



LTE Turbo UE Configuration Guide for EG8015Q-M11

Document Version: 01

About This Document

This document describes the configuration of the LteTurbo CPE for EG8015Q-M11. It is a guide that how to configure the device after its installation completes.

Copyright Notice

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

Disclaimer

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

Revision Record

Date	Version	Description
22 July, 2022	01	Initial released.

Contact Us

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

Menu

1. Configuration Overview	1
2. Installation	1
2.1 Part & Materials	1
2.2 Led	2
3. Login Web Client	5
3.1 Web Client Environmental Requirements	5
3.2 Connect Web Client to CPE	5
3.3 Set Up Client Computer	5
3.4 Log In	7
4. Network Setting	9
4.1 LAN Settings	9
4.2 WAN Settings	9
4.3 WLAN Settings	10
4.4 NGMWAN Settings	10
4.5 Static Routes	11
5. LTE Setting	12
5.1 Connection Mode	12
5.2 Scan Mode	12
5.3 APN Management	12
5.4 PIN Management	13
6. Security Setting	14
6.1 Zones	14
6.2 Port Forwards	14
6.3 Traffic Rules	15
6.4 Custom Rules	15
7. VPN Setting	16
7.1 IPSec	16

7.2	General VPN	16
7.3	OpenVPN	17
8.	System.....	18
8.1	NTP	18
8.2	Account	18
8.3	Dynamic DNS.....	19
8.4	WEB Setting.....	19
8.5	TR069.....	20
8.6	FTP Auto Upgrade	20
8.7	SNMP	21
8.8	Restore/Update.....	21
8.9	Ping Watchdog	22
8.10	SAS.....	22
		22
8.11	SAS Setting	23
8.12	SAS Certificates.....	23
8.13	Diagnosis	24
8.14	Reboot.....	24
9.	Regulatory Compliance.....	25
	FCC Compliance	25

1. Configuration Overview

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

The Baicells LteTurbo Outdoor 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.

2. Installation

2.1 Part & Materials

Item	Qty	Picture
EG8015Q-M11 unit	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.

2.2 Led

The CPE has 10 lights, divided into 6 groups according to the function: wifi signal light, lte signal light, power light, sim light, lan light, miu light (see figure below).



- **Wifi signal light**

Arc logo , Three lights indicate wifi signal strength according to the number of lights, full light indicates strong signal; full out when not connected

- **Lte signal light**

Vertical logo , Three lights indicate lte signal intensity according to the number of lights, full light indicates strong signal; flash when not connected

- **Power light**

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

- **Sim light**

Light on -> Insert the normal SIM card; otherwise no sim nor sim is bad.

- **Lan light**

Light on -> LAN port is connected

- Miu light

Reserved

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

3. Login Web Client

3.1 Web Client Environmental Requirements

Table 3-1 describes the requirements on computer of the client.

Table 3-1 Environmental Requirements of the Client

Item	Description
CPU	Above Intel Core 1GHz
Memory	Above 2G RAM
Hard disk	No less than 100 MB space available
Operating system	- Microsoft: Windows XP, Windows Vista or Windows7 - Mac: MacOSX10.5 or above
Screen resolution	Above 1024 x 768
Browser	Chrome 6 or higher

3.2 Connect Web Client to CPE

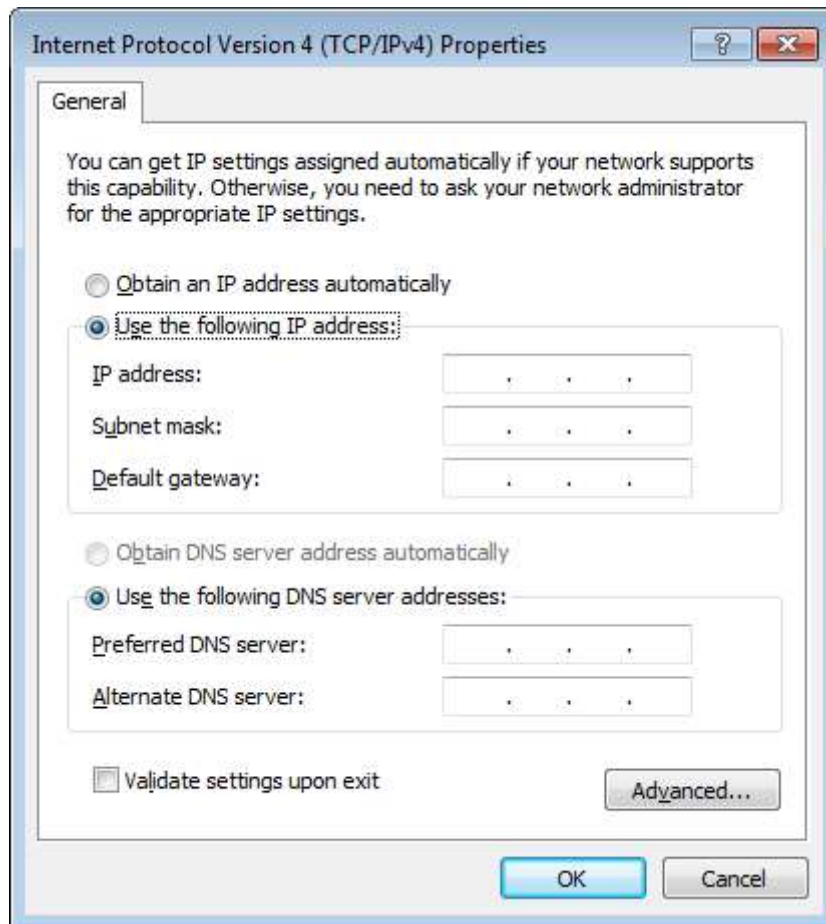
Connect the Ethernet interface of the computer to the **WAN** interface of the base station through the Ethernet cable.

3.3 Set Up Client Computer

Before logging into the Web client, the client computer's IP address needs to be set up first so that the connection between the client and the server is possible. Take Windows 7 as an example:

1. Click "**Start>Control Panel**" and later "**Network and Internet**" in the window that pops up.
2. Click "**View network status and tasks**" and later "**Local Connectivity**" in the window that pops up.
3. In "**Status of Local Connectivity**", click "**Properties**" to see the "**Properties of Local Connectivity**" pop-up window.
4. Select "**Internet Protocol Version (TCP/IPv4)**" and click "**Properties**" to see the pop-up window as Figure 3-.

Figure 3-1 Internet Protocol Version (TCP/IPV4)



Select either **“Obtain an IP address automatically”** or **“Use the following IP address”**:

- If **“Obtain an IP address automatically”** selected, go directly to step 7
- If **“Use the following IP address”** selected, follow step 5 ~ step 7

NOTE: In general, if the auto obtaining fails, one needs to set up the IP address manually.

5. Select **“Use the following IP address”**.
6. Input IP address, subnet mask, and default gateway, and then click **“OK”**.
 - IP address: 192.168.150. XXX: (recommended XXX: 100~254)
Because the LAN interface of the base station uses the IP address of 192.168.150.1, others should avoid using this address.
 - Subnet mask: 255.255.255.0
 - Default gateway: 192.168.150.1
7. In the command window, execute ping 192.168.150.1 and check whether the connection between the client computer and the server works or not.

3.4 Log In

1. Open a web browser, and enter <http://192.168.150.1>, as shown in Figure 3-1.

Figure 3-1 GUI Login

2. Input user name, password, and click **“Login”**. The homepage is given in Figure 3-2.

Default user/password : admin/admin

Figure 3-2 GUI Homepage

Product Name:	LTE-ROUTER	Software Version:	BaiCE_LT_1.0.22
Product Model:	EG550A-M11	Software Build Time:	20220706-185246
Hardware Version:	ver.A	SN:	1203000153224GB0001
Module Name:	GCT-model	Module Version:	BaiCE_BG_1.9.0.1-DBG
CloudKey:	-	TK Version:	0.3.4.1
System Up Time:	7 days, 18:35:47	NickName:	-

USIM Status:	available	IMSI:	460680003200058
LTE Mode:	TDD-LTE	IMEI:	867945040833293
PLMN:	-	Bandwidth:	- M
Cell ID:	-	RSRQ:	-
eNB ID:	NaN	Earfcn:	-
PCI:	-	Roam:	2
DL Frequency:	-	UL Frequency:	-
CINR1:	-	CINR2:	-

NOTE: The information may vary by product type or software version.

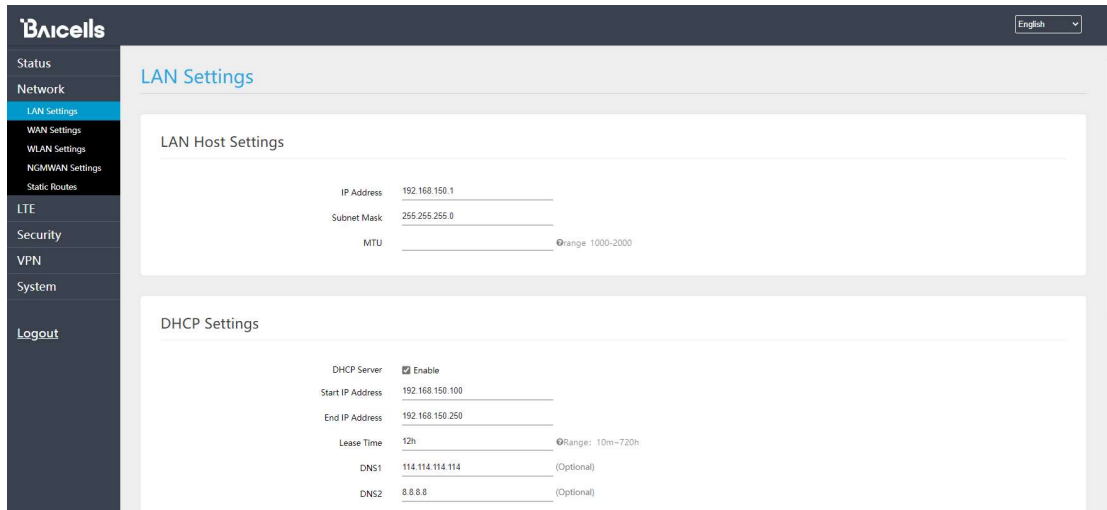
The front page shows the information as the basic information and status information of the LteTurbo CPE. The status information is dynamically refreshed, refreshed every 3 seconds.

On the left side of the home page is the navigation pane, showing the information as Status-> Overview. On the top of home page, showing the Basic information.

The status information area displays the WLAN connection status, rate statistics, LAN port connection status, and a list of connection devices.

4. Network Setting

4.1 LAN Settings



The screenshot shows the 'LAN Settings' page in the Baicells web interface. The left sidebar contains a navigation menu with options: Status, Network, LAN Settings (highlighted), WAN Settings, WLAN Settings, NGMWWAN Settings, Static Routes, LTE, Security, VPN, System, and Logout. The main content area is titled 'LAN Settings' and contains two sections: 'LAN Host Settings' and 'DHCP Settings'.

LAN Host Settings

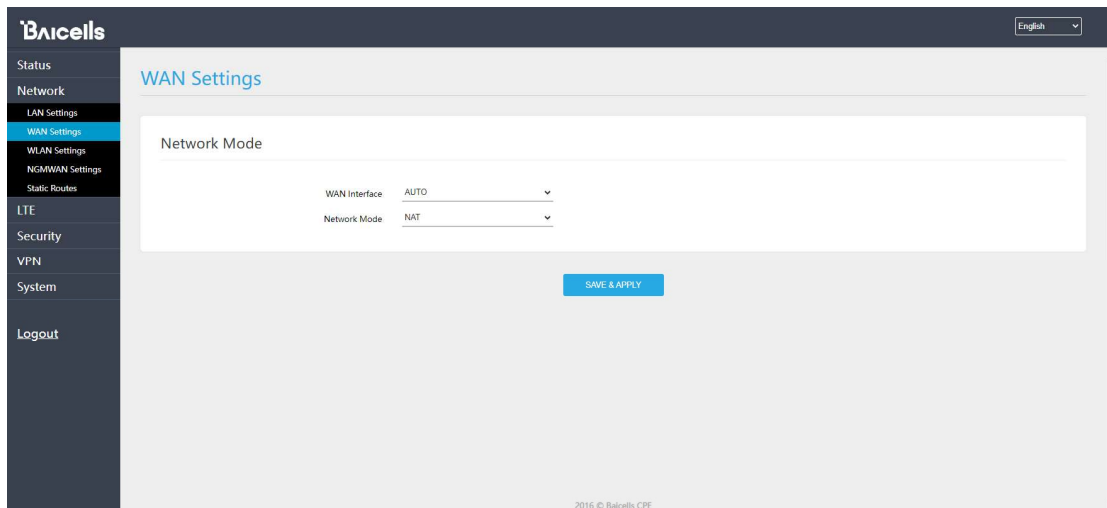
IP Address	192.168.150.1
Subnet Mask	255.255.255.0
MTU	(Range: 1000-2000)

DHCP Settings

DHCP Server	☒ Enable
Start IP Address	192.168.150.100
End IP Address	192.168.150.250
Lease Time	12h (Range: 10m-720h)
DNS1	114.114.114.114 (Optional)
DNS2	8.8.8.8 (Optional)

Config Lan IP and DHCP params

4.2 WAN Settings



The screenshot shows the 'WAN Settings' page in the Baicells web interface. The left sidebar is the same as in the LAN Settings page. The main content area is titled 'WAN Settings' and contains a section titled 'Network Mode'.

Network Mode

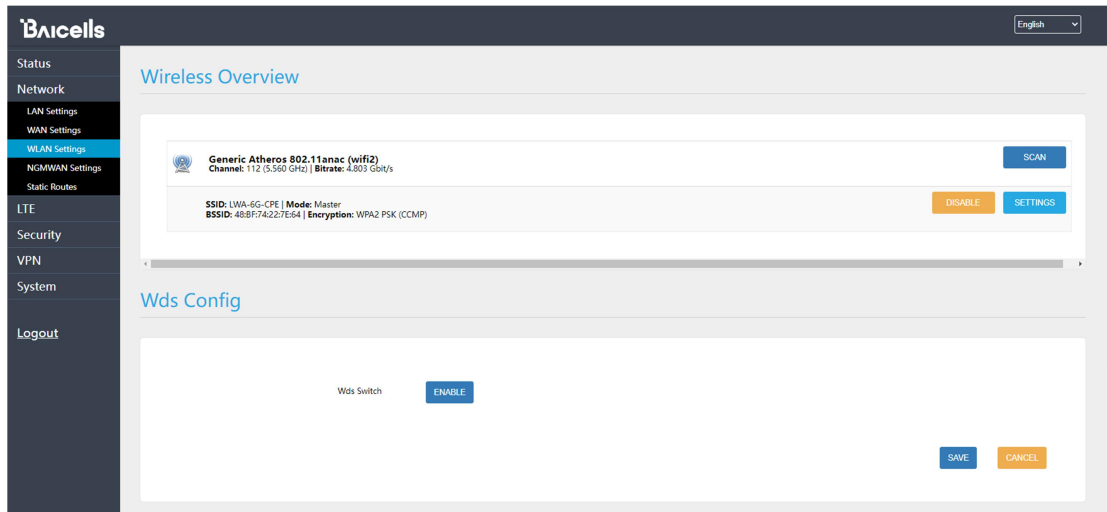
WAN Interface	AUTO
Network Mode	NAT

At the bottom of the form, there is a blue button labeled 'SAVE & APPLY'.

Wan Interface : support AUTO, LTE, WIFI, and ngmwan

Network Mode : support NAT and L2

4.3 WLAN Settings



Wireless Overview

Generic Atheros 802.11n ac (wifi2)
Channel: 112 (5.560 GHz) | Bitrate: 4.803 Gbit/s

SSID: LWA-6G-CPE | Mode: Master
BSSID: 48:BF:74:22:7E:64 | Encryption: WPA2 PSK (CCMP)

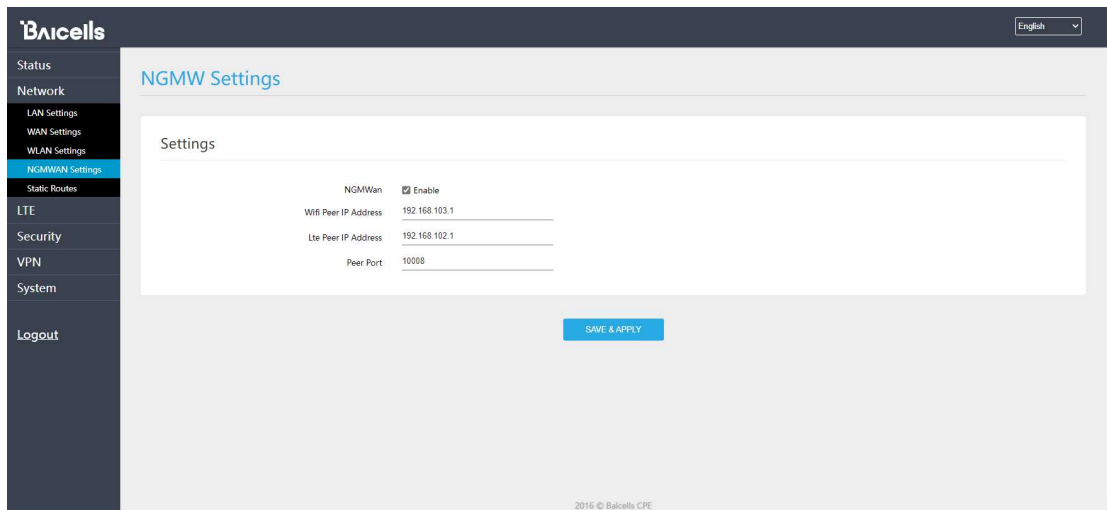
Wds Config

Wds Switch ☒ ENABLE

SAVE CANCEL

Config wireless params, and wds switch.

4.4 NGMWAN Settings



NGMW Settings

Settings

NGMWan ☒ Enable

Wifi Peer IP Address 192.168.103.1

Lte Peer IP Address 192.168.102.1

Peer Port 10008

SAVE & APPLY

2016 © BaiCells CPE

Config ngmwan params

4.5 Static Routes

Bicells

English

Status

Network

LAN Settings

WAN Settings

WLAN Settings

NGMWAN Settings

Static Routes

LTE

Security

VPN

System

Logout

Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Target	IPv4 Netmask	Interface	IPv4 Gateway	Metric
Host IP or Network	If target is a network			
This section contains no values yet				

ADD

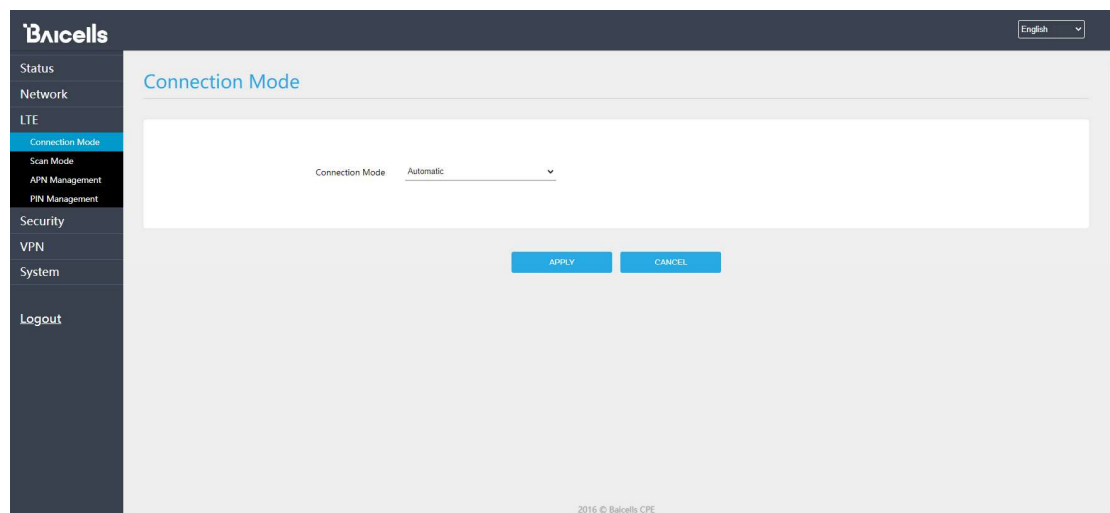
Static IPv6 Routes

Target	Interface	IPv6 Gateway	Metric
IPv6 Address or Network (CIDR)			
This section contains no values yet			

ADD

5. LTE Setting

5.1 Connection Mode

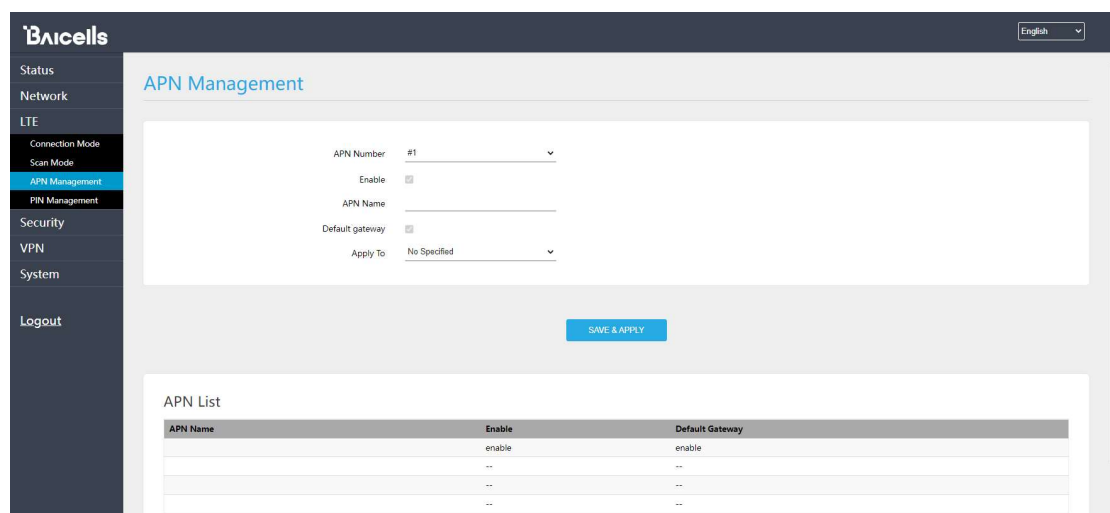


Support AUTO, Manual mode

5.2 Scan Mode

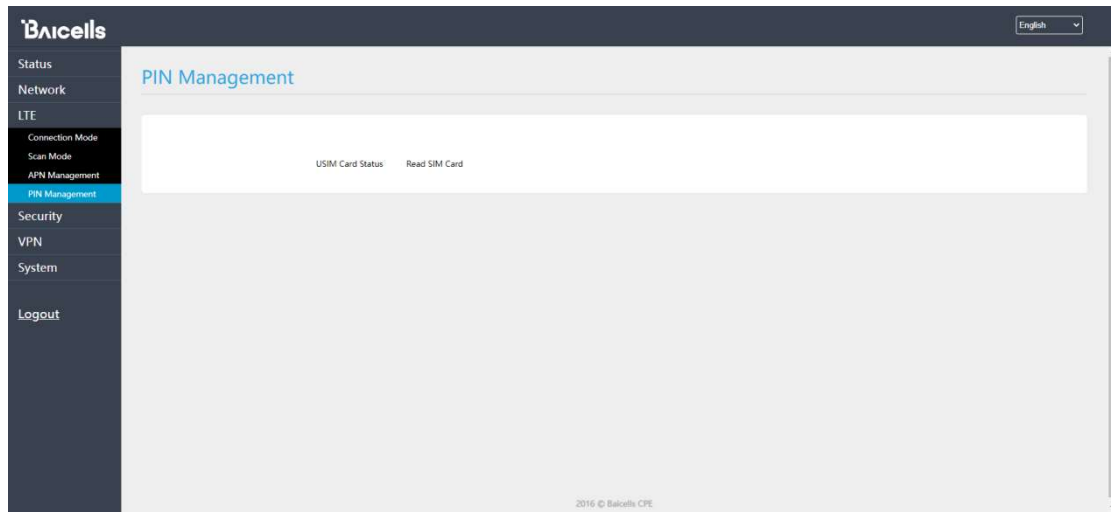
Support full band, fix pci, fix channel for lte scan.

5.3 APN Management



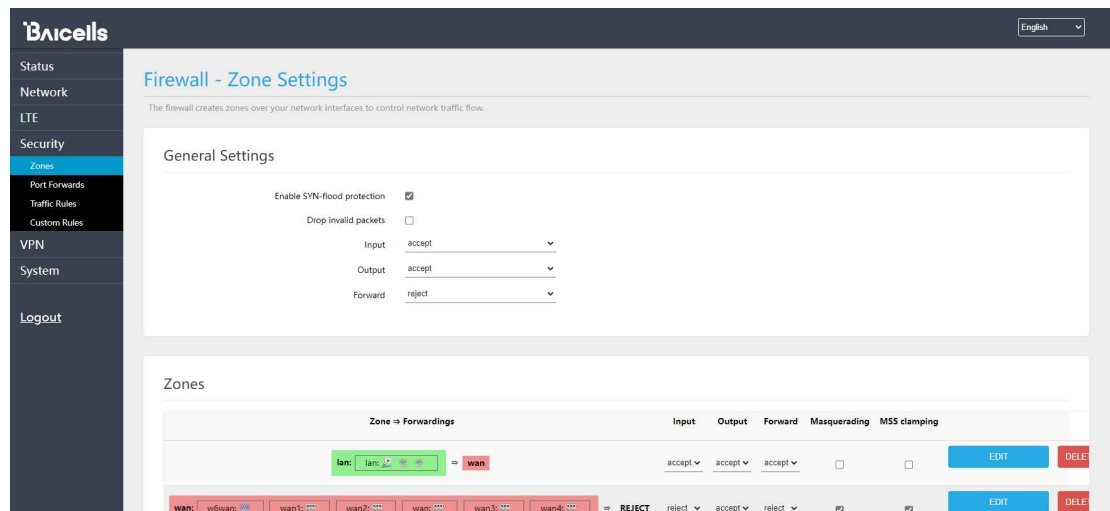
APN Name	Enable	Default Gateway
	enable	enable
	--	--
	--	--
	--	--

5.4 PIN Management



6. Security Setting

6.1 Zones



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

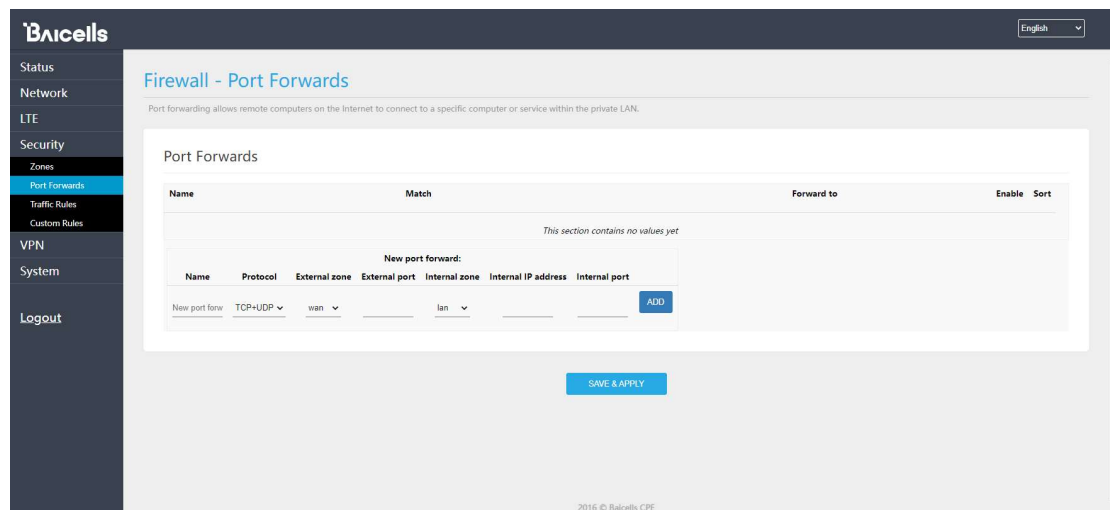
General Settings

- Enable SYN-flood protection: ☒
- Drop invalid packets: ☐
- Input: accept
- Output: accept
- Forward: reject

Zones

Zone	Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan	lan	accept	accept	accept	☐	☐	EDIT DELETE
wan	wan	reject	reject	reject	☒	☒	EDIT DELETE

6.2 Port Forwards



Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
This section contains no values yet				

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
New port forw	TCP+UDP	wan		lan		

ADD

SAVE & APPLY

2016 © Baicells CPE

6.3 Traffic Rules

The screenshot shows the Balcells web interface with the 'Traffic Rules' section selected in the left sidebar. The main content area displays the configuration for a rule named 'Accept forward'. The rule is active (checkbox checked) and has a blue 'EDIT' button and a red 'DELETE' button. The rule details are as follows:

- Open ports on router:** A table with columns 'Name', 'Protocol', and 'External port'. It shows a rule for 'New input rule' with protocol 'TCP+UDP' and an 'ADD' button.
- New forward rule:** A table with columns 'Name', 'Source zone', and 'Destination zone'. It shows a rule for 'New forward rule' with source zone 'lan' and destination zone 'wan', and an 'ADD AND EDIT...' button.

Below the rule configuration, there is a section for 'Source NAT' with a description: 'Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.' It includes a table with columns 'Name', 'Match', 'Action', 'Enable', and 'Sort', and a note 'This section contains no values yet'. At the bottom of this section is a 'New source NAT' form with fields for 'Name', 'Source zone', 'Destination zone', 'To source IP', and 'To source port', and an 'ADD AND EDIT...' button.

6.4 Custom Rules

The screenshot shows the Balcells web interface with the 'Custom Rules' section selected in the left sidebar. The main content area displays the 'Firewall - Custom Rules' configuration page. It includes a description: 'Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.' Below this is a large text area for entering custom rules, containing the following text:

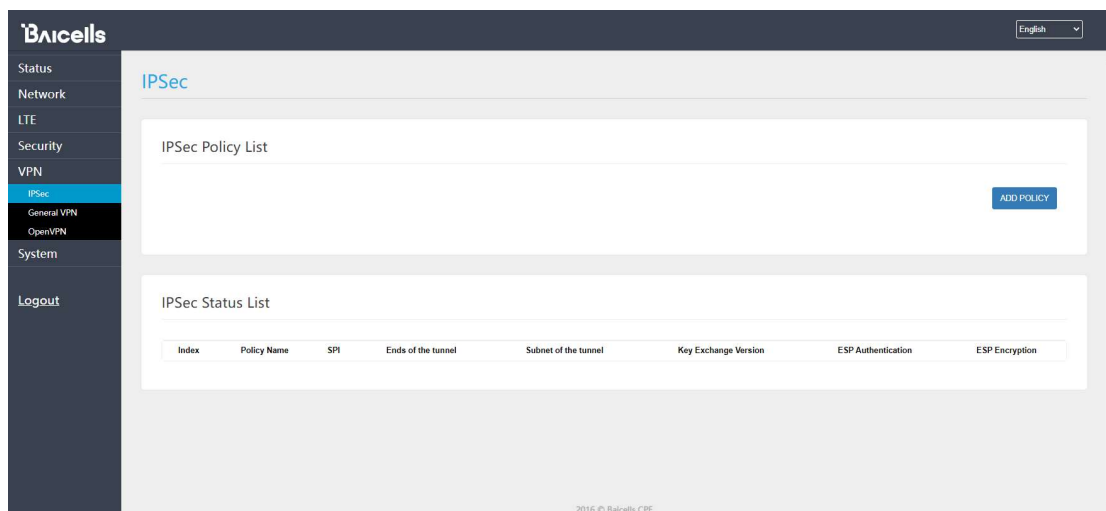
```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postouting_lan_rule.
```

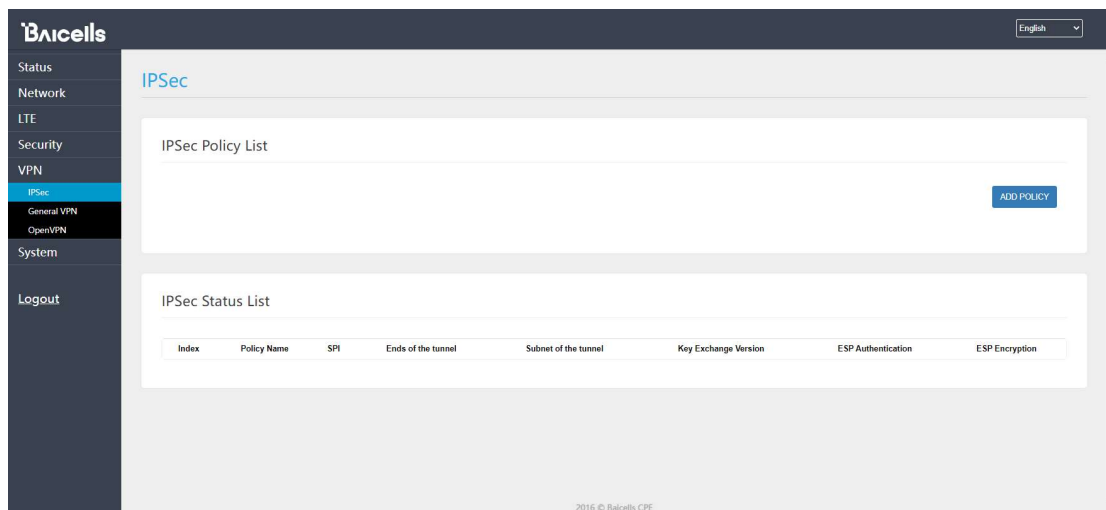
At the bottom of the page, there are 'SUBMIT' and 'RESET' buttons. The footer of the page indicates '2016 © Balcells CPE'.

7.VPN Setting

7.1 IPSec



7.2 General VPN



7.3 OpenVPN

Baicells

English

Status

Network

LTE

Security

VPN

IPSec

General VPN

OpenVPN

System

Logout

General VPN

Settings

VPN

☐ Enable

Protocol

L2TP

Mode

V2

Default GW

☐ Enable

Server IP

User Name

Password

IPSec Encryption

disable

Pre-Shared Key

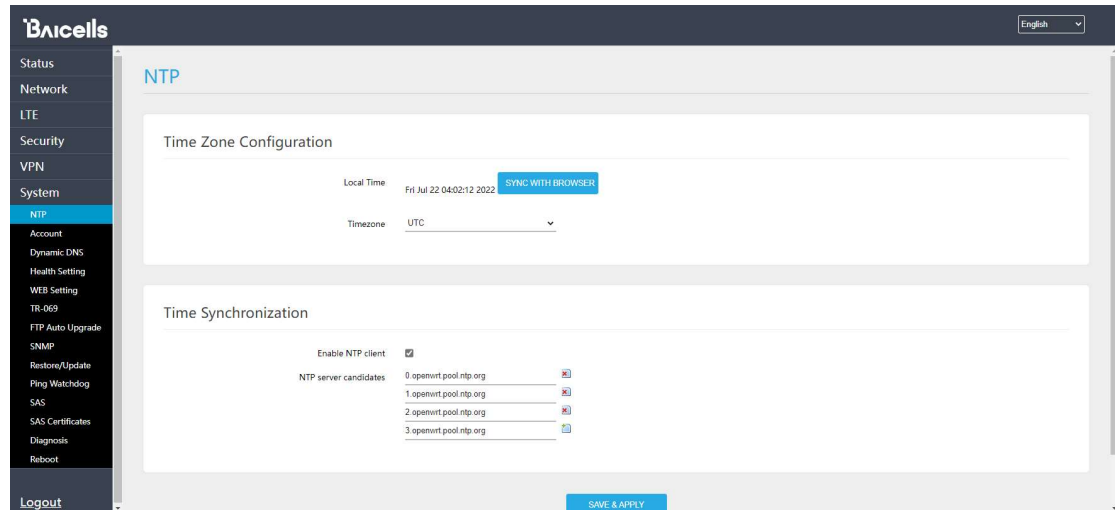
01 to 128 characters

Status

User Name	Local Address	Remote Address	Status
	0.0.0.0	0.0.0.0	Disconnected

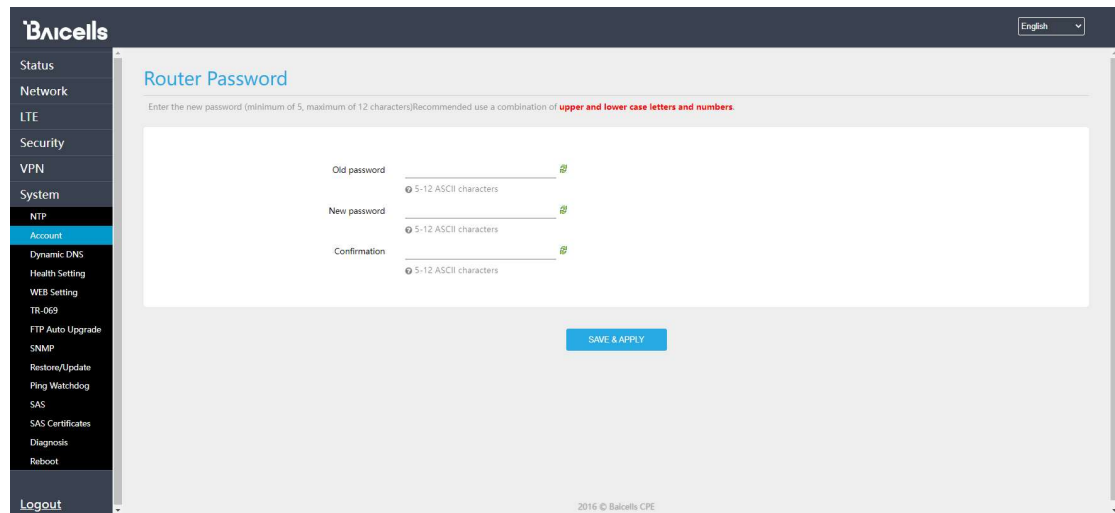
8. System

8.1 NTP



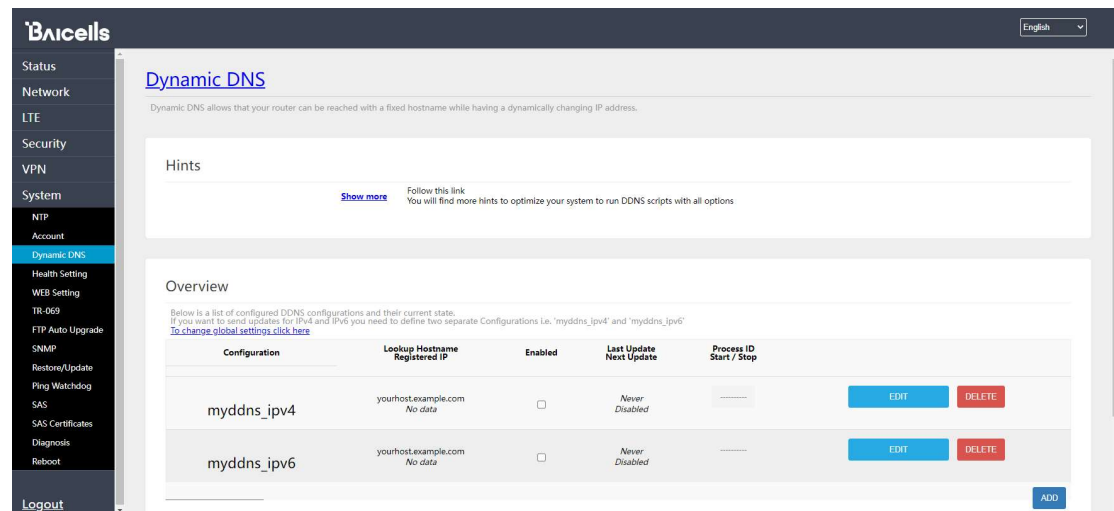
The screenshot shows the NTP configuration page in the Baicells web interface. The left sidebar contains a menu with options: Status, Network, LTE, Security, VPN, System, NTP (selected), Account, Dynamic DNS, Health Setting, WEB Setting, TR-069, FTP Auto Upgrade, SNMP, Restore/Update, Ping Watchdog, SAS, SAS Certificates, Diagnosis, Reboot, and Logout. The main content area is titled 'NTP' and contains two sections: 'Time Zone Configuration' and 'Time Synchronization'. In the 'Time Zone Configuration' section, the 'Local Time' is 'Fri Jul 22 04:02:12 2022' and the 'Timezone' is 'UTC'. There is a 'SYNC WITH BROWSER' button. In the 'Time Synchronization' section, the 'Enable NTP client' checkbox is checked. Below it, there are four 'NTP server candidates' listed as '0 opentv.pool.ntp.org', '1 opentv.pool.ntp.org', '2 opentv.pool.ntp.org', and '3 opentv.pool.ntp.org'. Each candidate has a small 'X' icon to its right. At the bottom right of the main content area is a 'SAVE & APPLY' button.

8.2 Account



The screenshot shows the 'Router Password' page in the Baicells web interface. The left sidebar is the same as in the previous screenshot, with 'Account' selected. The main content area is titled 'Router Password' and contains a form for changing the password. The form has three input fields: 'Old password', 'New password', and 'Confirmation'. Each field has a strength indicator (a green bar) and a note '5-12 ASCII characters'. Above the form, there is a instruction: 'Enter the new password (minimum of 5, maximum of 12 characters/Recommended use a combination of upper and lower case letters and numbers.' At the bottom right of the main content area is a 'SAVE & APPLY' button. The footer of the page shows '2016 © Baicells CPE'.

8.3 Dynamic DNS



Balcells English

Status
Network
LTE
Security
VPN
System
NTP
Account
Dynamic DNS
Health Setting
WEB Setting
TR-069
FTP Auto Upgrade
SNMP
Restore/Update
Ping Watchdog
SAS
SAS Certificates
Diagnosis
Reboot
Logout

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Hints

[Show more](#) Follow this link
You will find more hints to optimize your system to run DDNS scripts with all options

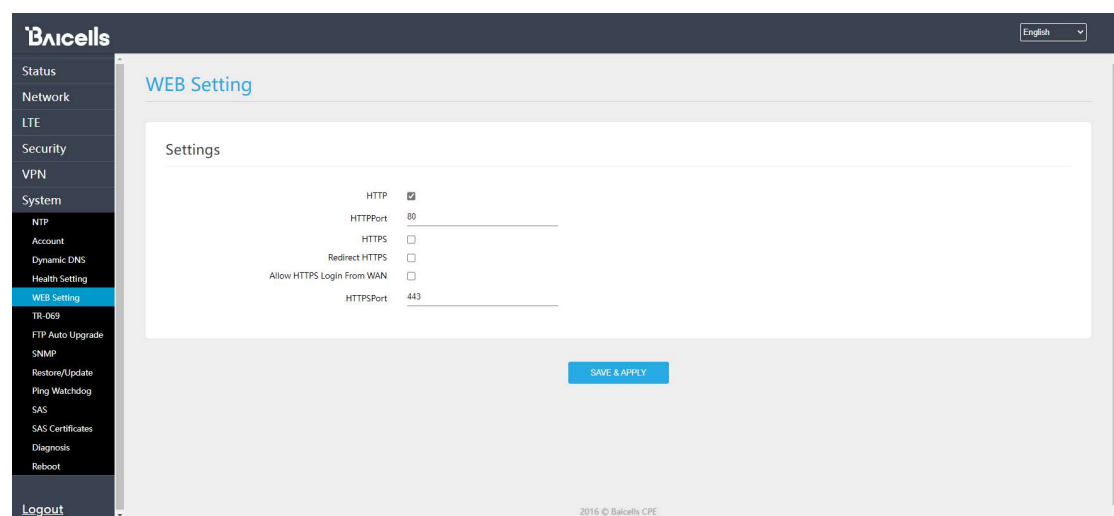
Overview

Below is a list of configured DDNS configurations and their current state.
If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'
[To change global settings click here](#)

Configuration	Lookup Hostname Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
myddns_ipv4	yourhost.example.com No data	☐	Never Disabled	---	EDIT DELETE
myddns_ipv6	yourhost.example.com No data	☐	Never Disabled	---	EDIT DELETE

[ADD](#)

8.4 WEB Setting



Balcells English

Status
Network
LTE
Security
VPN
System
NTP
Account
Dynamic DNS
Health Setting
WEB Setting
TR-069
FTP Auto Upgrade
SNMP
Restore/Update
Ping Watchdog
SAS
SAS Certificates
Diagnosis
Reboot
Logout

WEB Setting

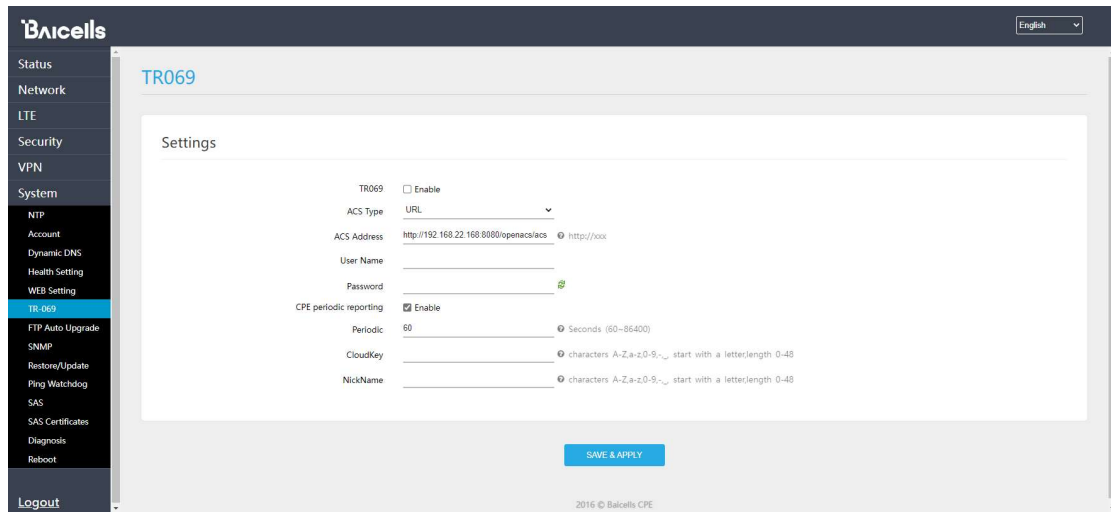
Settings

HTTP ☒
 HTTPPort 80
 HTTPS ☐
 Redirect HTTPS ☐
 Allow HTTPS Login From WAN ☐
 HTTPSPort 443

[SAVE & APPLY](#)

2016 © Balcells CPE

8.5 TR069



TR069

Settings

TR069 ☐ Enable

ACS Type

ACS Address

User Name

Password

CPE periodic reporting ☒ Enable

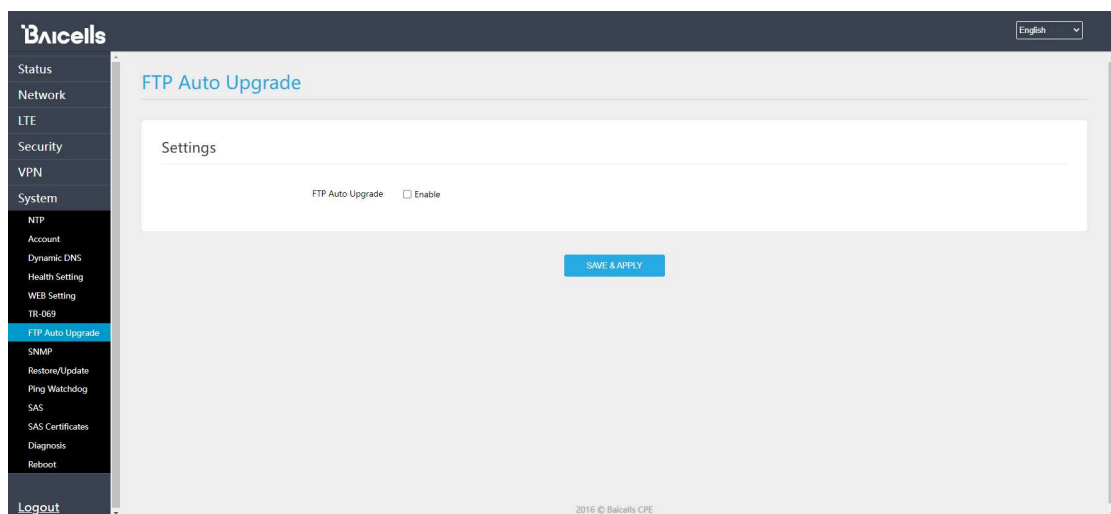
Periodic

CloudKey

NickName

2016 © Balcells CPE

8.6 FTP Auto Upgrade



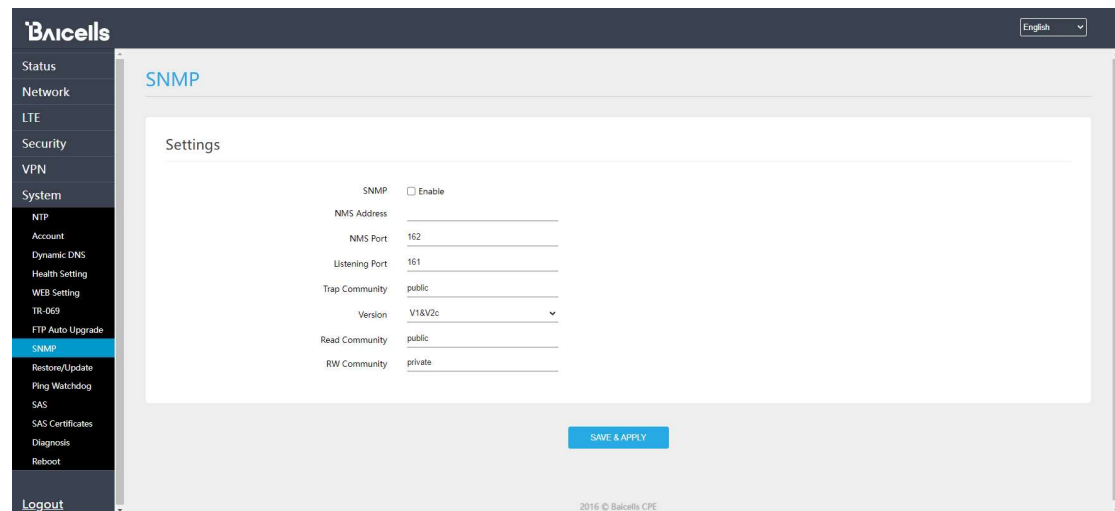
FTP Auto Upgrade

Settings

FTP Auto Upgrade ☐ Enable

2016 © Balcells CPE

8.7 SNMP

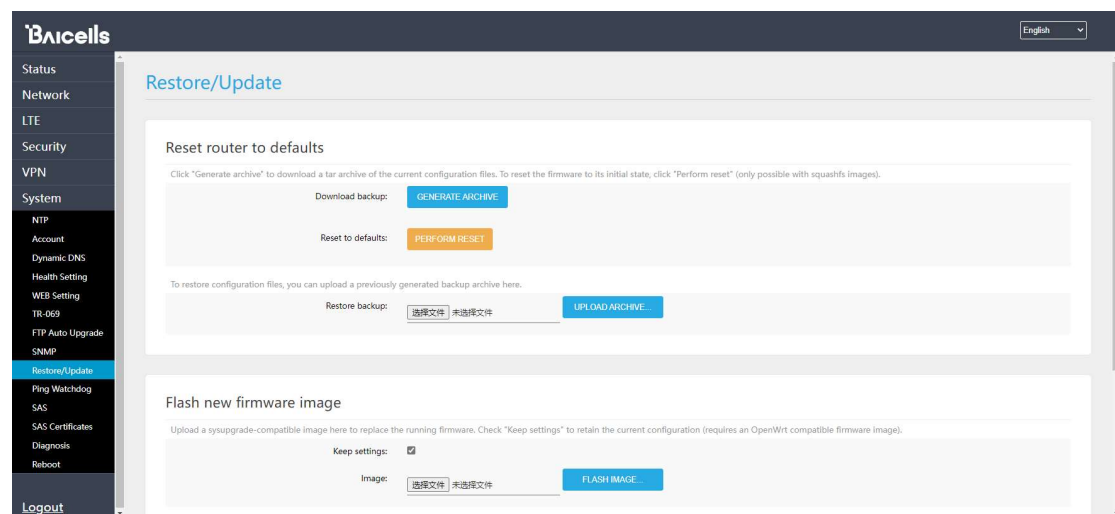


The screenshot shows the Baicells web interface for the SNMP settings page. The left sidebar contains a menu with options: Status, Network, LTE, Security, VPN, System, NTP, Account, Dynamic DNS, Health Setting, WEB Setting, TR-069, FTP Auto Upgrade, **SNMP**, Restore/Update, Ping Watchdog, SAS, SAS Certificates, Diagnosis, Reboot, and Logout. The main content area is titled "SNMP" and contains a "Settings" section. The settings are as follows:

Setting	Value
SNMP	☐ Enable
NMS Address	
NMS Port	162
Listening Port	161
Trap Community	public
Version	V1&V2c
Read Community	public
RW Community	private

At the bottom right of the settings section is a "SAVE & APPLY" button. The footer of the page indicates "2016 © Baicells CPE".

8.8 Restore/Update



The screenshot shows the Baicells web interface for the Restore/Update page. The left sidebar is identical to the previous page, with the "Restore/Update" option highlighted. The main content area is titled "Restore/Update" and contains two sections:

Reset router to defaults

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: [GENERATE ARCHIVE](#)

Reset to defaults: [PERFORM RESET](#)

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: [选择文件](#) [未选择文件](#) [UPLOAD ARCHIVE...](#)

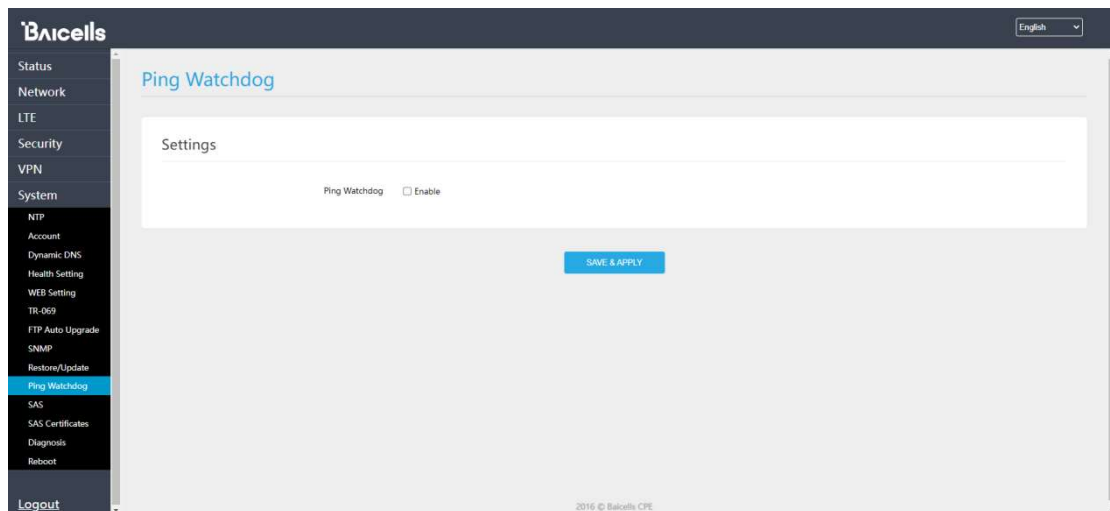
Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

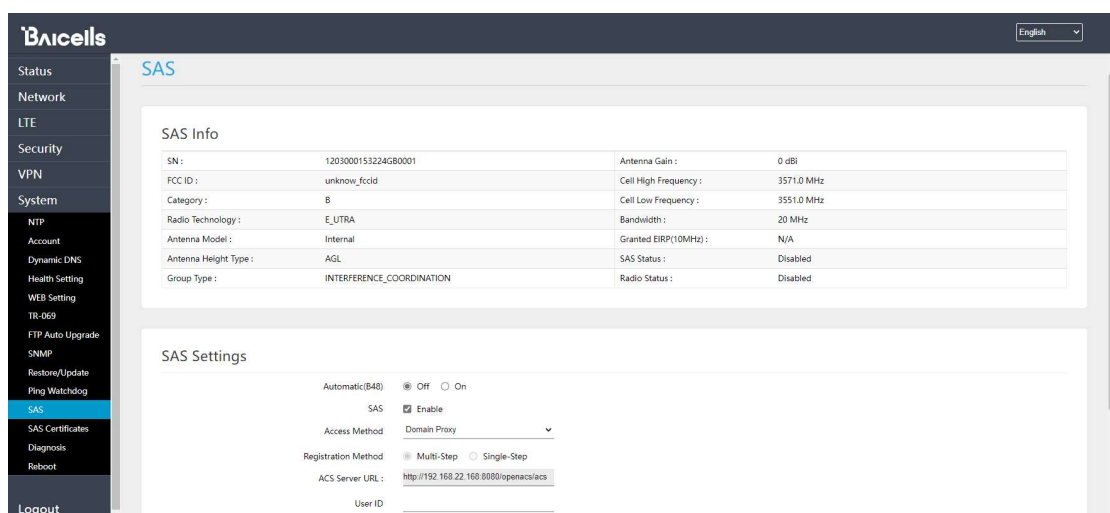
Keep settings: ☒

Image: [选择文件](#) [未选择文件](#) [FLASH IMAGE...](#)

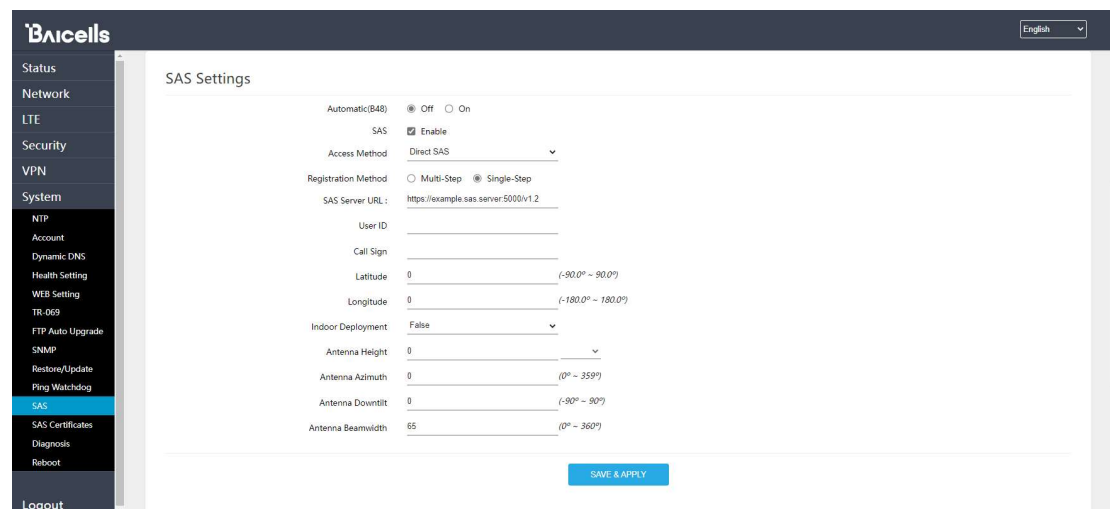
8.9 Ping Watchdog



8.10 SAS



8.11 SAS Setting



SAS Settings

Automatic(B48) ☒ Off ☐ On

SAS ☒ Enable

Access Method Direct SAS

Registration Method ☐ Multi-Step ☒ Single-Step

SAS Server URL: https://example.sas.server:5000/v1.2

User ID

Call Sign

Latitude 0 (-90.0° ~ 90.0°)

Longitude 0 (-180.0° ~ 180.0°)

Indoor Deployment False

Antenna Height 0

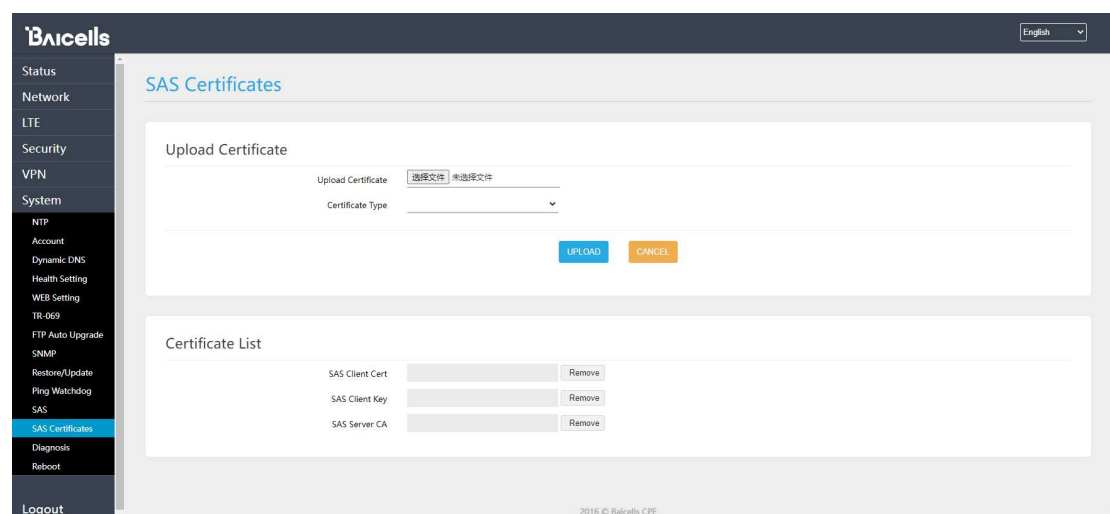
Antenna Azimuth 0 (0° ~ 359°)

Antenna Downtilt 0 (-90° ~ 90°)

Antenna Beamwidth 65 (0° ~ 360°)

SAVE & APPLY

8.12 SAS Certificates



SAS Certificates

Upload Certificate

Upload Certificate 选择文件 未选择文件

Certificate Type

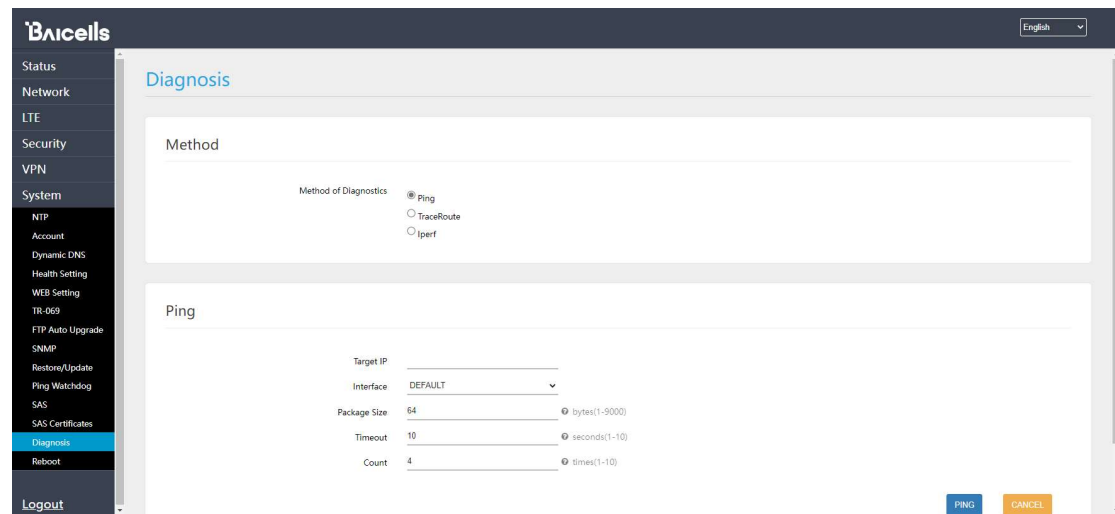
UPLOAD CANCEL

Certificate List

SAS Client Cert	Remove
SAS Client Key	Remove
SAS Server CA	Remove

2016 © BaiCells CPE

8.13 Diagnosis

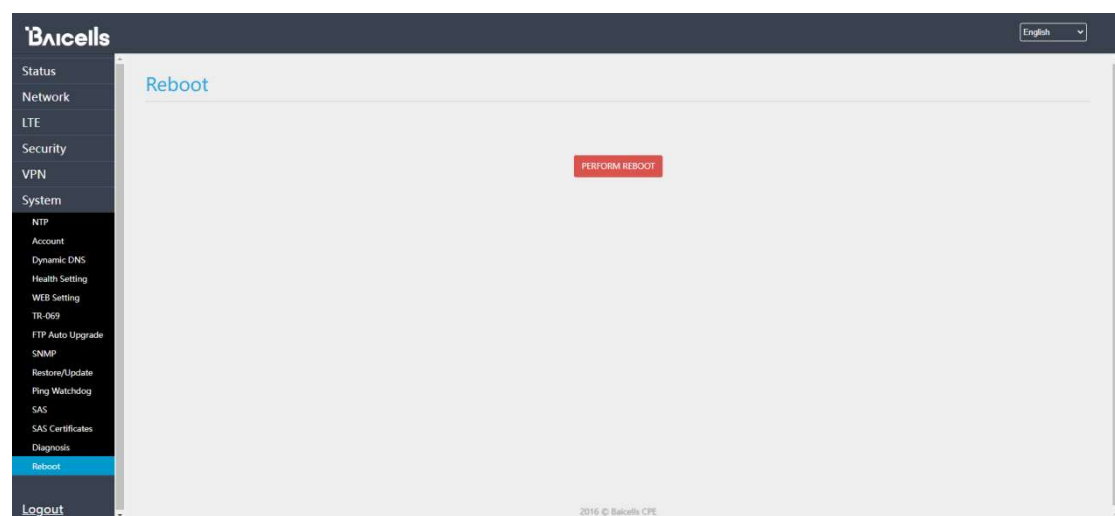


The screenshot shows the 'Diagnosis' page in the Baiocells web interface. The left sidebar contains a menu with 'Diagnosis' highlighted. The main content area has a 'Method' section with three radio buttons: 'Ping' (selected), 'TraceRoute', and 'Iperf'. Below this is a 'Ping' section with the following settings:

Target IP	
Interface	DEFAULT
Package Size	64 bytes(1-9000)
Timeout	10 seconds(1-10)
Count	4 times(1-10)

At the bottom right of the 'Ping' section are two buttons: 'PING' (blue) and 'CANCEL' (orange).

8.14 Reboot



The screenshot shows the 'Reboot' page in the Baiocells web interface. The left sidebar contains a menu with 'Reboot' highlighted. The main content area is mostly empty, with a single red button labeled 'PERFORM REBOOT' centered in the middle. At the bottom of the page, there is a small copyright notice: '2016 © Baiocells CPE'.

9. 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 50cm between the radiator & your body.