EG3015M-M30-HP-EUD
Configuration Guide

Document Version: 01

All rights reserved © Baicells Technologies Co., Ltd.

About This Document

This document describes the configuration of the LteTurbo CPE for EG3015M-M30-HP-EUD. It is a guide that how to configure the device after its installation completes.

Copyright Notice

Baicells Technologies Co., Ltd., copyrights the information in this document. No part of this document may be reproduced in any form or means without the prior written consent of Baicells Technologies Co., Ltd.

Disclaimer

The information in this document is subject to change at any time without notice. For more information, please consult with a Baicells technical engineer or the support team.

Revision Record

Date	Version	Description
21 Oct., 2022	01	Initial released.

Contact Us

	Baicells Technologies Co., Ltd.	**Baicells Technologies North America, Inc.**
	China	North America
Address	9-10F,1stBldg.,No.81BeiqingRoad,Haidian District,Beijing,China	555 Republic Dr., #200, Plano, TX 75074, USA
Phone	400-108-0167	+1-888-502-5585
Email	contact@Baicells.com or support@Baicells.com	sales_na@Baicells.com or support_na@Baicells.com
Website	www.Baicells.com	https://na.Baicells.com

Menu

1. Configuration Overview 1
2. Installation 1

2.1 Part & Materials 1

2.2 Led 2

3. Configuration 4

3.1 Status Menu 4

3.1.1 Overview 4

3.1.2 Routes 11

3.2 Network Menu 12

3.2.1 LAN Settings 12

3.2.2 WAN Settings 14

3.2.3 WLAN Settings 17

3.2.4 Static Routes 20

3.2.5 DMZ 20

3.3 LTE Menu 22

3.3.1 Connection Settings 22

3.3.2 Scan Mode 24

3.3.3 APN Management 28

3.3.4 PIN Management 29

3.4 Security Menu 30

3.4.1 Firewall Settings 30

3.4.2 MAC Filter 31

3.4.3 IP Filter 32

3.4.4 URL Filter 33

3.4.5 Port Forwarding 34

3.4.6 Port Triggering 35

3.4.7 ALG 35

3.4.8 UPnP 37
3.4.9 Attack Protection 38
3.5 VPN Menu 39
3.5.1 IPSec 39
3.5.2 OpenVPN 41
3.6 System Menu 43
3.6.1 NTP 43
3.6.2 Account 44
3.6.3 Dynamic DNS 45
3.6.4 WEB Setting 48
3.6.5 FTP Auto Upgrade 49
3.6.6 TR-069 50
3.6.7 SNMP 52
3.6.8 Restore/Update 54
3.6.9 Ping Watchdog 55
3.6.10 System Messages 56
3.6.11 Diagnosis 57
3.6.12 Reboot 60
3.7 Logout 61
4. Regulatory Compliance 62
FCC Compliance 62

1. Configuration Overview

The Baicells LteTurbo CPE is loaded with its own GUI for configuring its operating parameters. You can log in to the GUI either locally through the Local Maintenance Terminal (LMT), which is an Ethernet port, or remotely via IP address. You can also use the Baicells Operations Management Console (OMC) to configure the CPE; this document, however, focuses only on using the web GUI.

2. Installation

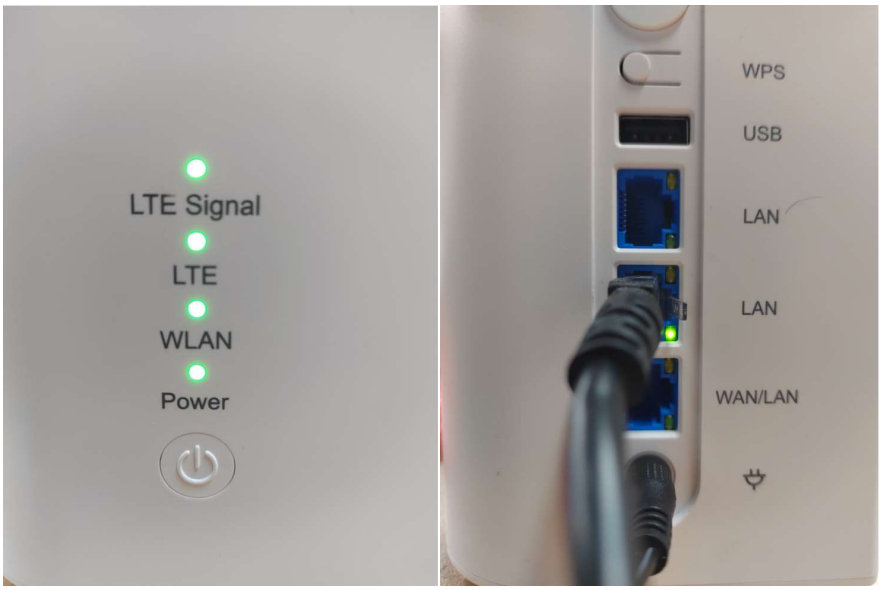
2.1 Part & Materials

Item	Qty	Picture
EG3015M-M30-HP-EUD unit	1	
DC Power Adaptor	1	

You will need standard tools, Ethernet cable, ground wire, and RJ-45 connectors for installing and connecting the outdoor unit.

2.2 Led

The CPE has 4 lights, divided into 5 groups according to the function: lte signal light, power light, LTE light, WLAN light,LAN light (see figure below).



- WLAN light

  1. 8 ssids are all off, red/green off
  2. Red light on during startup

     Startup completed Red light off
  3. One SSID is on, green on and red off
  4. A user successfully accesses, 1s green flash

- Lte signal light

  Strong signal green light on, red light off

  weak signal red light on, green light off

- Power light

  The power light is bright, indicating that the power supply is normal, otherwise the power supply is abnormal

- LTE light

1. SIM card is abnormally red
2. Red flash without network access
3. Successful network access, green light and red light out

- Lan light

1. The speed is 10/100Mbsps, and the orange and green lights are on at the same time
2. The speed is 1000Mbsps, and the green light is on

Note: The status of the lamp is meaningless during the start-on process, and wait for the start-on (5 minutes) before checking the LED status.

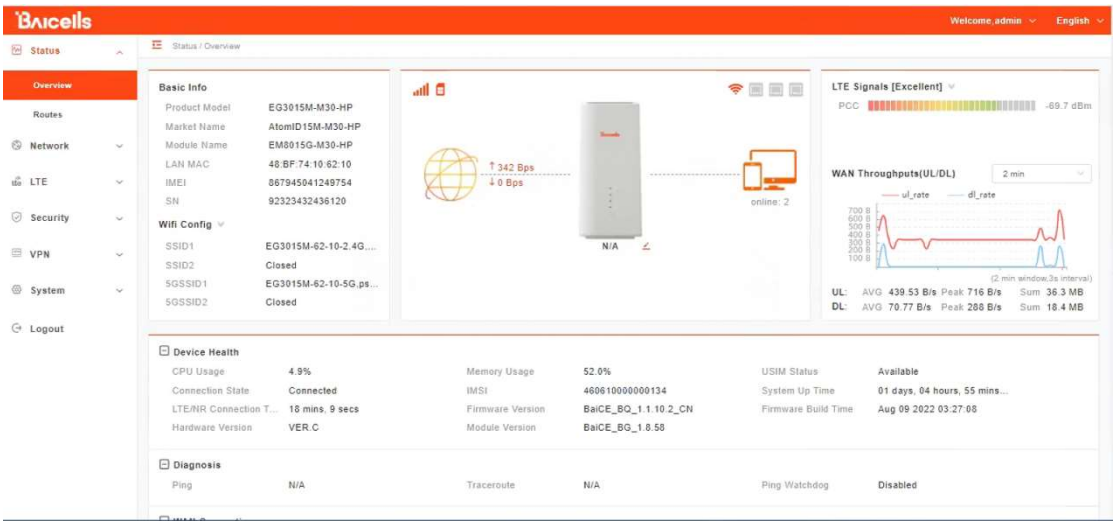
3. Configuration

3.1 Status Menu

3.1.1 Overview

After logging in, the GUI opens to the Status > Overview page (Figure 3-1). This page is a dashboard of key information regarding the CPE.

Figure 3-1 Overview

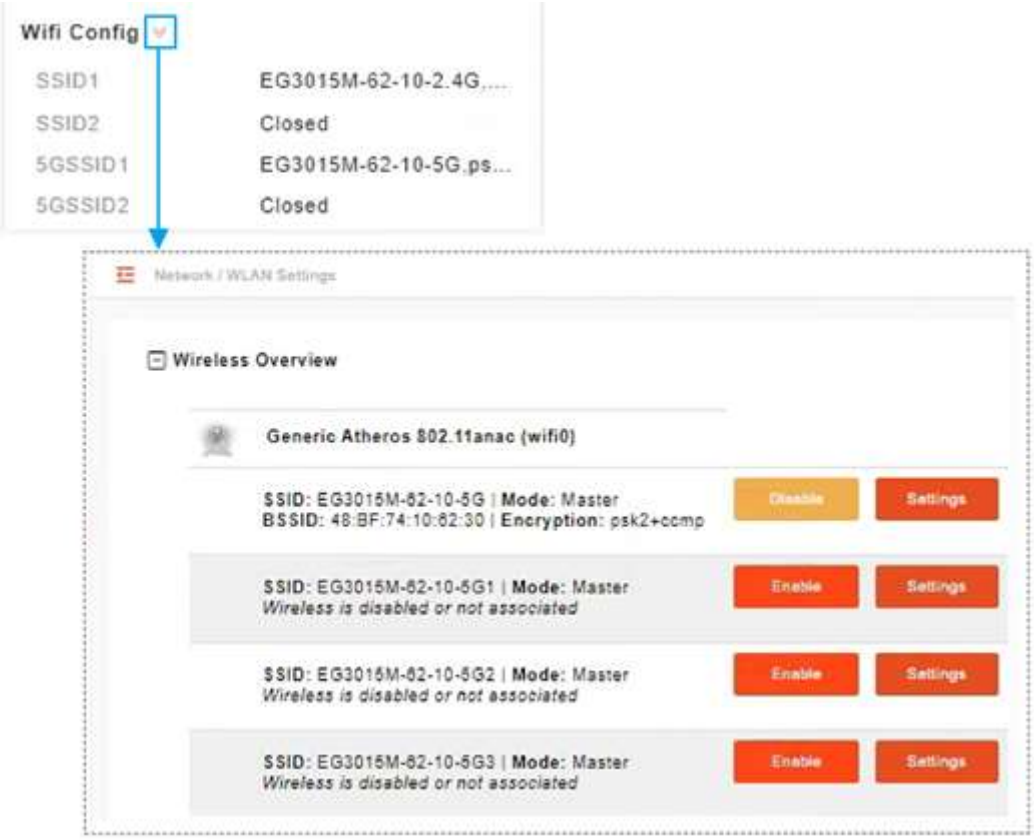


- The equipment connection status pane displays the connection status of CPE equipment with LTE network and WAN network. The icons are described as follows:

	LTE signal
	For SIM card, it is gray when checking SIM / disconnect, orange when SIM card is recognized, and red after network access.
	WiFi signal: red when WiFi is on and gray when WiFi is off.
	Wired interface, gray when there is no link, orange when negotiating 100M, and blue when negotiating 1000M.
	LTE network bearer. It is gold in case of bearing and gray in case of no bearing. The number next to the icon is WAN uplink and downlink data rate.
online: 2	User Number under LAN
	CPE equipment icon, click to modify the equipment name.

- The *Basic Info* pane displays the product model, module name, LAN MAC, IMEI, serial number, etc.

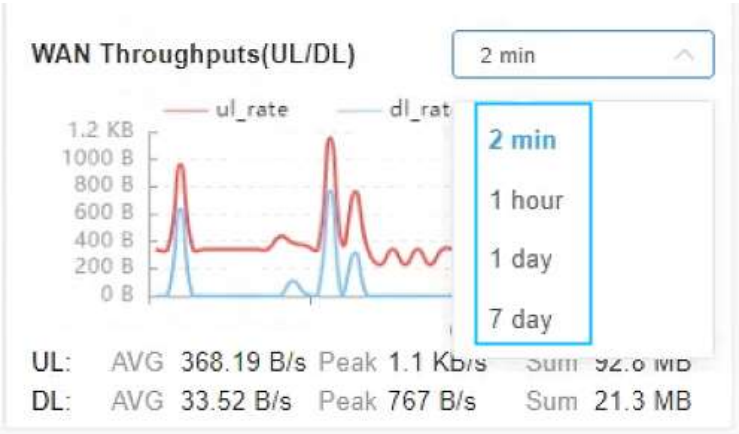
- The *Wifi Config* pane displays the SSIDs of the CPE device. Click the icon to jump to the WLAN settings page for WiFi configuration.



- The *LTE Signals* pane shows the signal quality of primary cell. Click icon to view LTE details, such as the CPE's SIM card status and its IMSI and IMEI numbers, wireless frequency being used, eNB connection status, and current signal strength and quality.

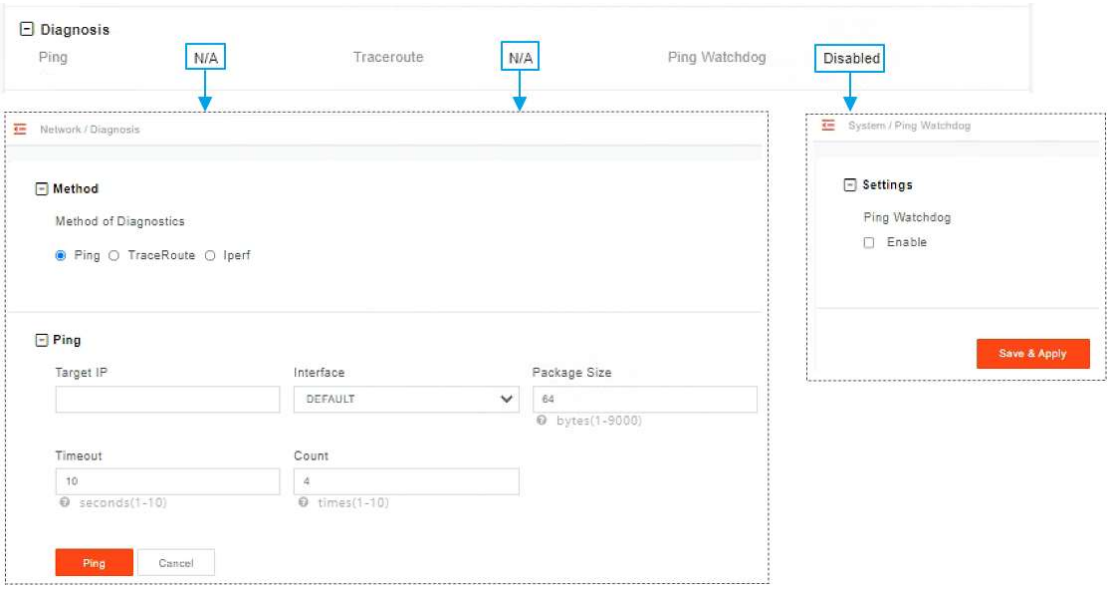
- Under *WAN Throughput* you will see downlink (DL) and uplink (UL) data rates for current throughput (kbps), average rates, peak rates, and total throughput.The flow statistics can be carried out at different times, including 2 min, 1 hour, 1 day and 7

days.



- The *Device Health* pane shows device health data, such as CPU Usage, Memory Usage, USIM Status, LTE/NR Connection Time, System Up Time, etc.

- The *Diagnosis* pane shows Ping diagnosis results, Traceroute diagnosis results, Ping Wathchdog configuration data. Click the displayed data to quickly enter the configuration page.



- The *WAN Connections* pane displays configured APN, IP address of gateway and DNS.

- The *LAN Connections* pane will show details about all smart devices currently connected through the CPE.

- The *WiFi Associated Stations* pane shows the device information currently accessing WiFi.

Refer to Table 3-1for a description of the *Status* fields.

Table 3-1 Status

Field Name	Description
Basic Info	
Product Model	CPE model number
Market Name	Market name of CPE products
Module Name	Type of LTE module in the CPE
LAN MAC	The MAC address of the LAN port. The same as the MAC on the label.
IMEI	International Mobile Equipment Identity is like a serial number for the SIM card
SN	Serial Number
Wifi Config	
SSID	2.4G service set ID
5GSSID	5G service set ID
LTE Signals	
USIM Status	The Universal Subscriber Identity Module, or SIM, card status is either available or not ready in the CPE

Field Name	Description
IMSI	The unique International Mobile Subscriber Identity (IMSI) number associated with the SIM card in the subscriber's CPE. The IMSI must be identifiable by the operator's LTE network in order to access it.
LTE Mode	The LTE network operates with either Time Division Duplexing (TDD) or Frequency Division Duplexing (FDD)
IMEI	International Mobile Equipment Identity is like a serial number for the SIM card
PLMN	The Public Land Mobile Number (PLMN), or operator network ID, to which the CPE is connected
Band	The range of frequencies within the band the CPE may use for wireless communications with an eNB, expressed in MHz
Cell ID	The operator's cell site ID to which the CPE is connected. A cell site may comprise more than one eNB. Each eNB is given a PCI to identify it.
RSRQ	Reference Signal Receiving Quality indicates the quality of the wireless signal
eNB ID	The operator's cell site ID to which the CPE is connected. A cell site may comprise more than one eNB. Each eNB is given a PCI to identify it.
EARFCN	The E-UTRA Absolute Radio Frequency Channel Number (band and frequency) within which the CPE operates
PCI	The Physical Cell Identifier (PCI) unique to each eNB. PCI indicates to which eNB the CPE is connected. An operator can have multiple eNBs serving the same cell.
DL Frequency	The frequency, in MHz, being used in the downlink (eNB to CPE). In LTE, the carrier frequency in the uplink and downlink is designated by the EARFCN, which identifies the LTE band and carrier frequency.
UL Frequency	The frequency, in MHz, that the CPE is using in the uplink (CPE to eNB). In LTE, the carrier frequency in the uplink and downlink is designated by the EARFCN, which identifies the LTE band and carrier frequency.
CINR	The Channel Signal-to-Interference-plus-Noise Ratio reflects the signal strength of the signal received from the two antennas in the eNB, expressed in decibels (dB) NOTE: Additional SINR values are reported when a transmitting device is using more than two antennas.

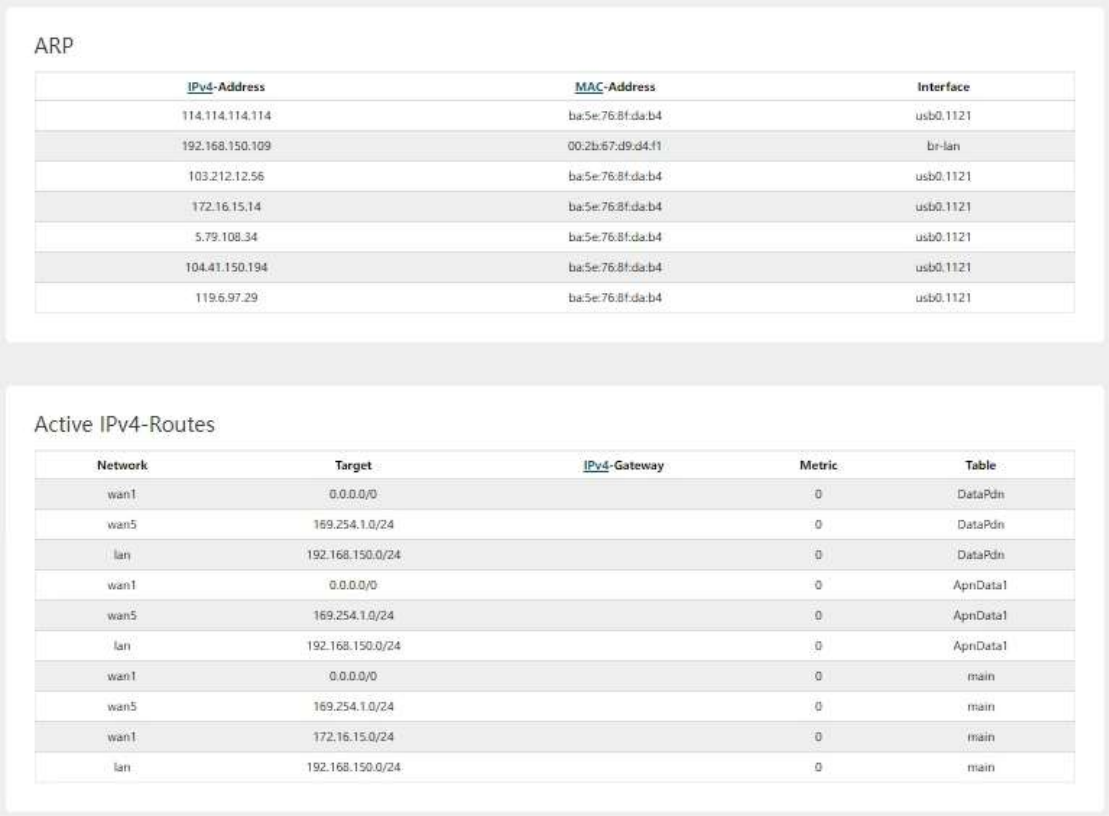
Field Name	Description
RSRP1 ~ RSRP4	The Signal-to-Interference-plus-Noise Ratio reflects the signal strength of the signal received from the two antennas in the eNB, expressed in decibels (dB) NOTE: Additional SINR values are reported when a transmitting device is using more than two antennas.
WAN Throughputs	
DL	The current downlink data throughput rate, in Kbps
UL	The current uplink data throughput rate, in Kbps
Average	The average DL and UL data throughput rates, in Kbps, for this CPE in the last 3 minutes
Peak	The peak DL and UL data throughput rates, in Kbps, for this CPE in the last 3 minutes
Sum	The total (sum) DL and UL data throughput rates, in Kbps
Device Health	
CPU Usage	CPU real-time usage rate, updated every 3s
Memory Usage	The memory usage rate of CPE, updated every 3s
USIM Status	The Universal Subscriber Identity Module, or SIM, card status is either available or not ready in the CPE
Connection State	Connection status between the CPE and the network –Checking SIM, Scanning, Registering, Acquiring IP, Connected, Disconnected.
IMSI	The unique International Mobile Subscriber Identity (IMSI) number associated with the SIM card in the subscriber's CPE. The IMSI must be identifiable by the operator's LTE network in order to access it.
System Up Time	CPE start time
LTE/NR Connection Time	LTE/NR network access success time
Firmware Version	Version number of the module
Firmware Build Time	Software version compilation time
Hardware Version	CPE hardware version
Module Version	CPE LTE module firmware version
Diagnosis	
Ping	Ping diagnosis results
Traceroute	Traceroute diagnosis results
Ping Watchdog	Ping Watchdog configuration result
WAN Connections	
Profile Name	APN Number
IPv4 Address/ IPv6 Address	IPv4or IPv6 address of the APN gateway

Field Name	Description
IPv4 DNS/ IPv6 DNS	IPv4 or IPv6 DNS
LAN Connections	
Device Name	The name of each smart device connected through the CPE
MAC Address	The MAC address of each smart device connected through the CPE
IP Address	The IP address of each device connected through the CPE
Lease Time	Amount of time a smart device's IP address has been leased
Type	Type of smart device connection
WiFi Associated Stations	
SSID	WIFI SSID
MAC Address	MAC address of the device accessing the SSID
IP Address	IP address of the device accessing the SSID
Signal	The signal strength of the connected device
Noise	WiFi signal noise
RX Rate	Wi-Fi real-time receiving rate
TX Rate	Wi-Fi real-time transmission rate

3.1.2 **Routes**

The Overview > Routes table lists all of the configured routing rules, including Allocation and Retention Policy (ARP) tables and active IPv4/IPv6 routes (Figure 3-2). For each item in the list, the IP address, MAC address, and interface type are displayed.

Figure 3-2 Routes



3.2 Network Menu

3.2.1 **LAN Settings**

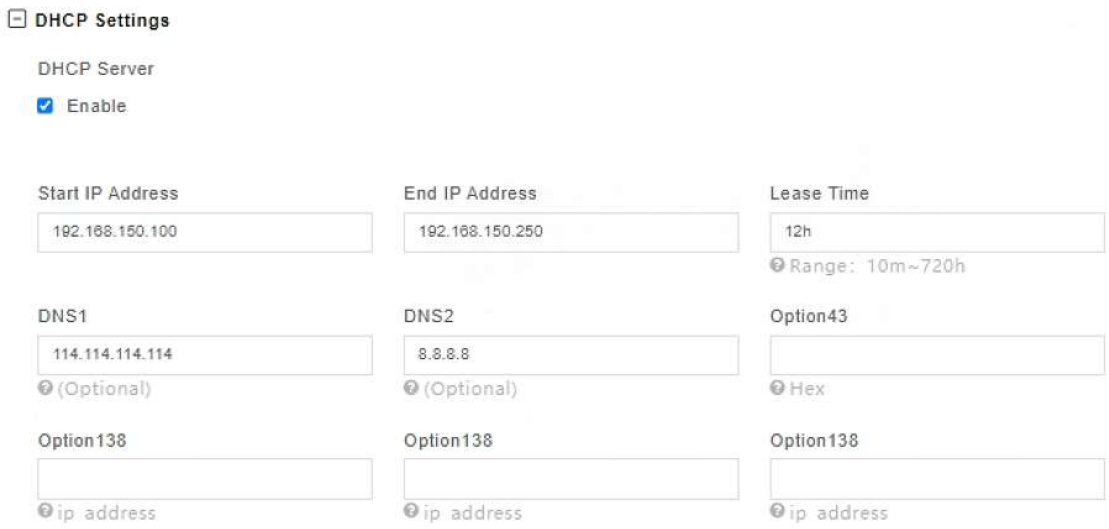
Enter the Network > LAN host IP address, subnet mask, and the Maximum Transmission Unit (MTU) size, in bytes (Figure 3-3). The range is 1000-2000 bytes. The default is 1500 bytes.

Figure 3-3 LAN settings

You can enable or disable the DHCP server (Figure 3-4). If enabled, enter the start and end IP addresses, and the lease time for IP address use - from 10 minutes to 720 hours. Optionally, you can enter one or two DNS server IP addresses, and one to three option 138 connection IP addresses for connecting to a Control and Provisioning of Wireless

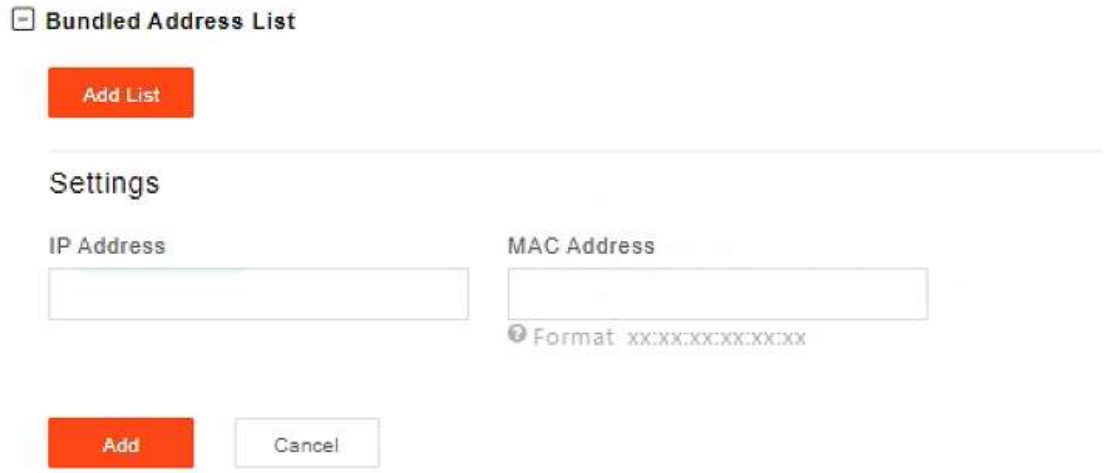
Access Points (CAPWAP) server. When using option 138, the device will connect with the server's LAN port and get an Access Controller (AC) IP address.

Figure 3-4 DHCP settings



The *DHCP Reservations* may be used to bind an IP address to a specific MAC address (Figure 3-5). In the bottom half of the pane, enter the IP address and the MAC address, and click on *ADD*. The IP address must be within the range of DHCP addresses. Any configured bindings will appear at the top of the window.

Figure 3-5 Bundled Address List

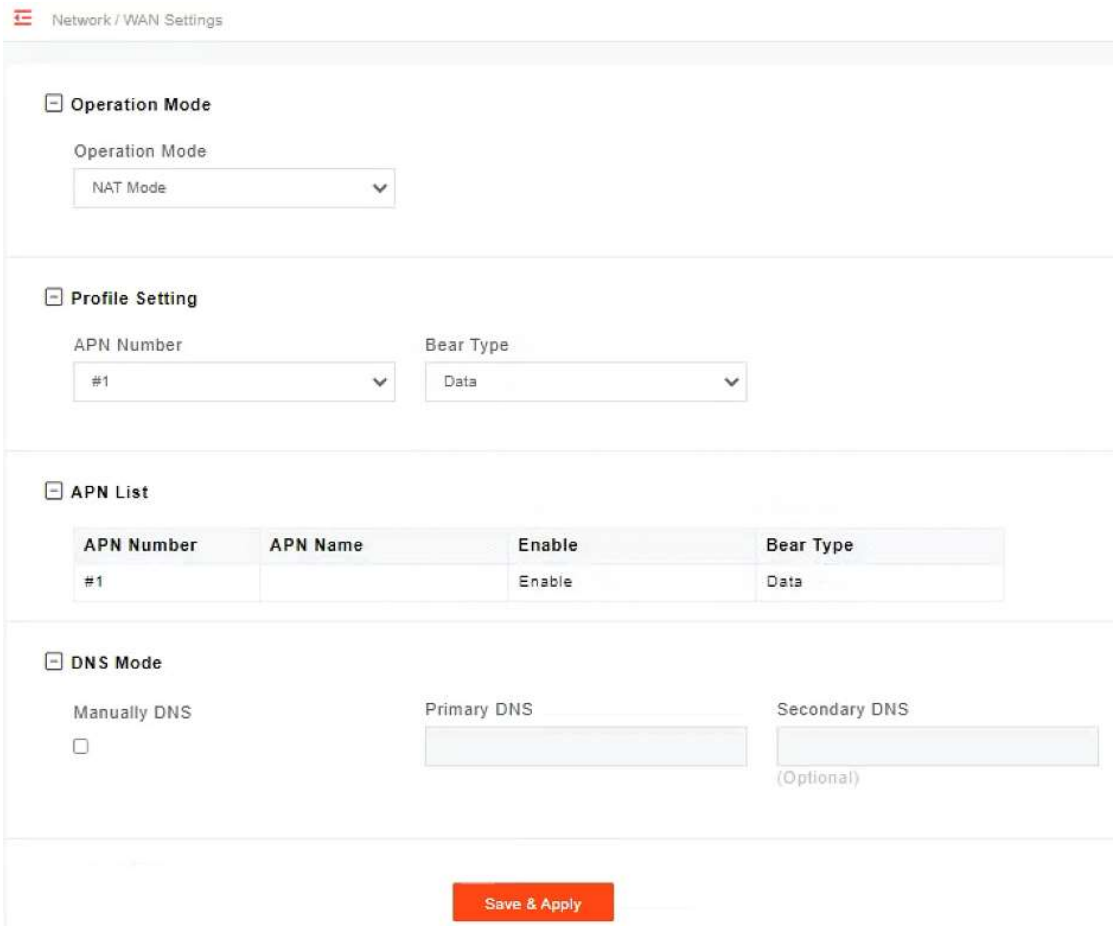


3.2.2 **WAN Settings**

3.2.2.1 NAT Mode

The CPE will be worked at NAT mode, and only 1 APN can be configured by Default Data bear types.

Figure 3-6 WAN Settings



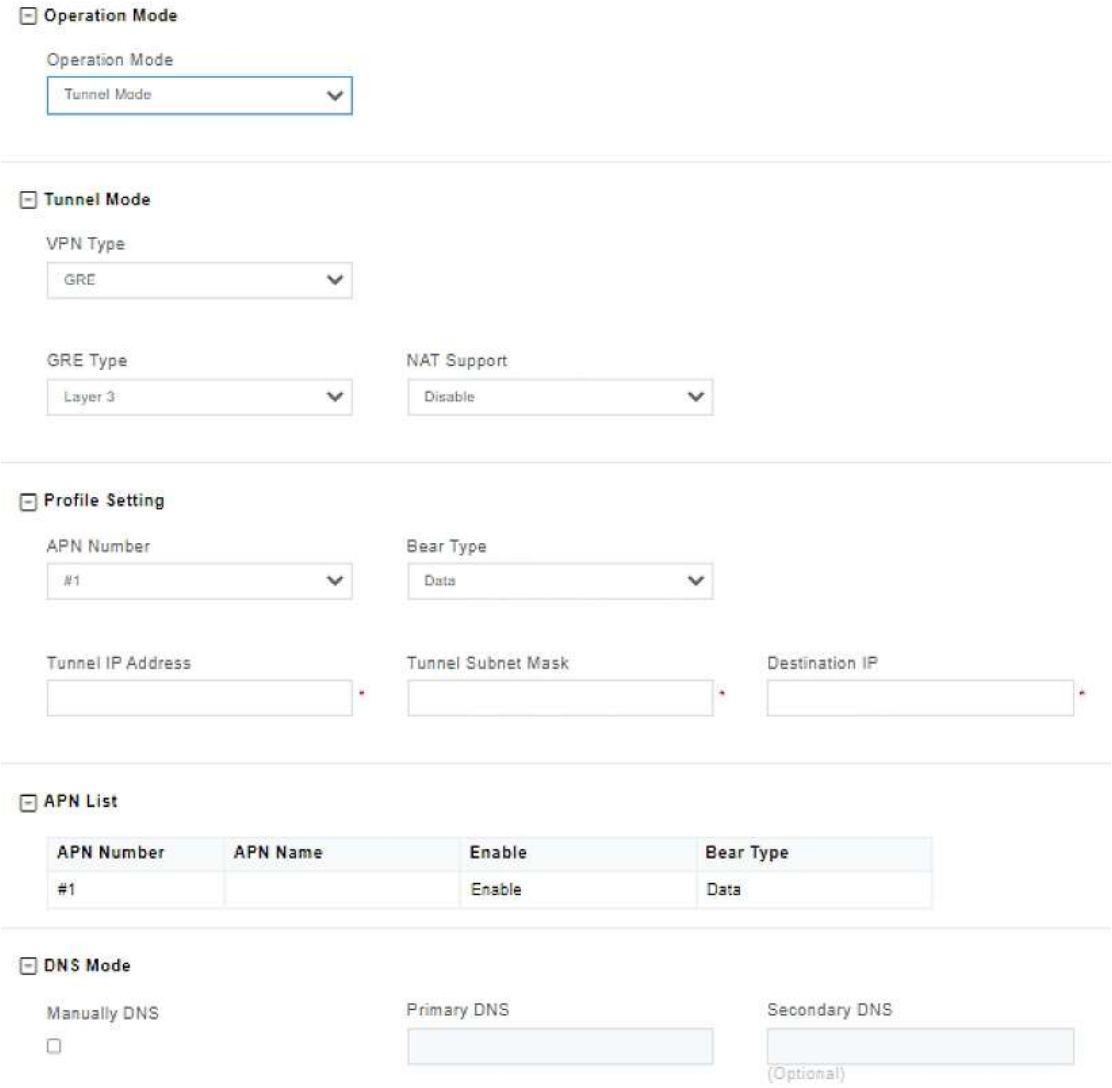
DNS Mode set how to get DNS server IP:

- Automatic: automatically obtain the DNS server IP assigned by EPC. If Manually DNS is not selected, it is automatic mode.
- Manually: manually configure the primary and standby DNS server IP.

3.2.2.2 Tunnel Mode

This CPE can support L2TP, GRE, PPTP, and VxLAN VPN type.

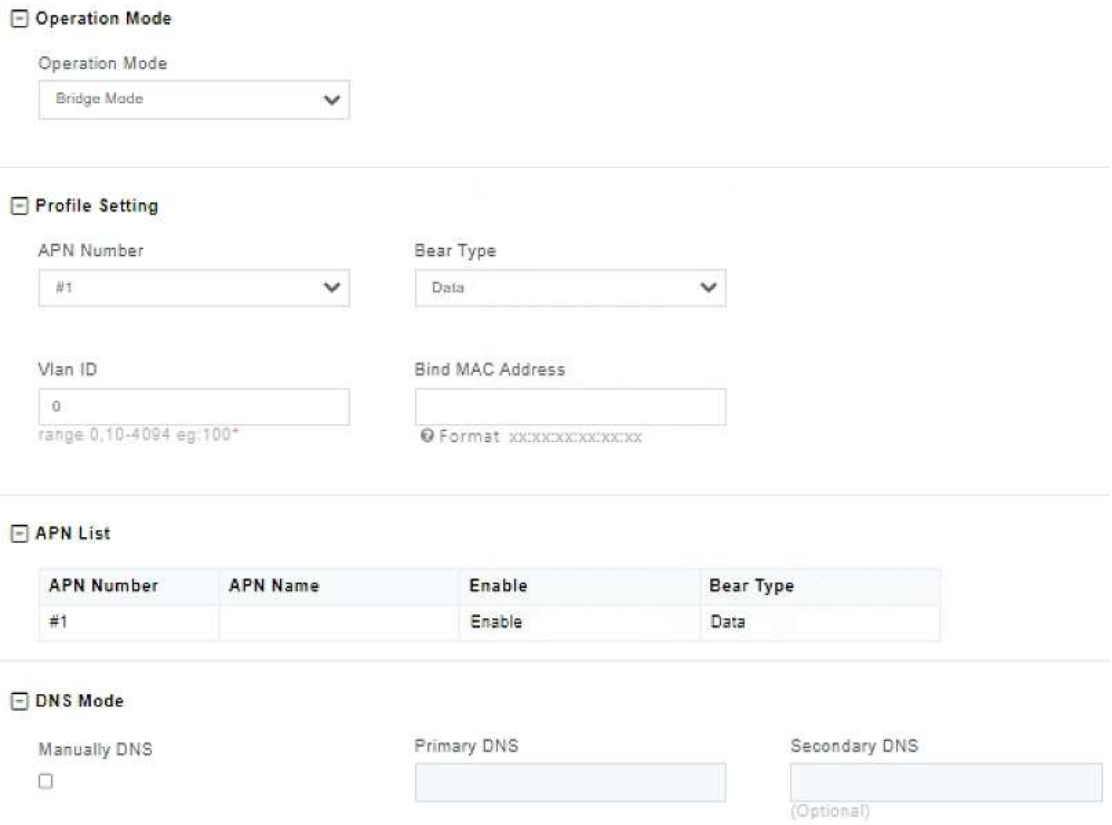
Figure 3-7 Tunnel Mode



3.2.2.3 Bridge Mode

When the CPE worked at Bridge mode, the WAN ports address will bridge to LAN port, and the LAN port will work at trunk mode.

Figure 3-8 Bridge Mode



3.2.3 **WLAN Settings**

Select **Network > WLAN Settings**, and set the WLAN Network, WLAN Expire time.

This function is only applicable to indoor CPE products. For outdoor CPE, WiFi will be turned off 10 minutes after startup by default.

Figure 3-9 WLAN Overview

The overview page displays the relevant information of the devices connected to the Wi-Fi hotspot. For each device displayed, you can operate enable / disable and settings.

Click the "**SETTINGS**" button to enter the network settings page. As shown in Figure 3-10.

Figure 3-10 WLAN Settings

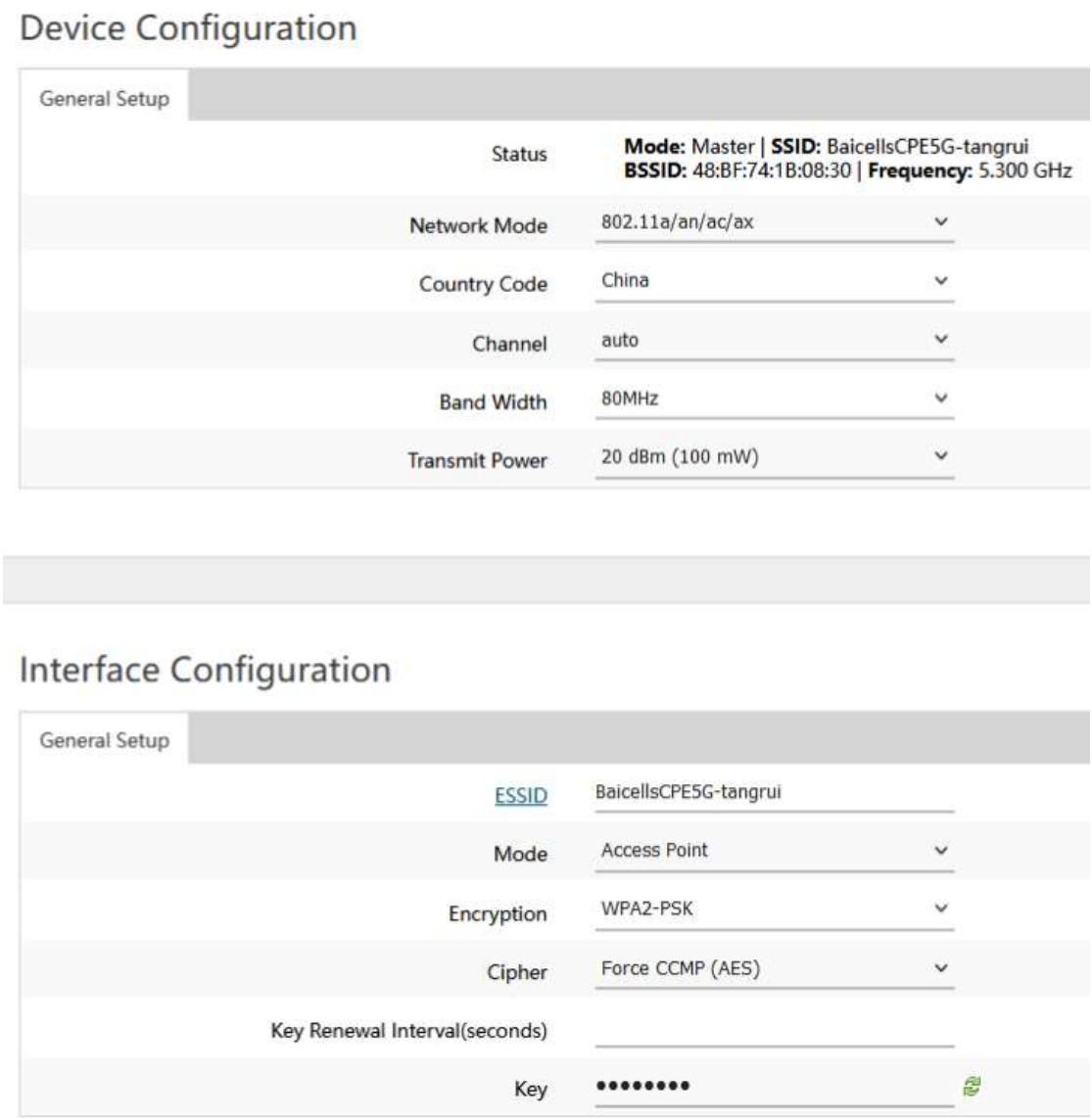


Table 3-2 WLAN Settings Parameters

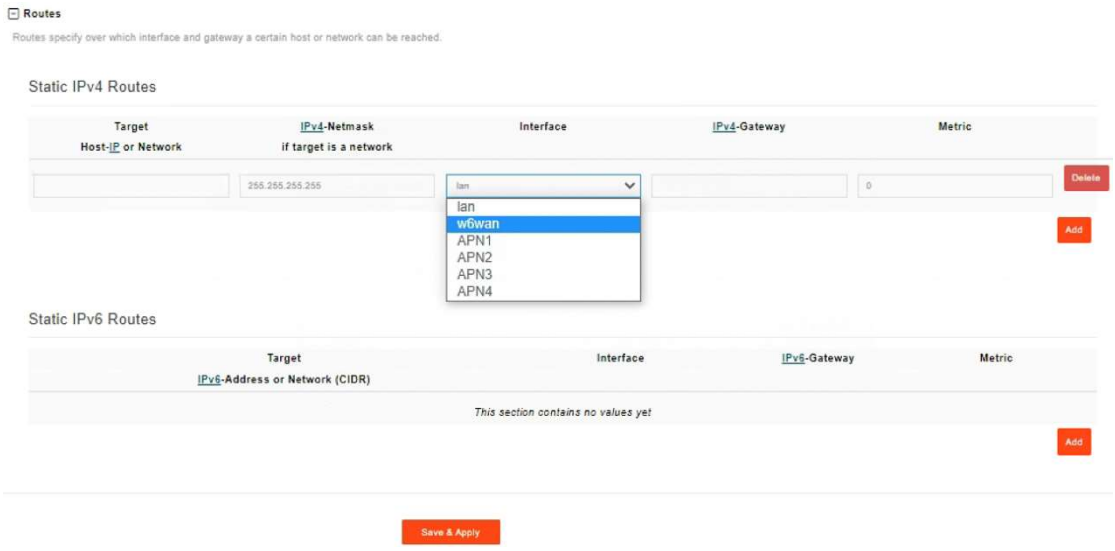
Field Name	Description
Device Configuration	
Network Mode	Support 80211 Wireless Protocol
Country Code	Country code
Channel	Configurable channel
Band Width	Wireless Supported Bandwidth
Transmit Power	Maximum power sent by WIFI
Interface Configuration	
ESSID	Service set ID. Wi-Fi assic string seen after the phone turns on Wi-Fi.

Field Name	Description
Mode	WIFI working mode: WIFI hotspot, WIFI STA. Default WIFI hotspot
Encryption	Encryption mode. Support No Encryption, WPA-PSK, and WPA2-PSK.
Cipher	Algorithm mode. Support CCMP (AES), TKIP, TKIP and CCMP (AES)
Key Renewal Interval(seconds)	Set the lifetime of the key used in secure sessions when WPA PSK is encrypted
Key	WIFI password

3.2.4 **Static Routes**

Select **Network > Static Routes**, and set the Static Routes.
To add a route, click on the *ADD* button to open a dialogue window where you can input the target IP address, netmask, interface type (APN, LAN, or WAN), and gateway address.

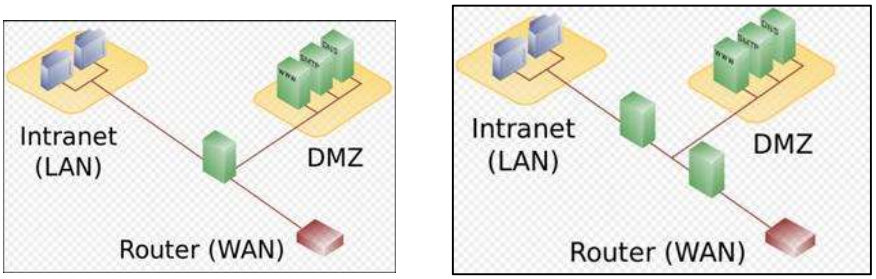
Figure 3-11 Static Routes



3.2.5 **DMZ**

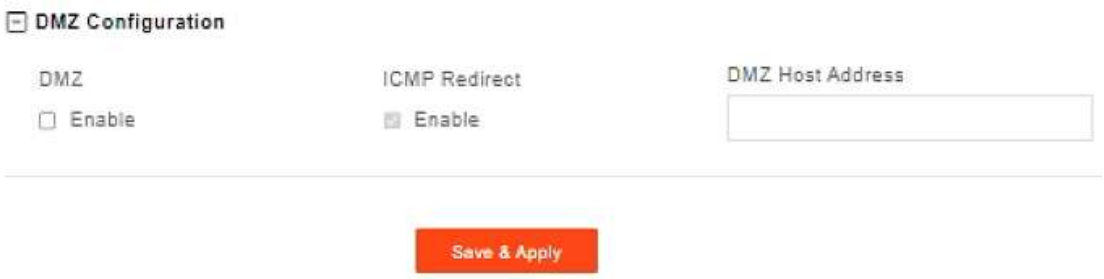
In technology, the DMZ refers to a firewall between incoming WAN traffic and the LAN to which the CPE is connected. Two basic DMZ methods are (a) using a single firewall, also known as the three-legged model, and (b) using dual firewalls (Figure 3-12). These architectures can be expanded to create complex architectures depending on the network requirements.

Figure 3-12 DMZ Examples



When the LAN has a DMZ/firewall server, you can enable DMZ on the CPE so that packets from the WAN are forwarded to the firewall (Figure 3-13). Alternatively, you can enable Internet Control Message Protocol (ICMP) redirect error messages to support Layer 2 multicast features.

Figure 3-13 DMZ



3.3 LTE Menu

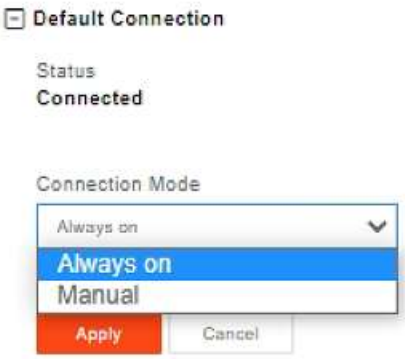
3.3.1 **Connection Settings**

LTE connection settings includes Default connection settings, Power Scan Option, Power Max Option, and 256QAM settings.

3.3.1.1 Default connection

If the **Connection Mode** is set to Always on, CPE will automatically access the LTE network after boot. If it is set to Manual, CPE needs to manually connect to the LTE network.

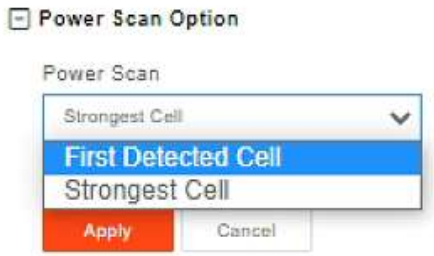
Figure 3-14 Default Connection Settings



3.3.1.2 Power Scan Option

The CPE support two power scan options, the first is First Detected Cell, and the second is the Strongest Cell.

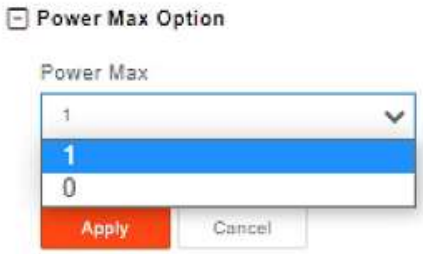
Figure 3-15 Scan Mode Settings



3.3.1.3 Power Max Option

Set whether to ignore the maximum power limit issued by the base station, 1: ignore, 0: do not ignore, Default value is 1.

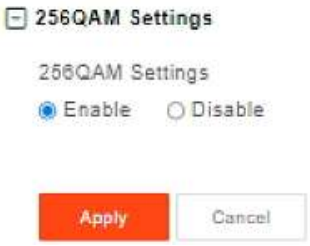
Figure 3-16 Power Max Option



3.3.1.4 256QAM Settings

Set whether to turn on 256QAM modulation for LTE module. Turn on by default for CAT15.

Figure 3-17 256QAM Setting

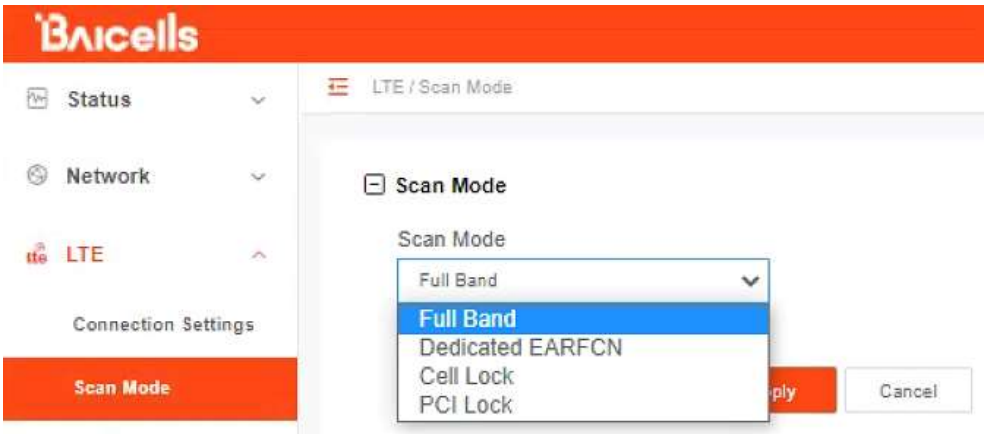


3.3.2 **Scan Mode**

The Scan Mode determines which frequencies the CPE's routine scan of available frequencies will cover. Scanning is a process of tuning to a specific frequency and measuring the simplest signal quality [e.g., Received Signal Strength Indication (RSSI)].

As part of the cell selection and reselection process, the CPE performs the scan first and then selects a small number of candidate cells to go through the next step of measuring and evaluating signals to select the best eNB that can serve it. The CPE frequently (milliseconds) performs the scan to ensure it has the best possible connection to the network. Refer to Figure 3-18.

Figure 3-18 Scan Mode



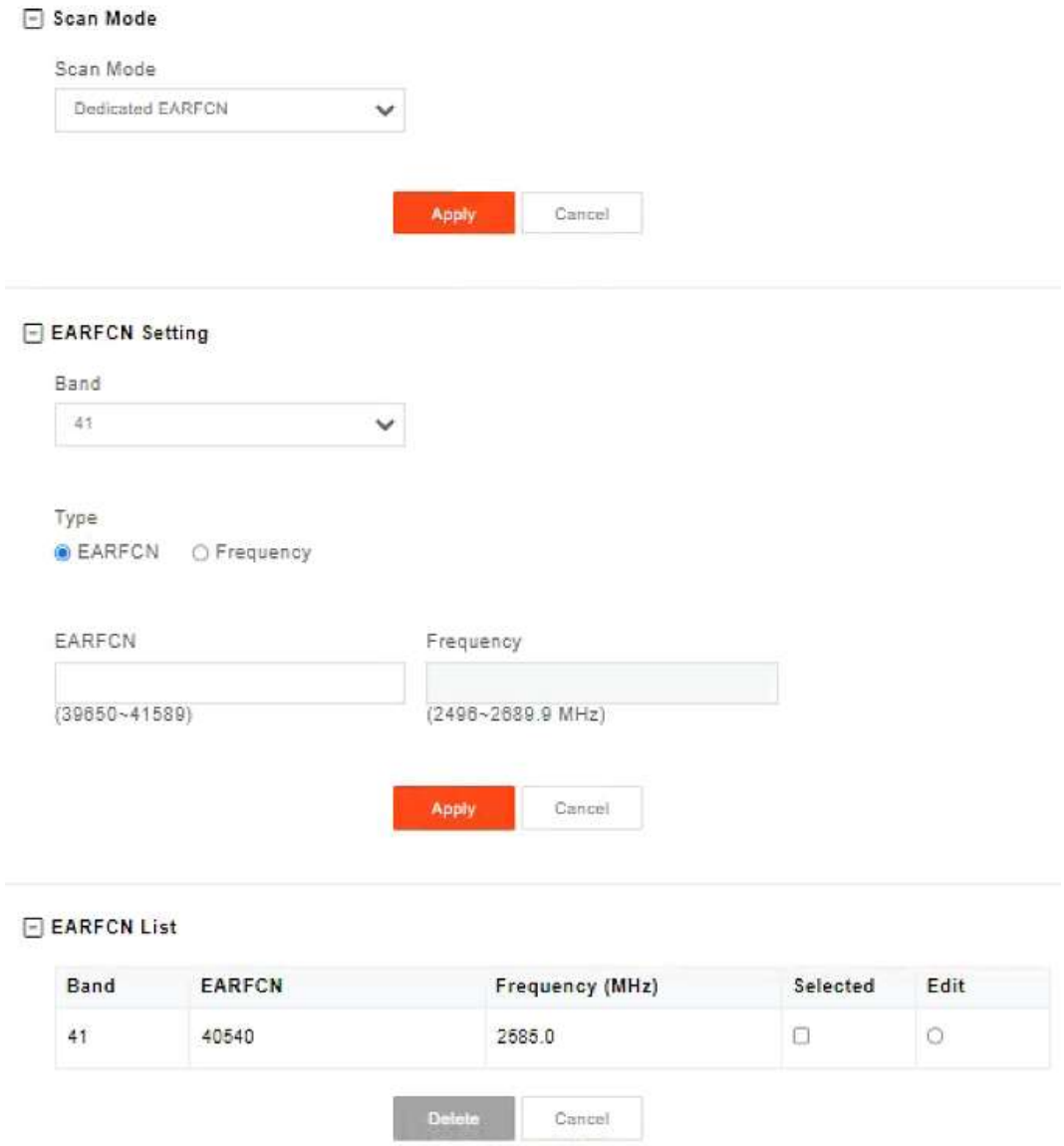
Select one of the following options:

- **Full Band** (default) – All channels in the band. (Figure 3-19)
  - The CPE will routinely scan all channels in the band and all EARFCNs, increasing the time it takes to connect compared to the other modes. The band is dependent on the CPE model.

Figure 3-19 Full Band

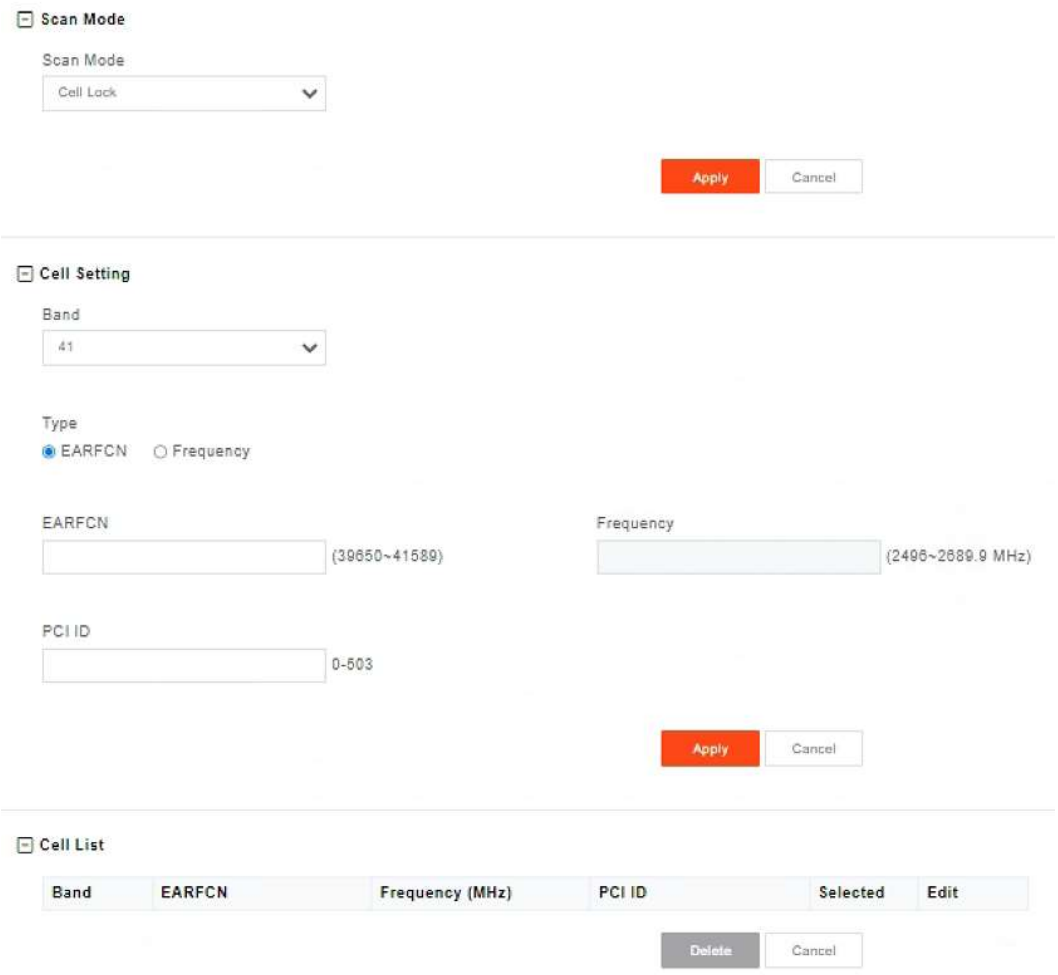
- **Dedicated EARFCN** – Specific EARFCNs or frequencies. (Figure 3-20)
  - The CPE will scan the dedicated EARFCN or frequency list first when it is powered on.
  - After the frequency locking point is configured, even if the locked frequency point cell cannot be accessed, CPE will not search and access cells other than the locked frequency point cell. Up to 10 frequency information can be added.

Figure 3-20 Dedicated EARFCN



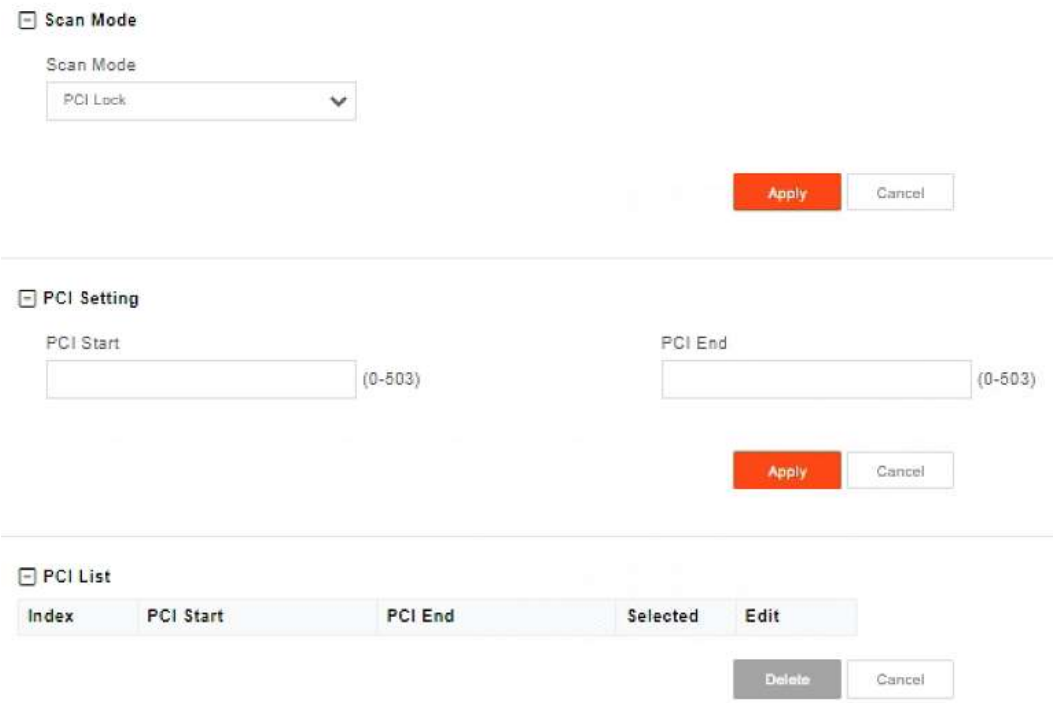
- **Cell Lock** – A combination of PCI + EARFCN or frequency. (Figure 3-21)
  - The CPE is limited to scanning a specific list of eNBs based on both their Physical Cell Identifier (PCI) and EARFCN or frequency. The CPE will scan the list of eNBs with the EARFCN and PCI combination. Using this mode can accelerate network access time. Up to 10 frequency and PCI information can be added.

Figure 3-21 Cell Lock



- **PCI Lock**– Specific PCIs only. Locks the CPE to a designated PCI or PCI range. (Figure 3-22)

Figure 3-22 PCI Lock



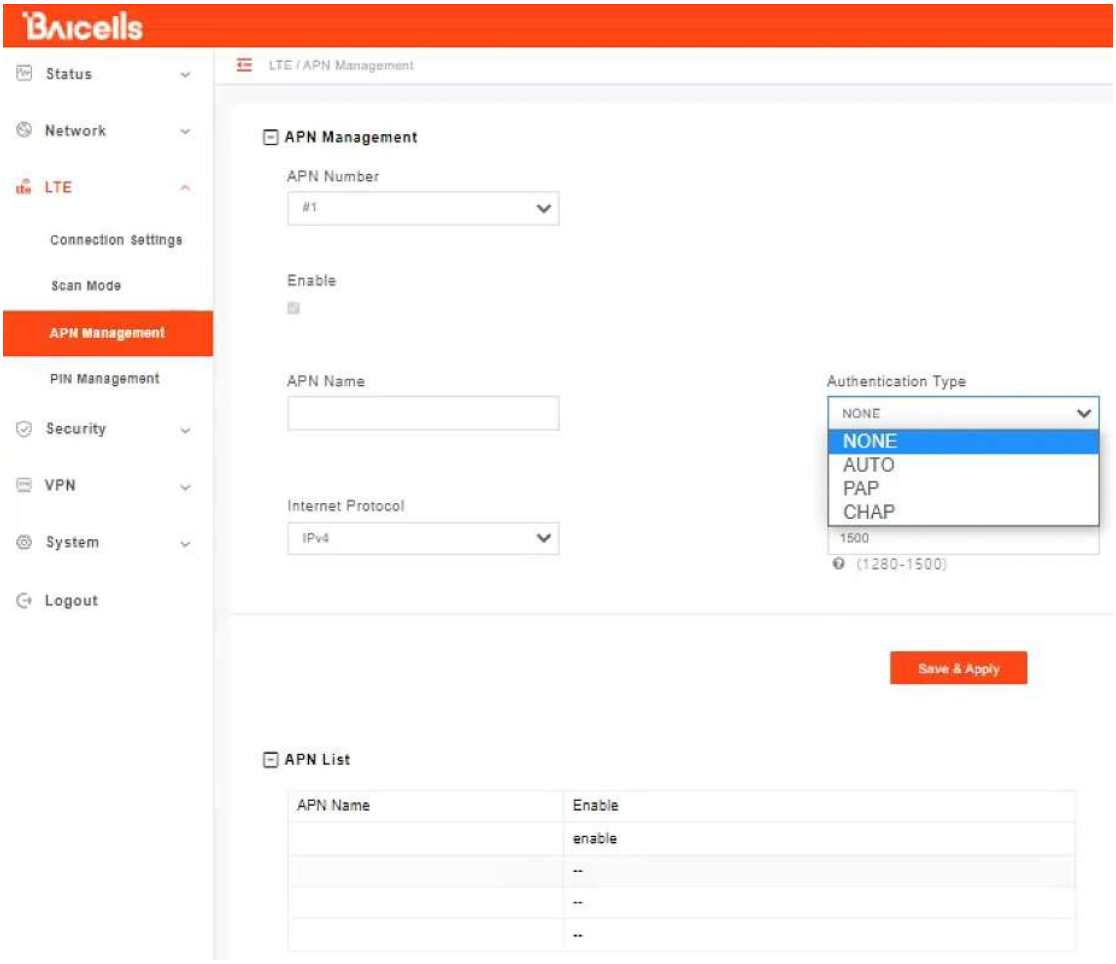
After selecting an option, enter the required information.

3.3.3 APN Management

An Access Point Name (APN) is the name of a gateway between a 3G/4G mobile network and another computer network, frequently the public Internet. Generally, multiple APNs are used for different business flows such as TR-069 management, voice, data, etc., and may support different services and QoS levels for different subscribers.

The CPE supports 4 APN configurations. At least one APN (TR-069) must be configured when the CPE/eNB connect to the Baicells CloudCore. In the window (Figure 3-23) you will select the APN number (1-4), enable it, enter an APN Name, select Authentication Type, select the type of IP addressing (IPv4), and set the MTU value for the APN.

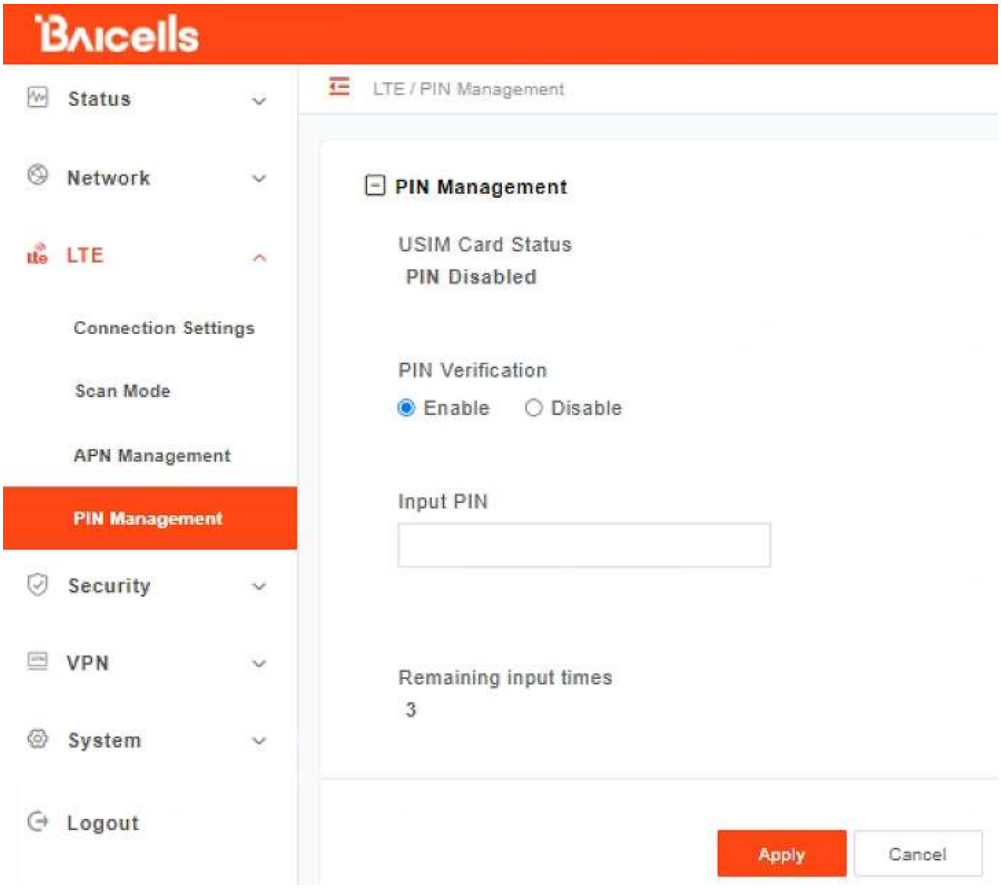
Figure 3-23 APN Management



3.3.4 PIN Management

Use the PIN Management feature if you want to require users to enter a PIN code before they can use the CPE to access the network (Figure 3-24). Once the PIN is enabled, you will need to remember it if you want to later modify the number. You are limited to 3 tries to enter the correct PIN code before getting locked out. If this happens, contact your service provider (end-users) or Baicells support (service providers).

Figure 3-24 PIN Management

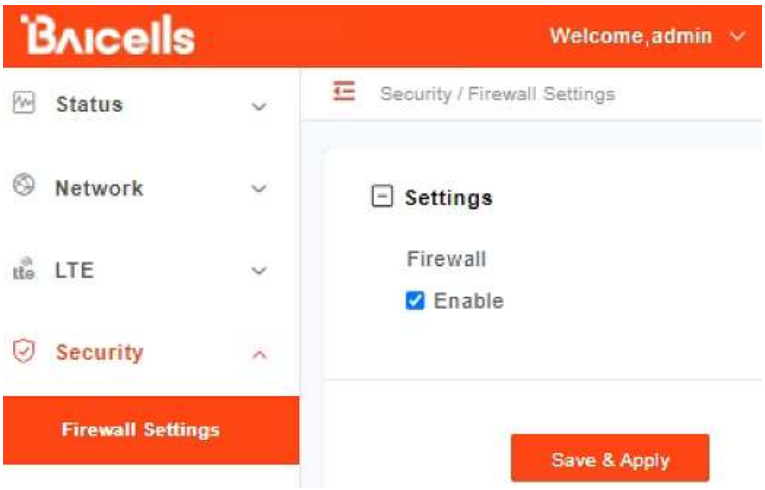


3.4 Security Menu

3.4.1 **Firewall Settings**

When using a firewall server in the local network, invoke this setting to enable or disable the firewall for this CPE (Figure 3-25).

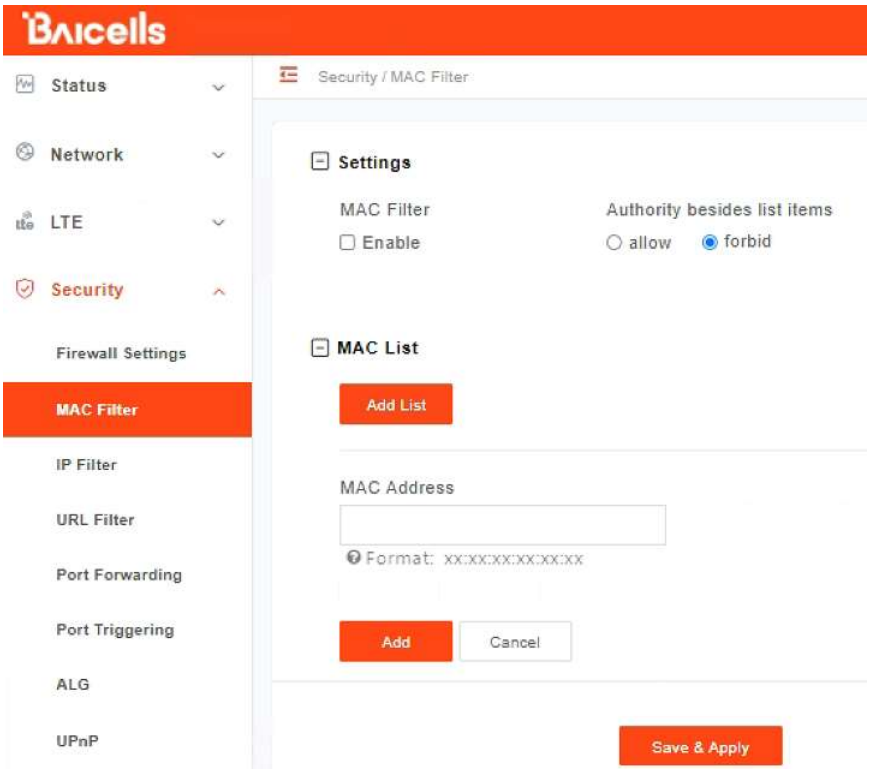
Figure 3-25 Firewall



3.4.2 **MAC Filter**

Media Access Control (MAC) Filtering allows you to identify a list of devices either allowed to access or forbidden from accessing the network through the CPE (Figure 3-26). Select *Enable* to enable MAC filtering, and then determine whether you will allow or forbid the defined MAC addresses to access the network.

Figure 3-26 MAC Filter



3.4.3 IP Filter

Internet Protocol (IP) Filtering allows you to filter services based on the IP address of the source device that is using the CPE to access the network (Figure 3-27). You can define a list of devices either allowed or forbidden from accessing the destination address range or port number range you enter.

To use this feature, select the *Enable* check box and then click on ADD LIST to open the settings window. Enter the source devices' IP addresses. Refer to Table 3-3 for a description of each field.

Figure 3-27 IP Filter

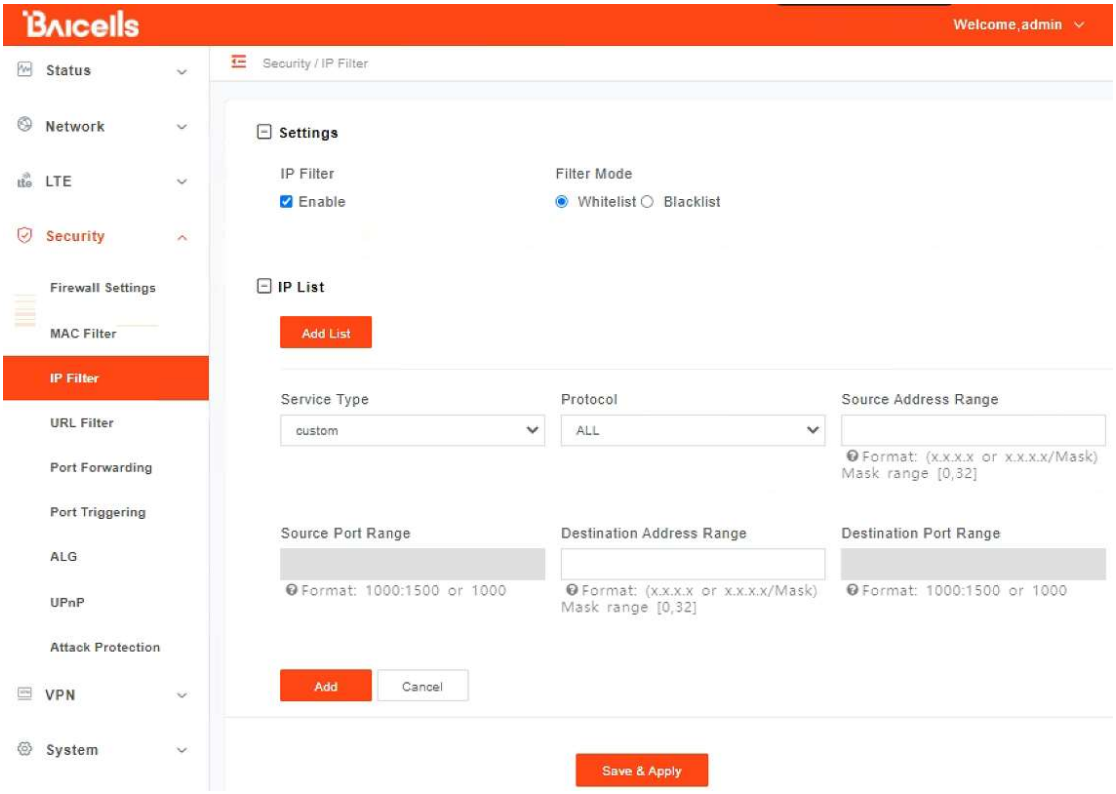


Table 3-3 IP Filter

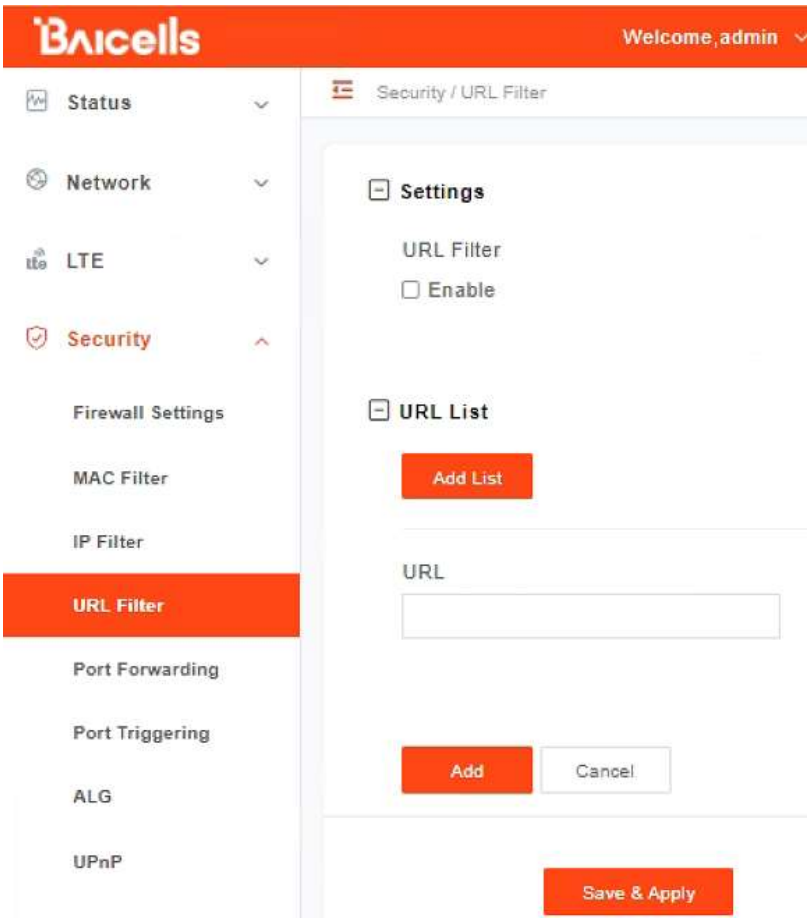
Field Name	Description
Service Type	Select the type of service, either custom, FTP, SSH, TELNET, SMTP, HTTP, POP3, HTTPs, or HTTP Proxy, the CPE will be allowed or forbidden to use
Protocol	Select the type of data protocol, either ALL, TCP, UDP, TCP&UDP, or ICMP the CPE will be allowed or forbidden to use
Source Address Range	Enter the IP address range for the source device(s) in the format of x.x.x.x or x.x.x.x/mask. The mask value may be 0 or 32.
Source Port Range	Enter the port number range for the source device(s) in the format of 1000 to 1500, or 1000.

Destination Address Range	Enter the IP address range for the destination device(s) to be filtered, in the format of x.x.x.x or x.x.x.x/mask. The mask value may be 0 or 32.
Destination Port Range	Enter the port number range for the destination device(s) to be filtered, in the format of 1000 to 1500, or 1000.

3.4.4 URL Filter

The Uniform Resource Location Filter (*URL Filter*) allows you to define a list of URL addresses users are forbidden from accessing. When you enable the filter, a *Settings* window appears. Enter the specific URL address users cannot access, as shown in Figure 3-28. To add more URL addresses, click on *ADD*. After entering the addresses and saving, the URL(s) you enter will appear in the URL List.

Figure 3-28 URL Filter



3.4.5 Port Forwarding

When NAT mode is enabled as the WAN interface type (section 2.2.2), you can redirect a communication request from one address and port number combination to another. Only the IP address on the WAN side is open to the Internet. If a computer on the LAN is enabled to provide services for the Internet (for example, work as an FTP server), port forwarding is required so that all access requests to the external server port from the Internet are redirected to the server on the LAN.

To add a port forwarding rule, select the *Enable* check box and click on *ADD LIST* (Figure 3-29). Enter the parameters per the field descriptions in Table 3-4.

Figure 3-29 Port Forwarding

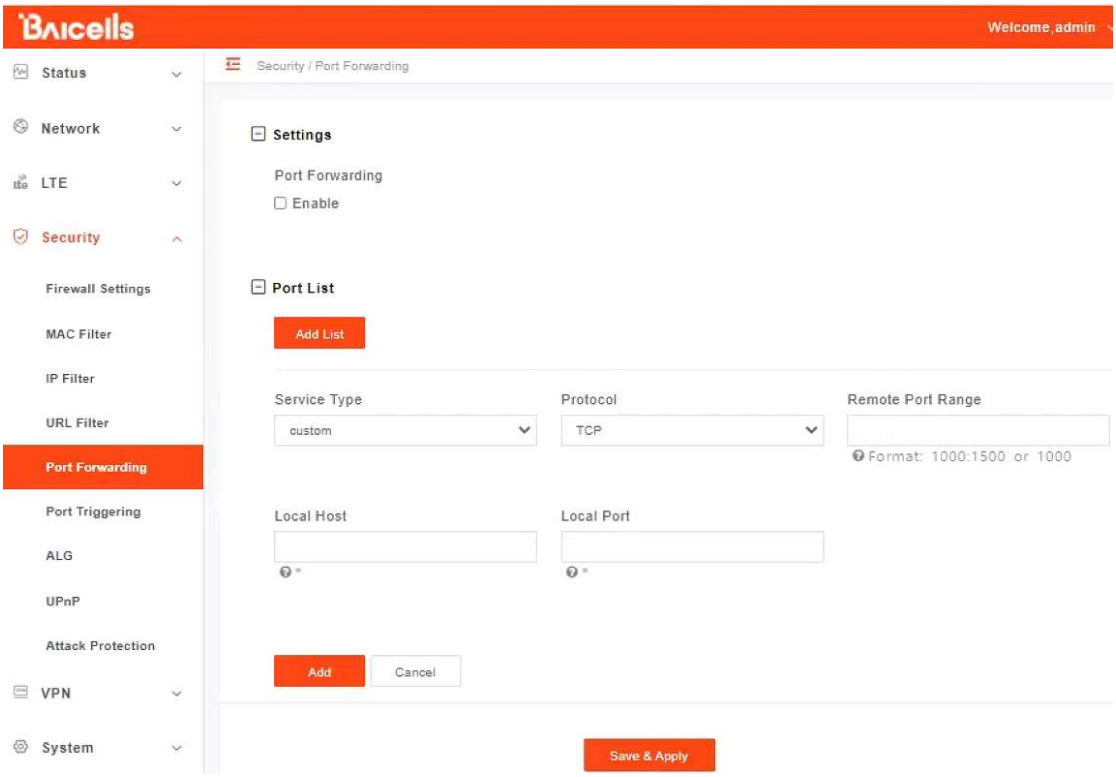


Table 3-4 Port Forwarding

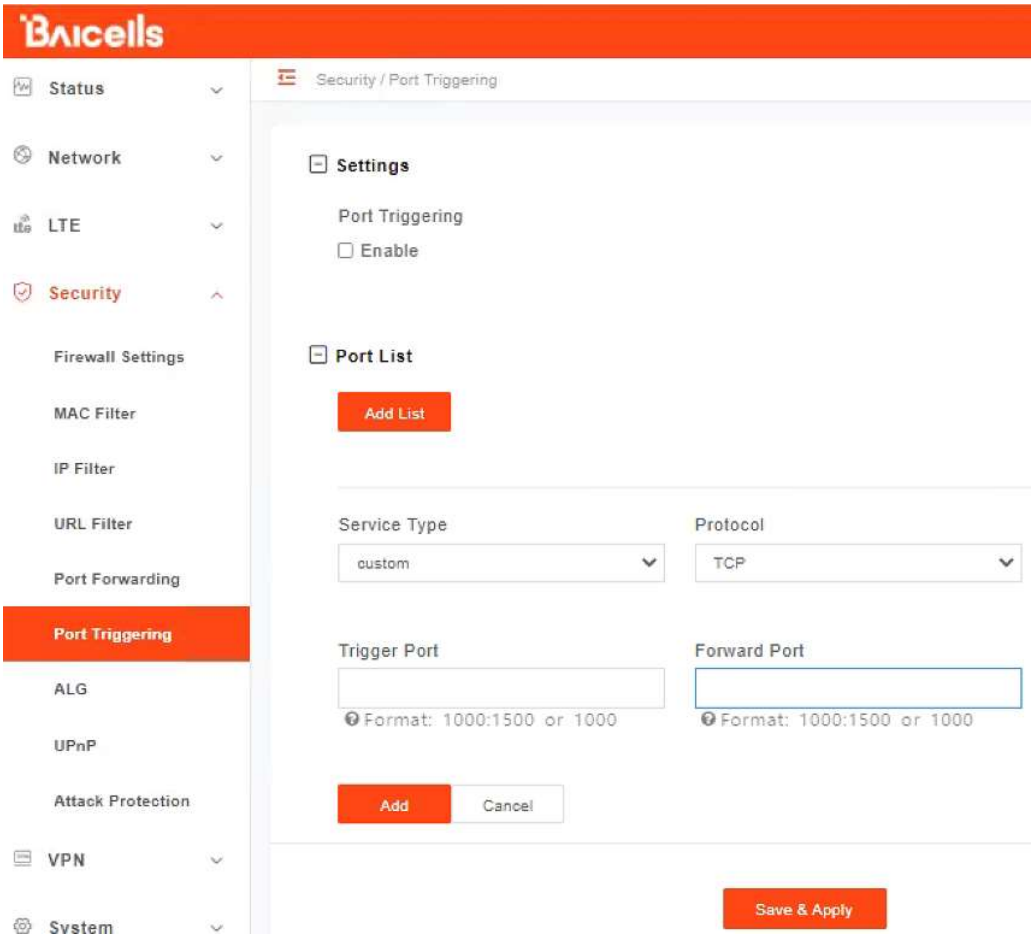
Field Name	Description
Service Type	Select the type of service, either Custom, DNS, FTP, IPSec, POP3, SMTP, PPTP, Realplay, SSH, HTTPs, SNMP, SNMP Trap, Telnet, TFTP, or HTTP
Protocol	Select the type of data protocol, either TCP, UDP, or TCP&UDP
Remote Port Range	Enter the port number range for the remote device in the format of 1000 to 1500
Local Host	Enter the local host IP address. The address must be different from the IP address that is set for the LAN Host Settings parameter, but

	they must be on the same network segment.
Local Port	Enter the local port number. Range is 1 to 65,535.

3.4.6 **Port Triggering**

Port Triggering is a configuration option on a router - in this case, the CPE - if it is operating in NAT mode as the WAN interface type (section 2.2.2). When an application uses a trigger port to build a connection, the CPE will forward the data to the forward port.
To configure the feature, click on the check box next to *Enable* and then click on *ADD LIST* to enter the service type, protocol, trigger port, and forward port (Figure 3-30).

Figure 3-30 Port Triggering

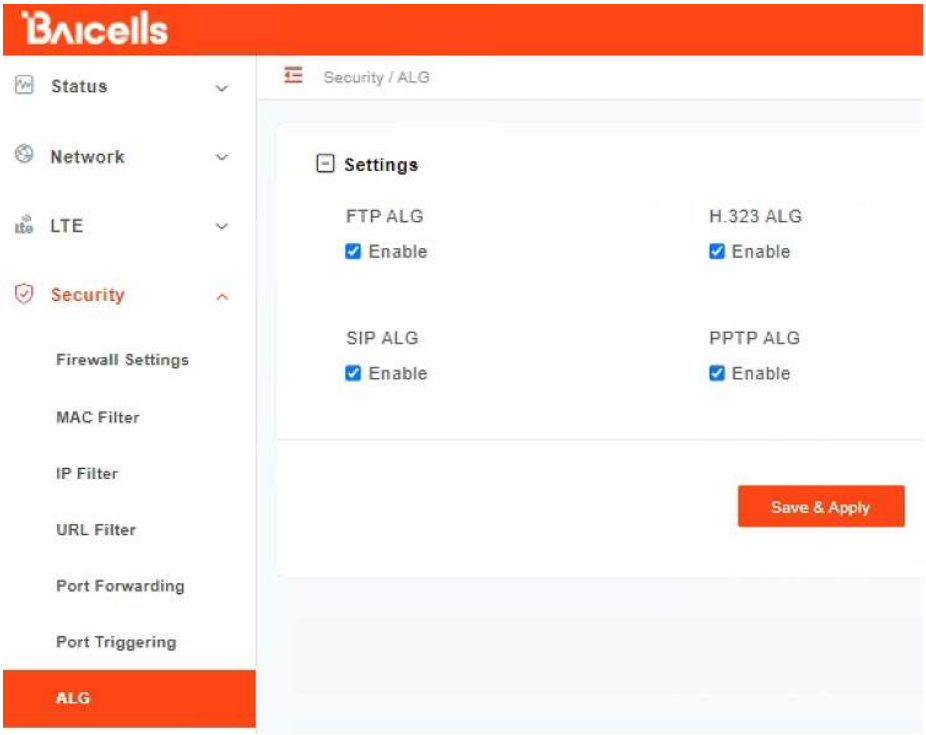


3.4.7 **ALG**

The Application Layer Gateway (ALG) function provides a security component that augments a firewall or the NAT used by the CPE (if WAN Network Mode = NAT). It allows customized NAT traversal filters to be plugged into the gateway to support address and port

translation for certain application layer control/data protocols such as FTP, H.323 ALG, SIP, and PPTP. You can enable the different types of application protocols by clicking on the check box next to the protocol name (Figure 3-31).

Figure 3-31 ALG

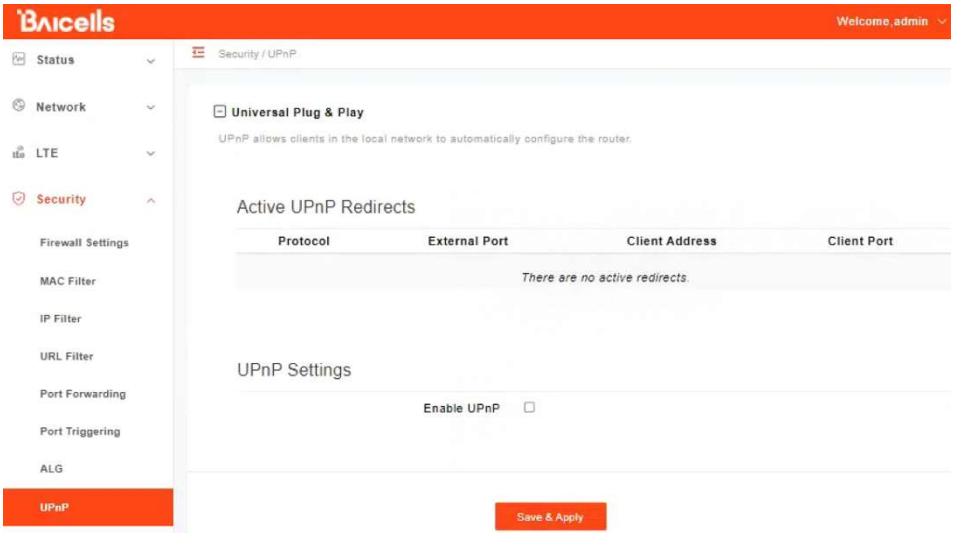


3.4.8 **UPnP**

The *Universal Plug & Play* (UPnP) function provides a set of networking protocols that allows device-to-device networking on a local network. When UPnP is enabled, devices seamlessly and dynamically discover each other's presence on the network and attach to one another and to network services. Often, UPnP is used for streaming media between devices on the network.

Go to Security > UPnP to enable the CPE to be searched by other devices (Figure 3-32). Once enabled, any redirects of traffic will display in the *Active UPnP Redirects* section of the window.

Figure 3-32 UPnP

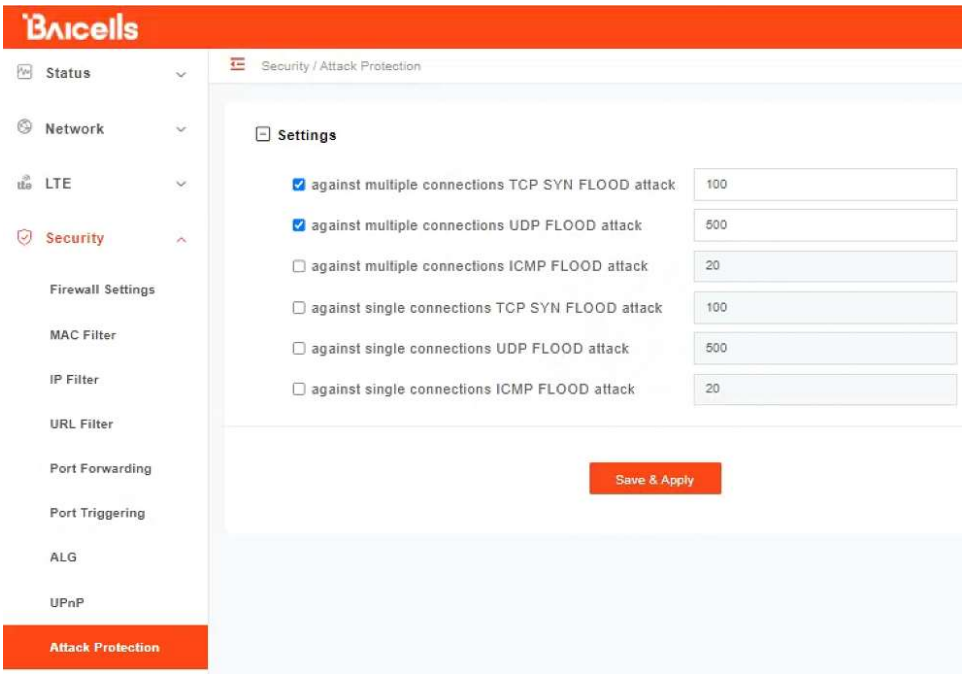


3.4.9 **Attack Protection**

The *Attack Protection* settings provide an additional security measure that helps prevent computer hacker attacks such as TCP SYN FLOOD, UDP FLOOD, and IMCP FLOOD for devices connected to the network through the CPE.

In the Security > Attack Protection window (Figure 3-33), select the check box next to the flood protection options you want to enable. When you click the check box, the field on the right becomes editable. Accept the default timer value, in seconds, or enter a value for each type of attack protection.

Figure 3-33 Attack Protection



3.5 VPN Menu

The Virtual Private Network (*VPN*) menu (Figure 3-34) enables you to configure a connection between the CPE and a VPN, e.g., to access a corporate network when telecommuting for work. You can enable a Layer 2 Tunneling Protocol (L2TP) gateway or a Layer 2 network connection to the VPN.

Figure 3-34: VPN Menu

3.5.1 **IPSec**

The IP security (IPSec) network protocol suite is used between 2 communication points across the IP network. The protocols provide data authentication, integrity, and confidentiality protection services. They are needed for secure key exchange and key management between the two network entities.

The top of the IPSec window is where you can add one or more security policies (Figure 3-35). The status of each policy you create will display in the lower half of the window.

Figure 3-35 IPSec

To configure an IPSec policy for this CPE, select the *ADD POLICY* button (Figure 3-36). Enter the policy name, remote gateway, local and remote subnets, and pre-shared key for the VPN connection. The *Advance Settings* offer additional parameters such as key exchange version, IKE encryption method, etc. Refer to Table 3-5.

Figure 3-36 IPSec

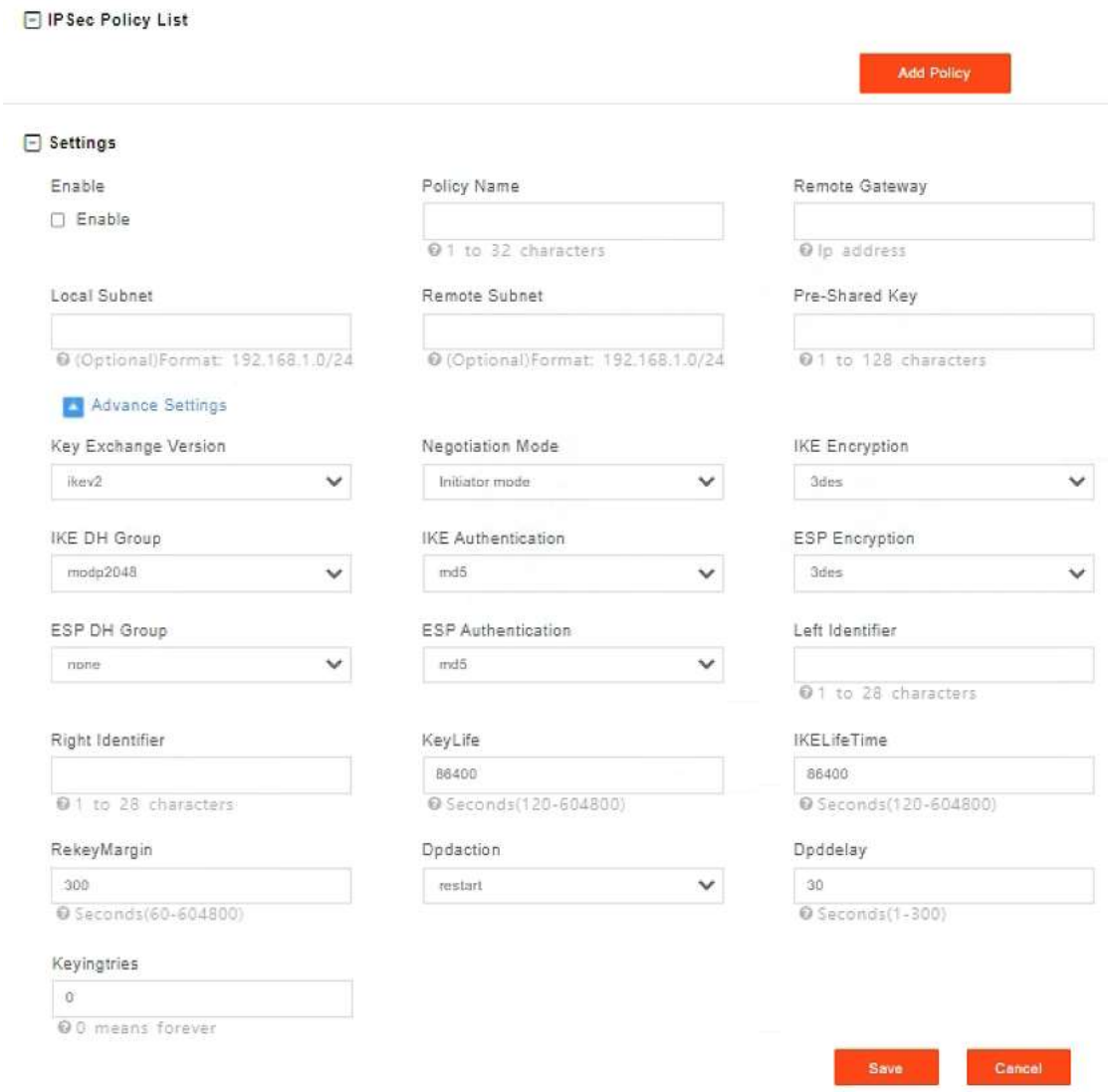


Table 3-5 IPSec

Field Name	Description
Enable	Click on the check box to enable IPSec
Policy Name	Enter a policy name using up to 32 characters
Remote Gateway	IP address of the remote gateway
Local Subnet	Optional: IP address of the local subnet
Remote Subnet	Optional: IP address of the remote subnet
Pre-Shared Key	Up to 128 characters
Key Exchange Version	Internet Key Exchange (IKE) encryption method version 2 or version 1. IKE is a protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access.
Negotiation Mode	Initiator mode or Responder mode

IKE Encryption	des, 3des, aes128, aes192, or aes256
IKE DH Group	modp768, modp1024, modp1536, modp2048, or modp4096
IKE Authentication	md5, sha1, sha256, sha384, or sha512
ESP Encryption	des, 3des, aes128, aes192, or aes256
ESP DH Group	none, modp768, modp1024, modp1536, modp2048, or modp4096
ESP Authentication	md5, sha1, sha256, sha384, or sha512
Left Identifier	1-28 characters
Right Identifier	1-28 characters
KeyLife	120-604800 seconds
IKELifeTime	120-604800 seconds
RekeyMargin	120-604800 seconds
Dpdaction	none, clear, hold, or restart
Dpddelay	1-300 seconds
Keyingtries	0 means forever

3.5.2 **OpenVPN**

OpenVPN is an open-source, Virtual Private Network (VPN) encryption protocol. As well as being extremely secure, OpenVPN is highly customizable and can be implemented in a number of different ways. For that reason, using this VPN method requires significant networking experience to implement. The range of options includes remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions. The remote access solutions support robust capabilities such as load balancing, failover, and more granular access controls, e.g., articles, examples, security overview, and non-English languages.

OpenVPN implements OSI Layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol. It supports flexible client authentication methods based on certificates, smart cards, and/or two-factor authentication, and allows user or group-specific access control policies using firewall rules applied to the VPN interface. Setting up OpenVPN involves configuring server and client settings. Refer to Figure 3-37, Figure 3-38 (server), and Figure 3-39 (client) configuration fields.

Figure 3-37 OpenVPN

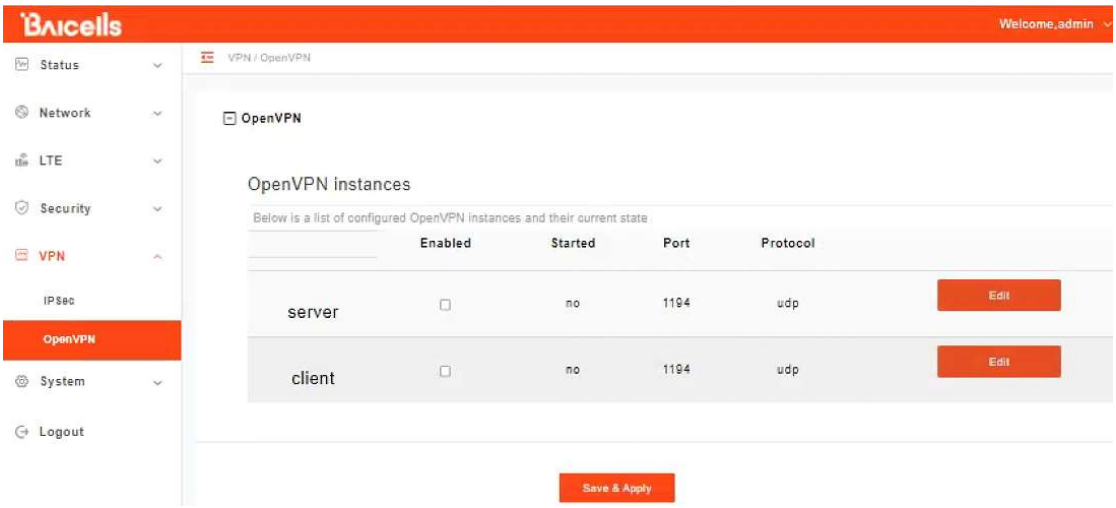


Figure 3-38 Server

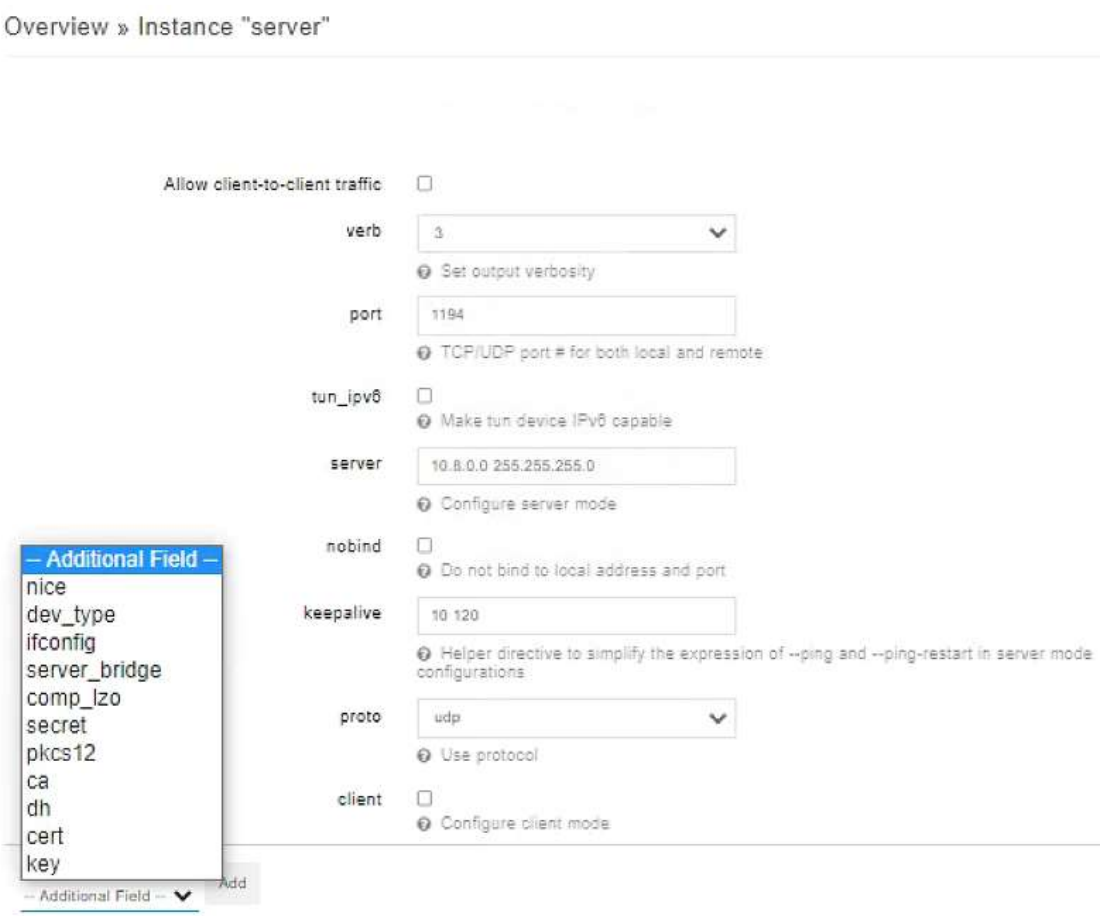
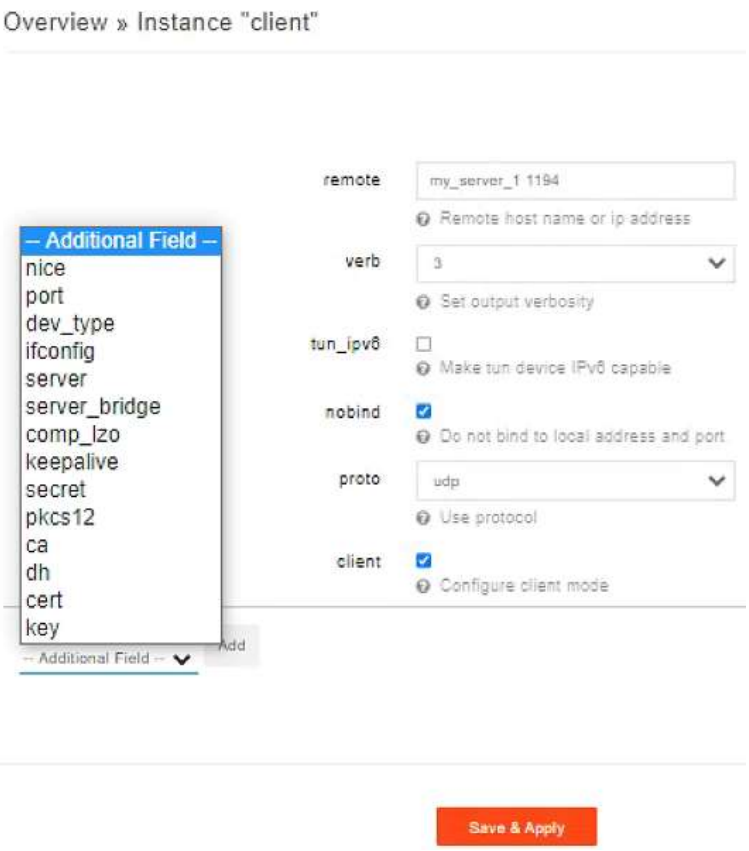


Figure 3-39 Client

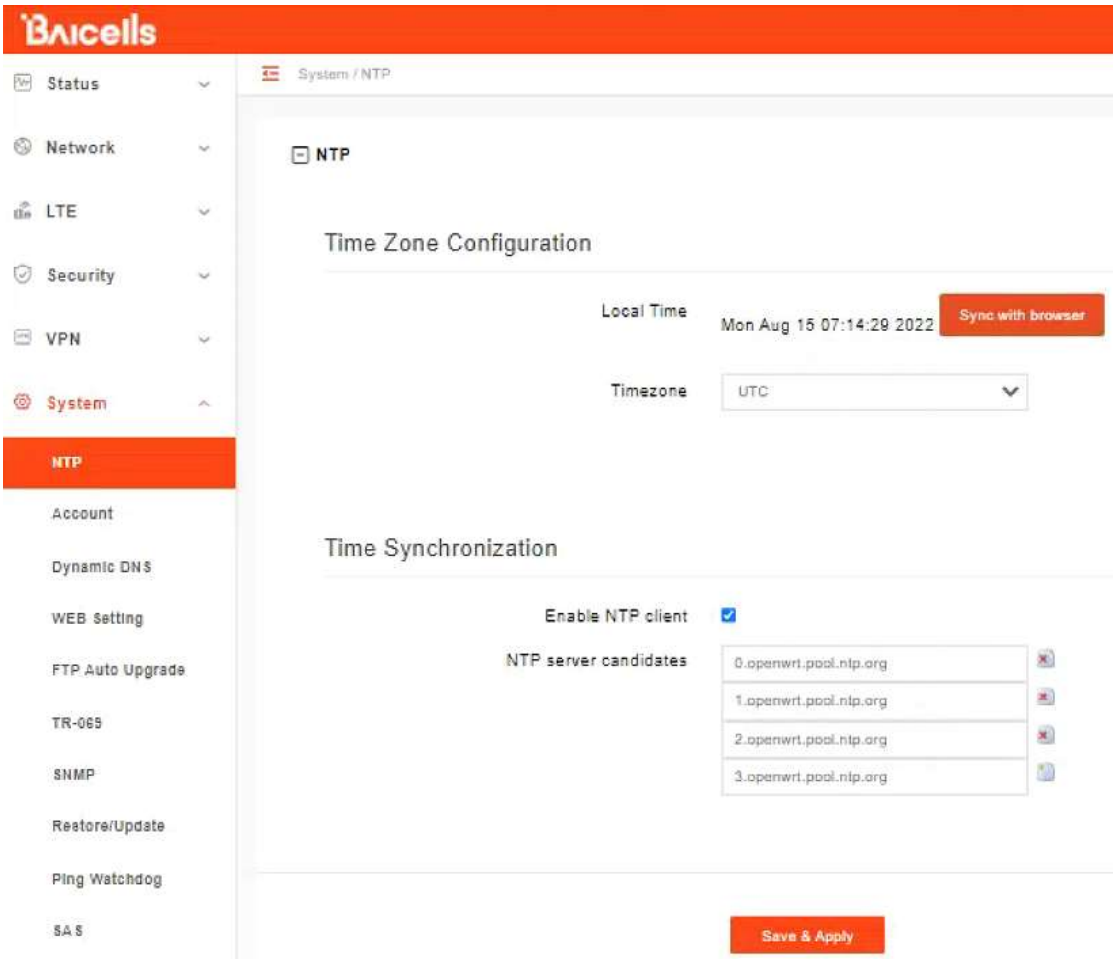


3.6 System Menu

3.6.1 **NTP**

The operator's network may use up to 4 Network Time Protocol (NTP) servers to provide correct time-of-day to network devices. In the CPE GUI you can refresh the local time display using the *SYNC WITH BROWSER* button; select the time zone that the CPE is in; and enable NTP client to use the default or specified NTP servers for synchronization (Figure 3-40).

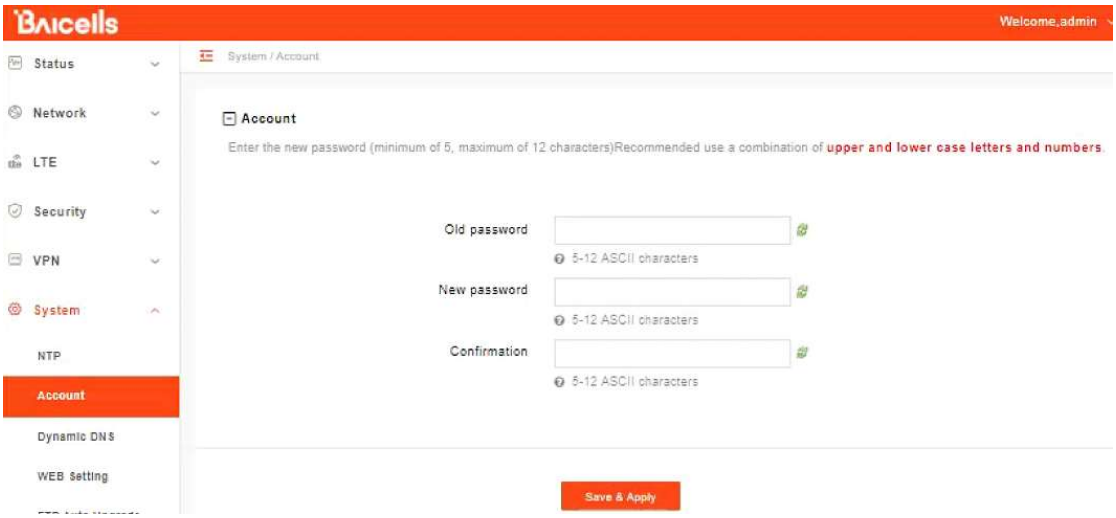
Figure 3-40 NTP



3.6.2 **Account**

This menu is used to change the login password for the CPE (Figure 3-41). The password must be 5 to 12 characters. Baicells recommends using a combination of upper- and lower-case letters and numbers.

Figure 3-41 Account



3.6.3 **Dynamic DNS**

The dynamic DNS function is to map the user's dynamic IP address to a fixed domain name resolution service. Each time the user connects to the network, the client program will transmit the dynamic IP address of the host to the server program located on the host of the service provider through information transmission. The server program is responsible for providing DNS service and realizing dynamic domain name resolution.

Figure 3-42 Dynamic DNS Overview

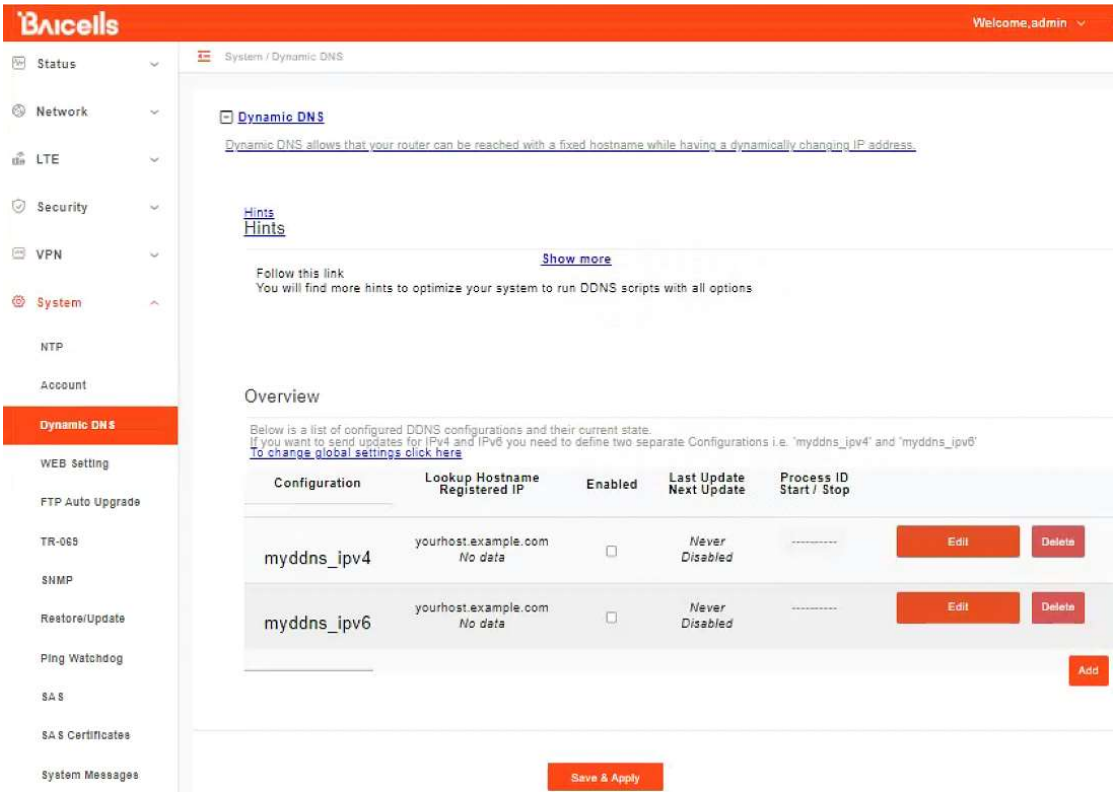


Figure 3-43 Dynamic DNS Global Settings

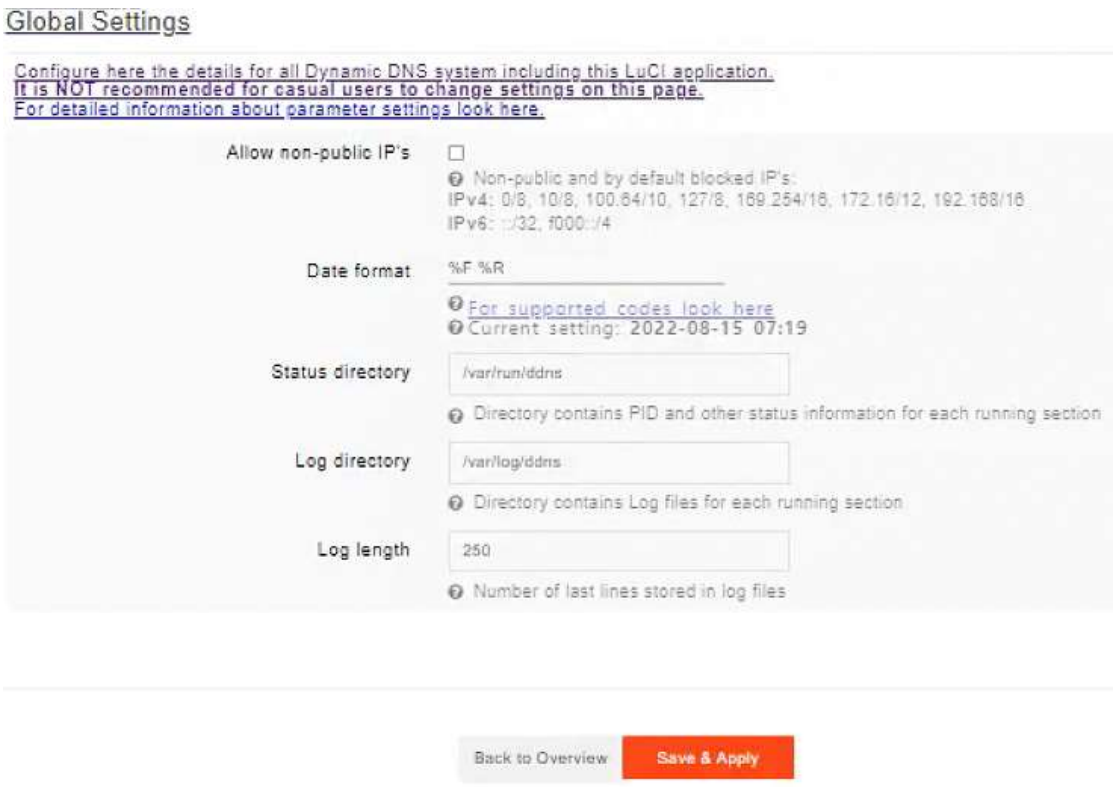


Figure 3-44 IPv4 DDNS configuration

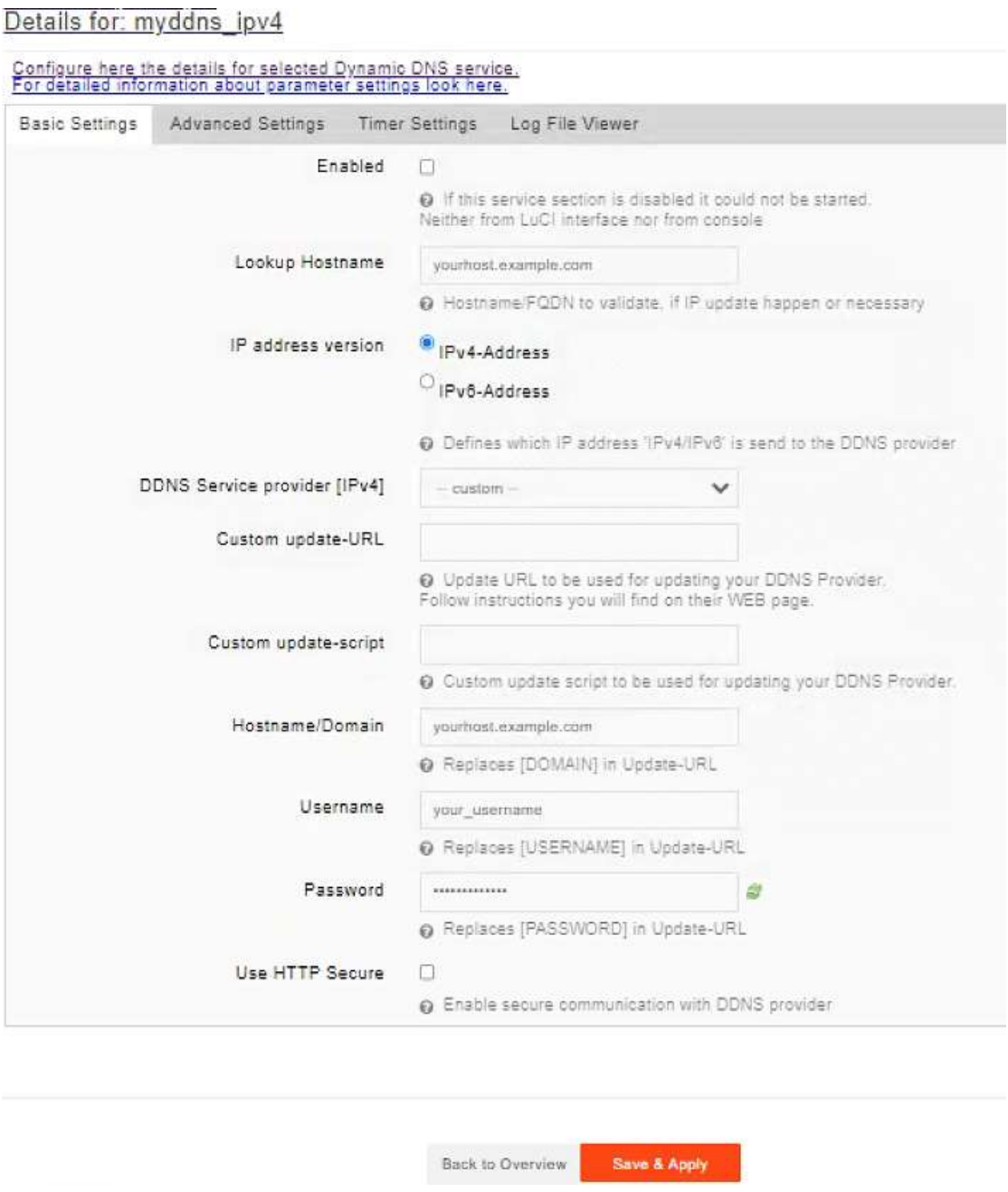


Figure 3-45 IPv6 DDNS configuration

3.6.4 **WEB Setting**

WEB Setting provides the ability to configure and manage the CPE remotely (Figure 3-46). This is especially helpful when a user calls in for technical assistance. In “**错误!未找到引用源。 错误!未找到引用源。**”, you used this Web application with the default URL of http://192.168.150.1. Refer to Table 3-6 for a description of each field.

Figure 3-46 WEB Setting

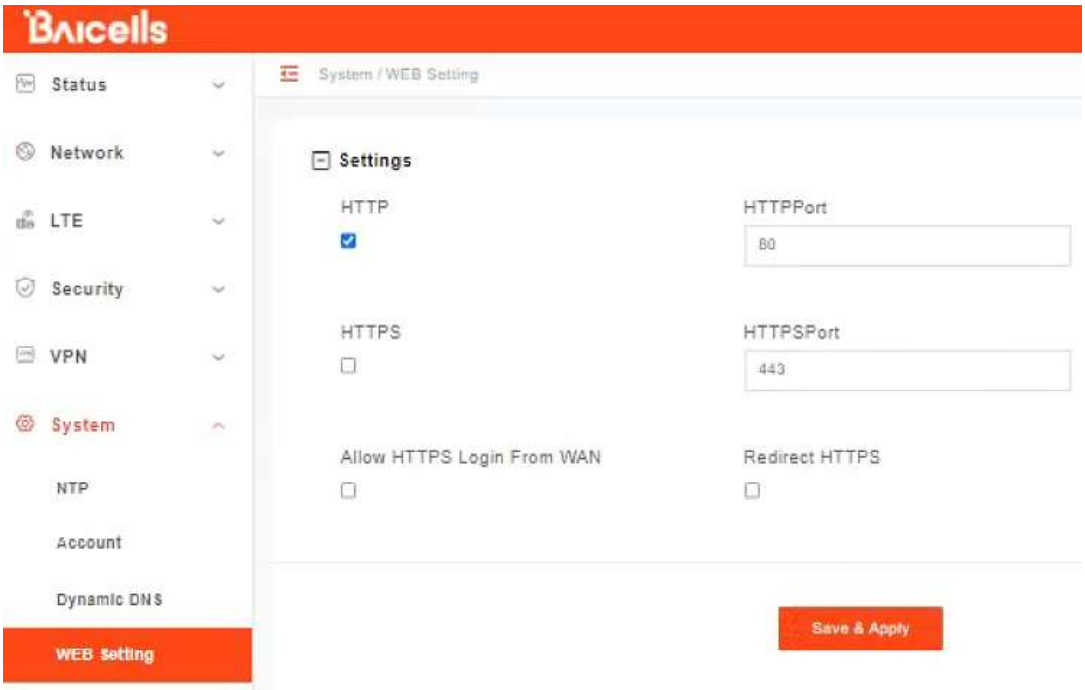


Table 3-6 WEB Setting

Field Name	Description
HTTP	Select the check box next to Enable to log in to an HTTP Web address
HTTPPort	Enter the HTTP port number to be used. Range is 80 to 65,535. Default is port 80. Note: Port cannot be set to 8080. Because 8080 is already occupied by the module port number.
HTTPS	Select the check box next to Enable to log in to an HTTPS Web address
Redirect HTTPS	Select the check box to allow HTTP addresses to be redirected to more secure HTTPS addresses
Allow HTTPS Login From WAN	Select the check box next to enable log in to an HTTPS Web address from the WAN
HTTPSPort	Enter the HTTPS port number to be used. Range is 80 to 65,535. Default is port 80. Note: Port cannot be set to 8081. Because 8081 is already occupied by the module port number.

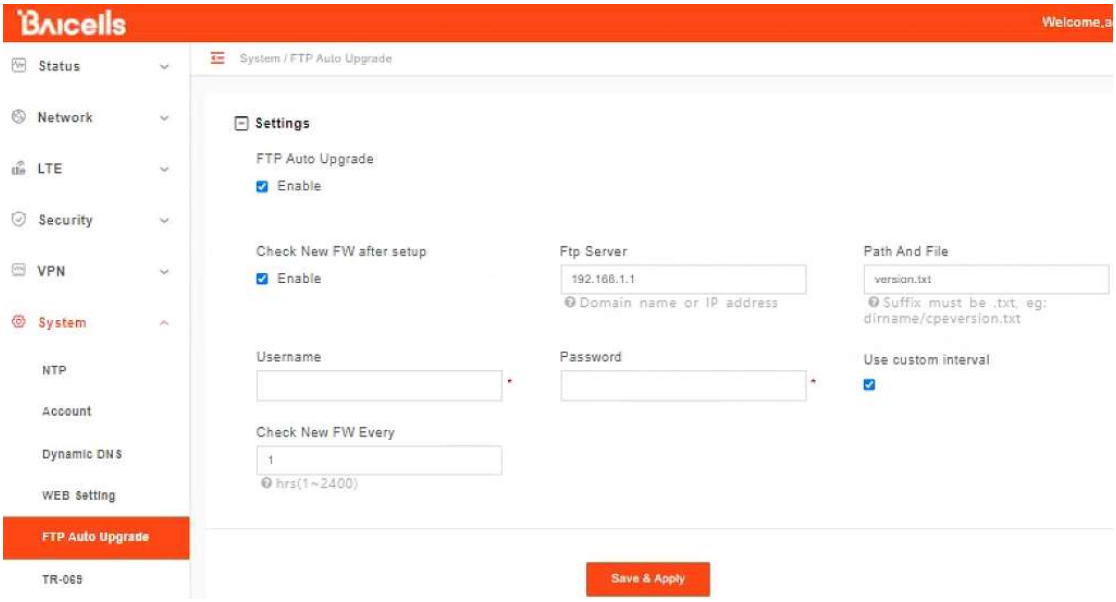
3.6.5 FTP Auto Upgrade

The FTP Auto Upgrade feature is used for over-the-air (OTA) upgrades. The CPE will

detect a new version of firmware on the dedicated FTP server, if available, and will automatically upgrade to the new version.

If you are using a dedicated FTP server for this purpose, select the *Enable* check boxes next to *FTP Auto Upgrade* and *Check New FW after setup* (Figure 3-47). Enter the FTP server IP address and the *Path And File* text suffix. If login permissions are required to access the server, enter the username and password. To configure a set interval for the CPE to check the server for new firmware, select the check box next to *Use custom Interval* and enter the interval time, in hours. The range is 1-2400 hours.

Figure 3-47 FTP Auto Upgrade



3.6.6 **TR-069**

If your network operates using a TR-069 auto-configuration server (ACS), the ACS will automatically provide the CPE configuration settings. Once you set up both the ACS and the CPE, you do not need to enter any other parameters through the CPE GUI. Use the *TR069* sub-menu to enable the TR-069 function for the CPE (Figure 3-48). Refer to Table 3-7 for a description of each field.

Figure 3-48 TR-069

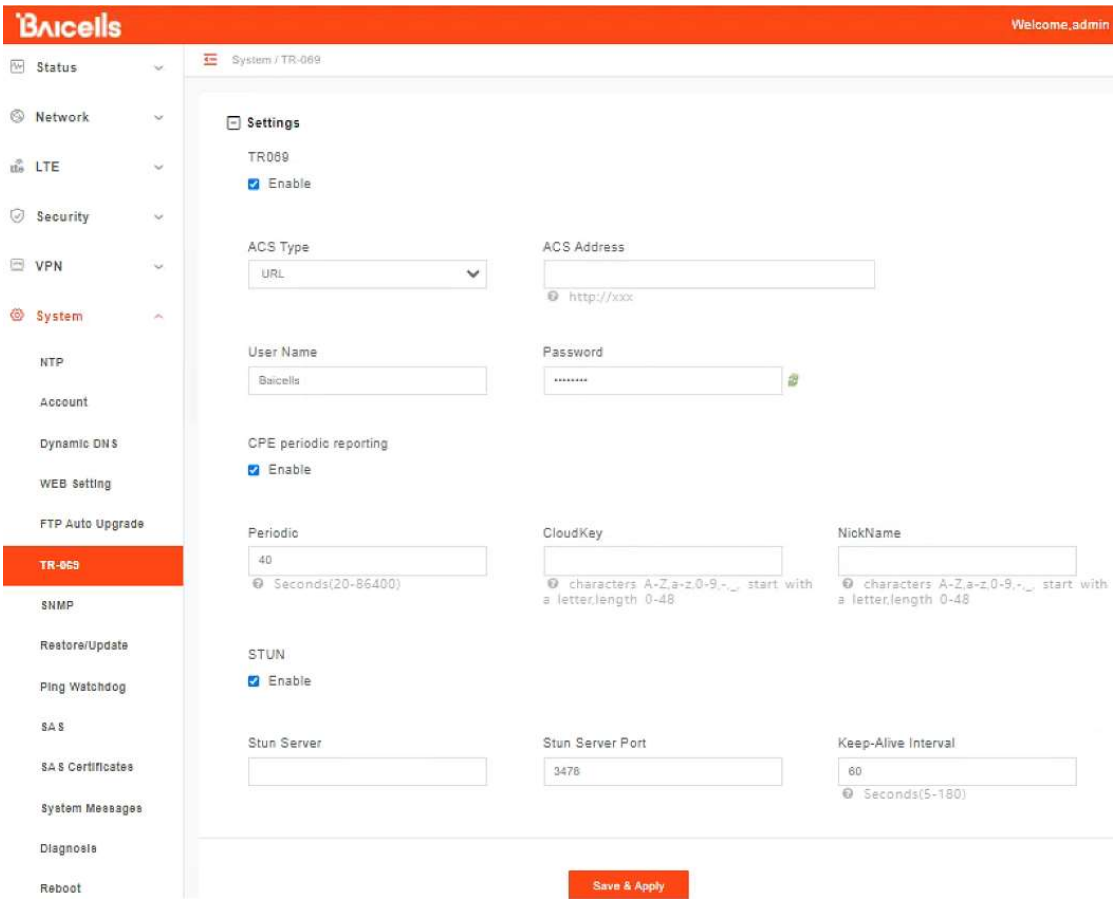


Table 3-7 TR-069

Field Name	Description
TR069	Select the check box next to Enable if using a TR-069 auto-configuration server (ACS) to configure the CPE
ACS Type	Select URL or DHCP to identify the source of the ACS server. When you select URL, the next field (ACS Address) appears.
ACS Address	Enter the server Web address
User Name	Enter the user name to access the ACS server
Password	Enter the password to access the ACS server
CPE periodic reporting	Select the check box next to Enable to enable the CPE to periodically check with the ACS server for new software
Periodic	If you enabled CPE periodic reporting, input how often the CPE should check the ACS server for new information. The range is 20 to 86,400 seconds.
CloudKey	If using the Baicells CloudCore, enter the operator's unique CloudKey. When the device powers up the first time it will automatically be added to the operator's OMC account.
NickName	Optional – enter a nickname to identify the server

Field Name	Description
STUN	TR069 supports NAT penetration, and OMC can send TR069 request to CPE
Stun Server	Nat penetration server address
Stun Server Port	Nat penetration server port
Keep-Alive Interval	Interaction cycle between CPE and NAT server

3.6.7 **SNMP**

The Simple Network Management Protocol (SNMP) is used for connecting a device with a Network Management System (NMS) server. An operator's NMS can monitor and control the connected CPEs that have SNMP enabled. The NMS is able to collect event logs, alarm logs, and other data from those CPEs.

To enable SNMP, select the *Enable* check box (Figure 3-49). Complete the settings per the field descriptions in Table 3-8.

Figure 3-49 SNMP

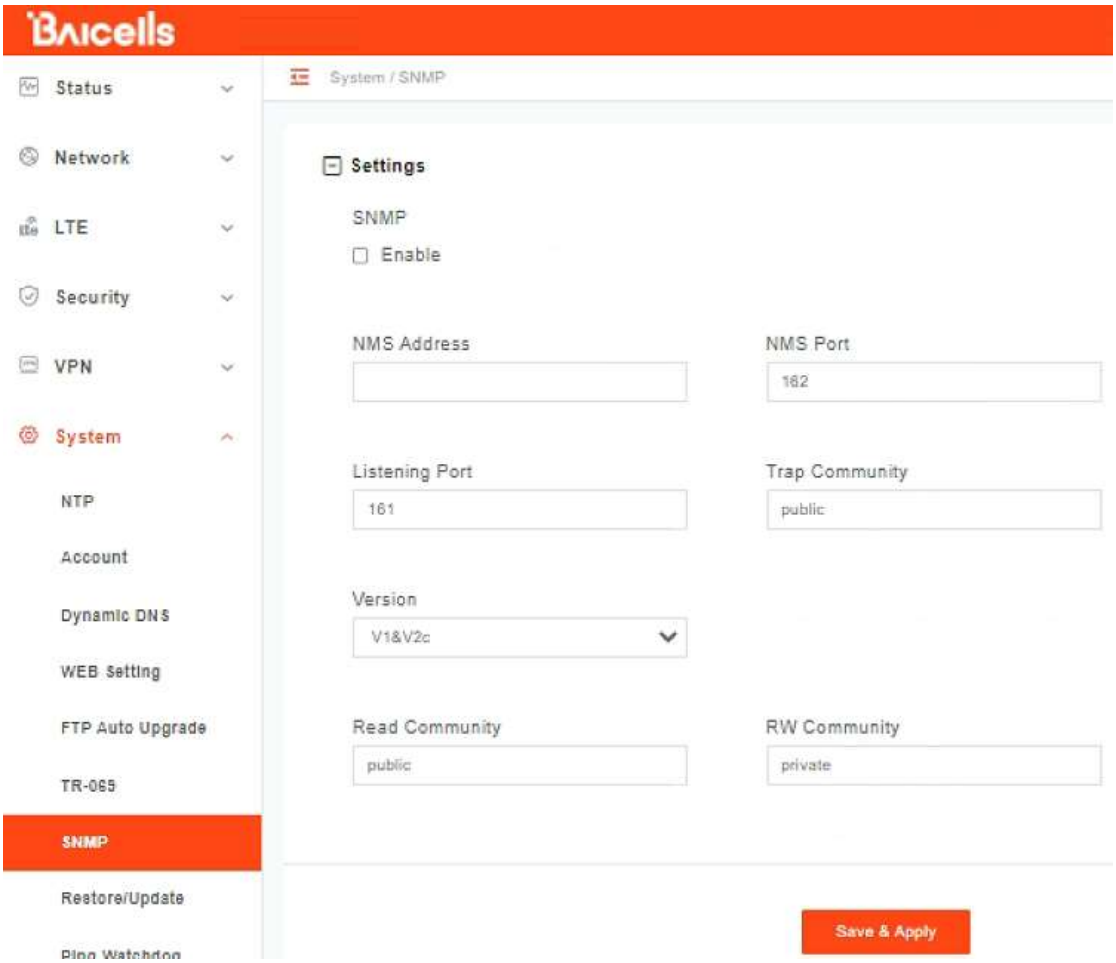


Table 3-8 SNMP

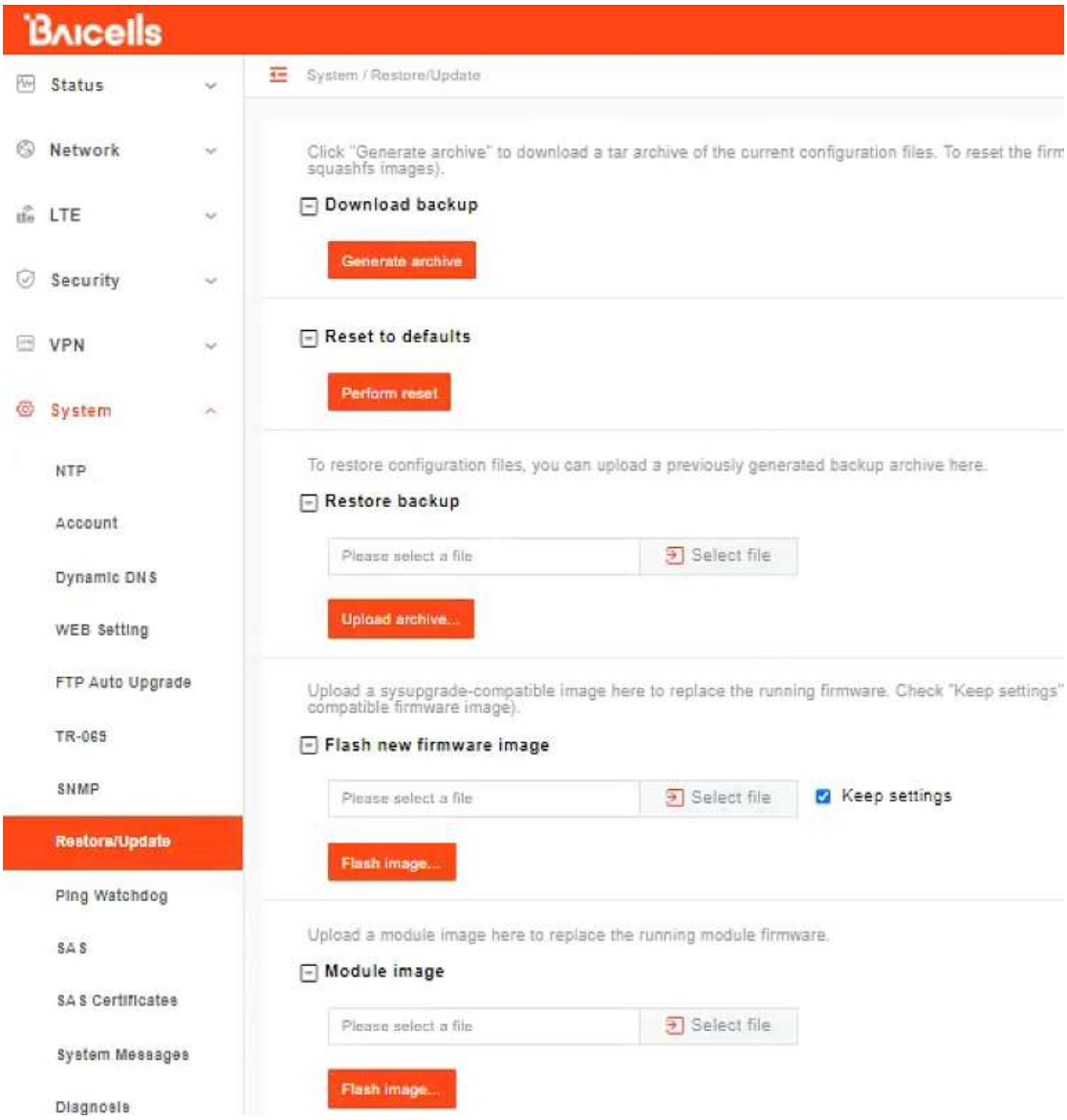
Field Name	Description
SNMP	Enable the Simple Network Management Protocol by clicking the check box.
NMS Address	NMS server IP address
NMS Port	NMS server port number
Listening Port	CPE port number
Trap Community	Public or private - identifier to distinguish read/write permissions for data
Version	Select the SNMP version you are implementing - V1&V2c (for SNMPv1+SNMPv2c) or V3 (for SNMPv3)
Read Community	Public or private read-only community name
RW Community	Public or private read/write community name

3.6.8 **Restore/Update**

Use the System > Restore/Update menu to reset the CPE to its factory default settings, to manually update the firmware, or to manually update a module within the firmware - meaning to apply a patch to the current firmware (Figure 3-50).

Caution: Performing a restore or update action will disrupt service.

Figure 3-50 Restore/Update



3.6.8.1 Restore

To initiate a restore action, click on the **PERFORM RESET** button. The CPE will automatically reset its configuration to the factory default values.

To back up current settings, click the **GENERATE ARCHIVE** button.

To restore configuration files, select backed up file on your computer, and then click the **UPLOAD ARCHIVE** button.

3.6.8.2 Update Firmware

Caution: Do not power off the CPE or disconnect it from the computer during an upgrade.

To update (upgrade) the CPE to a different firmware version (Figure 3-50):

1. Download the image file from the Baicells support website (Baicells > Support > Downloads), and save it to your computer.
2. Under *Flash new firmware image*, determine if you want to keep the current configuration settings on the CPE. If you do, select the check box next to **Keep settings**.
3. Click on **Choose File** to navigate to the new image file on your computer, and then click on **FLASH IMAGE** to initiate the upgrade.

After the upgrade, the CPE will restart automatically running the newer version of code.

3.6.8.3 Update Firmware Module (Patch)

To upgrade a specific module, meaning to apply a patch to the current firmware (Figure 3-50):

1. Download the image file from the Baicells support website (Baicells > Support > Downloads), and save it to your computer.
2. Under *Module upgrade*, click on **Choose File** and navigate to the new module image file.
3. Click on **FLASH IMAGE** to initiate the patch upgrade.

3.6.9 **Ping Watchdog**

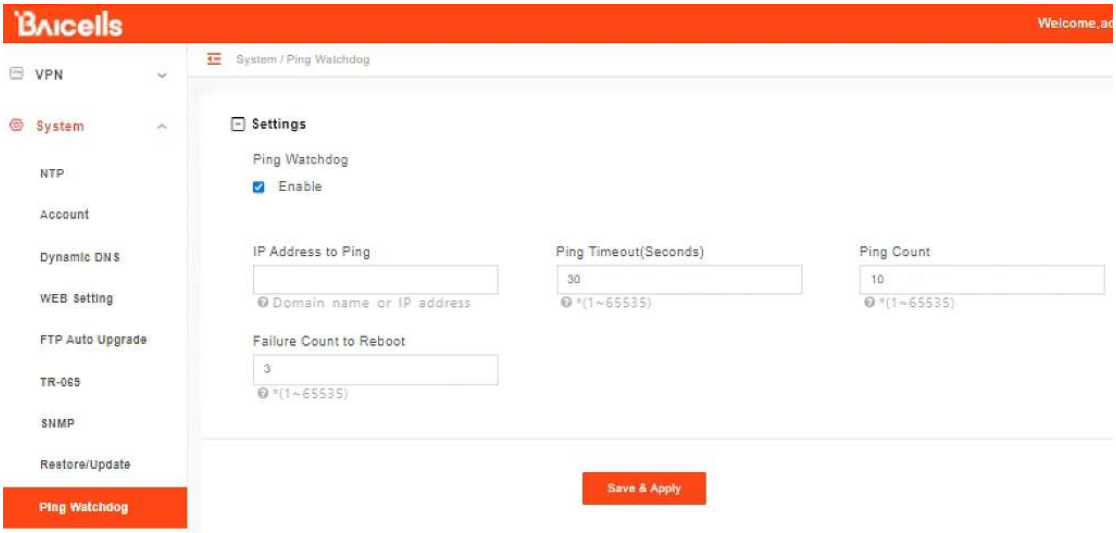
Ping Watchdog is a feature used for detecting the Internet connection state of the CPE. If the CPE cannot connect to the Internet, if this feature is enabled it will reset the LTE module in the CPE firmware or reboot the CPE in an attempt to recover the connection.

To enable the watchdog function (Figure 3-51):

1. Select the check box next to Enable and enter an IP address accessible by Internet for the CPE to try to ping.

2. Set the period of time, in seconds, for the ping to timeout. The range is 1-65535 seconds.
3. Enter the number of times to try to ping the address, in the range of 1-65535 times.
4. Enter the maximum number of times the CPE can try the ping but fail before the CPE initiates a reboot. The range is 1-65535 times.

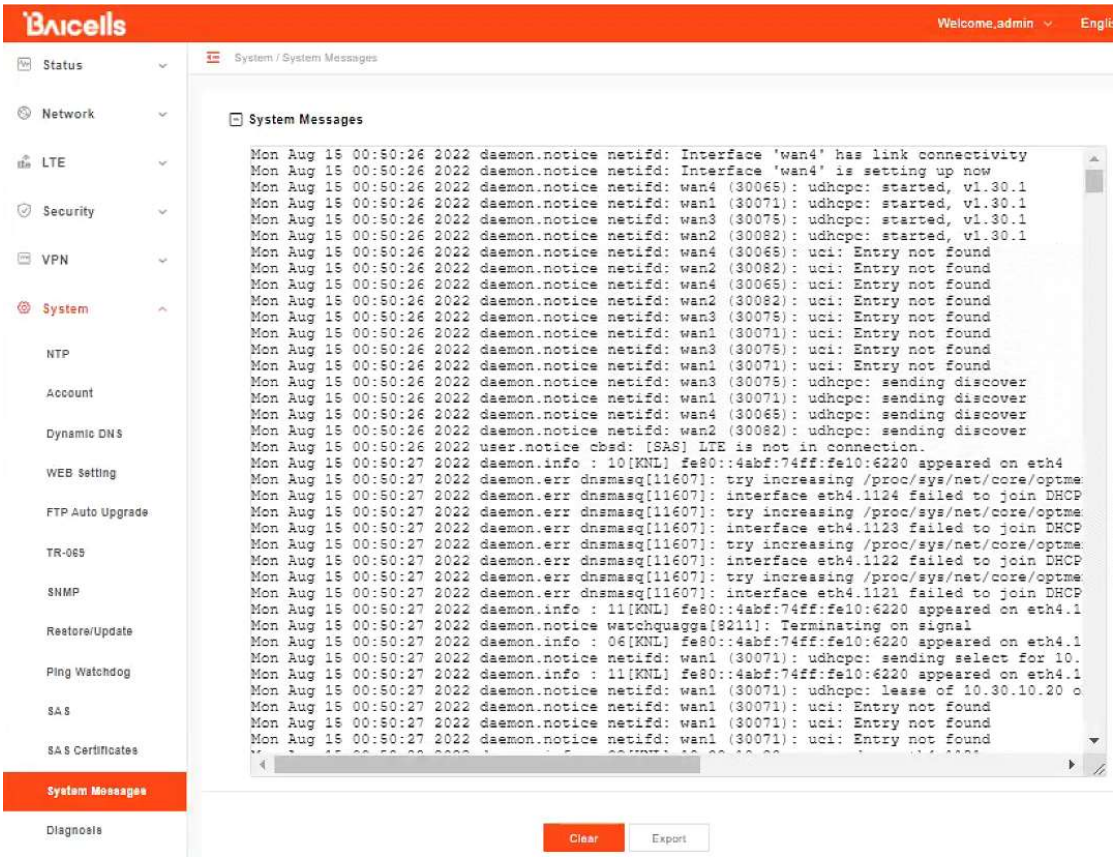
Figure 3-51 Ping Watchdog



3.6.10 System Messages

Use this Web-GUI, you can Export System Message, collect real-time system information and transfer system message to PC.

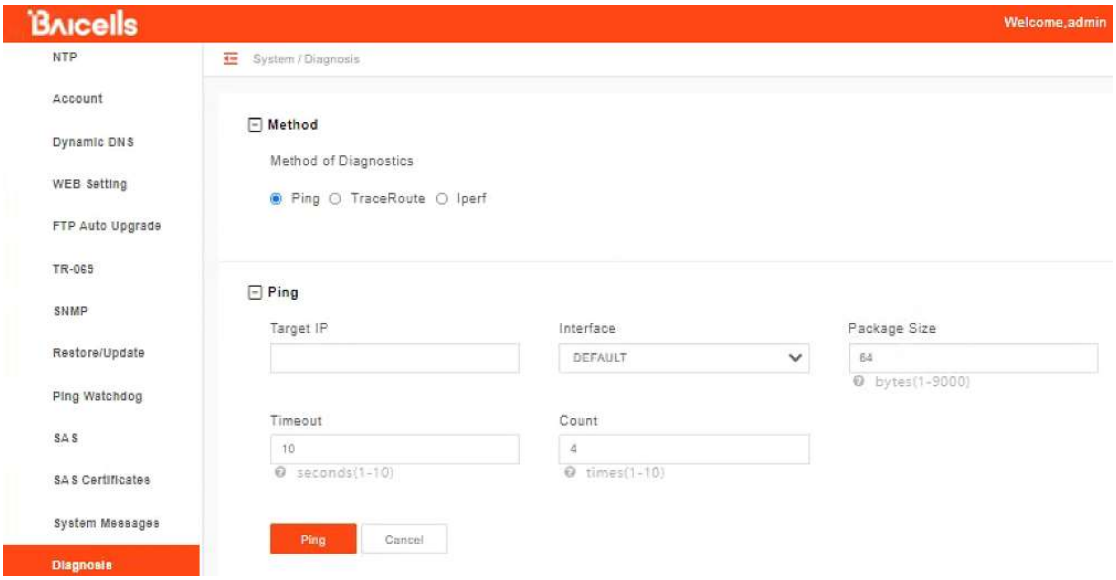
Figure 3-52 System Messages



3.6.11 Diagnosis

The System > Diagnosis menu provides 3 types of diagnostic tests that may be used for troubleshooting connection issues: Ping and Traceroute (Figure 3-53).

Figure 3-53 Diagnosis



3.6.11.1 Ping

Ping is used to manually initiate a ping test to check connection status. Running a ping test will send data packets of a specified size from the CPE over the network to a target IP address. The results of ping determine if there is a connection and if there is any packet loss.

Figure 3-54 Ping Diagnosis Settings

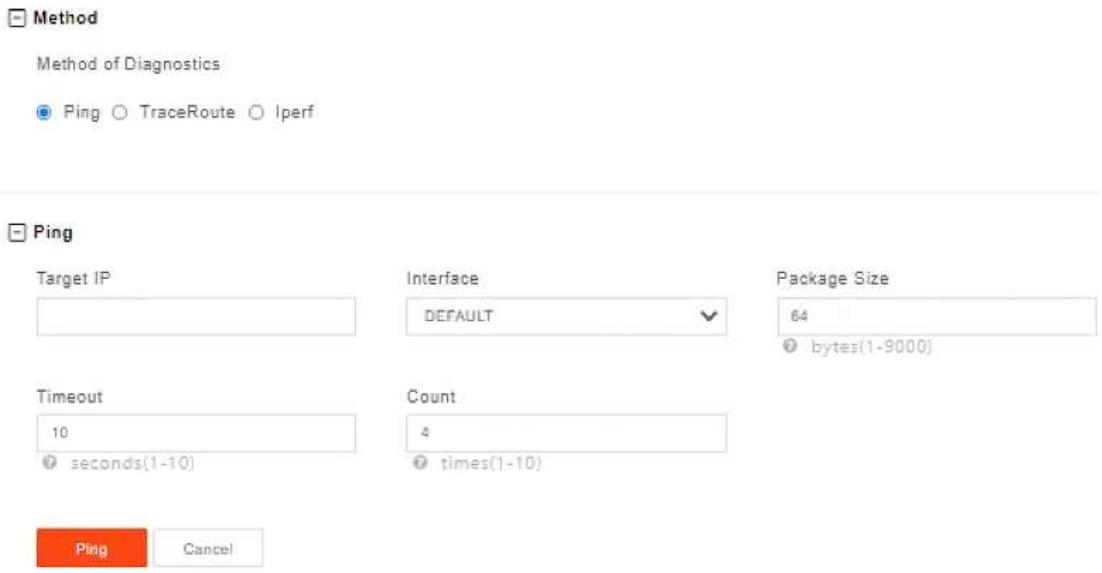


Table 3-9 Ping Diagnosis parameters

Field Name	Description
Target IP	A target IP address for the CPE to ping
Interface	The interface the CPE should use, either DEFAULT (APN1) or APN 2, 3, or 4.
Package Size	The data packet size to be sent to the target IP address, in bytes. The range is 1-9000 bytes.
Timeout	A timeout period, in seconds. The range is 1-10 seconds.
Count	The number of times (Count) for the ping test to execute. The range is 1-10.

3.6.11.2 Trace Route

Running a traceroute test will display the route a packet takes from the CPE to a target IP address. The test provides an indication of where there may be delays in the transmission of packets across the IP network.

Figure 3-55 Trace Diagnosis Settings

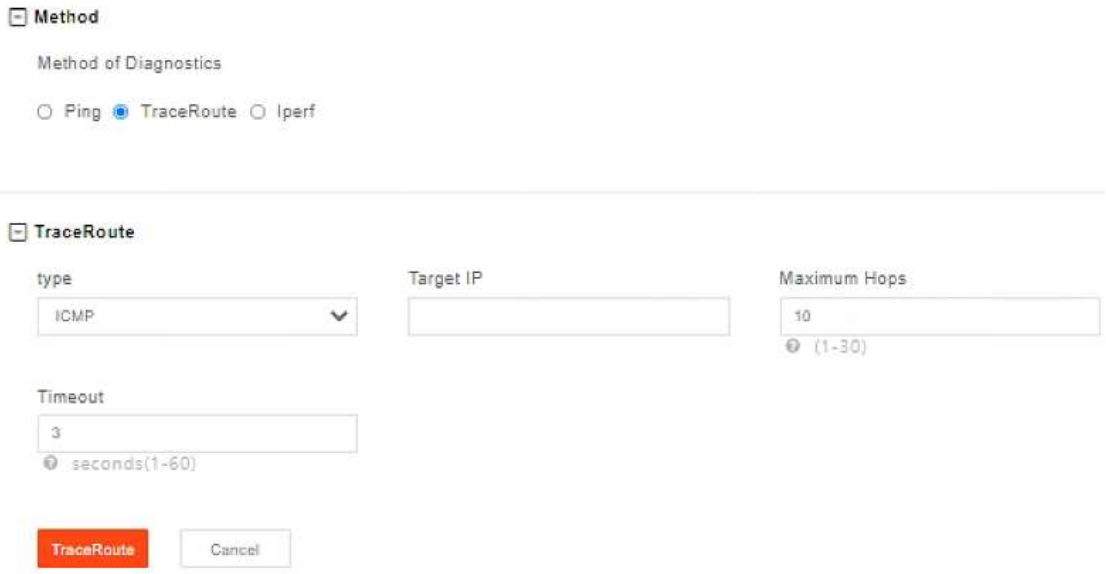


Table 3-10 Trace Diagnosis parameters

Field Name	Description
Type	The protocol type is ICMP or UDP.
Target IP	A target IP address for the CPE to send packets to.
Maximum Hops	The maximum number of hops between network nodes you want the packets to take. If the traceroute hits that number, the test will end.
Timeout	A timeout period, in seconds. The range is 1-60 seconds.

Results of the traceroute will appear at the bottom of the window, showing the target IP address, the maximum number of hops that it took from CPE to the destination, the packet size, and the time between hops.

3.6.11.3 Iperf

Iperf diagnostic debugging is used to test throughput.

Figure 3-56 Iperf Diagnosis Settings

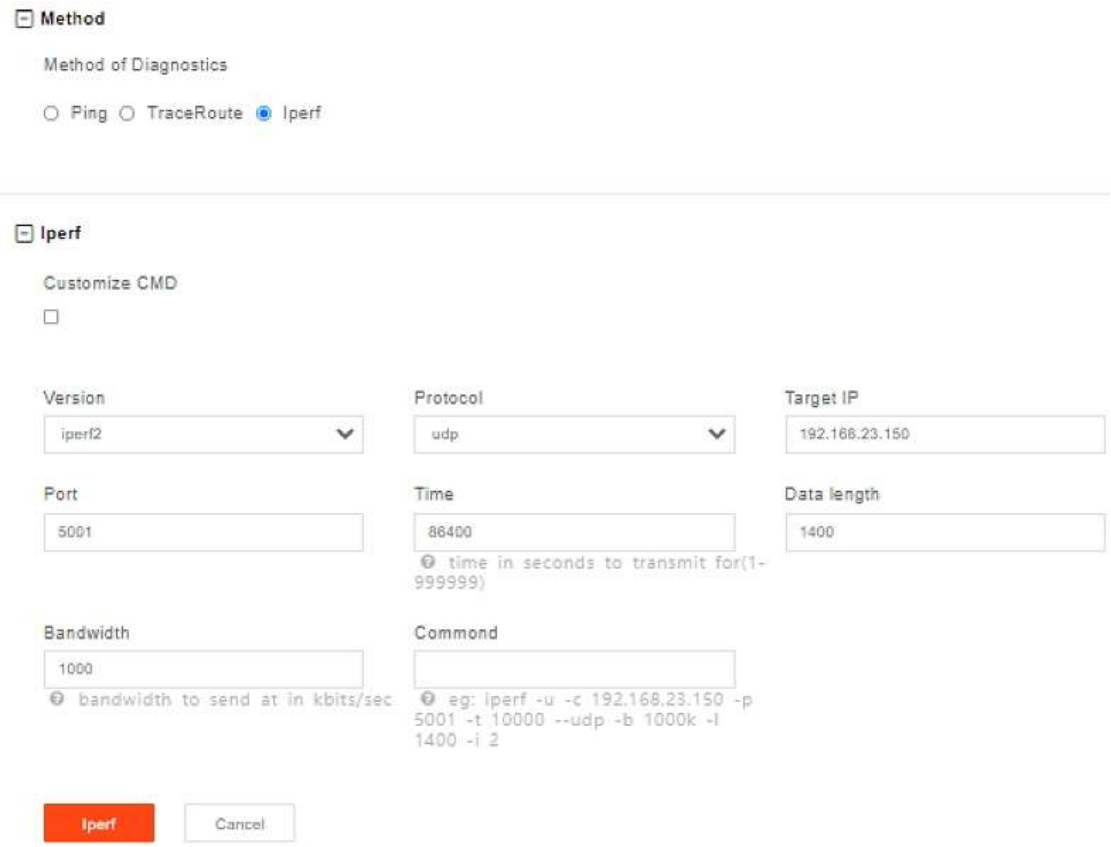


Table 3-11 Iperf Diagnosis parameters

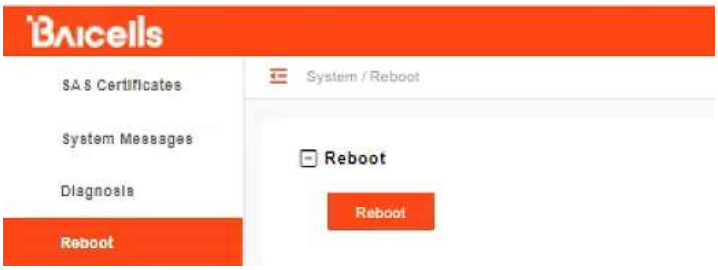
Field Name	Description
Version	The version of iperf supports iperf2 and iperf3.
Protocol	TCP or UDP
Target IP	Specifies the destination IP for iperf diagnostics
Port	Specifies the port number for iperf diagnostics
Time	Iperf diagnostic time
Data length	Specify the data length of UDP protocol
Bandwidth	Specify the bandwidth of UDP protocol

3.6.12 Reboot

Use the Reboot menu to perform a reboot of the CPE, as shown in Figure 3-57. It can take several minutes for the reboot to complete. After it reboots, the CPE GUI will display the login screen.

Caution: The reboot action will disrupt service.

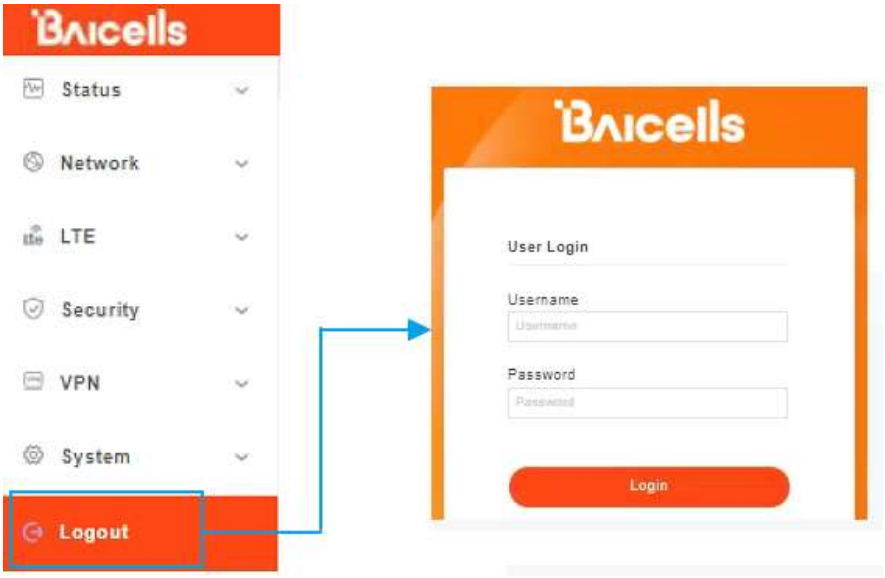
Figure 3-57 Reboot



3.7 Logout

When you click on the Logout menu, you are automatically logged out of the CPE and returned to the login screen (Figure 3-58).

Figure 3-58 Logout



4. Regulatory Compliance

FCC Compliance

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.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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.

Warning:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.