSID	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Bandwidth	<input type="radio"/> 20 MHz <input checked="" type="radio"/> 20/40 MHz

**Wi-Fi 2.4GHz Security**

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

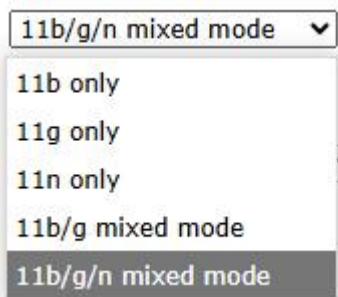
**Wi-Fi 2.4GHz QR Code****Figure 76 WiFi 2.4G Settings**

- **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".



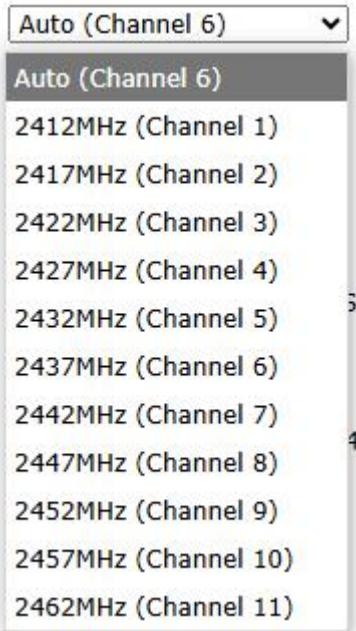
**Figure 77 WiFi 2.4G Standard**

- **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:** TKIP, 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.

<b>Wi-Fi 5GHz Settings</b>	
Wi-Fi Status	Enabled <input type="button" value="▼"/>
Wi-Fi Standard	11n/ac mixed mode <input type="button" value="▼"/>
Network Name (SSID)	POTSCAST_5G_BB99C6
Frequency (Channel)	Auto (Channel 52) <input type="button" value="▼"/>
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
<b>Wi-Fi 5GHz Security</b>	
Security Mode	WPA2-PSK <input type="button" value="▼"/>
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES
Password	RHYpQHb9
Key Renewal Interval	3600 Seconds(0 ~ 4194302)
<b>Wi-Fi 5GHz QR Code</b>	
	
<input type="button" value="Apply"/>	<input type="button" value="Clear"/>

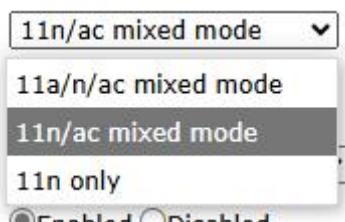
**Figure 80** WiFi 5GHz Settings

- **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".

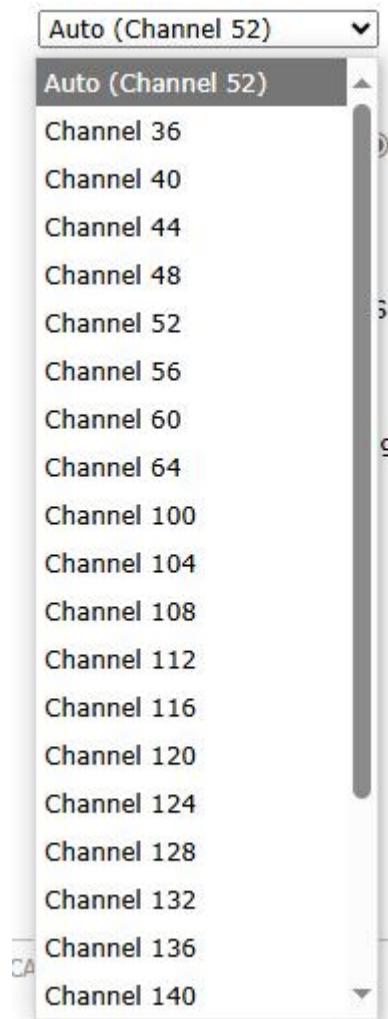
**Figure 81** WiFi 5GHz standard

- **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.

**Wi-Fi 5GHz Security**

Security Mode	<input style="border: 1px solid #ccc; padding: 2px 10px; width: 100%; height: 25px; border-radius: 5px; background-color: #fff; font-size: 10px; font-weight: bold; margin-bottom: 5px;" type="button" value="WPA2-PSK"/>
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP/AES
Password	<input style="width: 100%; border: 1px solid #ccc; padding: 2px 10px; border-radius: 5px; margin-bottom: 10px;" type="text" value="RHYpQHb9"/>
Key Renewal Interval	<input style="width: 50px; border: 1px solid #ccc; padding: 2px 5px; border-radius: 5px; margin-right: 10px;" type="text" value="3600"/> Seconds(0 ~ 4194302)

**Wi-Fi 5GHz QR Code**



Apply

Clear

**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 use 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 84** 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	<input type="button" value="Disabled ▾"/>
<input type="button" value="Apply"/>	

**Wi-Fi Guest 5GHz Settings**

Wi-Fi Status	<input type="button" value="Disabled ▾"/>
<input type="button" value="Apply"/>	

**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.

Selected Hotspot																																																																																																					
SSID	<input type="text"/>																																																																																																				
Password	<input type="password"/>																																																																																																				
Status	Disconnected																																																																																																				
<input type="button" value="Connect"/>																																																																																																					
<b>Wi-Fi Scan Results</b> <table border="1"> <thead> <tr> <th>No.</th> <th>SSID</th> <th>AuthMode</th> <th>EncryptType</th> <th>Signal</th> <th>Select</th> </tr> </thead> <tbody> <tr><td>1</td><td>Guest_192477</td><td>WPA2PSK</td><td>AES</td><td>Good</td><td><input type="radio"/></td></tr> <tr><td>2</td><td>TP-LINK_F438</td><td>WPAPSKWPA2PSK</td><td>AES</td><td>Good</td><td><input type="radio"/></td></tr> <tr><td>3</td><td>Atel_Guest</td><td>OPEN</td><td>NONE</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>4</td><td>GM200_3B97</td><td>OPEN</td><td>NONE</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>5</td><td>Atel_Staff</td><td>WPA2</td><td>AES</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>6</td><td>Atel_Guest</td><td>OPEN</td><td>NONE</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>7</td><td>Atel_Staff</td><td>WPA2</td><td>AES</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>8</td><td>Atel_Guest</td><td>OPEN</td><td>NONE</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>9</td><td>Atel_Staff</td><td>WPA2</td><td>AES</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>10</td><td>PW550_195407</td><td>WPA2PSK</td><td>AES</td><td>Middle</td><td><input type="radio"/></td></tr> <tr><td>11</td><td>MD310-880_MTN_9336CD</td><td>WPA2PSK</td><td>AES</td><td>Middle</td><td><input type="radio"/></td></tr> <tr><td>12</td><td>LEGO</td><td>WPAPSKWPA2PSK</td><td>AES</td><td>Good</td><td><input type="radio"/></td></tr> <tr><td>13</td><td>Wireless-N-2.4G-test</td><td>WPAPSKWPA2PSK</td><td>AES</td><td>Good</td><td><input type="radio"/></td></tr> <tr><td>14</td><td>Atel_Staff</td><td>WPA2</td><td>AES</td><td>Poor</td><td><input type="radio"/></td></tr> <tr><td>15</td><td>Atel_Guest</td><td>OPEN</td><td>NONE</td><td>Poor</td><td><input type="radio"/></td></tr> </tbody> </table>						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"/>
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 86** WWAN Hostport

#### 4.6.4 LAN Settings

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

IP Address	192.168.7.1
Subnet Mask	255.255.255.0
DHCP	Enabled
Start IP Address	192.168.7.2
End IP Address	192.168.7.254
Lease Time	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"/>

Apply      Clear

**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.

**LAN Settings**

IP Address	192.168.7.1	
Subnet Mask	255.255.255.0	
DHCP	Enabled ▾	
Start IP Address	192.168.7.2	
End IP Address	192.168.7.254	
Lease Time	86400	
Static IP 1	MAC:	IP:
Static IP 2	MAC:	IP:
Static IP 3	MAC:	IP:
Static IP 4	MAC:	IP:
Static IP 5	MAC:	IP:

**Apply** **Clear**

**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 2.

LAN Port Setting	
LAN port 1	Enabled <input type="button" value="▼"/>
LAN port 2	Enabled <input type="button" value="▼"/>
<input type="button" value="Apply"/>	

**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