ATOM OD06 CPE

Installation & Configuration Guide

Model EG8013L-M11

April 2020

Version 1.2

About This Document

This document is for operators who will be installing and configuring the Baicells ATOM OD06 CPEs, model EG8013L This document version is based on the firmware version BaiCE_BG_1.6.11.

Related Documents

All technical specifications and documents are on the Baicells website under Resources > Documentation.

- Baicells SNAP PoE+ Router Data Sheet
- Baicells SNAP PoE+ Router User Manual
- Baicells ATOM OD06H/L Data Sheet

Copyright Notice

Revision Record

Date	Version	Description	SMEs/Contributors	Author/Editor
18-Aug-2020	v1.0	Draft	-	Tang Houcheng

Support Resources

- Documentation - Baicells product data sheets, this document, and other technical manuals may be found at Baicells > Resources > Documentation.
- Support - Open a support ticket, process an RMA, and the Support Forum are at Baicells > Support.

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:	+86-10-62607100	+1-888-502-5585
Email:	contact@Baicells.com	sales_na@Baicells.com or support_na@Baicells.com36T
Website:	www.Baicells.com	https://na.Baicells.com

Table of Contents

List of Figures

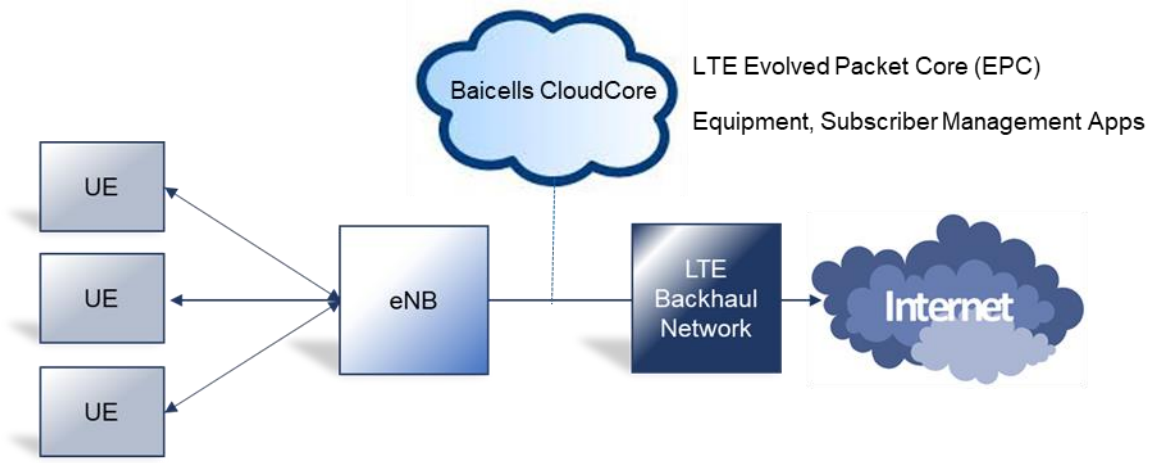
List of Tables

1. Introduction

1.1. Description

The Baicells Atom OD0406 Outdoor Low-Gain and Outdoor High-Gain User Equipment (UE) is part of a broadband wireless access system that integrates with Long-Term Evolution (LTE) backhaul networks to provide subscribers with Internet access. The UE, also referred to as Customer Premise Equipment (CPE), communicates through a wireless connection to the operator's eNodeB's (eNB) at cell sites located in the region. The eNBs communicate with the backhaul network (Figure 1).

Figure 2: LTE Network Architecture



The outdoor low-gain or high-gain UE may be selected because of the distance between the user's location and the closest eNB or for environments where there may be blockage or partial blockage in the wireless signal path between the UE and eNBs in the area - e.g., dense trees or buildings.

As an LTE standards-based product, the Baicells equipment provides higher near-line-of-sight (nLOS) and non-line-of-sight (NLOS) signal penetration than other wireless technologies. The high-gain UE has a higher antenna gain than the low-gain UE, making it possible to get the strongest possible signal reception for subscribers.

The LTE standards organization that defines certain characteristics of user equipment across manufacturers labels each progression of the standards as releases, such as Release 9, Release 10, etc., and categories, such as Category 4 (CAT4) and Category 6/7 (CAT6/7).

Typically the difference from one release/category to the next is in capacity, i.e., higher throughput. There is no physical difference between the CAT4 and CAT6/7 UE, but the low-gain UE and the high-gain UE do look different from one another. A physical comparison is provided in section 4.

1.2. ODU Modes

This device can work at two modes, ODU standalone or IDU+ODU mode.

(1) ODU standalone Mode

Standalone mode, ODU can worked at NAT/TUNNEL/BRIDGE mode

a) NAT Mode, the ODU work as a LTE and Ethernet Gateway, it converts LTE network data to local Ethernet data.

b) Tunnel Mode, the ODU can build a L2 or L3 VPN tunnel with a designated VPN server.

c) Bridge Mode, the ODU can bridge it LTE IP address to LAN port devices, when configured as the bridge, the CPE's LAN port will work as trunk mode, so it can't assign IP address to any no-trunk devices (like PC), so you have to Manual Configure the PC's IP address in the same broadcast domain (e.g. 192.168.150.88).

(2) IDU+ODU Mode

When the ODU connect to a IDU device (Baicells PoE router), it will automatic be configured as Bridge mode, and assign all its LTE IP to IDU, at that mode, the IDU will take the place of ODU to control all the CPE functions.

CAUTION:

Before contacting Baicells FAE or your distributor, please **DO NOT** mixed use the two modes.

1.3. Features

The Baicells Atom UEs provide robust throughput and are designed for growth and expansion as technology evolves. Some of the key features and attributes of the Atom outdoor UEs are listed below. Exact specifications vary by model. For the latest information, please refer to the Baicells website for your specific UE model.

- Standardized LTE TDD bands 42, 43, 48. Customization may be requested.
- Complies with 3GPP Release 10 (CAT6/7)
- 1000 Mbps Ethernet interface (CAT6/7)
- Built-in bipolar directional LTE antenna
- Power supply using Power Over Ethernet (PoE)
- Cell lock, SIM lock, and Pin lock
- Pole or wall mount options
- TR-069 management protocol support
- Local and remote GUI management

2. Installation

2.1. Part & Materials

Refer to Table 1 for a list of the components that you should receive with the Baicells outdoor UE.

Table 1: Parts

Item	Qty	Picture
Atom OD06L-EG8013L-M11 CPE	1	
Power Cable	1	
PoE Power Adaptor	1	

You will need standard tools, Ethernet cable, ground wire, and RJ-45 connectors for installing and connecting the outdoor unit (Table 2).

Table 2: Materials

Item	Description
Ethernet Cable	Outdoor shield CAT5E, shorter than 330 feet
Ground Wire	16mm^2 yellow-green wire

2.2. Dimensions

The Baicells Atom outdoor low-gain and high-gain models of user equipment are powerful, standards-based devices designed to connect seamlessly to any standard LTE eNB operating on the same frequency band. The devices have a small, sleek form factor (Figure 3), yet are ruggedized for the most challenging outdoor environments.

Figure 4: Dimensions

All models of the low-gain and high-gain UEs have external LED status indicator lights and interface connectors (Figure 3). These external features make it easier to determine the UE's operational status and to check cables.

2.3. LEDs & Interfaces

On the low-gain UE the LEDs are on the side of the unit, and the connection interfaces are on the bottom of the unit. On the high-gain UE both the LEDs and the interfaces are on the side of the unit. Refer to Table 3 for a description of the LEDs and Table 4 for a description of the interfaces.

Figure 5: Low-Gain LEDs & Interfaces

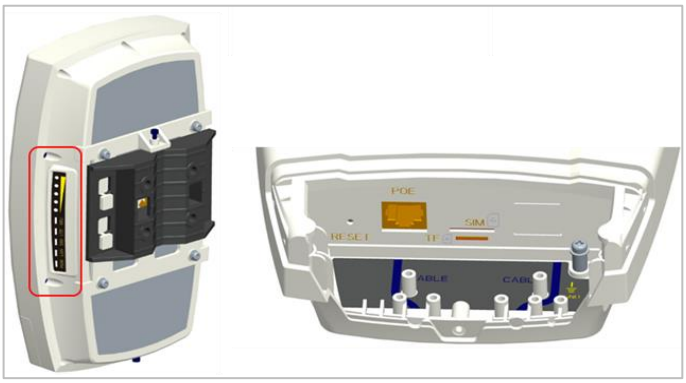


Table 3: LEDs

LEDs vary by model – not all models will have all of the LEDs listed below.

Identity	Description	Color	Status	Description
MIU	-	Yellow	Off	Reserved for future use
			Steady On	Reserved for future use
			Blinking	Reserved. for future use
LTE	LTE network status	Blue	Off	The UE is not connected to the network
			Steady On	The UE is connected to the LTE network
SIM/USIM	SIM/USIM card status	Yellow	Steady On	The USIM card is functioning normally
			Blinking	The USIM card is not inserted or is not functioning normally
LAN	100 or 1000 Mbps Local Area Network Ethernet status	Yellow	Off	No Ethernet connection established
			Steady On	Ethernet connection is normal
			Blinking	Data is transmitting
PWR	Power status	Yellow	Off	No power supply to the UE
			Steady On	Power to the UE is on
LTE Signal	1, 2, 3, 4, or 5 bars to indicate wireless connection status. The more bars, the stronger the signal between the UE and a network cell (eNB).	Green	All Off	The signal is too weak for the UE to connect to the network
			Steady On	Bars will light steadily according to signal strength
			Blinking	The UE is scanning the network
				The UE is authenticating with the network
				The UE is getting an IP address from the network

Table 4: Interfaces

Interfaces vary by model – not all models will have all of the interfaces listed below.

Interfaces	Description
PoE	Power over Ethernet (PoE) power adaptor
TF or SD Slot	Card slot for a secure digital (SD) card
SIM/USIM Slot	Universal Subscriber Identity Module card slot, 1.8V/3.0V USIM 2FF
RESET	Reset/restore button
GND	Ground lug. The unit is connected to Earth by conductor.

2.4. Preparing to Install

To help ensure a smooth and successful installation, check that you have all of the parts, materials, and tools you will need, per section 2.1 Parts & Materials. When selecting the best outdoor location for the installation, plan on placing the UE so that it faces the nearest eNB. You may need to adjust the tilt and angle for optimum signal reception.

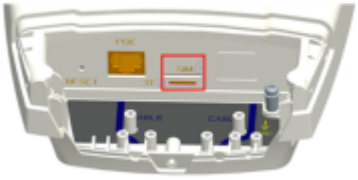
2.5. Installation

1. Loosen the screws on the UE's waterproof cover, and open the cover.

2. Insert the service provider's SIM/USIM card into the card slot (Figure 6).

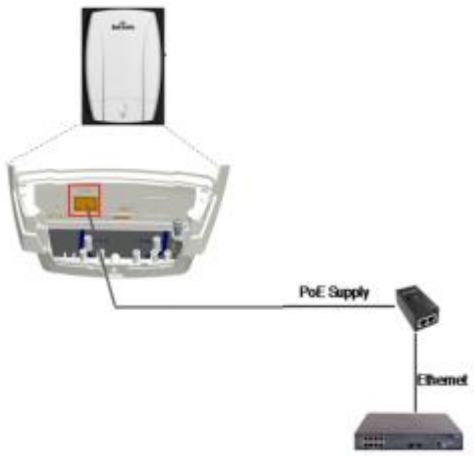
> ⚠ **Attention:** Never power on the unit while installing or uninstalling the USIM card. Doing so could damage the card and the unit.

Figure 7: LTE Network Architecture



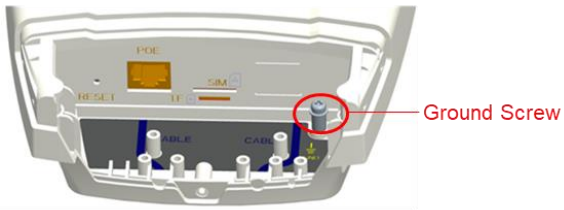
3. Prepare the outdoor shielded CAT5E Ethernet cable. The Ethernet cable will run between the outdoor UE and the inside of the facility, where it will connect to the PoE adaptor and LAN. Cable length will vary by location.
4. Connect one end of the Ethernet cable to the PoE port on the unit. Connect the other end to the power adaptor (Figure 8).

Figure 9: PoE Adaptor



5. Close the UE's waterproof cover, and tighten the screws.
6. Prepare the 16mm^2 yellow-green ground wire, and follow the steps below. Once the unit is fully installed, make sure the grounding cable is connected to a solid grounding point (earth).
    a. Atom Low-Gain UE: Connect the ground cable to the ground screw (Figure 10).

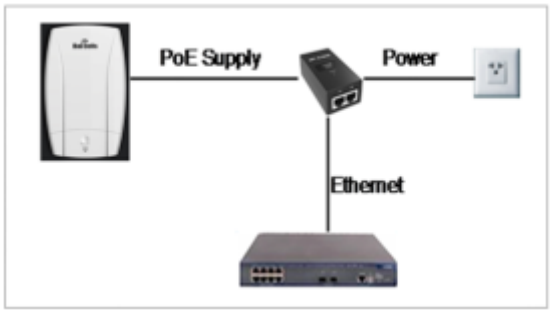
Figure 11: Low gain CPE Grounding



b. Atom High-Gain UE: Connect the ground cable to the grounding screw in the ground row (Figure 6). The figure is showing the UE mounted on a pole; mounting is covered in step 8.

7. Plug the power adaptor into an electrical outlet (Figure 12). Pay attention to the power adaptor interface directions noted on the adaptor itself. The LED indicators should light up when the unit is powered on.

Figure 13: Power Adaptor



8. Mount the UE: If you are installing the UE on a pole, e.g., to attach to a roof, go to step 9. If you are installing the UE on an outside wall, go to step 10.

9. Pole installation:

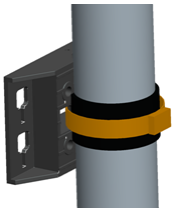
   a. Low-Gain UE:

a1) Attach a heavy-duty anti-slip rubber band on the pole (Figure 14).

Figure 15: Rubber Band

a2) Fix the UE bracket over the band using the hoop (Figure 16).

Figure 17: Bracket



a3) Attach the UE to the bracket, and tighten the screw (Figure 18).

Figure 19: Attach UE

a4) The UE is now ready for installation at its final outside location. Then, proceed to section 7 Basic Configuration.

10. Wall installation:

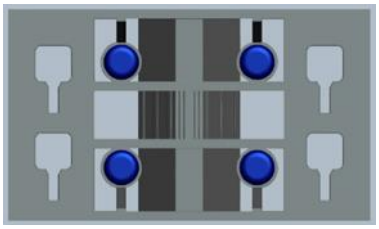
a. Low-Gain UE:

a1) Slip the bracket off of the Atom unit, and fit it on the wall to mark the drilling locations (Figure 11), The marked locations, drill four 10-mm diameter and 70-mm depth holes.

Figure 20: Mark Holes for Drilling

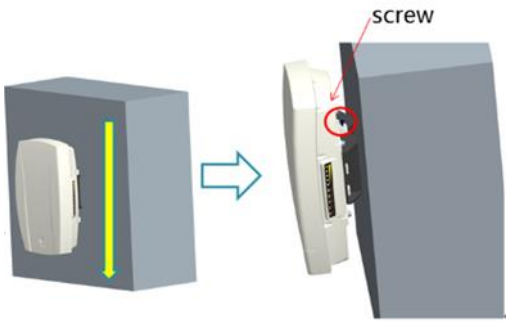
a2) Check the up/down direction of the bracket, and then fix it on the wall using the M5 tapping screws (Figure 12).

Figure 21: Fix Bracket to Wall



a3) Attach the UE to the bracket, and tighten the screw (Figure13).

Figure 22: Attach UE

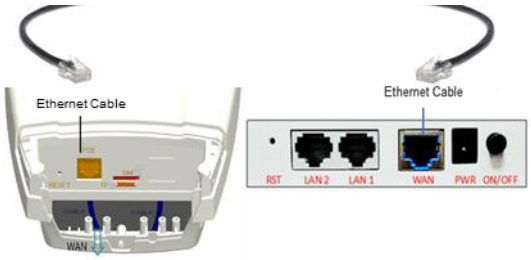


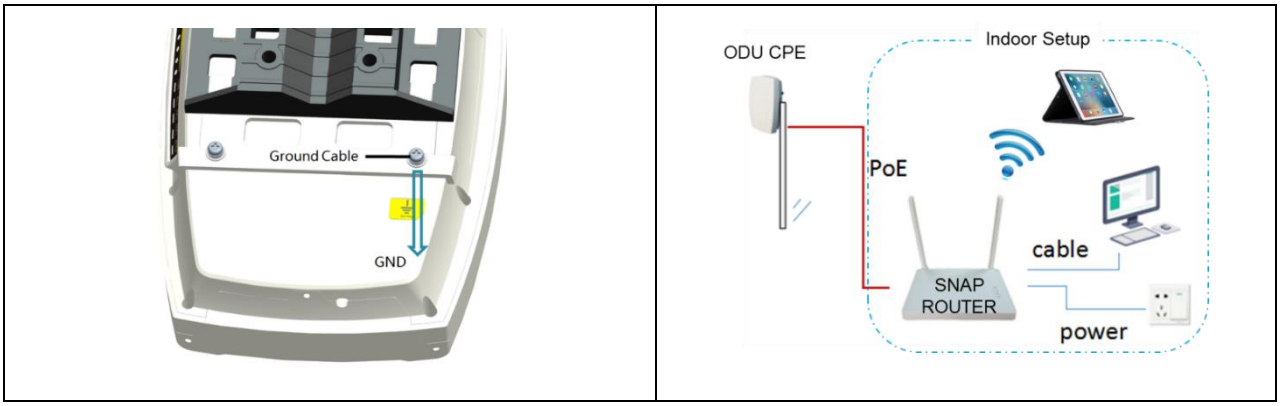
a4) Proceed to section 7 Basic Configuration.

2.6. Installation with Baicells SNAP Router

To explain the installation, the procedure in Table 3 uses a Baicells Atom OD04L Outdoor Low-Gain CPE as the example. Refer to the CPE user manual on the Baicells website to complete some steps as indicated.

Table 4: Installation Procedure

<table>
<tr>
<td>1. With the CPE powered OFF, loosen the screws on the waterproof cover and lift to access the interfaces.
2. Insert the SIM card into the SIM slot.
⚠ Attention: Never power on the CPE while installing or uninstalling the SIM card. Doing so could damage the card and the unit.</td>
<td>3. Using the Ethernet cable, connect the CPE PoE port and the router WAN port.
⚠ Caution: Do not connect unsupported devices to the router WAN port, as it may cause damage.</td>
</tr>
<tr>
<td>  </td>
<td> 
</td>
</tr>
<tr>
<td>Per the associated steps in the CPE user manual installation procedure:
4. Prepare the ground wire and connect one end of it to the CPE ground terminal and the other end to a reliable grounding point (earth).
5. Close the CPE's waterproof cover, and tighten the screws.
6. Mount the CPE at its outdoor location, assuring proper alignment to the nearest eNB tower.
7. Power the CPE ON, and check the satus of the LEDs to ensure it is operating as expected.</td>
<td>8. Connect the router's power adapter to the power connector on the back of the unit, and the other end to a power outlet.
9. Turn power to the router ON.
10. Check the LED indicators to verify normal operating status per Table 2 in section 2.2 of this guide.</td>
</tr>
</table>



NOTE: If either the CPE or the router is not running the correct firmware, the router's LTE signal LED will be OFF. Check for the latest firmware on the Baicells website, or contact Baicells support.

The setup is complete and ready to work. To configure features using the CPE GUI, go to the next section.

3. Configuration

3.1. Computer Requirements

The computer you use to connect with the CPE GUI must meet the requirements shown in Table 5.

Table 5: Computer Requirements

Item	Description
CPU	Pentium 500 MHz or higher
Memory	128 MB RAM or higher
Hard Disk	50MB available space
Operating System	Microsoft : Windows XP, Windows Vista, Windows 7 or higher Mac: MacOSX 10.5 or higher
Screen Resolution	1024 x 768 pixels or higher
Browser	Google Chrome 9 or later Internet Explorer 7.0 or later Mozilla Firefox 3.6 or later Safari 5 or later

3.2. CPE Software

The firmware of the CPE should be BaiCE_BG_1.5.4 or above, if the CPE is not running this version, please download it from the Baicells website > Resources > Firmware or contact Baicells support.

3.3. Login

The CPE comes preloaded with a GUI to configure the device. With the CPE turned on and connected to the router, access the GUI login page by opening a Web browser and entering http://192.168.150.1.

Figure 23: Login

Initially, use the default Username = *admin*/Password = *admin* (Figure 21). Once you are in the GUI, you will want to change the password; please refer to section 3.9.1 Account.

3.4. Status Menu

3.4.1. Overview

After logging in, the GUI opens to the Status > Overview page (Figure 24). This page is a dashboard of key information regarding the CPE. The top row, *Current State*, shows the network connection status, signal intensity, LAN link status, and the number of smart devices (cell phones, pc's, laptops) connected to the Internet through the CPE.

The *Device Info* pane displays the product name, software version, serial number, etc. The *LTE Status* pane shows important operational information, 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 *Throughput Statistics* you will see downlink (DL) and uplink (UL) data rates for current throughput (kbps), average rates, peak rates, and total throughput. The data is measured during a 3-second interval every 5 minutes. The *APN Status* pane displays any gateway connections. The bottom pane, *Devices List*, will show details about all smart devices currently connected through the CPE. Refer to Table 5 for a description of the *Status* fields.

Figure 25: Status

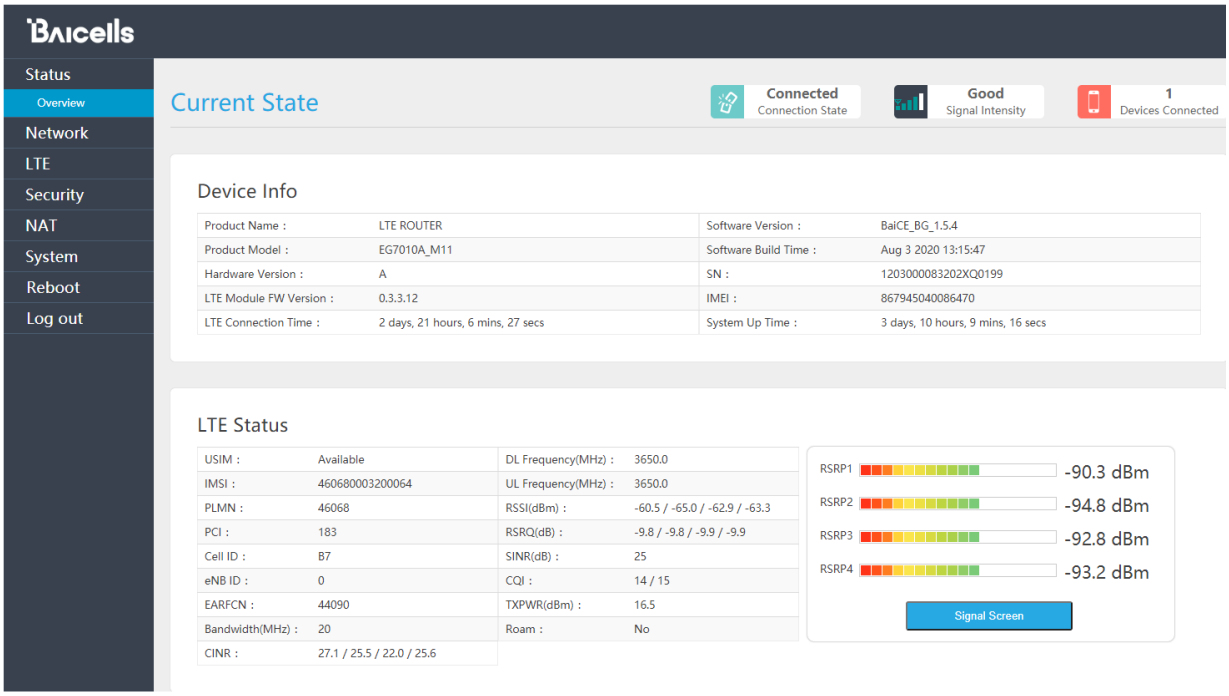


Figure 26: Throughput Statistics

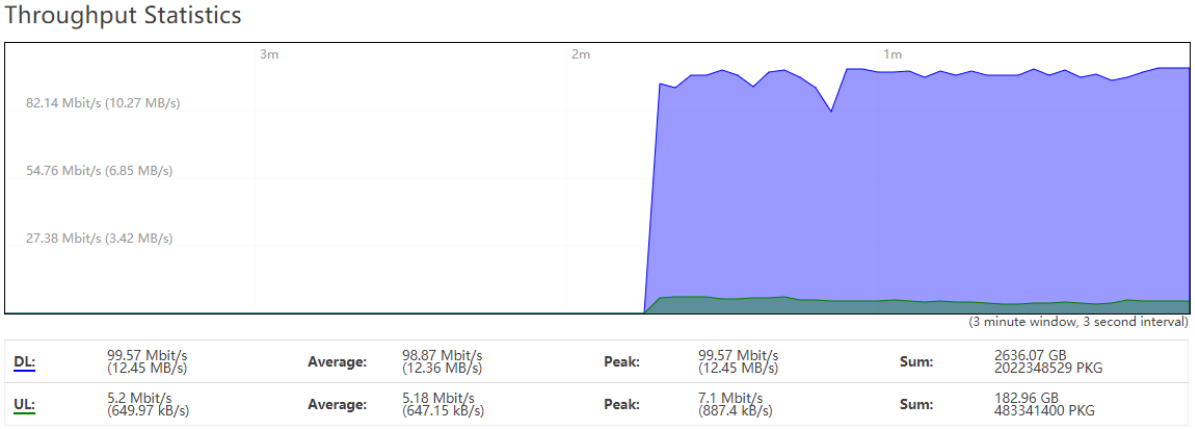


Figure 27: Internet Statistics

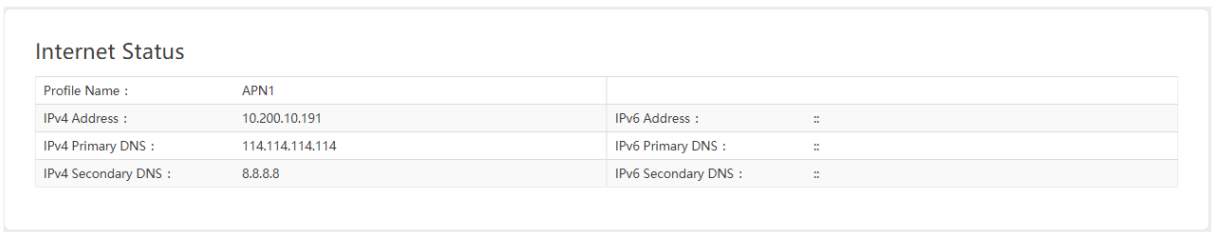


Figure 28: LAN Status

Figure 29: Device List

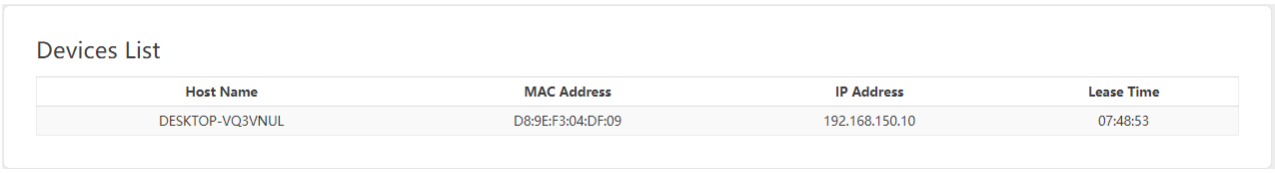


Table 6: Status

Field Name	Description
Connection State	Connection status between the CPE and the network – either Checking SIM, Scanning, Registering, Acquiring IP, Connected, or Disconnected
Signal Intensity	Indicates the strength of the signal between this CPE and the serving eNB, either excellent, good, general, bad, or severe. The ODU CPE hardware typically displays 1 to 5 LEDs to indicate this level (Figure 3&4).
Devices Connected	The number of smart devices connected to the Internet through this CPE via a LAN
Device Info	
Product Name	LTE ROUTER indicates the CPE is operating as a router
Product Model	ODU CPE model number
Hardware Version	ODU CPE hardware version
LTE Module FW Name	LTE Module FW's version
LTE Connection Time	The timer will be reset after every LTE connections
Software Version	ODU CPE operating software version
Software Build Time	Date and time the software was built
SN	Serial Number
IMEI	International Mobile Equipment Identity is like a serial number for the SIM card
System Up Time	The timer will be reset after reboot
LTE Status	
USIM	The Universal Subscriber Identity Module, or SIM, card status is either available or not ready in the ODU CPE
IMSI	The unique International Mobile Subscriber Identity (IMSI) number associated with the SIM card in the subscriber's ODU CPE. The IMSI must be identifiable by the operator's LTE network in order to access it.
PLMN	The Public Land Mobile Number (PLMN), or operator network ID, to which the CPE is connected
PCI	The Physical Cell Identifier (PCI) unique to each eNB. PCI indicates to which eNB the ODU CPE is connected. An operator can have multiple eNBs serving the same cell.
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

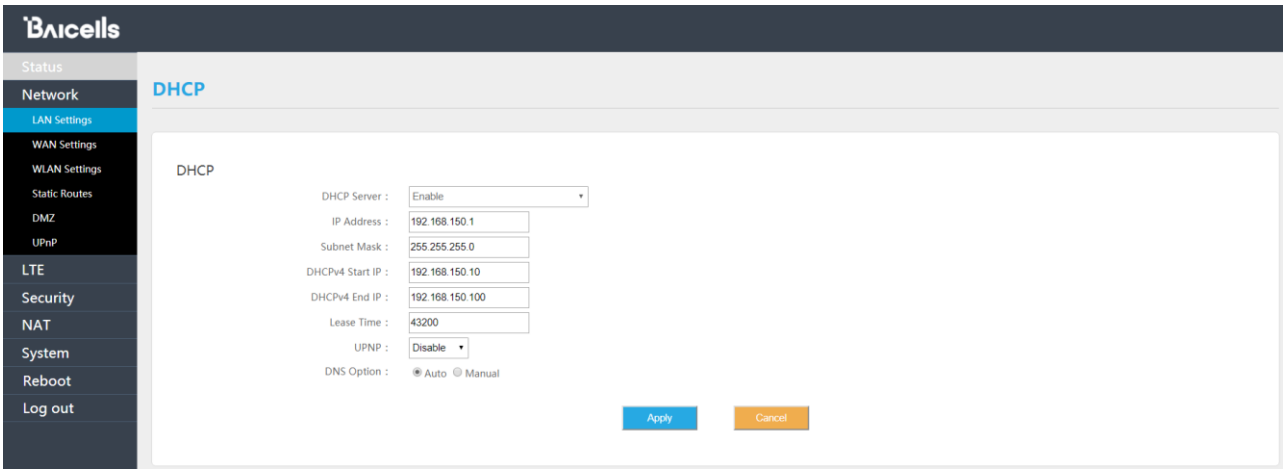
	which the CPE operates
Bandwidth	The range of frequencies within the band the CPE may use for wireless communications with an eNB, expressed in MHz
CINR	The Channel Signal-to-Interference-plus-Noise Ratio reflects the signal strength of the signal received from the two antennas in the eNB, expressed in decibels (dB) NOTE: Additional SINR values are reported when a transmitting device is using more than two antennas.
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.
RSSI (dBm)	
RSRQ (dBm)	Reference Signal Receiving Quality indicates the quality of the wireless signal
CQI	Channel Quality indication
TXPWR (dBm)	Real time UE TX power
Roam	Roam status
Throughput Statistics	
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
Internet Status	
APN Number	Access Point Name (gateway) connection to other network devices. At least one APN must be configured to establish the TR-069 connection to the CloudCore or other NMS
Enable	Indicates if the APN is enabled or disabled
MAC Address	MAC address of the APN gateway
Connection Type	Type of network connection
IP Address	IPv4, IPv6, or IPv4v6 address of the APN gateway
DNS server	Domain Name Server IP address
LAN Status	
MAC Address	MAC address of the LAN device, e.g., router, to which the CPE is connected
IP Address	The IP address of the LAN device
Netmask	The subnet mask of the LAN device
Devices List	
Index	Numerical ID assigned to each smart device connected through the ODU CPE
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

3.5. Network Menu

3.5.1. LAN Settings

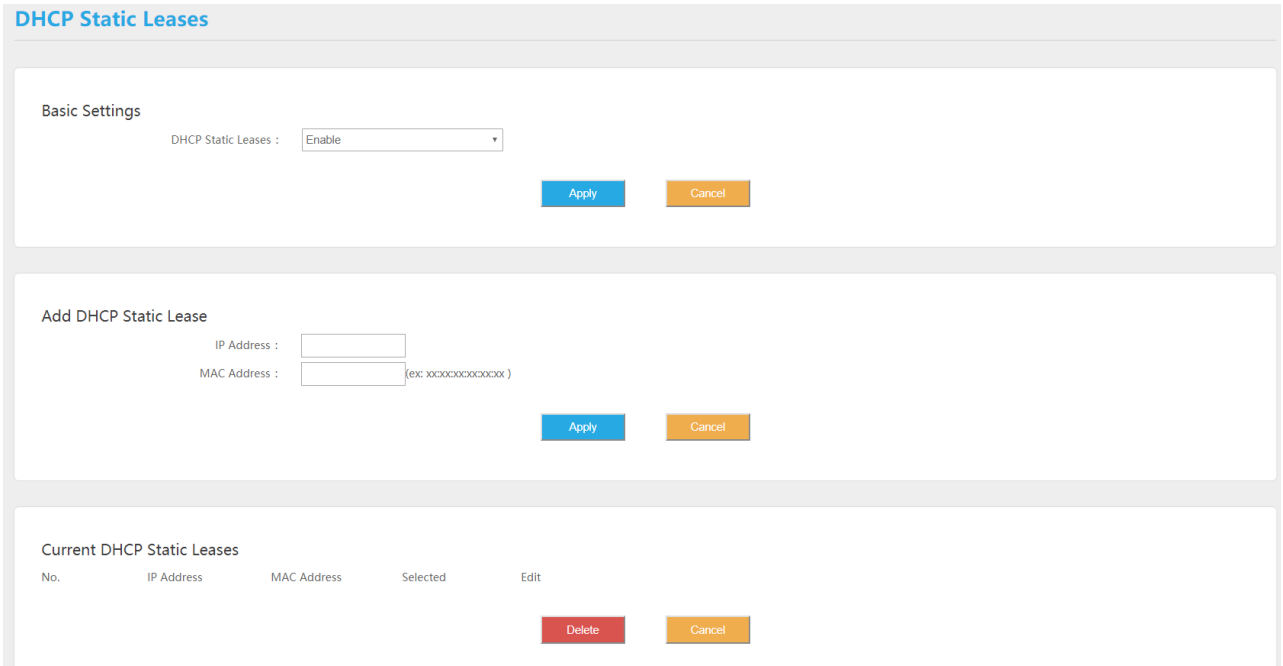
Enter the Network > LAN DHCP Server enable, IP address, subnet mask, DHCP range, lease time, UPNP enable.

Figure 30: DHCP Settings



DHCP Static Leases settings can set by the host's MAC address.

Figure 31: DHCP Static Leases

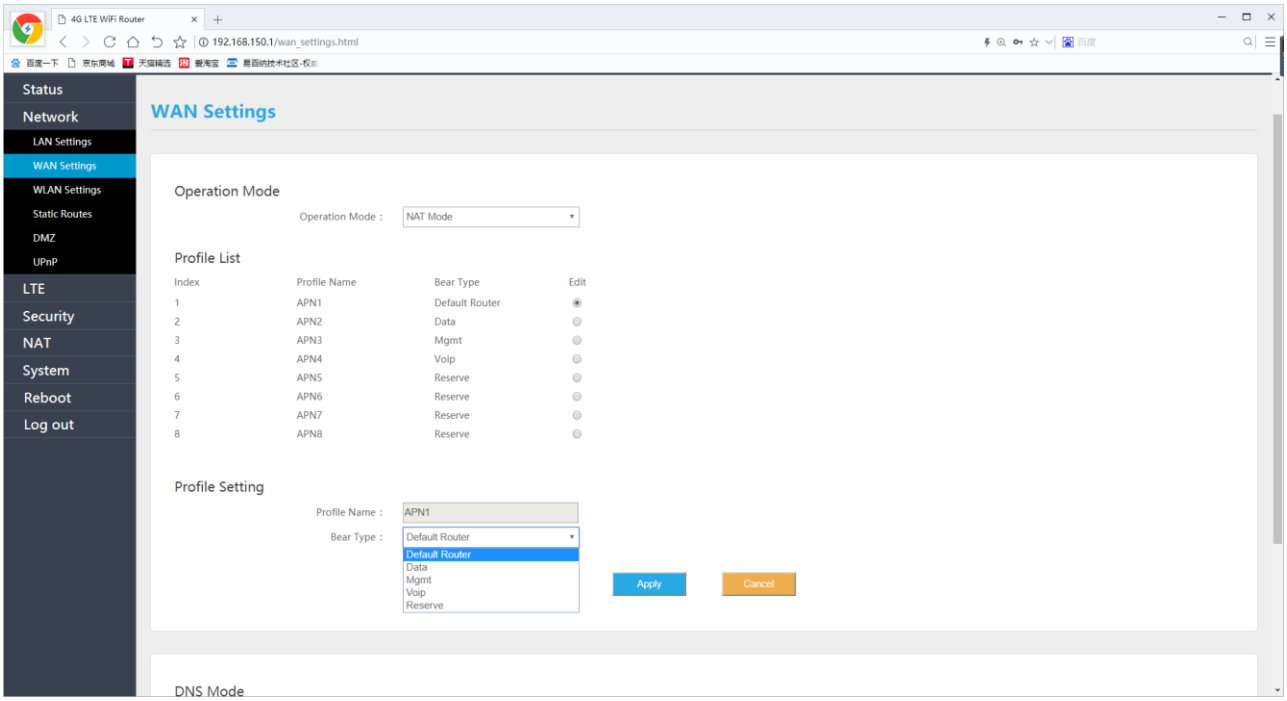


3.5.2. WAN Settings

3.5.2.1. NAT Mode

The CPE will be worked at NAT mode, and all 8 APNs can be configured by Default router/Data/Mgmt/Voip bear types.

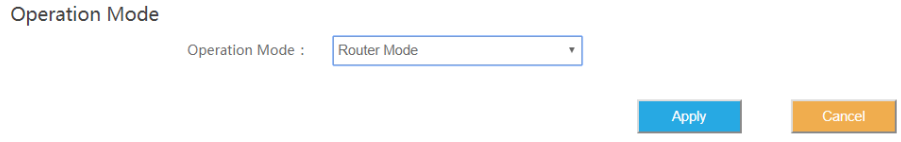
Figure 32: WAN Settings



3.5.2.2. Router Mode

When selected Router mode, the CPE will worked at router mode, it can dynamic update router tables.

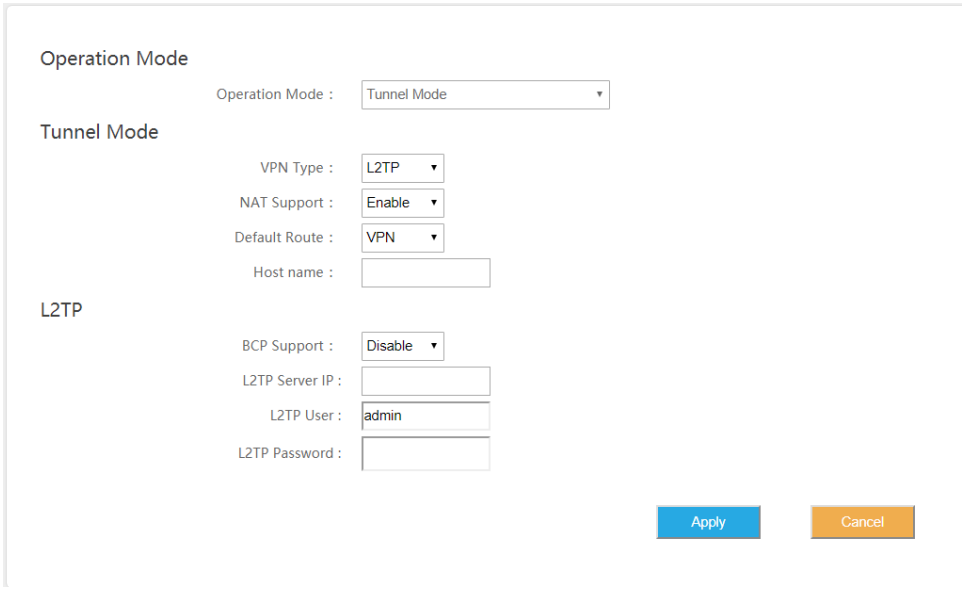
Figure 33: Router Mode



3.5.2.3. Tunnel Mode

This CPE can support L2TP and GER VPN mode.

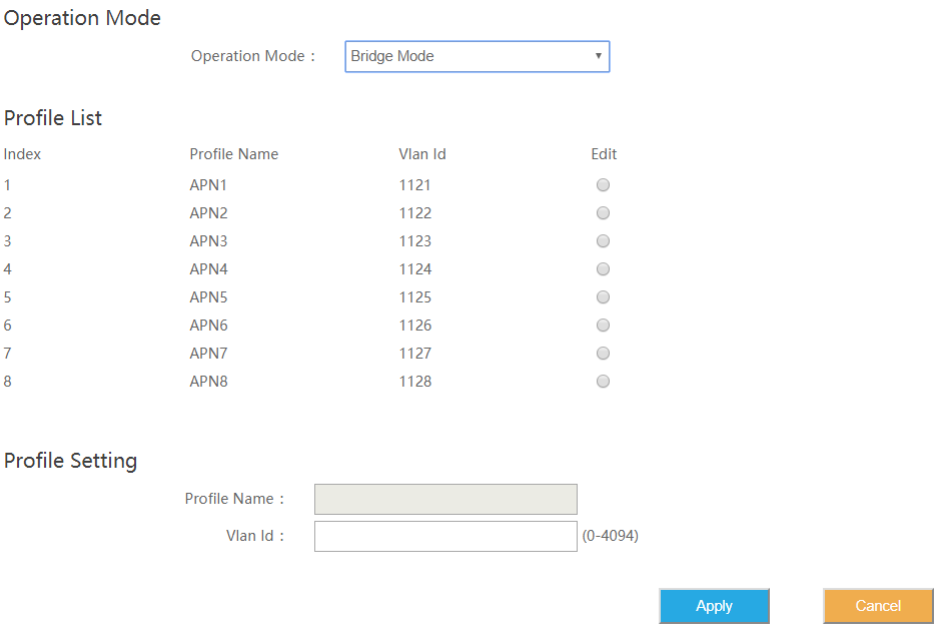
Figure 34: Tunnel Mode



3.5.2.4. Bridge Mode

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

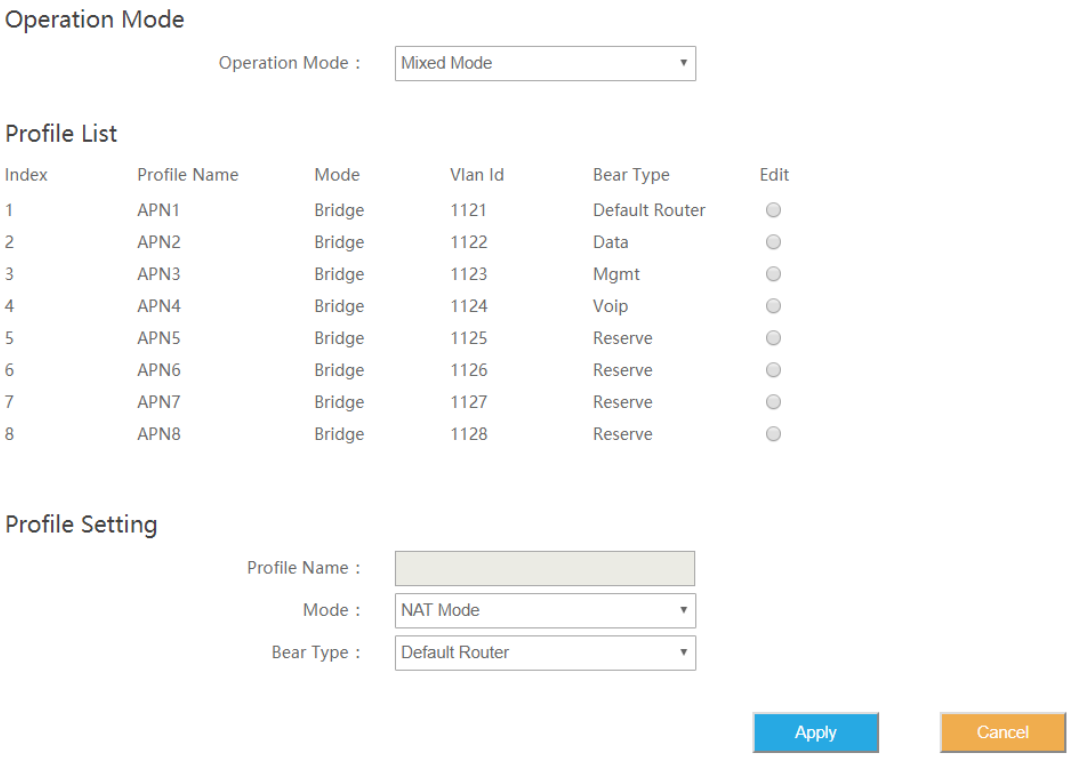
Figure 35: Bridge Mode



3.5.2.5. Mixed Mode

Mixed mode can configured every APN with different mode (e.g. Bridge), this is a professional mode.

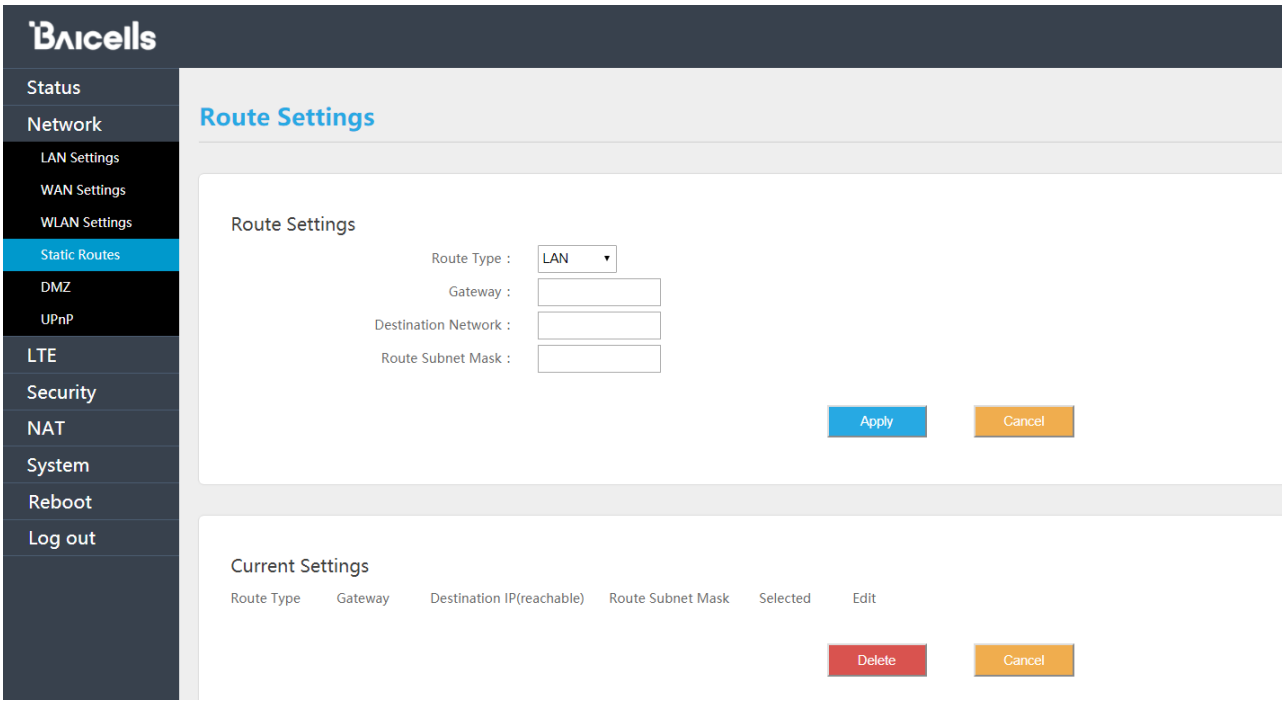
Figure 36: Mixed Mode



3.5.3. Static Routes

Set Static routes of the CPE, it can configure LAN or WAN port routes, Gateway, Destination Network and Route Subnet Mask, in Current Settings, show all activated static routes.

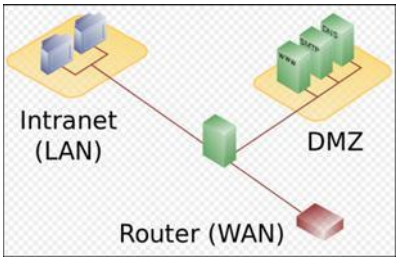
Figure 37: Static routes



3.5.4. DMZ

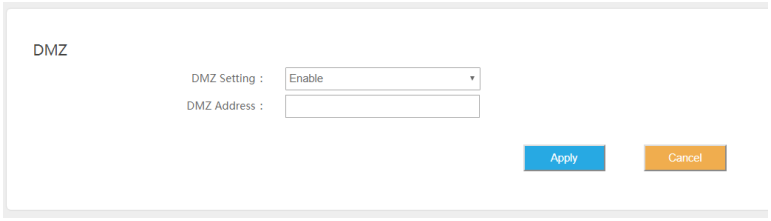
In technology, the DMZ refers to a firewall between incoming WAN traffic and the LAN to which the CPE is connected. Two basic DMZ methods are (a) using a single firewall, also known as the three-legged model, and (b) using dual firewalls (Figure 36). These architectures can be expanded to create complex architectures depending on the network requirements.

Figure 38: DMZ



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 37). Alternatively, you can enable Internet Control Message Protocol (ICMP) redirect error messages to support Layer 2 multicast features.

Figure 39: DMZ Settings

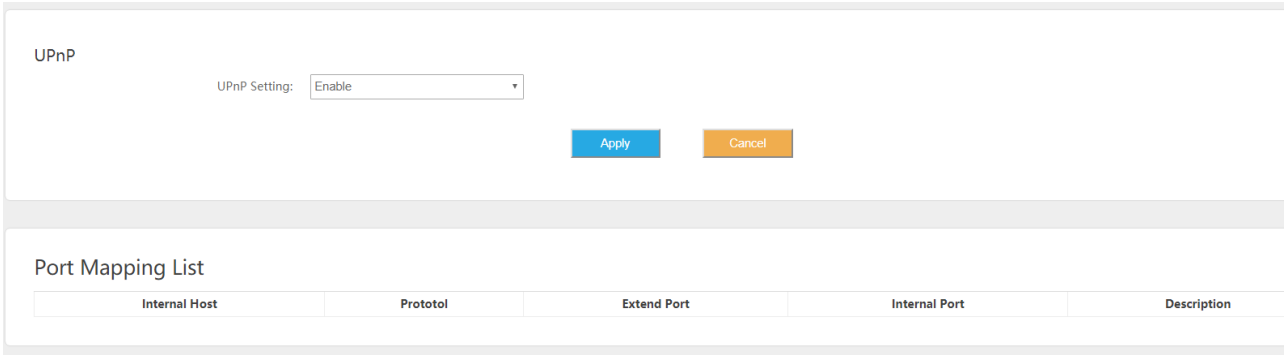


3.5.5. UPnP

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 38). Once enabled, any redirects of traffic will display in the *Active UPnP Redirects* section of the window.

Figure 40: UPnP Settings

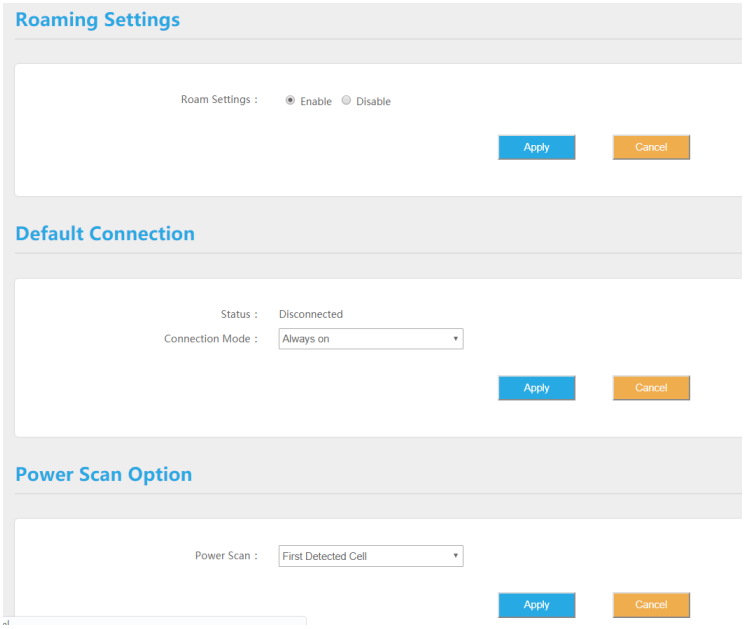


3.6. LTE Menu

3.6.1. Connection Settings

LTE connection settings includes Roaming settings, Default connection settings and Power Scan Option.

Figure 41: Connection Settings



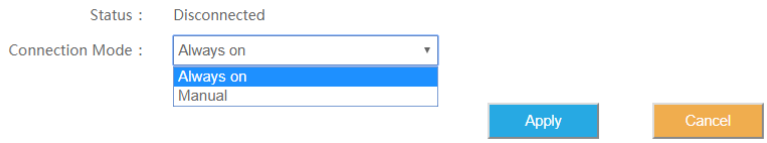
3.6.1.1. Roaming setting

If set Roam enable, the CPE can access to other PLMN network, else the CPE just can access the network PLMN same with the SIM card.

3.6.1.2. Default connection

If set always on, the CPE will automatic access the LTE network after booting, if set manual, the CPE need manual connection to the LTE network.

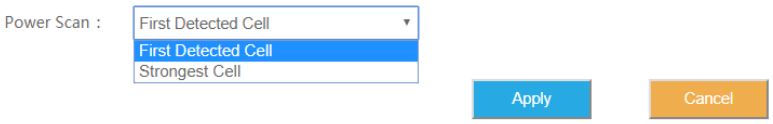
Figure 42: Default Connection Settings



3.6.1.3. Power Scan Option

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

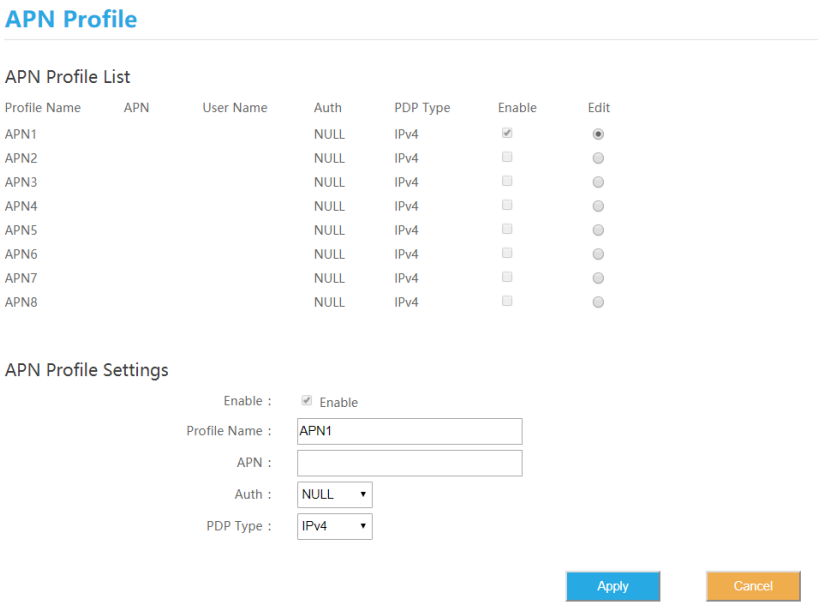
Figure 43: Scan mode Settings



3.6.2. Edit APN Profile

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.

Figure 44: APN Profiles

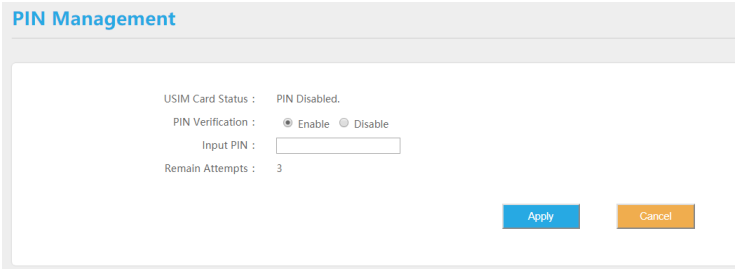


The CPE supports 8 APN configurations. At least one APN (TR-069) must be configured when the CPE/eNB connect to the Baicells CloudCore. In the window (Figure 42) you will select the APN number (1-8), enable it, enter an APN Name, select the type of IP addressing (IPv4, IPv6, or IPv4v6), identify if it is the default gateway, and choose which type of protocol will be supported on it.

3.6.3. 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 43). 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 45: PIN Management

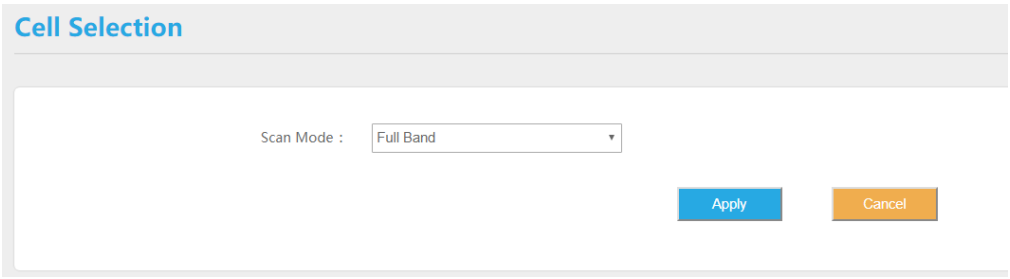


3.6.4. Cell selection

The Cell selection 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 re-selection 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 Figure 44.

Figure 46: Cell selections



Select one of the following options:

- **Full Band** (default) – All channels in the band.
  - 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.
- **Dedicated EARFCN** – Specific EARFCNs or frequencies. (Figure 45)
  - The CPE will scan the dedicated EARFCN or frequency list first when it is powered on.
  - If the CPE cannot connect to the LTE network after scanning the list, it will scan other supported bands and frequencies. You can add up to 10 EARFCNs or frequencies.
- **Cell Lock** – A combination of PCI + EARFCN or frequency. (Figure 46)
  - 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.
- **PCI Lock** – Specific PCIs only. Locks the CPE to a designated PCI or PCI range. (Figure 47)

After selecting an option, enter the required information and select *ADD*.

Figure 47: Dedicated EARFCN

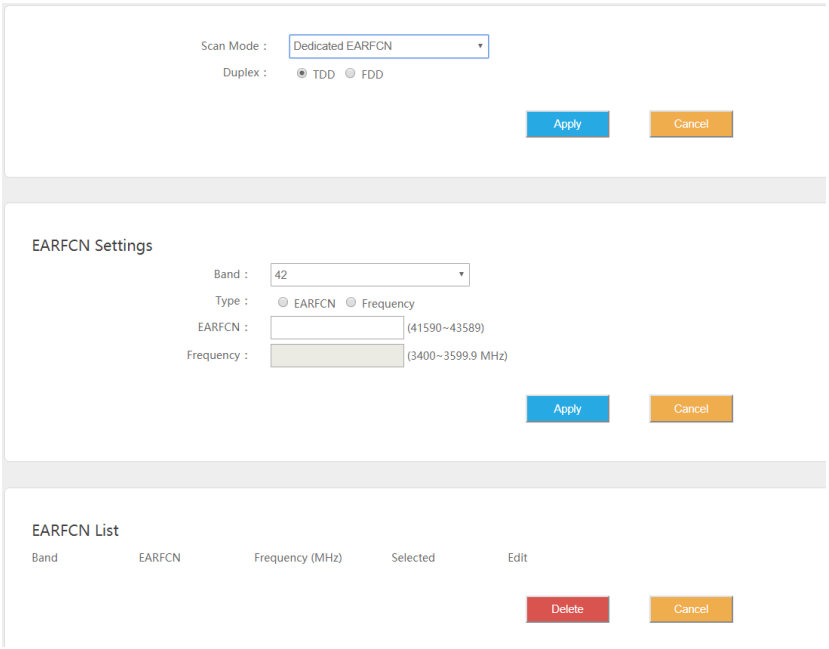


Figure 48: Cell Lock

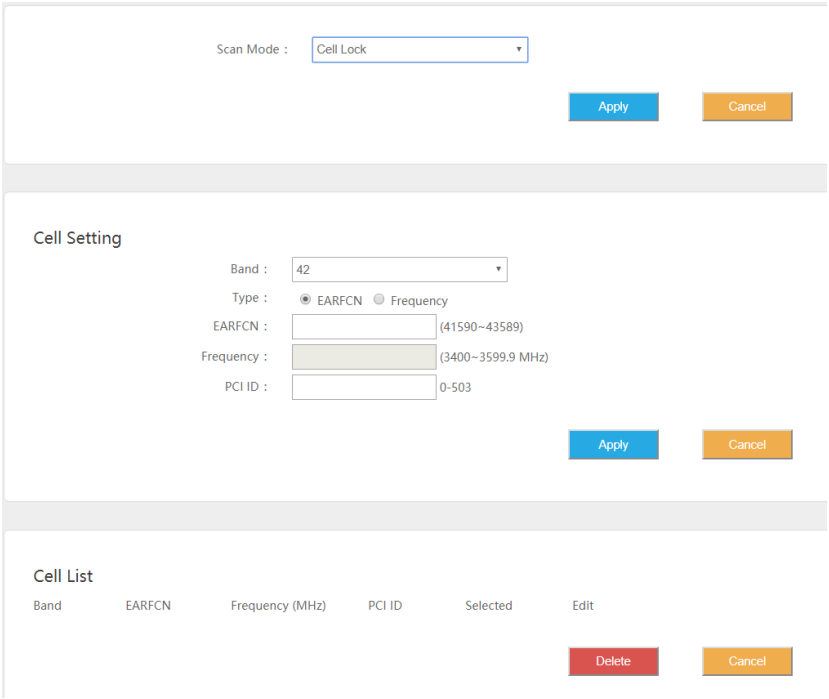
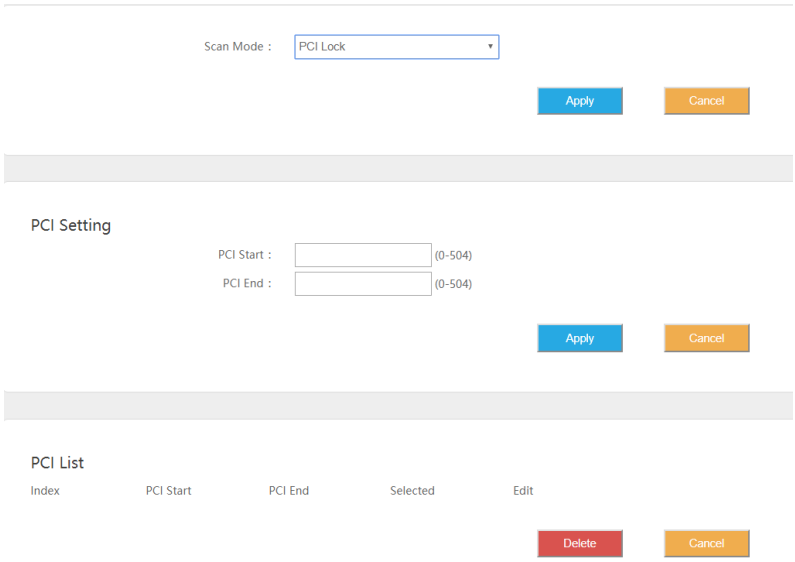


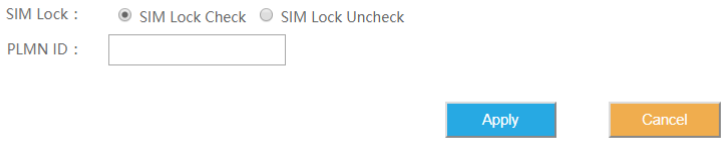
Figure 49: PCI Only Lock



3.6.5. SIM Lock Settings

This feature may be used to lock the SIM card to the operator's network (Figure 48). Each operator has a unique Public Land Mobile Network (PLMN) number. Locking the SIM prohibits the users from accessing another operator's network.

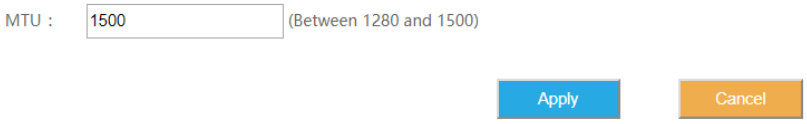
Figure 50: Throughput Statistics



3.6.6. MTU

This is for setting the MTU of WAN (LTE) port, the range is from 1280 to 1500 Bytes.

Figure 51: MTU Settings

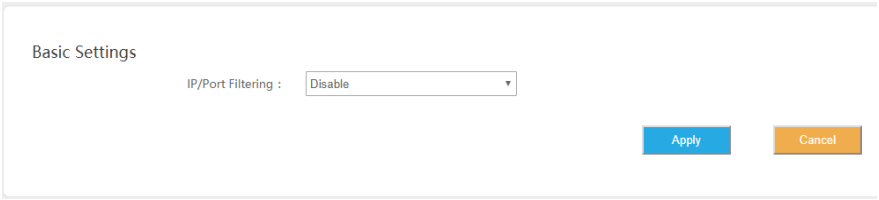


3.7. Security Menu

3.7.1. IP Filtering

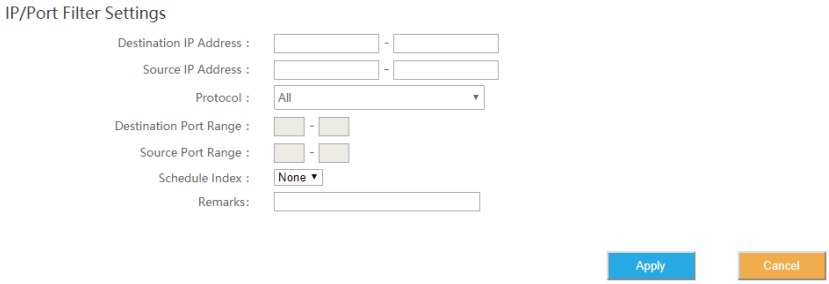
When using a firewall server in the local network, invoke this setting to enable or disable the firewall for this CPE (Figure 50).

Figure 52: Firewall Basic Settings



When enable IP/Port Filtering, then the IP/Port Filter can be set.

Figure 53: IP / Port Filtering



Settings:

(1) IP/Port Filtering Mode: Blacklist, White list

(2) IP/Port Filtering Log Dropped: enable / disable

(3) Destination IP Address: the destination IP Address of the filter

(4) Source IP Address: the source IP Address of the filter

(5) Protocol: TCP, UDP, TCP/UDP, ICMP, ALL

(6) Destination Port Range: the range of port

(7) Source Port Range: the range of port

(8) Schedule Index: Select box, if can be schedule by APPs

(9) Remarks

3.7.2. IPv6 Filtering

When enable IP/Port Filtering, then the IP/Port Filter can be set.

Figure 54: IPv6 Filtering

Settings:

(1) IPv6 Filtering Mode: Blacklist, White list

(2) IPv6 Filtering Log Dropped: enable / disable

(3) Destination IP Address: the destination IP Address of the filter

(4) Source IP Address: the source IP Address of the filter

(5) Protocol: TCP, UDP, TCP/UDP, ICMPv6, ALL

(6) Destination Port Range: the range of port

(7) Source Port Range: the range of port

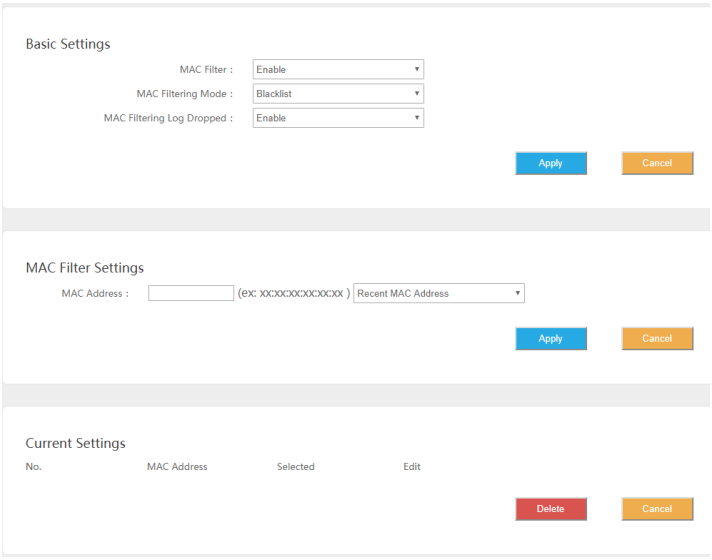
(8) Schedule Index: Select box, if can be schedule by APPs

(9) Remarks

3.7.3. MAC Filtering

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 53). Select *Enable* to enable MAC filtering, and then determine whether you will allow or forbid the defined MAC addresses to access the network.

Figure 55: MAC Filtering



Settings:

(1) MAC Filtering Mode: Blacklist, White list

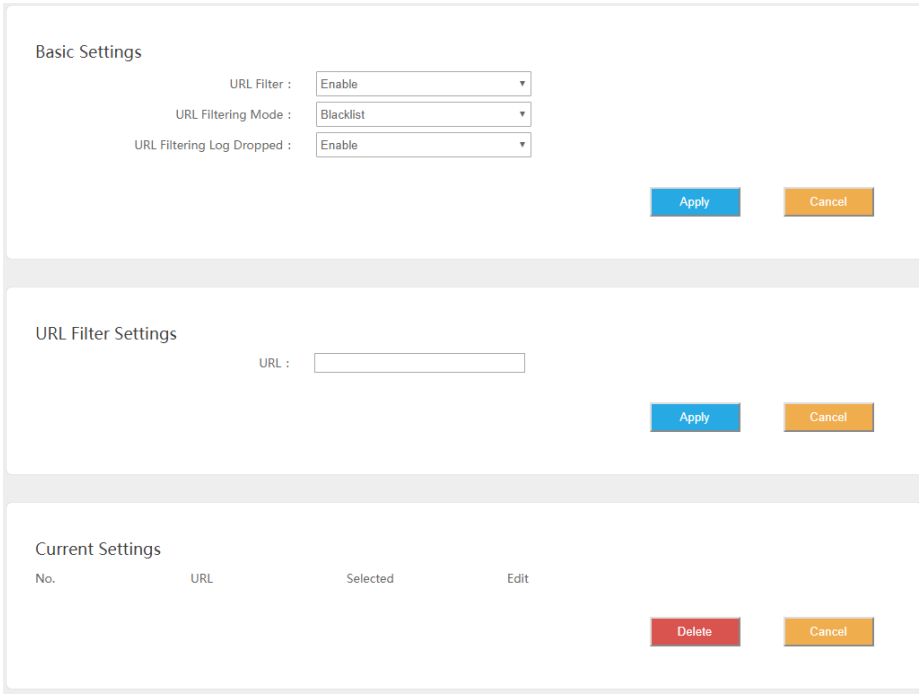
(2) MAC Filtering Log Dropped: enable / disable

(3) MAC Address: the filtering MAC address

3.7.4. URL Filtering

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 54. 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 56: URL Filtering



Settings:

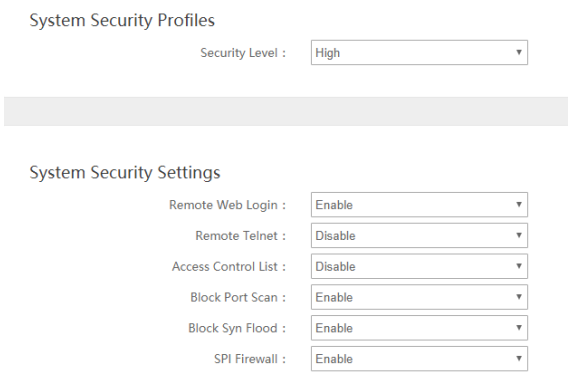
(1) URL Filtering Mode: Blacklist, White list

(2) URL Filtering Log Dropped: enable / disable

(3) URL: the filtering URL

3.7.5. System Security

Figure 57: System Security



System Security Profiles, include High, Medium, None and Custom, every profiles will corresponding with a set of System Security Settings.

Settings:

(1) Remote Web Login: enable / disable

(2) Remote Telnet: enable / disable

(3) Access Control List: enable / disable

(4) Block Port Scan: enable / disable

(5) Block Syn Flood: enable / disable

(6) SPI Firewall: enable / disable

3.7.6. Connect Limit

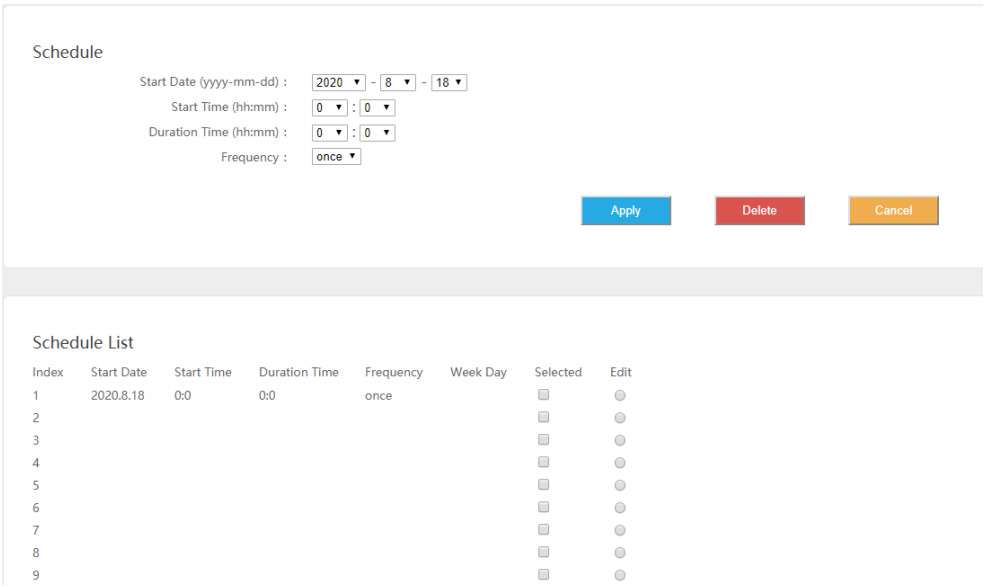
Connect Limit feature is used to control the number of connections through the UE to a host device, for example, a peer-to-peer file sharing application such as BitTorrent. Such apps require a large amount of bandwidth. By limiting the number of connections to the host device, you can control how much bandwidth each active connection receives. You can configure a Connect Limit for up to 16 host devices.

Figure 58: Connect Limit

3.7.7. Schedule

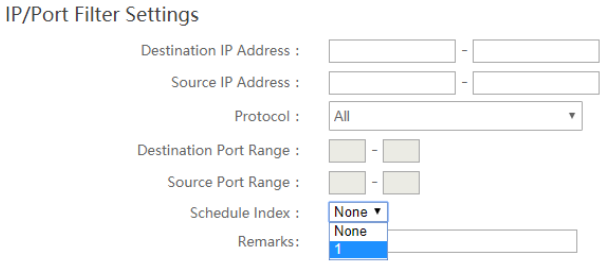
This feature is set for a group schedule list, like start from 2020.8.18 to 2020.8.20 as a index of the schedule.

Figure 59: Schedule List



In previous Filter configurations, you can select the schedule index like below figure.

Figure 60: Schedule Settings



3.8. NAT Menu

3.8.1. Port Forwarding

When NAT mode is enabled as the WAN interface type (section 3.5.2), 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 59). Enter the parameters per the field descriptions in Table 7.

Figure 61: Port Forwarding settings

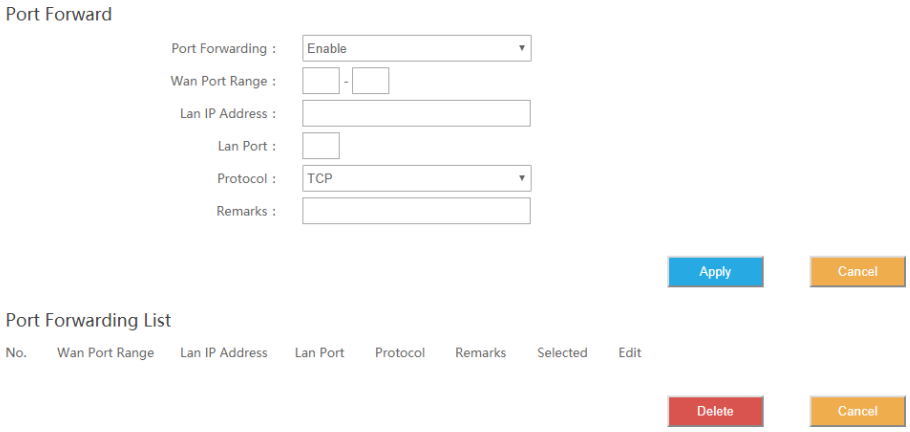


Table 7: Port Forwarding

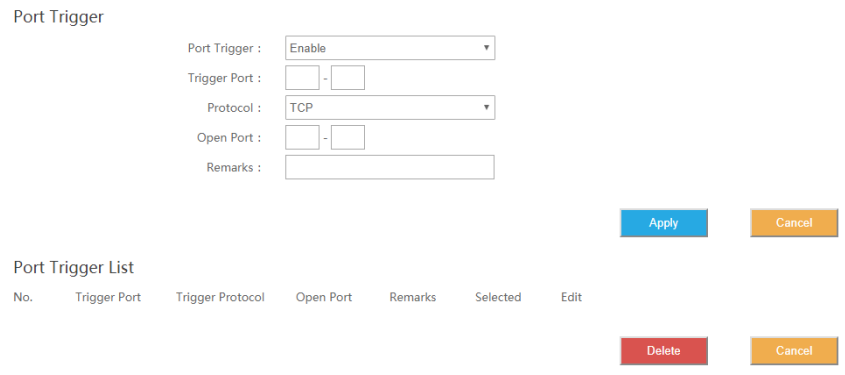
Field Name	Description
WAN Port Range	Enter the port number range for the remote device in the format of 1000 to 1500
LAN IP Address	Enter the local host IP address. The address must be different from the IP address that is set for the LAN Host Settings parameter, but they must be on the same network segment.
LAN Port	Enter the local port number. Range is 1 to 65,535.
Protocol	Select the type of data protocol, either TCP, UDP, or TCP&UDP
Remarks	

3.8.2. 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 3.5.2). 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 60).

Figure 62: Port Triggering Settings



3.8.3. 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 SIP, TFTP, PPTP, L2TP and IPSeC. You can enable the different types of application protocols by clicking on the check box next to the protocol name (Figure 61).

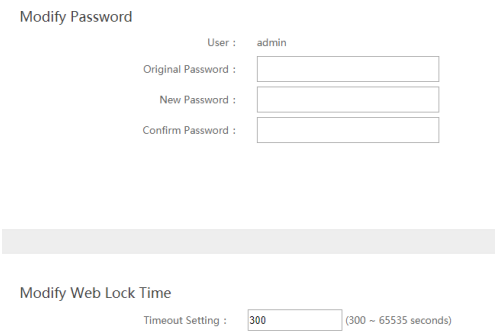
Figure 63: Throughput Statistics

3.9. System Menu

3.9.1. Account

This menu is used to change the login password for the CPE (Figure 62). The password must be 5 to 12 characters. Baicells recommends using a combination of upper- and lower-case letters and numbers.

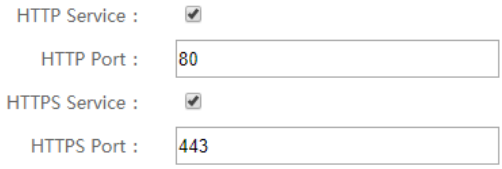
Figure 64: Account



3.9.2. WEB Settings

WEB Setting provides the ability to configure and manage the CPE remotely (Figure 63). This is especially helpful when a user calls in for technical assistance. In section 3.3 Login, you used this Web application with the default URL of http://192.168.150.1. Refer to Figure 65 for a description of each field.

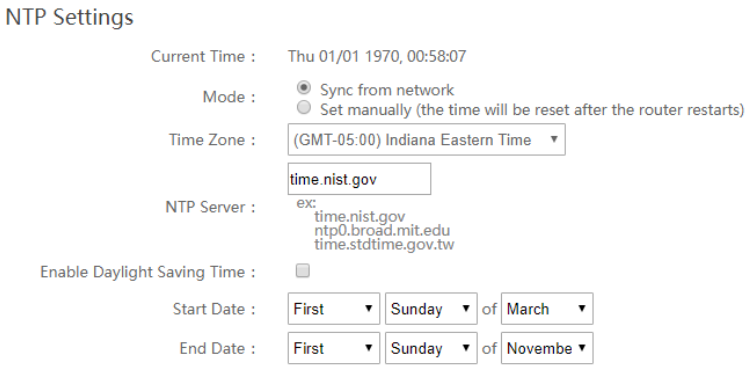
Figure 66: WEB Settings



3.9.3. NTP

The operator's network may 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 64).

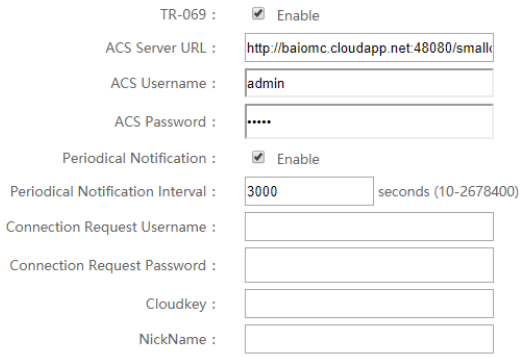
Figure 67: NTP Settings



3.9.4. 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 65). Refer to Figure 57 for a description of each field.

Figure 68: Throughput Statistics



3.9.5. TR-069 Certificate

This feature is used to upload the TR-069 certificate.

Figure 69: TR-069 Certificate

3.9.6. 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 67).

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

3.9.6.1. Firmware Update

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 67):

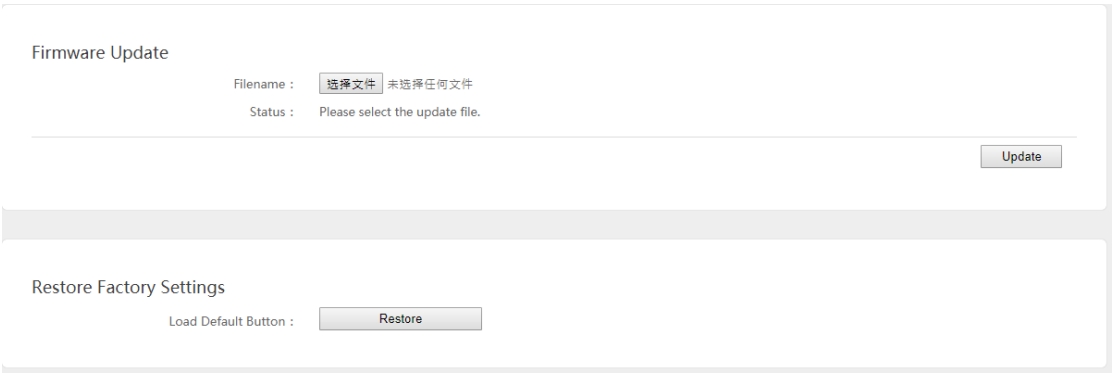
1. Download the image file from the Baicells support website (Baicells > Support > Downloads), and save it to your computer.
2. Under *Flash new firmware image*, determine if you want to keep the current configuration settings on the CPE . If you do, select the check box next to *Keep settings*.
3. Click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

3.9.6.2. Restore Factory Settings

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

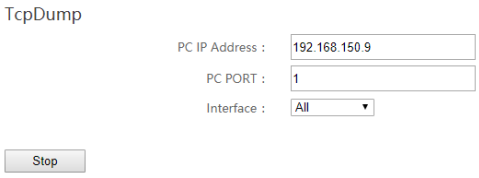
Figure 70: Restore & update



3.9.7. Diagnosis

3.9.7.1. TCPDump

Figure 71: TCPDump Settings



Settings:

(1) PC IP Address

(2) PC PORT

(3) Interface: ALL, LTE0PDN0 (APN0)

3.9.7.2. Ping

Figure 72: Ping Diagnosis Settings

Settings:

(1) IPv4/IPv6: Select the protocol

(2) IP Address/Domain: IP Address or URL

(3) Count: number of ping count

(4) Fragment: yes or no

(5) Packet size: 56~1400 Bytes (non-fragment)

3.9.7.3. Trace

Figure 73: Trace Diagnosis Settings

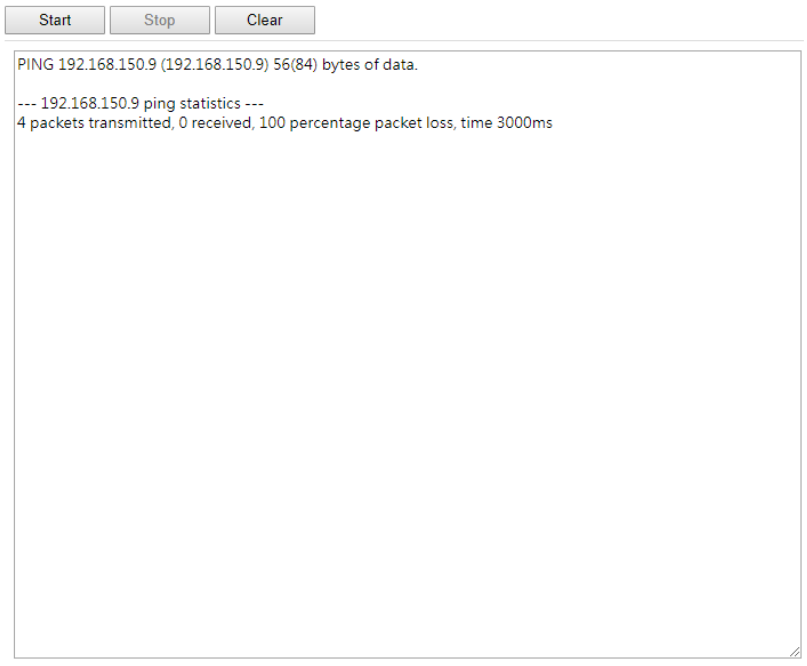
Settings:

(1) IPv4/IPv6: Select the protocol

(2) IP Address/Domain: IP Address or URL

3.9.7.4. Result

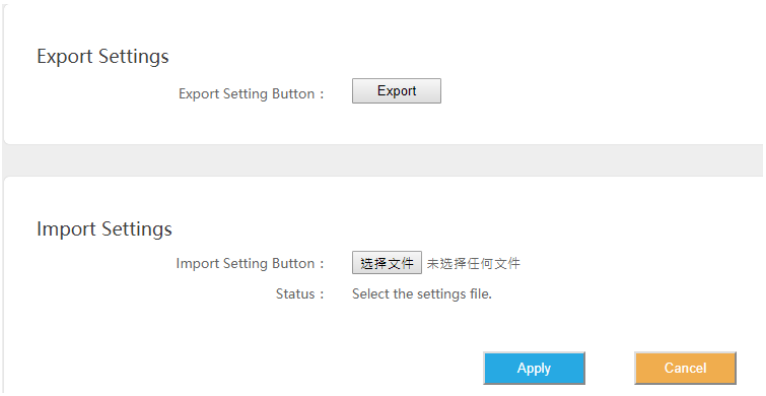
Figure 74: Diagnosis results



3.9.8. Backup Settings

This feature is used to backup the user settings, from the Web-GUI, you can Import / Export the settings.

Figure 75: Backup Settings



3.9.9. System Log

System log is the debug information of the CPE, when select the Setting, it can Export or Clear Logs.

Figure 76: System Log

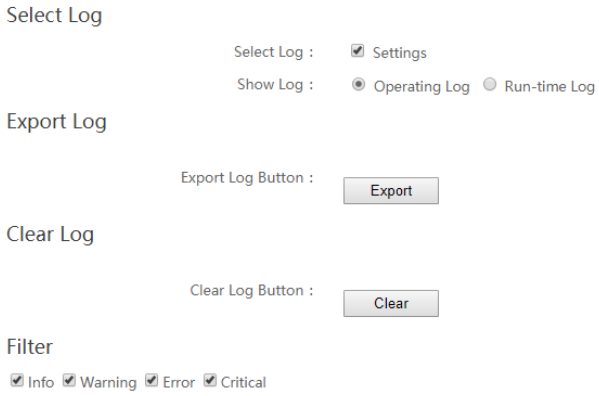
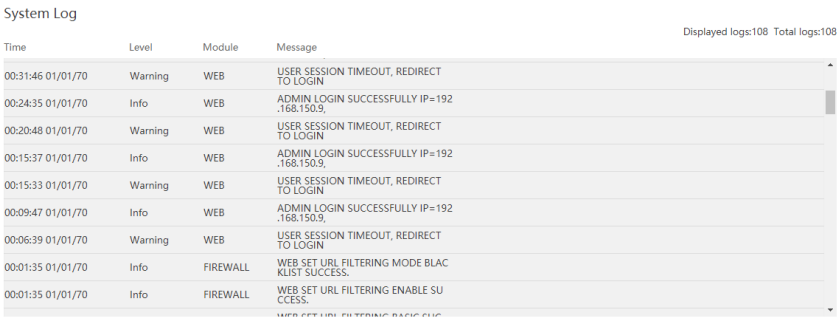


Figure 77: System logs



3.9.10. System Messages

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

Figure 78: System Message Settings

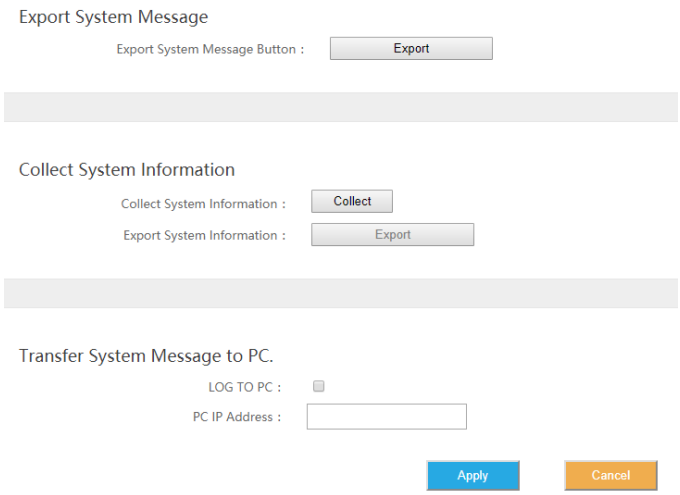
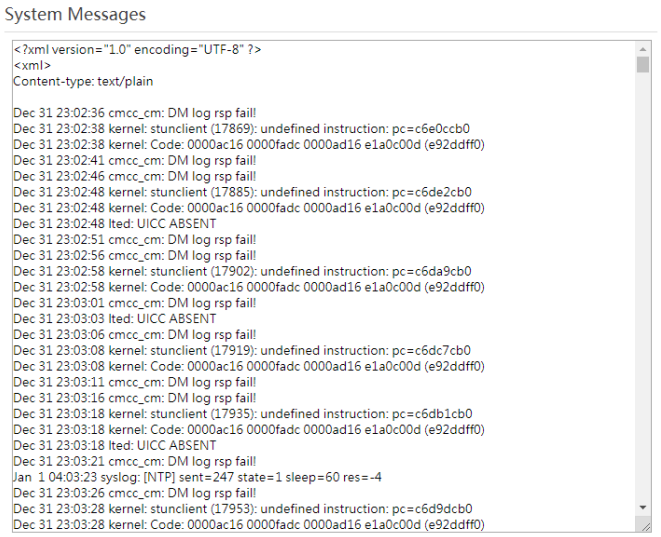
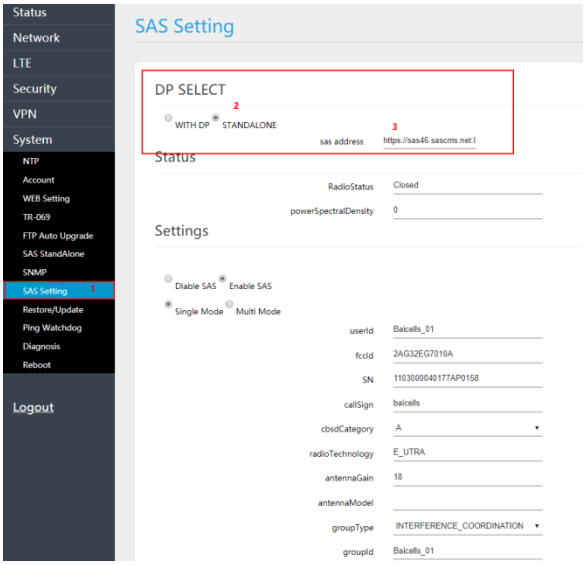


Figure 79: System Messages



3.9.11. SAS Settings



This model can support DP and standalone modes, and all SAS parameters can be configured in Web-GUI,

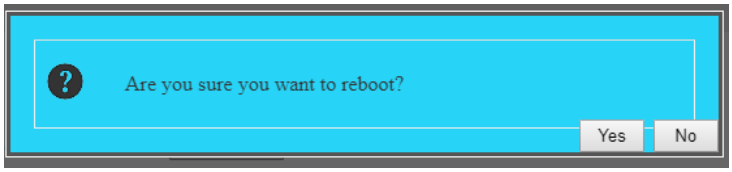
Reboot after you finish setting.

3.10. Reboot

Use the Reboot menu to perform a reboot of the CPE, as shown in Figure 77. 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.

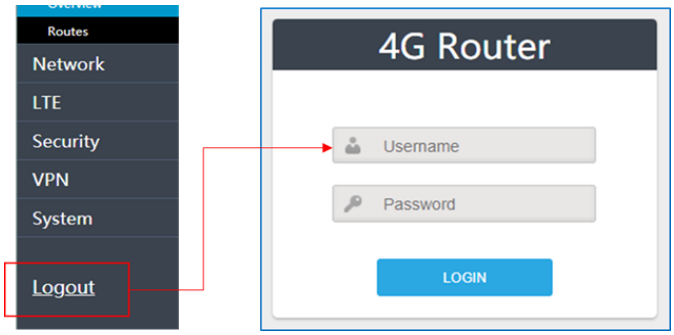
Figure 80: Reboot



3.11. Logout

When you click on the Logout menu, you are automatically logged out of the CPE and returned to the login screen (Figure 78).

Figure 81: Throughput Statistics



Appendix: 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 40cm between the radiator & your body.

ISEDC Compliance

This device complies with Innovation, Science, and Economic Development
Canada licence-exempt RSS standard(s).

Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d' Innovation, Science et Développement

économique Canada applicables aux appareils radio exempts de licence.
L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 40cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter, End-Users must be provided with transmitter operation conditions for satisfying RF exposure compliance.

Les antennes utilisées pour cet émetteur doivent être installées de façon à offrir une distance de séparation d'au moins 40cm entre toutes les personnes et ne doivent pas être colocalisées ou fonctionner conjointement avec d'autres antennes ou transmetteurs. pour satisfaire la conformité à l'exposition RF.