



LTE Outdoor CPE

Installation & Configuration Guide

Model EG8015G-M11-HP-EUD

June 2022

Version 1.0

About This Document

This document is for operators who will be installing and configuring the Baicells ATOM OD15 CPEs, model EG8015G-M11-HP-EUD.

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 OD15HP Data Sheet

Copyright Notice

Baicells Technologies, Inc., 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, Inc. The Baicells logo is a proprietary trademark of Baicells Technologies, Inc. Other trademarks mentioned in this document belong to their owners.

Revision Record

Date	Version	Description	SMEs/Contributors	Author/Editor
1-June-2022	v1.0		-	HuangHu

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.com 36T
Website:	www.Baicells.com	https://na.Baicells.com

Table of Contents

1.	Introduction	5
1.1.	Description.....	5
1.2.	ODU Modes	5
1.3.	Features	7
2.	Installation	7
2.1.	Part & Materials.....	7
2.2.	LEDs & Interfaces	8
2.3.	CPE Software.....	9
2.4.	Login	9
2.5.	Status Menu.....	9
2.5.1.	Overview	9
2.6.	Network Menu.....	13
2.6.1.	LAN Settings	13
2.6.2.	WAN Settings	14
2.6.2.1.	NAT Mode	14
2.6.2.2.	Router Mode.....	14
2.6.2.3.	Tunnel Mode.....	14
2.6.2.4.	Bridge Mode	15
2.6.2.5.	Mixed Mode	15
2.6.3.	Static Routes.....	16
2.6.4.	DMZ	17
2.6.5.	UPnP	17
2.7.	LTE Menu	18
2.7.1.	Connection Settings.....	18
2.7.1.1.	Roaming setting.....	18
2.7.1.2.	Default connection	18
2.7.1.3.	Power Scan Option	18
2.7.2.	Edit APN Profile	19
2.7.3.	PIN Management.....	19
2.7.4.	Cell selection	20
2.7.5.	SIM Lock Settings.....	22
2.7.6.	MTU	22
2.8.	Security Menu.....	23
2.8.1.	IP Filtering.....	23
2.8.2.	IPv6 Filtering.....	23
2.8.3.	MAC Filtering	24
2.8.4.	URL Filtering	25
2.8.5.	System Security.....	26
2.8.6.	Connect Limit.....	26
2.8.7.	Schedule	27
2.9.	NAT Menu	28
2.9.1.	Port Forwarding.....	28
2.9.2.	Port Triggering	28

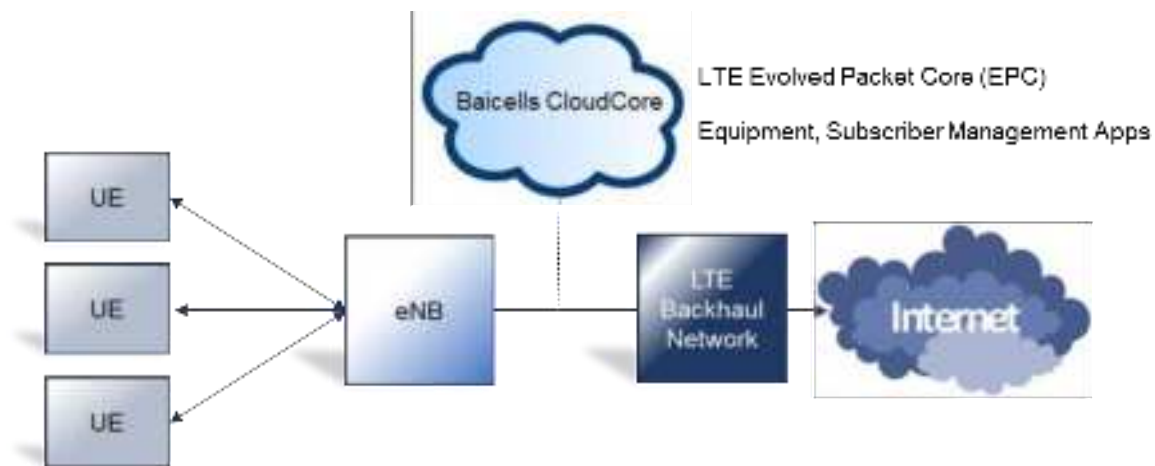
2.9.3.	ALG	29
2.10.	System Menu	29
2.10.1.	Account.....	29
2.10.2.	WEB Settings	30
2.10.3.	NTP	30
2.10.4.	TR-069	30
2.10.5.	TR-069 Certificate.....	31
2.10.6.	Restore / Update	31
2.10.6.1.	Firmware Update	31
2.10.6.2.	Restore Factory Settings	32
2.10.7.	Diagnosis	32
2.10.7.1.	TCPDump	32
2.10.7.2.	Ping	32
2.10.7.3.	Trace	33
2.10.7.4.	Result	33
2.10.8.	Backup Settings	34
2.10.9.	System Log.....	34
2.10.10.	System Messages.....	34
2.11.	Reboot	36
2.12.	Logout.....	36
	Appendix: Regulatory Compliance	37
	FCC Compliance	37

1. Introduction

1.1. Description

The Baicells Atom OD15 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: 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 work 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 11 (CAT12/15)
- 1000 Mbps Ethernet interface
- 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 OD15 unit	1	
Power Cable	1	
PoE Power Adaptor	1	

Atom OD15 Mounting Bracket	1 each	
----------------------------	--------	--

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. 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. for a description of the LEDs . for a description of the interfaces.

Table 3: LEDs

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

Identity	Description	Color	Status	Description
L&S	LTE network and USIM status	Blue	Off	The UE is not connected to the network
			Steady On	The UE is connected to the LTE network
PWR	Power status	Yellow	Off	No power supply to the UE
			Steady On	Power to the UE is on
LTE Signal	L/M/H 3 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

Interfaces	Description
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.

2.3. 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.

2.4. 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 2: 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](#).

2.5. Status Menu

2.5.1. Overview

After logging in, the GUI opens to the Status > Overview page. 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 3: Status

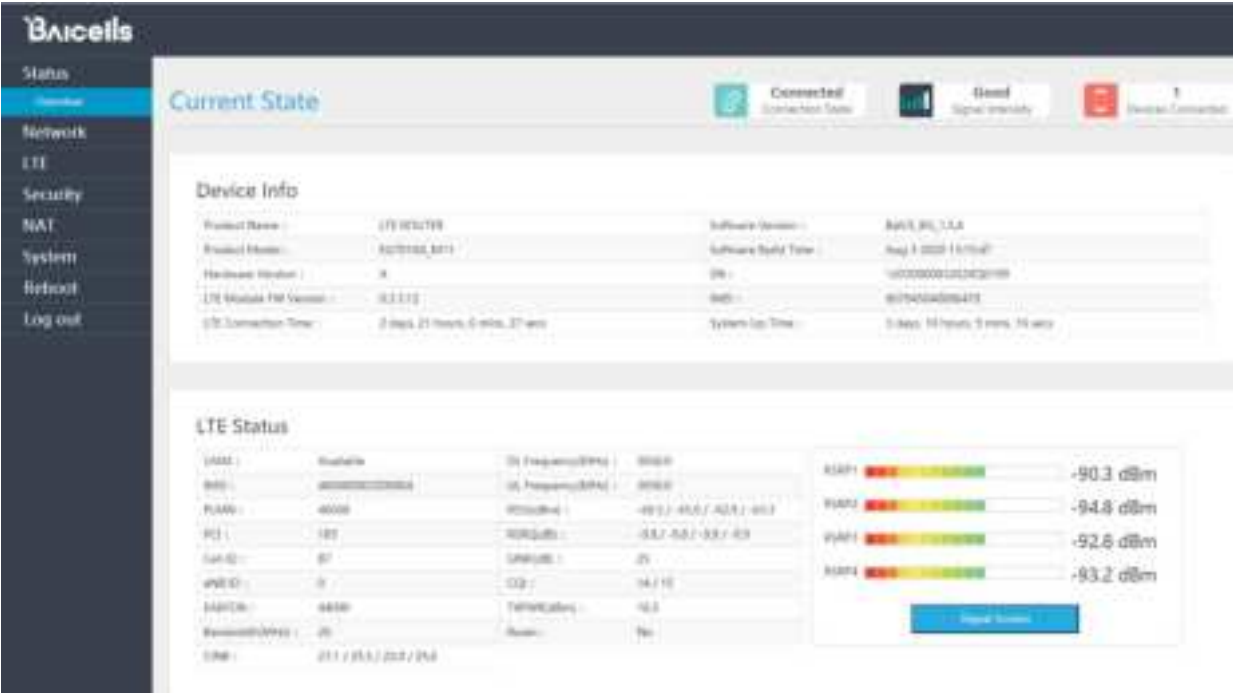


Figure 4: Throughput Statistics

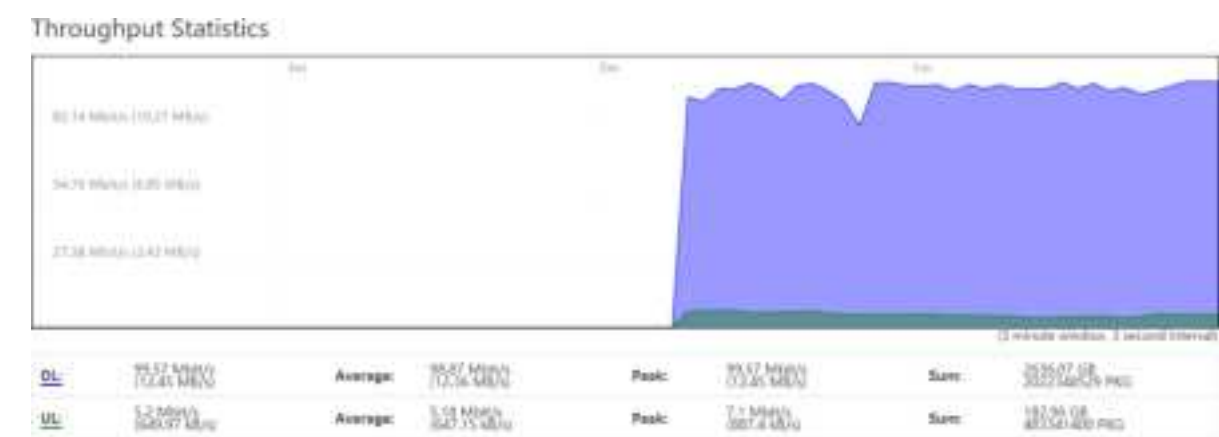


Figure 5: Internet Statistics



Figure 6: LAN Status

LAN Status			
IPv4 Address :	192.168.150.1	IPv6 Address :	
IPv4 Netmask :	255.255.255.0	IPv6 Prefix :	
IPv4 MAC Address :	48:bf:74:0d:a1:c4	IPv6 Prefix Len :	

Figure 7: Device List

Devices List			
Host Name	MAC Address	IP Address	Lease Time
DESKTOP-VQJWNL	D8:9E:F3:04:CF:D9	192.168.150.10	07:48:53

Table 3: 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 or Wireless LAN (WLAN)/Wi-Fi connection
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

2.6. Network Menu

2.6.1. LAN Settings

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

Figure 8: DHCP Settings

The screenshot shows the 'DHCP' configuration page. On the left is a sidebar menu with options: Network, LAN Settings, WAN Settings, Mobile Settings, Static Routes, DMZ, Other, LTE, Security, NAT, System, Backup, and Log view. The 'LAN Settings' section is active. The 'DHCP' settings include: 'DHCP Server' (Enabled), 'IP Address' (192.168.1.1), 'Subnet Mask' (255.255.255.0), 'DHCP Start IP' (192.168.1.10), 'DHCP End IP' (192.168.1.254), 'Lease Time' (6000), 'UPNP' (Enabled), and 'DHCP Settings' (Auto, 15 Minutes). There are 'Save' and 'Cancel' buttons at the bottom right.

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

Figure 9: DHCP Static Leases

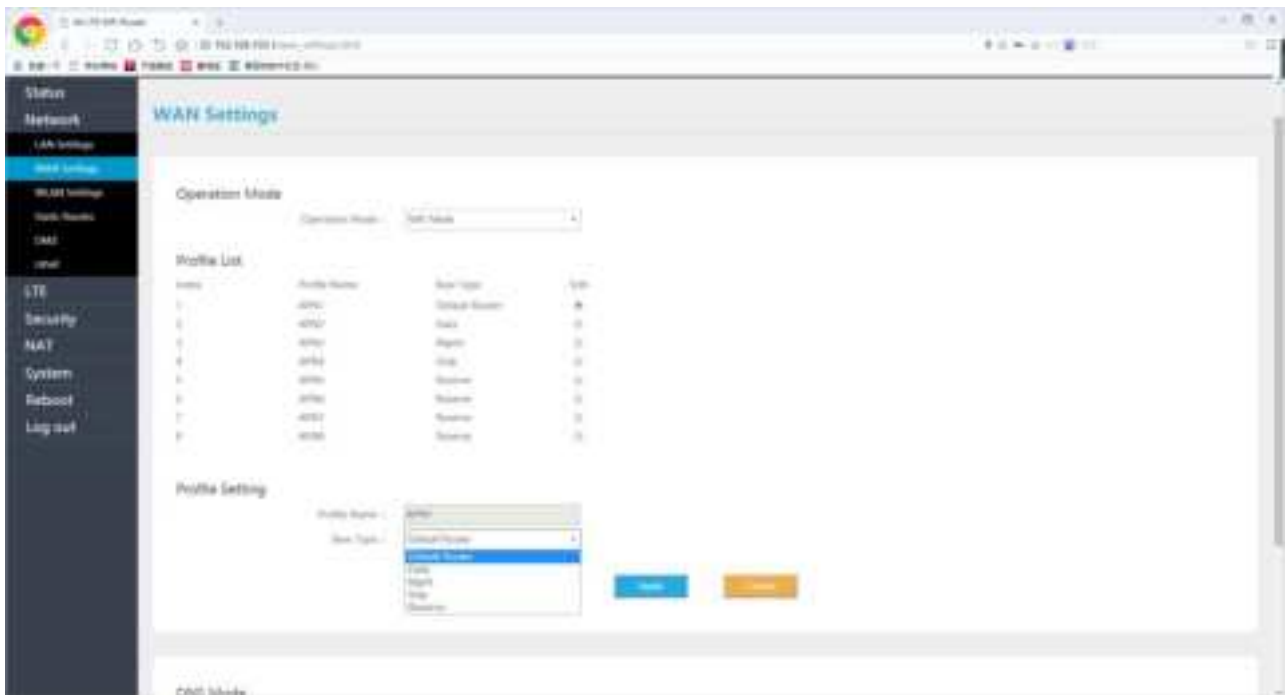
The screenshot shows the 'DHCP Static Leases' configuration page. It has three main sections: 'Basic Settings', 'Add DHCP Static Lease', and 'Current DHCP Static Leases'.
1. 'Basic Settings': 'DHCP Static Leases' is set to 'Enable'. There are 'Apply' and 'Cancel' buttons.
2. 'Add DHCP Static Lease': Fields for 'IP Address' and 'MAC Address' (with a placeholder '(no mac addresses)') are present. There are 'Apply' and 'Cancel' buttons.
3. 'Current DHCP Static Leases': A table with columns 'No.', 'IP Address', 'MAC Address', 'Selected', and 'Edit'. Below the table are 'Delete' and 'Cancel' buttons.

2.6.2. WAN Settings

2.6.2.1. 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 10: WAN Settings



2.6.2.2. Router Mode

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

Figure 11: Router Mode



2.6.2.3. Tunnel Mode

This CPE can support L2TP and GER VPN mode.

Figure 12: Tunnel Mode

Operation Mode : Tunnel Mode

Tunnel Mode

VPN Type : L2TP

NAT Support : Enable

Default Route : VPN

Host name :

L2TP

BCP Support : Disable

L2TP Server IP :

L2TP User : admin

L2TP Password :

Apply Cancel

2.6.2.4. 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 13: Bridge Mode

Operation Mode : Bridge Mode

Profile List

Index	Profile Name	Vlan Id	Edit
1	APN1	1121	⊙
2	APN2	1122	⊙
3	APN3	1123	⊙
4	APN4	1124	⊙
5	APN5	1125	⊙
6	APN6	1126	⊙
7	APN7	1127	⊙
8	APN8	1128	⊙

Profile Setting

Profile Name :

Vlan Id : (0-4094)

Apply Cancel

2.6.2.5. Mixed Mode

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

Figure 14: Mixed Mode

Operation Mode

Operation Mode : Mixed Mode

Profile List

Index	Profile Name	Mode	Vlan Id	Bear Type	Edit
1	APN1	Bridge	1121	Default Router	
2	APN2	Bridge	1122	Data	
3	APN3	Bridge	1123	Mgmt	
4	APN4	Bridge	1124	Voip	
5	APN5	Bridge	1125	Reserve	
6	APN6	Bridge	1126	Reserve	
7	APN7	Bridge	1127	Reserve	
8	APN8	Bridge	1128	Reserve	

Profile Setting

Profile Name :

Mode : NAT Mode

Bear Type : Default Router

Apply

Cancel

2.6.3. 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 15: Static routes

Bicells

Status

Network

LAN Settings

WAN Settings

WLAN Settings

Static Routes

DMZ

UPnP

LTE

Security

NAT

System

Reboot

Log out

Route Settings

Route Settings

Route Type : LAN

Gateway :

Destination Network :

Route Subnet Mask :

Apply

Cancel

Current Settings

Route Type	Gateway	Destination IP(Reachable)	Route Subnet Mask	Selected	Edit

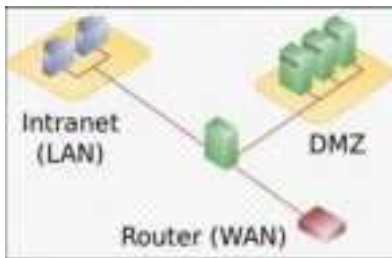
Delete

Cancel

2.6.4. 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 16: 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 17: DMZ Settings

The screenshot shows a window titled 'DMZ'. Inside, there is a 'DMZ Setting' dropdown menu set to 'Enable'. Below it is a 'DMZ Address' text input field. At the bottom right, there are two buttons: 'Apply' (blue) and 'Cancel' (orange).

2.6.5. 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 18: UPnP Settings

The screenshot shows a window titled 'UPnP'. Inside, there is a 'UPnP Setting' dropdown menu set to 'Enable'. Below it are 'Apply' (blue) and 'Cancel' (orange) buttons. At the bottom, there is a section titled 'Port Mapping List' with a table. The table has five columns: 'Internal Host', 'Protocol', 'External Port', 'Internal Port', and 'Description'.

Internal Host	Protocol	External Port	Internal Port	Description
---------------	----------	---------------	---------------	-------------

2.7. LTE Menu

2.7.1.1. Connection Settings

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

Figure 19: Connection Settings

The screenshot displays the 'LTE Connection Settings' interface. It is divided into three main sections: 'Roaming Settings', 'Default Connection', and 'Power Scan Option'.
1. **Roaming Settings**: At the top, it shows 'Roam Settings' with radio buttons for 'Enable' (selected) and 'Disable'. Below this are 'Apply' and 'Cancel' buttons.
2. **Default Connection**: The middle section shows 'Status' as 'Disconnected' and 'Connection Mode' as a dropdown menu currently set to 'Always on'. It also features 'Apply' and 'Cancel' buttons.
3. **Power Scan Option**: The bottom section shows 'Power Scan' as a dropdown menu currently set to 'First Detected Cell'. It also features 'Apply' and 'Cancel' buttons.

2.7.1.2. 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.

2.7.1.3. 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 20: Default Connection Settings

This is a close-up of the 'Default Connection' section from Figure 19. It shows the 'Status' as 'Disconnected' and the 'Connection Mode' dropdown menu. The dropdown is open, showing three options: 'Always on' (highlighted in blue), 'Always on', and 'Manual'. 'Apply' and 'Cancel' buttons are visible to the right.

2.7.1.4. Power Scan Option

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

Figure 21: Scan mode Settings



2.7.2. 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 22: 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.

2.7.3. 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 23: PIN Management

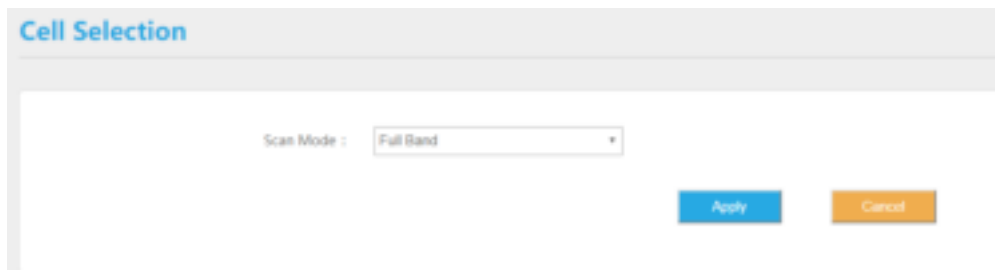


2.7.4. Cell selection

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 24: 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 25: Dedicated EARFCN

Scan Mode:

Dedicated EARFCN

Display:

RF

FDD

Apply

Cancel

EARFCN Settings

Band:

42

Type:

0: EARFCN

1: Frequency

EARFCN:

(41500-41800)

Frequency:

(1400-1400.4 MHz)

Apply

Cancel

EARFCN List

Band	EARFCN	Frequency (MHz)	Selected	Lock
------	--------	-----------------	----------	------

Create

Refresh

Figure 26: Cell Lock

Scan Mode:

Cell Lock

Apply

Cancel

Cell Setting

Band:

42

Type:

0: EARFCN

1: Frequency

EARFCN:

(41500-41800)

Frequency:

(1400-1400.4 MHz)

PCI ID:

(0-502)

Apply

Cancel

Cell List

Band	EARFCN	Frequency (MHz)	PCI ID	Selected	Lock
------	--------	-----------------	--------	----------	------

Create

Refresh

Figure 27: PCI Only Lock

The screenshot shows a web-based configuration interface for 'PCI Only Lock'. At the top, there is a 'Search Module' dropdown menu with 'PCI Lock' selected. Below this are 'Apply' and 'Cancel' buttons. The main section is titled 'PCI Setting' and contains two input fields: 'PCI Lock 1' and 'PCI Lock 2', both with a range of '(0-1000)'. Below these fields are 'Apply' and 'Cancel' buttons. At the bottom, there is a 'PCI List' section with a table containing columns for 'Index', 'PCI Lock', 'PCI Lock', 'Network', and 'Status'. Below the table are 'Apply' and 'Cancel' buttons.

2.7.5. 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 28: Throughput Statistics

The screenshot shows a web-based configuration interface for 'SIM Lock Settings'. It features a 'SIM Lock' section with two radio buttons: 'SIM Lock Check' (selected) and 'SIM Lock Uncheck'. Below this is a 'PLMN ID' input field. At the bottom are 'Apply' and 'Cancel' buttons.

2.7.6. MTU

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

Figure 29: MTU Settings

The screenshot shows a web-based configuration interface for 'MTU Settings'. It features an 'MTU' input field with the value '1500' and a hint '(Between 1280 and 1500)'. At the bottom are 'Apply' and 'Cancel' buttons.

2.8. Security Menu

2.8.1. 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 30: Firewall Basic Settings



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

Figure 31: 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

2.8.2. IPv6 Filtering

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

Figure 32: IPv6 Filtering

IPv6/Port Filter settings

Destination IP Address :

Source IP Address :

Protocol : All

Destination Port Range : -

Source Port Range : -

Remarks :

Apply Cancel

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

2.8.3. 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 33: MAC Filtering

Basic Settings

MAC Filter : Enable

MAC Filtering Mode : Blacklist

MAC Filtering Log Dropped : Enable

Apply Cancel

MAC Filter Settings

MAC Address : 00:00:00:00:00:00 Recent MAC Address

Apply Cancel

Current Settings

No.	MAC Address	Selected	Edit

Delete Cancel

Settings:

- (1) MAC Filtering Mode: Blacklist, White list

- (2) MAC Filtering Log Dropped: enable / disable
- (3) MAC Address: the filtering MAC address

2.8.4. 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 34: URL Filtering

The screenshot shows a web-based configuration interface for URL filtering. It is organized into three distinct sections, each with its own title and controls.

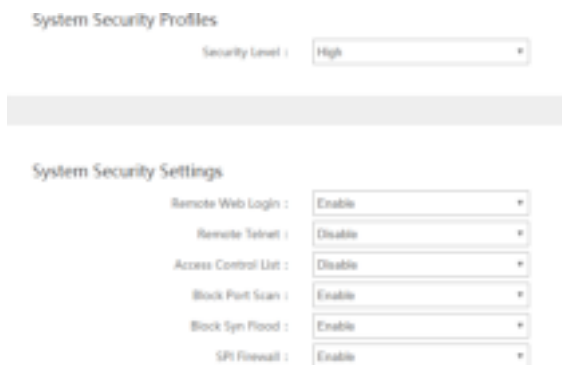
- Basic Settings:** This section contains three dropdown menus: 'URL Filter' (set to 'Enable'), 'URL Filtering Mode' (set to 'Blacklist'), and 'URL Filtering Log Dropped' (set to 'Enable'). Below these are 'Apply' and 'Cancel' buttons.
- URL Filter Settings:** This section features a single text input field labeled 'URL :'. Below the input field are 'Apply' and 'Cancel' buttons.
- Current Settings:** This section displays a table with the following headers: 'No.', 'URL', 'Selected', and 'Edit'. Below the table are 'Delete' and 'Cancel' buttons.

Settings:

- (1) URL Filtering Mode: Blacklist, White list
- (2) URL Filtering Log Dropped: enable / disable
- (3) URL: the filtering URL

2.8.5. System Security

Figure 35: System Security



System Security Profiles

Security Level : High

System Security Settings

Remote Web Login : Enable

Remote Telnet : Disable

Access Control List : Disable

Block Port Scan : Enable

Block Syn Flood : Enable

SPI Firewall : Enable

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

2.8.6. 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 36: Connect Limit



Connect Limit : Enable

Lan IP Address : -

Limit Value :

Schedule Index : None

Remarks :

2.8.7. 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 37: Schedule List

Index	Start Date	Start Time	Duration Time	Frequency	Week Day	Selected	Edit
1	2020.8.18	00:00	00:00	once		X	X
2						X	X
3						X	X
4						X	X
5						X	X
6						X	X
7						X	X
8						X	X
9						X	X

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

Figure 38: Schedule Settings

IP/Port Filter Settings

Destination IP Address: [] - []

Source IP Address: [] - []

Protocol: All

Destination Port Range: [] - []

Source Port Range: [] - []

Schedule Index: None

Remarks: []

2.9. NAT Menu

2.9.1. 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 4.

Figure 39: Port Forwarding settings

Port Forward

Port Forwarding :

Wan Port Range : -

Lan IP Address :

Lan Port :

Protocol :

Remarks :

Apply Cancel

Port Forwarding List

No.	Wan Port Range	Lan IP Address	Lan Port	Protocol	Remarks	Selected	Edit
-----	----------------	----------------	----------	----------	---------	----------	------

Delete Cancel

Table 4: 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	

2.9.2. 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 40: Port Triggering Settings

Port Trigger

Port Trigger :

Enable

Trigger Port :

-

Protocol :

TCP

Open Port :

-

Remarks :

Apply

Cancel

Port Trigger List

No.	Trigger Port	Trigger Protocol	Open Port	Remarks	Selected	Edit
-----	--------------	------------------	-----------	---------	----------	------

Delete

Cancel

2.9.3. 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 41: Throughput Statistics

ALG Settings

SIP :

Enable

TFTP :

Enable

PPTP Passthrough :

Enable

L2TP Passthrough :

Enable

IPsec Passthrough :

Enable

2.10. System Menu

2.10.1. 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 42: Account

Modify Password

User :

admin

Original Password :

New Password :

Confirm Password :

Modify Web Lock Time

Timeout Setting :

300

(300 ~ 65535 seconds)

2.10.2. 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> for a description of each field.

Figure 43: WEB Settings

HTTP Service : ☒

HTTP Port :

HTTPS Service : ☒

HTTPS Port :

2.10.3. 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 64).

Figure 44: NTP Settings

NTP Settings

Current Time : Thu 01/01 1970, 00:00:00

Mode : ☒ Sync from network
☐ Set manually (the time will be reset after the router restarts)

Time Zone : (GMT-05:00) Indiana Eastern Time

NTP Server : time.nist.gov

Enable Daylight Saving Time : ☐

Start Date : First * Sunday * of March *

End Date : First * Sunday * of November *

2.10.4. 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 45).

Figure 45: Throughput Statistics

TR-069 : ☒ Enable

ACS Server URL :

ACS Username :

ACS Password :

Periodical Notification : ☒ Enable

Periodical Notification Interval : seconds (10-2678400)

Connection Request Username :

Connection Request Password :

Cloudkey :

NickName :

2.10.5. TR-069 Certificate

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

Figure 46: TR-069 Certificate

TR-069 Cert : ☒ Enable

Upload Button :

2.10.6. 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.

2.10.6.1. 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.

2.10.6.2. 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 47: Restore & update

The screenshot shows two sections of a web interface. The top section, titled 'Firmware Update', contains a 'Filename' field with a '选择文件' (Select File) button and a 'Status' field with the text 'Please select the update file.'. Below this is an 'Update' button. The bottom section, titled 'Restore Factory Settings', contains a 'Load Default Button' field with a 'Restore' button.

2.10.7. Diagnosis

2.10.7.1. TCPCDump

Figure 48: TCPCDump Settings

The screenshot shows the 'TcpDump' settings form. It includes three input fields: 'PC IP Address' with the value '192.168.168.9', 'PC PORT' with the value '1', and 'Interface' with a dropdown menu showing 'All'. Below these fields is a 'Stop' button.

Settings:

- (1) PC IP Address
- (2) PC PORT
- (3) Interface: ALL, LTEOPDNO (APNO)

2.10.7.2. Ping

Figure 49: Ping Diagnosis Settings

The screenshot shows the 'Diagnostics' settings form. It includes several input fields: 'Command' with a dropdown menu showing 'Ping', 'IPv4/IPv6' with a dropdown menu showing 'IPv4', 'IP Address/Domain' with an empty text box, 'Count' with an empty text box, 'Fragment' with a dropdown menu showing 'Yes', and 'Packet size' with a text box showing '64'.

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)

2.10.7.3. Trace

Figure 50: Trace Diagnosis Settings

Diagnostics

Command :

IPv4/IPv6 :

IP Address/Domain :

Settings:

- (1) IPv4/IPv6: Select the protocol
- (2) IP Address/Domain: IP Address or URL

2.10.7.4. Result

Figure 51: Diagnosis results

Start Stop Clear

IPv6 192.168.150.9 (192.168.150.9: 56(84) bytes of data:

--- 192.168.150.9 ping statistics ---

4 packets transmitted, 0 received, 100 percentage packet loss, time 5000ms

2.10.8. Backup Settings

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

Figure 52: Backup Settings



2.10.9. System Log

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

Figure 53: System Log

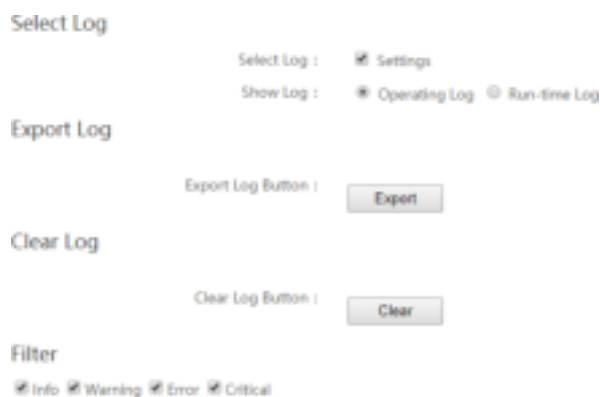


Figure 54: System logs

The screenshot shows a table titled 'System Log' with columns for 'Time', 'Level', 'Source', and 'Message'. The table contains several log entries with timestamps, levels (Warning, Info), sources (e.g., /usr/sbin/sshd), and messages (e.g., 'sshd: [user] connection closed by user').

Time	Level	Source	Message
2023-08-10 10:00:00	Warning	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:01	Info	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:02	Warning	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:03	Info	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:04	Warning	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:05	Info	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:06	Warning	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:07	Info	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:08	Info	/usr/sbin/sshd	sshd: [user] connection closed by user
2023-08-10 10:00:09	Info	/usr/sbin/sshd	sshd: [user] connection closed by user

2.10.10. System Messages

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

Figure 55: System Message Settings

Figure 56: System Messages

System Messages

```

vTerm version: 1.2 encoding: UTF-8 />
^C
Content type: text/plain

Dec 31 23:02:38 cmrc_jm: DM log rfp fail
Dec 31 23:02:38 kernel: stunchent [17899]: undefined instruction: pc=0x0c0198
Dec 31 23:02:38 kernel: Code: 0000a10 0000fa: 0000a10 e1a00000 (e10a00ff)
Dec 31 23:02:41 cmrc_jm: DM log rfp fail
Dec 31 23:02:46 cmrc_jm: DM log rfp fail
Dec 31 23:02:46 kernel: stunchent [17899]: undefined instruction: pc=0x0c0198
Dec 31 23:02:46 kernel: Code: 0000a10 0000fa: 0000a10 e1a00000 (e10a00ff)
Dec 31 23:02:46 host: UNCC ABSENT
Dec 31 23:02:51 cmrc_jm: DM log rfp fail
Dec 31 23:02:56 cmrc_jm: DM log rfp fail
Dec 31 23:02:58 kernel: stunchent [17900]: undefined instruction: pc=0x0c0198
Dec 31 23:02:58 kernel: Code: 0000a10 0000fa: 0000a10 e1a00000 (e10a00ff)
Dec 31 23:03:01 cmrc_jm: DM log rfp fail
Dec 31 23:03:03 host: UNCC ABSENT
Dec 31 23:03:04 cmrc_jm: DM log rfp fail
Dec 31 23:03:08 kernel: stunchent [17900]: undefined instruction: pc=0x0c0198
Dec 31 23:03:08 kernel: Code: 0000a10 0000fa: 0000a10 e1a00000 (e10a00ff)
Dec 31 23:03:11 cmrc_jm: DM log rfp fail
Dec 31 23:03:14 cmrc_jm: DM log rfp fail
Dec 31 23:03:18 kernel: stunchent [17900]: undefined instruction: pc=0x0c0198
Dec 31 23:03:18 kernel: Code: 0000a10 0000fa: 0000a10 e1a00000 (e10a00ff)
Dec 31 23:03:18 host: UNCC ABSENT
Dec 31 23:03:21 cmrc_jm: DM log rfp fail
Dec 31 23:03:23 syslog: [9779] sent=247 stream: [seq=62] len=4
Dec 31 23:03:26 cmrc_jm: DM log rfp fail
Dec 31 23:03:28 kernel: stunchent [17900]: undefined instruction: pc=0x0c0198
Dec 31 23:03:28 kernel: Code: 0000a10 0000fa: 0000a10 e1a00000 (e10a00ff)

```

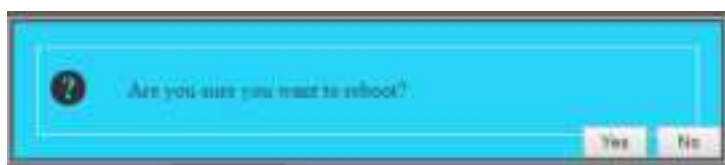
2.11. Reboot

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 58: Reboot



2.12. 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 59: 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 20cm between the radiator & your body.