CPE Configuration Guide

CAT4: BaiCE_AP_2.4.7_NA
CAT6/7/15: BaiCE_BG_1.6.20

December 2021

Version 1.07

About This Document

This document describes the Baicells indoor and outdoor CAT4 and CAT6/7/15 Customer Premise Equipment (CPE) GUIs, and explains how to configure the various features and functions that are available. The primary audiences for this document are equipment installers, network administrators, and support technicians.

NOTE: Installation procedures can be found in the CPE user manuals on the website Baicells.com > Resources > *Documents*.

This publication of the document is written to the following software versions:

- **CAT4:** BaiCE_AP_2.4.7_NA
- **CAT6/7/15**: BaiCE_BG_1.6.20

Terms used in this document or related to LTE are listed in alphabetical order and described in *Acronyms and Abbreviations*, which can be found at Baicells.com > Resources > *Documents*.

New in This Release

The following updates have been provided in this release:

- Updated the Spectrum Access System (SAS) information in *section 9.15.2*.

Copyright Notice

Disclaimer

All products, services, and features bought from Baicells Technologies, Inc., are subject to the constraints of the company's business contract and terms. All or part of the products, services, or features described in this document might not be your specific Baicells network. Unless stated in the contract, Baicells Technologies, Inc., does not make any explicit or default statement or guarantee about the contents of this document.

Unless stated otherwise, this document serves only as a user guide, and all descriptions / information / suggestions mean no guarantee, neither explicit nor implicit.

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. Refer to the *Contact Us* section.

Revision Record

Date	Version	Description	SMEs/Contributors	Author/Editor
22-Dec-2021	V1.07	Updated SAS procedures.	Anna Ch	Kathy Clark
9-Dec-2021	V1.06	Updated for BaiCE_BG_1.6.20 and added CAT15 data	Anna Ch, Seng Tang, Blake Volk	Kathy Clark
18-Dec-2020	V1.05	Updated for BaiCE_AP_2.4.7_NA and BaiCE_BG_1.6.5.3	Jesse Raasch	Jocelyn Watson
19-Oct-2020	V1.04	Updated for BaiCE_AP_2.4.5 and BaiCE_BG_1.6.4	Nitisha Potti, Jesse Raasch	Jocelyn Watson
8-Oct-2020	V1.03	Incorporated SME review comments	Nitisha Potti	Sharon Redfoot
28-Sep-2020	V1.02 V1.01	Created separate manual from previous Configuration & Network Administration Guide section 3. Integrated and updated content for v2.4.4 (CAT4) and v1.6.1 (CAT6/7).	TangHoucheng, WangYong, Nitisha Potti, Sonny May, Pengyu Chen	Sharon Redfoot

Support Resources

- **Documentation** - Baicells product datasheets and technical manuals can be found at Baicells.com > Resources > *Documents*.
- **Support** - Open a support ticket, process an RMA, and the Support Forum are at Baicells.com > *Support*.

Contact Us

Baicells Technologies Co., Ltd. China	Baicells Technologies North America, Inc. North America
Address: 3F, Bldg. A, No. 1 Kai Tuo Rd, Haidian Dist, Beijing, China	Address: 5700 Tennyson Pkwy, #300, Plano, TX 75024, USA
Phone: +86-10-62607100	Phone: +1-888-502-5585
E-mail: *contact@Baicells.com*	Email: *sales_na@Baicells.com* or *support_na@Baicells.com*
Website: *www.Baicells.com*	Website: *https://na.Baicells.com*

Table of Contents

List of Figures

List of Tables

1 Introduction

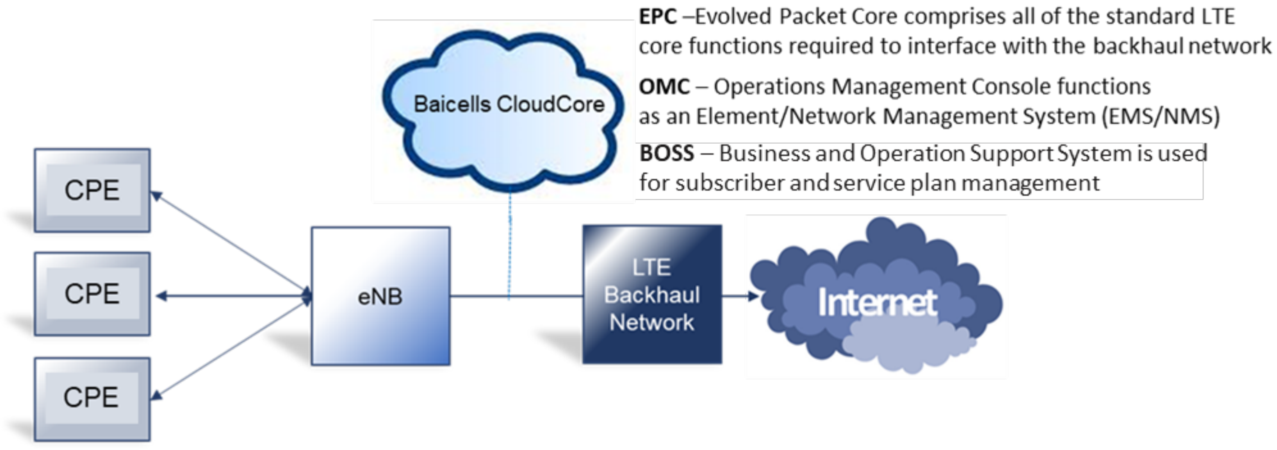
The indoor (ID) and outdoor (OD) Customer Premise Equipment (CPE), also referred to as User Equipment (UE), is part of the Baicells broadband wireless access system (Figure 1-1). This system integrates with Long-Term Evolution (LTE) backhaul networks to provide subscribers with Internet access. The CPE, typically in or at a home or office, communicates with the operator's eNodeBs (eNBs), also called base stations, at cell sites located in the region.

The eNBs communicate with the LTE Evolved Packet Core (EPC) functions to handle traffic between CPEs and the backhaul network. The Baicells EPC is part of a cloud solution called CloudCore. Baicells owns and manages the CloudCore EPC. Operators have the option to host their own instance of the EPC in their private network.

CloudCore also provides two applications to which each Baicells operator is given an account:

- Operations Management Console (OMC) for network element management
- Business and Operation Support System (BOSS) for subscriber and service plan management

Figure 1-1: Network Architecture



EPC –Evolved Packet Core comprises all of the standard LTE core functions required to interface with the backhaul network

OMC – Operations Management Console functions as an Element/Network Management System (EMS/NMS)

BOSS – Business and Operation Support System is used for subscriber and service plan management

Though many subscribers can get good Internet service using an indoor CPE, others who are in more remote or heavily dense locations may require an outdoor CPE for clearer line-of-sight to a nearby eNB. Generally speaking, the indoor CPE has the lowest antenna gain of the Baicells models, and the outdoor high-gain CPE has the highest antenna gain. Specifications for each CPE model can be found on the website Baicells.com > Resources > *Documents*.

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 6/7/15 (CAT6/7/15). Typically the difference from one release/category to the next is in capacity, i.e., higher throughput.

The CAT4 and CAT6/7/15 GUIs have some variations, as those products were released at separate times. This document covers both indoor and outdoor and both CAT4 and CAT6/7/15 CPE configuration options.

2 Launching the CPE GUI

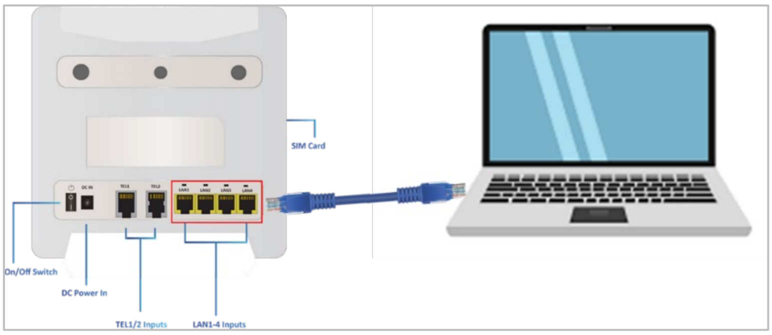
The minimum computer requirements for accessing the CPE GUI are listed in Table 2-1.

Table 2-1: Computer Requirements

Item	Description
CPU	Pentium 500 MHz or higher
Memory	128 MB RAM or higher
Hard Disk	50 MB available space
Operating System	Microsoft: Windows XP, Windows Vista, or Windows 7 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

The CPE comes preloaded with a GUI to configure the device. The GUI can be accessed through a physical cable connection or through remote Web access. The local connection is typically used during installation, when the installer connects an Ethernet cable between the CPE LAN port and a computer LAN port (example in Figure 2-1). Post-installation, the CPE can be accessed remotely if the WEB Setting is enabled (*section 9.4*).

Figure 2-1: Local Connection to CPE (Example)



Follow the steps below to access the GUI and log in.

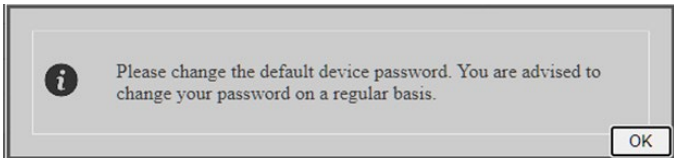
1. Install the CPE as instructed in the user manual for your CPE model. The user manual instructions include how to access the GUI and enter basic configuration settings, including remote access. If you do not have the user manual, please go to Baicells.com > Resources > *Documents* to download a copy.
2. Open a Web browser, and enter http://192.168.150.1.

NOTE 1: Older CPEs referred to as "Gen 1" or "G1" use http://192.168.254.1.

NOTE 2: Gen 1 CAT4 CPEs are now EOL.

3. The first time you log in you may be prompted to change your password to protect your CPE from unauthorized access (Figure 2-2).

Figure 2-2: First Login - Change Password

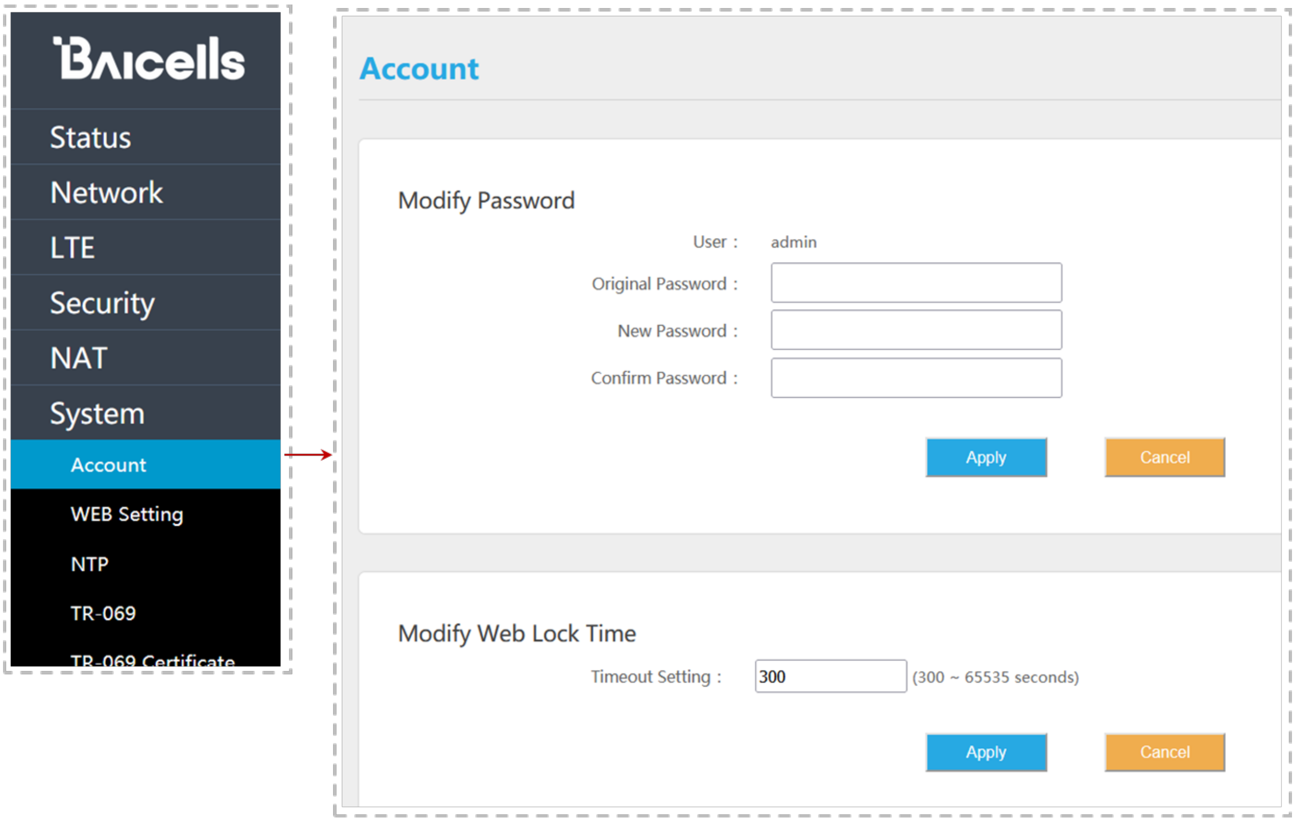


Please change the default device password. You are advised to change your password on a regular basis.

When you click on *OK*, you will be taken to the *System > Account* window (Figure 2-3). Change the password using five to 16 ASCII characters (letters, numbers, and special characters). Baicells recommends using a mix of upper and lower case letters plus numbers. Click on *Apply*.

While in the *System > Account* window you can also change the length of time of inactivity before the system logs you out. In the *Modify Web Lock Time* pane, the default time is set to 300 seconds (five minutes). You can increase the timeout setting up to 65535 seconds (~18 hrs).

Figure 2-3: Change Password

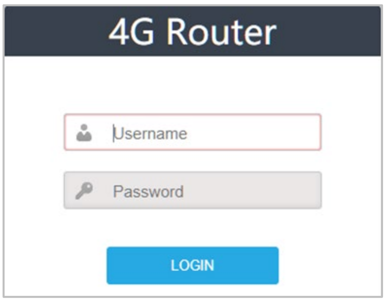


User : admin

Timeout Setting : 300 (300 ~ 65535 seconds)

4. At the 4G Router (CPE) login window (Figure 2-4), enter the default user name (**admin**) and your password. If you were not prompted to change the password upon initial login, enter the default password (**admin**). Click on *LOGIN*.

Figure 2-4: Login

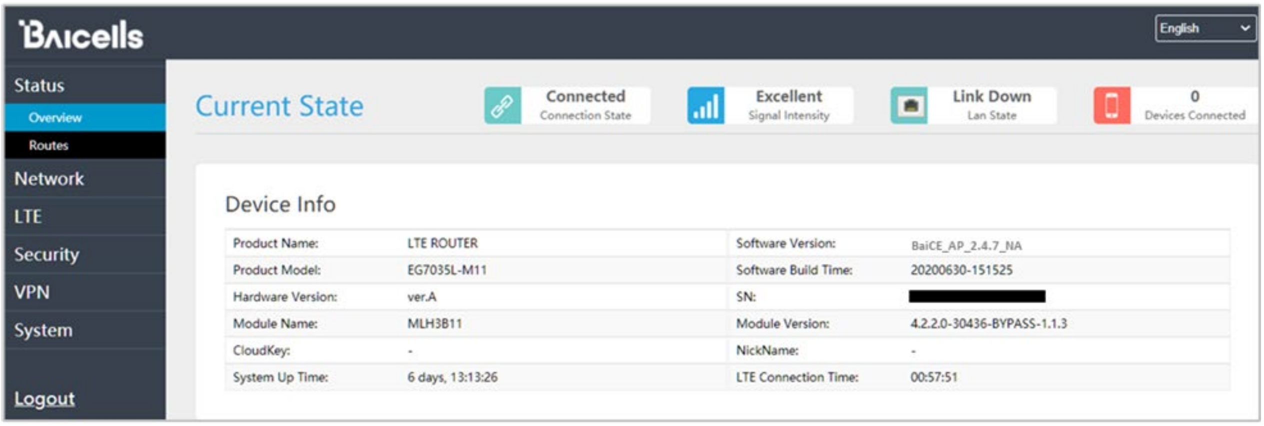


After you log in, all of the main GUI menus are shown in the left navigation pane on the home page (Figure 2-5).

NOTE: The GUI menus vary somewhat between CAT4 and CAT6/7/15 CPEs.

Figure 2-5: Home Page

CAT4



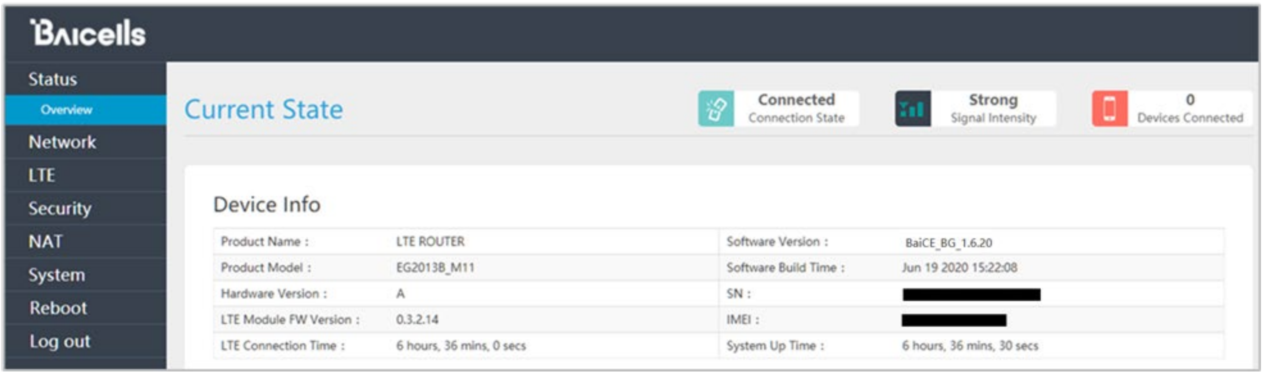
Current State

Connected Connection State | Excellent Signal Intensity | Link Down Lan State | 0 Devices Connected

Device Info

Product Name:	LTE ROUTER	Software Version:	BaiCE_AP_2.4.7_NA
Product Model:	EG7035L-M11	Software Build Time:	20200630-151525
Hardware Version:	ver.A	SN:	[redacted]
Module Name:	MLH3B11	Module Version:	4.2.2.0-30436-BYPASS-1.1.3
CloudKey:	-	NickName:	-
System Up Time:	6 days, 13:13:26	LTE Connection Time:	00:57:51

CAT6/7/15



Current State

Connected Connection State | Strong Signal Intensity | 0 Devices Connected

Device Info

Product Name :	LTE ROUTER	Software Version :	BaiCE_BG_1.6.20
Product Model :	EG2013B_M11	Software Build Time :	Jun 19 2020 15:22:08
Hardware Version :	A	SN :	[redacted]
LTE Module FW Version :	0.3.2.14	IMEI :	[redacted]
LTE Connection Time :	6 hours, 36 mins, 0 secs	System Up Time :	6 hours, 36 mins, 30 secs

3 Status Menu

The *Status* menu is a dashboard of key information about the CPE. It provides the model number, software version, serial number, operational state, usage data, and more. The sub-menus, *Overview* (CAT4 and CAT6/7/15) and *Routes* (CAT4 only), are explained in this section.

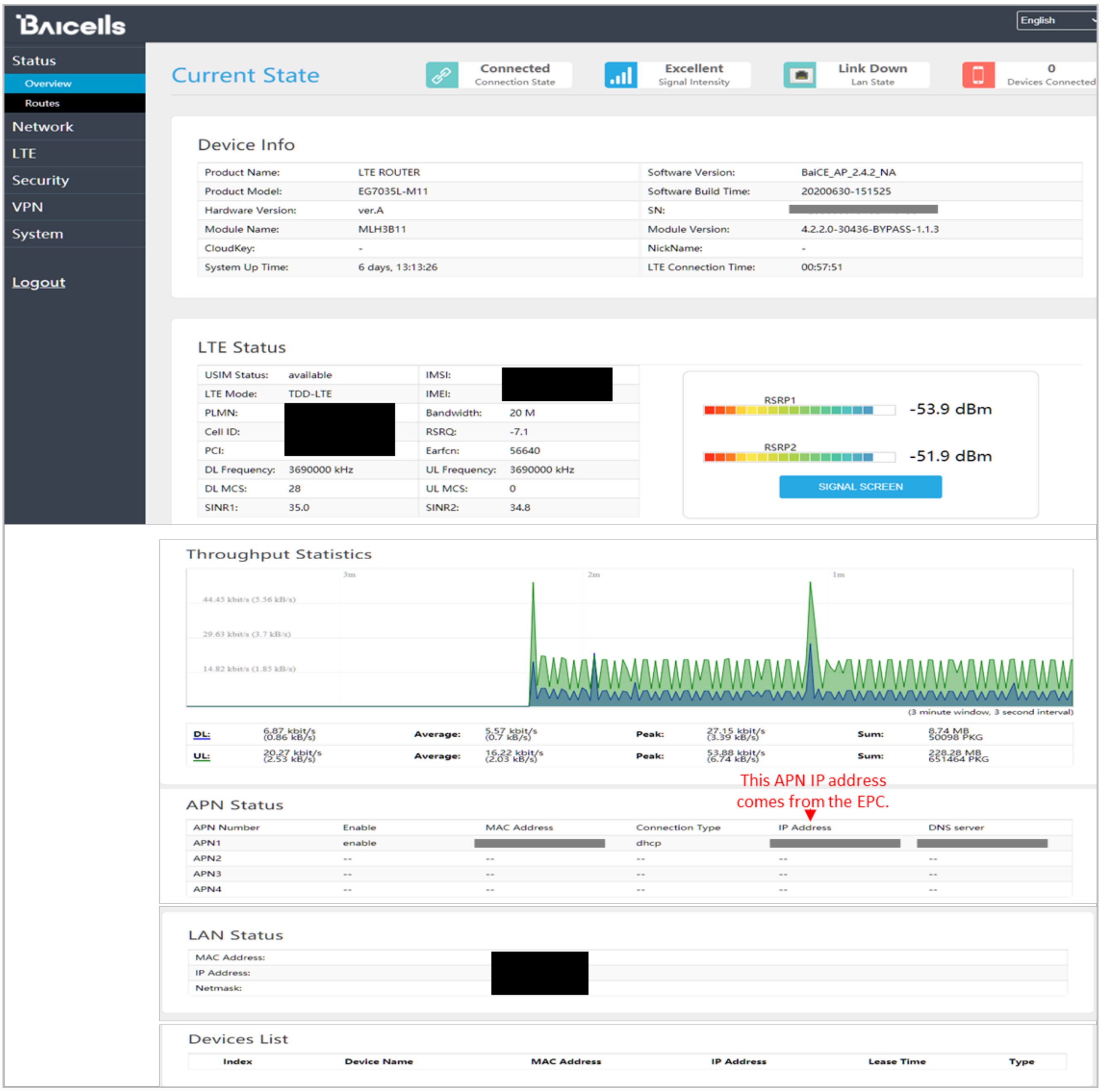
3.1 Overview

The *Status* > *Overview* sub-menu provides system and device status information for the CPE - Figure 3-1 (CAT4) and Figure 3-2 (CAT6/7/15). The top row, *Current State*, shows the network connection status, signal intensity, LAN link status (CAT4 only), and the number of smart devices 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, its IMSI number, wireless frequency being used, eNB connection status, current signal strength and quality, and so forth.

Under *Throughput Statistics* you will see a graph and the data for downlink (DL) and uplink (UL) throughput (kbps), average rates, peak rates, and total throughput. The data is measured during a three-second interval every five minutes. The *APN Status* pane (CAT4) and *Internet Status* pane (CAT6/7/15) displays any external gateway connections. The *LAN Status* pane shows the CPE's Media Access Control (MAC) address, IP address, and netmask. The bottom pane, *Devices List*, will show details about all smart devices currently connected through the CPE. Each field is described in Table 3-1.

Figure 3-1: Status > Overview (CAT4)



Current State

Connected
Connection State | Excellent
Signal Intensity | Link Down
Lan State | 0
Devices Connected

Device Info

Product Name:	LTE ROUTER	Software Version:	BaiCE_AP_2.4.2_NA
Product Model:	EG7035L-M11	Software Build Time:	20200630-151525
Hardware Version:	ver.A	SN:	[redacted]
Module Name:	MLH3B11	Module Version:	4.2.2.0-30436-BYPASS-1.1.3
CloudKey:	-	NickName:	-
System Up Time:	6 days, 13:13:26	LTE Connection Time:	00:57:51

LTE Status

USIM Status:	available	IMSI:	[redacted]
LTE Mode:	TDD-LTE	IMEI:	[redacted]
PLMN:	[redacted]	Bandwidth:	20 M
Cell ID:	[redacted]	RSRQ:	-7.1
PCI:	[redacted]	Earfcn:	56640
DL Frequency:	3690000 kHz	UL Frequency:	3690000 kHz
DL MCS:	28	UL MCS:	0
SINR1:	35.0	SINR2:	34.8

RSRP1 -53.9 dBm

RSRP2 -51.9 dBm

Throughput Statistics

DL:	6.87 kbit/s (0.86 kB/s)	Average:	5.57 kbit/s (0.7 kB/s)	Peak:	27.15 kbit/s (3.39 kB/s)	Sum:	8.74 MB 50098 PKG
UL:	20.27 kbit/s (2.53 kB/s)	Average:	16.22 kbit/s (2.03 kB/s)	Peak:	53.88 kbit/s (6.74 kB/s)	Sum:	228.28 MB 651464 PKG

This APN IP address comes from the EPC.

APN Status

APN Number	Enable	MAC Address	Connection Type	IP Address	DNS server
APN1	enable	[redacted]	dhcp	[redacted]	[redacted]
APN2	--	--	--	--	--
APN3	--	--	--	--	--
APN4	--	--	--	--	--

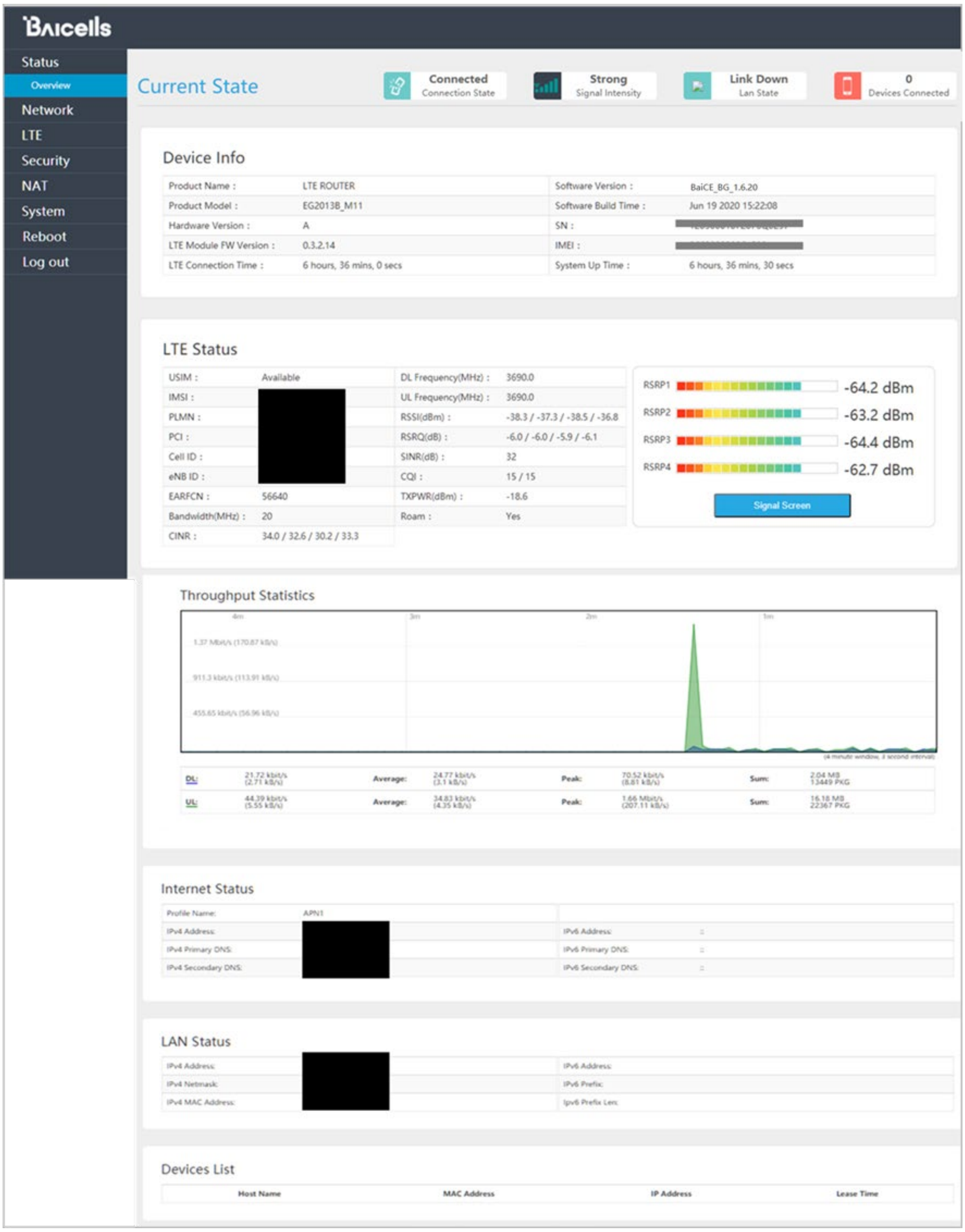
LAN Status

MAC Address:	[redacted]
IP Address:	[redacted]
Netmask:	[redacted]

Devices List

Index	Device Name	MAC Address	IP Address	Lease Time	Type

Figure 3-2: Status > Overview (CAT6/7/15)


Baicells
Status
Overview
Network
LTE
Security
NAT
System
Reboot
Log out
Signal Screen
4m
3m
2m
1m
1.37 Mbit/s (170.87 kB/s)
911.3 kbit/s (113.91 kB/s)
455.65 kbit/s (56.96 kB/s)
(4 minute window, 3 second interval)

Current State

Connected	Strong	Link Down	0
Connection State	Signal Intensity	Lan State	Devices Connected

Device Info

Product Name :	LTE ROUTER	Software Version :	BaiCE_BG_1.6.20
Product Model :	EG2013B_M11	Software Build Time :	Jun 19 2020 15:22:08
Hardware Version :	A	SN :	[redacted]
LTE Module FW Version :	0.3.2.14	IMEI :	[redacted]
LTE Connection Time :	6 hours, 36 mins, 0 secs	System Up Time :	6 hours, 36 mins, 30 secs

LTE Status

USIM :	Available	DL Frequency(MHz) :	3690.0
IMSI :	[redacted]	UL Frequency(MHz) :	3690.0
PLMN :	[redacted]	RSSI(dBm) :	-38.3 / -37.3 / -38.5 / -36.8
PCI :	[redacted]	RSRQ(dB) :	-6.0 / -6.0 / -5.9 / -6.1
Cell ID :	[redacted]	SINR(dB) :	32
eNB ID :	[redacted]	CQI :	15 / 15
EARFCN :	56640	TXPWR(dBm) :	-18.6
Bandwidth(MHz) :	20	Roam :	Yes
CINR :	34.0 / 32.6 / 30.2 / 33.3		

RSRP1	-64.2 dBm
RSRP2	-63.2 dBm
RSRP3	-64.4 dBm
RSRP4	-62.7 dBm

Throughput Statistics

DL:	21.72 kbit/s (2.71 kB/s)	Average:	24.77 kbit/s (3.1 kB/s)	Peak:	70.52 kbit/s (8.81 kB/s)	Sum:	2.04 MB 13449 PKG
UL:	44.39 kbit/s (5.55 kB/s)	Average:	34.83 kbit/s (4.35 kB/s)	Peak:	1.66 Mbit/s (207.11 kB/s)	Sum:	16.18 MB 22367 PKG

Internet Status

Profile Name:	APN1		
IPv4 Address:	[redacted]	IPv6 Address:	::
IPv4 Primary DNS:	[redacted]	IPv6 Primary DNS:	::
IPv4 Secondary DNS:	[redacted]	IPv6 Secondary DNS:	::

LAN Status

IPv4 Address:	[redacted]	IPv6 Address:	
IPv4 Netmask:	[redacted]	IPv6 Prefix:	
IPv4 MAC Address:	[redacted]	Ipv6 Prefix Len:	

Devices List

Host Name	MAC Address	IP Address	Lease Time

Table 3-1: Status > Overview Fields

Field	Description
Current State	
Connection State	Indicates the 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 CPE unit typically displays one to five LEDs to indicate this level.

Field	Description
Lan State	The connection between the CPE and the local area network is either Link Up or Link Down.
Devices Connected	A count of the devices connected to the Internet through this CPE via a LAN or a Wireless LAN connection
Device Info	
Product Name	LTE ROUTER indicates the CPE is operating as a router between the local network and the backhaul network
Product Model	Baicells's hardware model name
Hardware Version	The version of hardware for this CPE unit
Module Name	CAT4 only. Indicates the processor used in the CPE unit
CloudKey	CAT4 only. Operator's unique CloudCore account number issued by Baicells
System Up Time	Number of days, hours, minutes, and seconds the CPE has been powered on. The timer will reset after a CPE reboot.
Software Version	The version of software running on this CPE
Software Build Time	Baicells's software build date
SN	The CPE's unique serial number
Module Version or LTE Module FW Version	The CPE's LTE module firmware version
IMEI	See *LTE Status > IMEI* description below*
NickName	CAT4 only. Optional name the operator can enter to identify the CPE and/or its user
LTE Connection Time	Hours, minutes, and seconds the CPE has been connected to the LTE backhaul network
LTE Status	
USIM or USIM Status	The Universal Subscriber Identity Module status is either available or not ready
LTE Mode	CAT4 only. The CPE is operating in either Frequency Division Duplexing (FDD) or Time Division Duplexing (TDD) mode
PLMN	The Public Land Mobile Network (PLMN) to which the CPE is connected
Cell ID	The cell site ID to which the CPE is connected
eNB ID	CAT6/7/15 only. Indicates the serving eNB's identification number.
PCI	The Physical Cell Identifier (PCI) ID is unique to each eNB. PCI indicates to which eNB device the CPE is connected. An operator can have multiple eNB devices in the same cell.
DL Frequency(MHz)	The frequency that the CPE is using in the downlink (eNB to CPE). In LTE, the carrier frequency in the uplink and downlink is designated by the E-UTRA Absolute Radio Frequency Channel Number (EARFCN), which identifies the LTE band and carrier frequency.
DL MCS	CAT4 only. The downlink signal (eNB to CPE) Modulation and Coding Scheme (MCS) currently being used. This index represents the overall channel conditions and helps to indicate the maximum throughput available to the CPE.
SINR1 or SINR(dB)	CAT4 GUI reports SINR1 and SINR2. CAT6/7/15 GUI reports SINR. Signal-to-Interference-Plus-Noise Ratio – A value that reflects the signal strength of the signal received from one of the antennas in the eNB, expressed in decibels (dB)
CQI	CAT6/7/15 only. The Channel Quality Indicator indicates how good or bad the communication channel quality is for data being transmitted from the eNB to the CPE. Value range is 1-15.

Field	Description
TXPWR(dBm)	CAT6/7/15 only. Transmit power, in dBm.
Roam	CAT6/7/15 only. Yes or No, roaming is enabled on this CPE.
IMSI	The unique International Mobile Subscriber Identity (IMSI) number associated with the SIM card in the CPE. The IMSI must be identifiable by the operator's LTE network in order to access it.
*IMEI	The CPE's unique International Mobile Equipment Identity (IMEI) number, a 15- or 17-digit code that is essentially a serial number for the SIM card
Bandwidth(MHz)	The range of frequencies within the band the CPE can use for transmitting a signal
CINR	CAT6/7/15 only. Carrier-to-Interference-Plus-Noise-Ratio. CINR represents the ratio of the RF signal to the total power of interfering signals plus thermal noise.
RSRQ(dB)	Reference Signal Received Quality – A value that reflects the signal quality of the received reference signal. Indicates the noise floor.
Earfcn	The E-UTRA Absolute Radio Frequency Channel Number (band and frequency) within which the CPE operates
UL Frequency(MHz)	The frequency 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.
UL MCS	CAT4 only. The uplink signal (CPE to eNB) Modulation and Coding Scheme (MCS) currently being used. This index represents the overall channel conditions and indicates the maximum throughput available to the CPE.
SINR2	CAT4 only. Signal-to-Interference-Plus-Noise Ratio 2 – A value that reflects the signal strength of the signal received from a second antenna in the eNB, expressed in decibels (dB)
RSSI(dBm)	CAT6/7/15 only. Received Signal Strength Indicator – A linear mean value of all the signals that the user equipment has received, including the intra-frequency signal and interference, the inter-frequency interference, and thermal noise.
RSRP1	Reference Symbol Received Power 1 – A value, in dBm, that reflects the linear average over the power contributions for the resource elements in one antenna that carry cell-specific reference signals within the frequency bandwidth
RSRP2	See "RSRP1" description.
RSRP3	CAT6/7/15 only. See "RSRP1" description.
RSRP4	CAT6/7/15 only. See "RSRP1" description.
Throughput Statistics	
DL	The current downlink data throughput rate, in Kbps, for this CPE in the last three minutes
UL	The current uplink data throughput rate, in Kbps, for this CPE in the last three minutes
Average	The average DL and UL data throughput rates, in Kbps, for this CPE in the last three minutes
Peak	The peak DL and UL data throughput rates, in Kbps, for this CPE in the last three minutes
Sum	The total (sum) DL and UL data throughput rates, in Kbps, for this CPE in the last three minutes
APN Status or Internet Status	
APN Number or Profile Name	Access Point Name (APN) is a gateway between a 3G/4G mobile network and another computer network, frequently the public Internet. At least one APN must be configured to

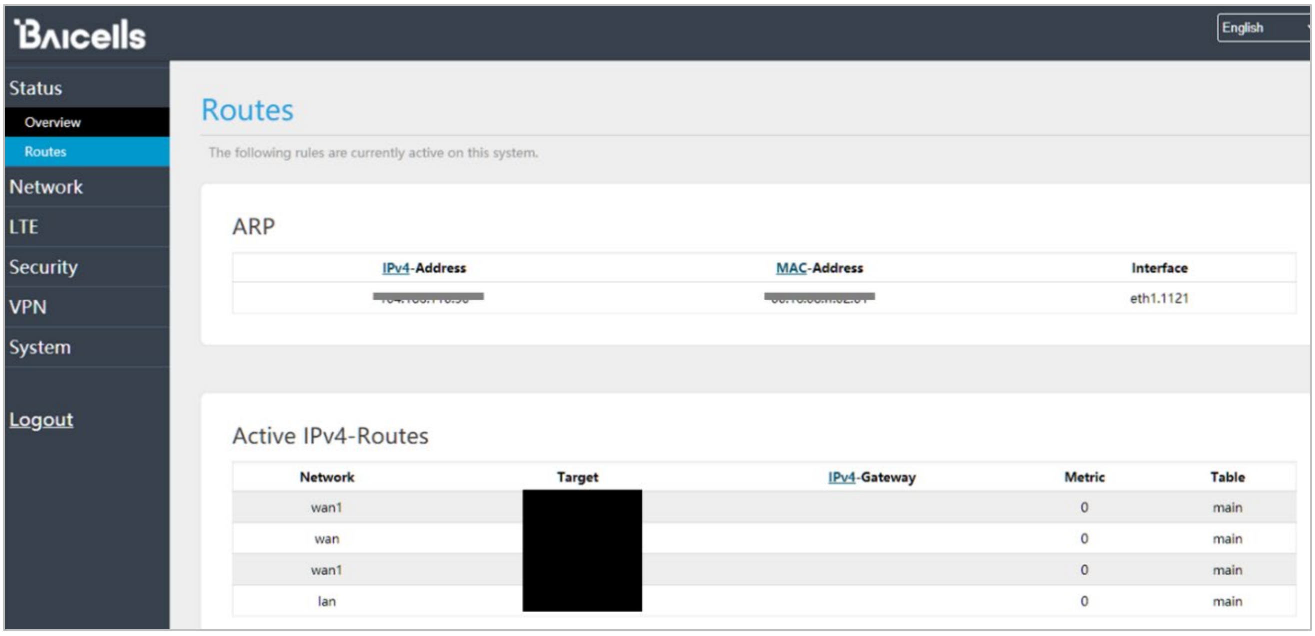
Field	Description
	establish the TR-069 connection to the CloudCore or other NMS.
Enable	CAT4 only. Shows the status of APN 1, 2, 3, or 4 - enable or disable
MAC Address	CAT4 only. The APN gateway's Media Access Control address
Connection Type	CAT4 only. Indicates the type of local area network connection the CPE uses to connect to the APN, e.g., dhcp for Dynamic Host Configuration Protocol
IP Address or IPv4 Address or IPv6 Address	The Internet Protocol address of the APN to which the CPE is connected
DNS Server or IPv4 Primary DNS or IPv4 Secondary DNS or IPv6 Primary DNS or IPv6 Secondary DNS	The Domain Name Server used by the APN to which the CPE is connected. In CAT6/7/15, you can identify a primary and a secondary DNS for IPv4 and for IPv6.
LAN Status	
MAC Address or IPv4 MAC Address	The Media Access Control address of the local area network
IP Address or IPv4 Address or IPv6 Address	The IP address currently used by the local area network. In CAT6/7/15, you can differentiate between IPv4 and IPv6 addresses. For IPv6 addressing, enter the prefix and length.
Netmask or IPv4 Netmask	The subnet mask address currently used by the local area network
Devices List	
Index	CAT4 only. An integer assigned to each device connected to the CPE
Device Name or Host Name	The name of a device connected to the CPE
MAC Address	The Media Access Control address of a device connected to the CPE
IP Address	The Internet Protocol address of a device connected to the CPE
Lease Time	Amount of time a device's IP address has been leased
Type	CAT4 only. Identifies whether or not the device got its IP address from the LAN DHCP service

3.2 Routes

The *Status* > *Routes* sub-menu that displays in the CAT4 GUI shows the current routing rules defined for the CPE, including Address Resolution Protocol *(ARP)* and *Active IPv4-Routes* (Figure 3-3). ARP is a protocol for mapping a Layer 3 network IP address to each device's Layer 2 MAC address on the local network.

The IP version rules will display according to how the settings for *Network* > *Static Routes* are configured (see *section 4.5*). The fields in the *Status* > *Routes* screen are described in Table 3-2 according to the example in the figure.

Figure 3-3: Routes



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
[redacted]	[redacted]	eth1.1121

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan1	[redacted]		0	main
wan	[redacted]		0	main
wan1	[redacted]		0	main
lan	[redacted]		0	main

Table 3-2: Routes

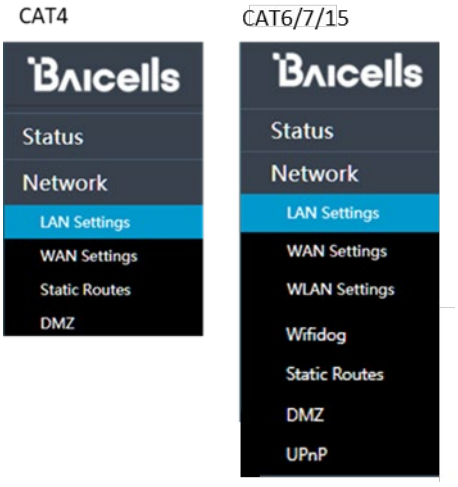
Field Name	Description
ARP	
IPv4-Address	Current or most recently used Internet Protocol address of the target device
MAC-Address	Current or most recently used Media Access Control address of the target device
Interface	The local area network interface through which the IP address reaches the target device
Active IPv4-Routes	
Network	Name of the external network
Target	IP address range for traffic on the external network
IPv4-Gateway	The gateway address for IPv4 addresses
Metric	Number of times the CPE accessed the external network
Table	Name of the routing table used by the gateway

4 Network Menu

The *Network* menu opens to the sub-menus shown in Figure 4-1. Both CAT4 and CAT6/7/15 GUIs include *LAN Settings*, *WAN Settings*, *Static Routes*, and *DMZ* functions. In addition, CAT6/7/15 includes *WLAN Settings, Wifidog,* and *UPnP*. This section explains each sub-menu.

NOTE: The UPnP function is available in CAT4 under the *Security* menu (*section 6.12*).

Figure 4-1: Network Menu



4.1 LAN Settings

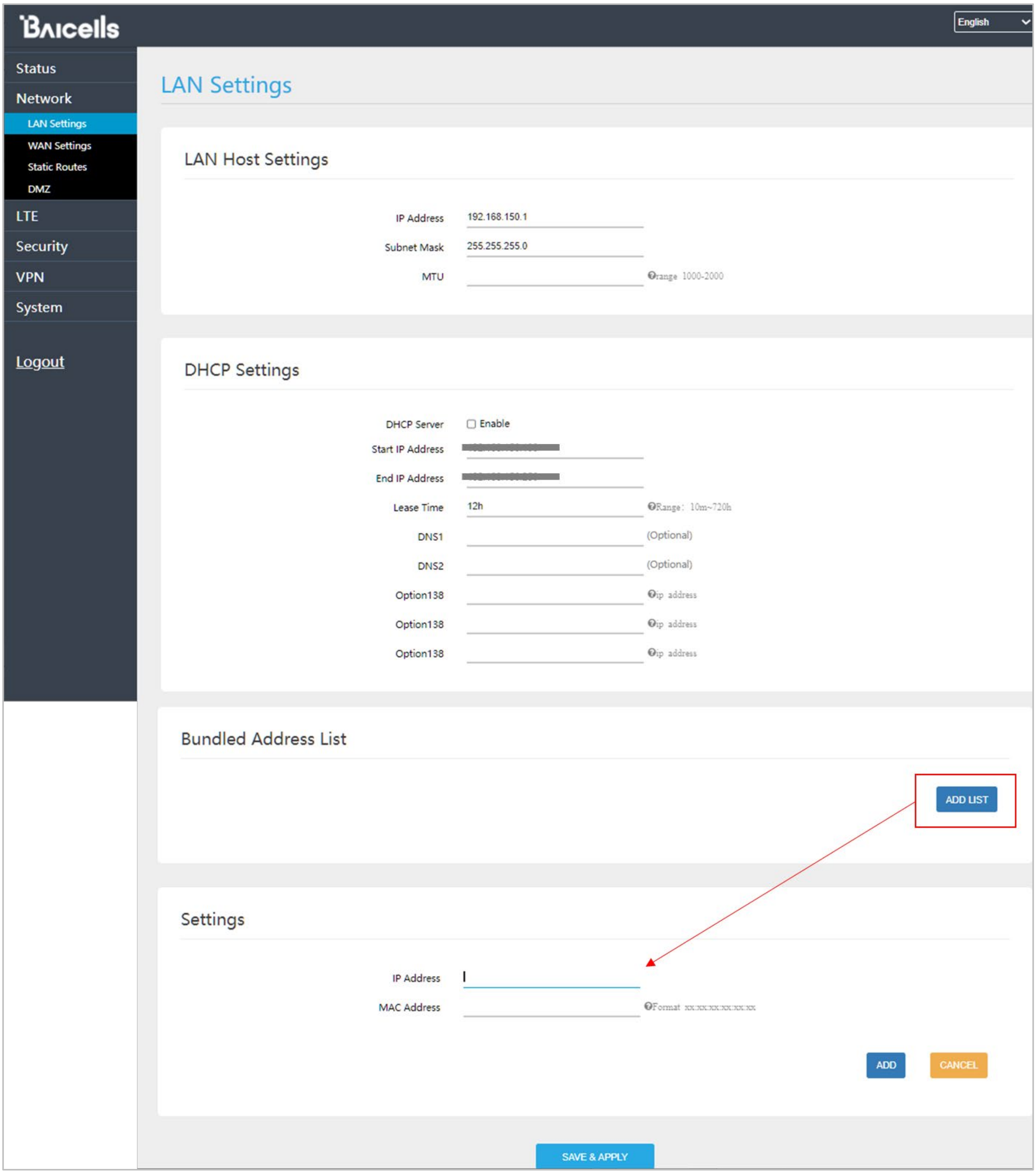
The *Network > LAN Settings* sub-menu [Figure 4-2 (CAT4) and Figure 4-3 (CAT6/7/15)] is used to configure the LAN host and DHCP IP address settings for the CPE. By default, the LAN or DHCP IP address is 192.168.150.1 (Gen 2 CPEs) or 192.168.254.1 (Gen 1 CPEs) and the subnet mask is 255.255.255.0.
If you edit how the address displays - for example, by changing it to a name to make the address easier to remember - make sure the address you choose is unique to your network. You will use the address for remote access to the GUI.

DHCP dynamically assigns an IP address and other network configuration parameters to each device on the network so they can communicate with other IP networks. You can bind an IP address to the CPE based on its MAC address. If binding is configured, the CPE will provide IP addresses to any devices that connect to it.

When configured as a DHCP server, the CPE automatically provides the TCP/IP configuration for the LAN clients that support DHCP client capabilities. If DHCP services are disabled, you must have another DHCP server on the LAN or each client must be configured manually.

The fields are slightly different between CAT4 and CAT6/7/15, as shown in the figures. Refer to Table 4-1 for a description of all the fields.

Figure 4-2: LAN Settings (CAT4)



LAN 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 [redacted]

End IP Address [redacted]

Lease Time 12h ❓Range: 10m~720h

DNS1 (Optional)

DNS2 (Optional)

Option138 ❓ip address

Option138 ❓ip address

Option138 ❓ip address

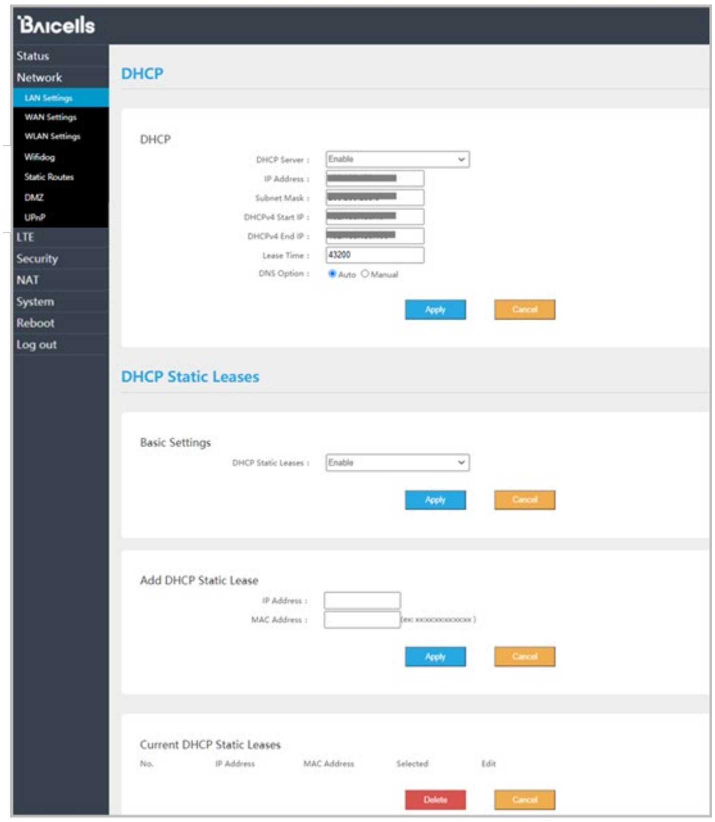
Bundled Address List

Settings

IP Address

MAC Address ❓Format xx:xx:xx:xx:xx:xx

Figure 4-3: LAN Settings (CAT6/7/15)



DHCP

DHCP

DHCP Server : Enable
IP Address : [redacted]
Subnet Mask : [redacted]
DHCPv4 Start IP : [redacted]
DHCPv4 End IP : [redacted]
Lease Time : 43200
DNS Option : ● Auto ○ Manual

DHCP Static Leases

Basic Settings

DHCP Static Leases : Enable

Add DHCP Static Lease

IP Address :
MAC Address : (ex: xxxxxxxxxxxx)

Current DHCP Static Leases

No.	IP Address	MAC Address	Selected	Edit

Table 4-1: LAN Settings

Field Name	Description
LAN Host Settings (CAT4 only)	
IP Address	Accept the default CPE IP address, or enter a new one
Subnet Mask	Accept the default CPE subnet mask, or enter a new one
MTU	Maximum Transmission Unit - maximum packet size for this CPE. Range: 1000-2000 bytes
DHCP Settings	
DHCP Server	Three options: • Disable (or leave the Enable checkbox unchecked) - do not configure the CPE as a DHCP server (CAT4 and CAT6/7/15) • Enable - configure the CPE as a DHCP server (CAT4 and CAT6/7/15) • Enable DHCP relay - the CPE will forward packets between devices connected to the CPE and the DHCP server (CAT6/7/15 only)
IP Address	CAT6/7/15 only. Accept the default CPE IP address, or enter a new one
Subnet Mask	CAT6/7/15 only. Accept the default CPE subnet mask, or enter a new one
Start IP Address or DHCPv4 Start IP	Enter the starting IP address that the DHCP server can use for individual clients associated with this CPE.
End IP Address or DHCPv4 End IP	Enter the last IP address that the DHCP server can use for individual clients associated with this CPE.
Lease Time	Enter the lease time (in minutes). The range is 10 to 720 minutes. The default of 720 minutes is recommended.
DNS1 & DNS2	CAT4 only. If using a Domain Name Server, enter the IP address. You can configure one or

Field Name	Description
	two DNS servers.
Option 138	CAT4 only. Option to enable DHCP Option 138 Control And Provisioning of Wireless Access Points. Up to three Option 138 IP addresses can be entered.
DNS Option	CAT6/7/15 only. Select Auto if you want to allow any of the defined DNS servers to be used. Select Manual to designate a Primary DNS, Secondary DNS, and/or Third DNS IP address.
Bundled Address List (CAT4 only)	
ADD LIST	You can bind a device's IP address to the CPE based on its MAC address. If binding is configured, the CPE will provide IP addresses to those devices that connect to it. You can add multiple bundled addresses.
IP Address	Device's IP address to bundle with the CPE MAC address
MAC Address	Device's MAC address
DHCP Static Leases (CAT6/7/15 only)	
Basic Settings	
DHCP Static Leases	Enable or disable use of static IP addresses on this CPE
Add DHCP Static Lease	
IP Address	Device's IP address to bundle with the CPE MAC address
MAC Address	Device's MAC address

4.2 WAN Settings

The *Network* > *WAN Settings* pertain to how the CPE interfaces with the Wide Area Network (WAN) - typically the Internet; the network or operation mode; and Domain Name Server (DNS) information. Because the GUI screens for this function are laid out differently between CAT4 and CAT6/7/15, each is described separately in the sections below. Refer to Table 4-2 for a description of all fields in both GUIs.

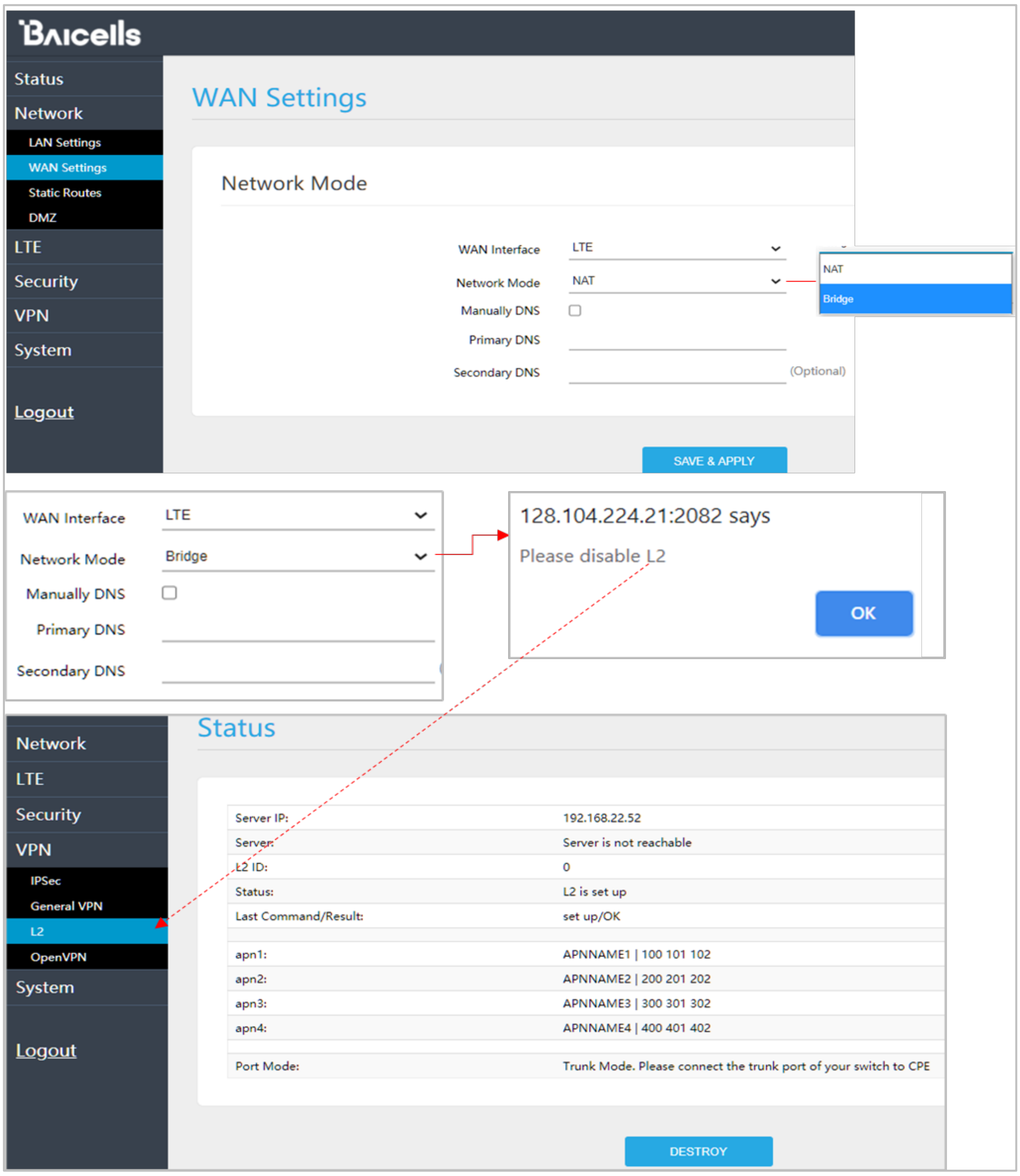
4.2.1 WAN Settings (CAT4)

Looking at the CAT4 GUI in Figure 4-4, the only option for the first field - *WAN Interface* - is *LTE*. Therefore, you can leave the default setting for this field. For *Network Mode*, you can configure the CAT4 CPE in either *NAT* or *Bridge* mode, depending on your network topology.

Network Address Translation (NAT) mode allows multiple hosts on a private network to access the Internet using a single public IP address. Bridge mode disables NAT and allows the CPE to create a Layer 2 (L2) link and function as a DHCP server without IP address confliction. If you have enabled L2 in the *VPN* > *L2* sub-menu, the system will prompt you to disable those L2 settings first before changing the network mode to *Bridge*. When you get this prompt, click *OK,* go to the *VPN* > *L2* sub-menu, and select ***Destroy*** (refer to *section 8.3*).

In addition to the DNS server(s) configured for the LAN in the *Network* > *LAN Settings*, you can configure one or more DNS servers for the WAN. The DNS translates domain names such as *www.na.baicells.com* into their underlying IP addresses. The ISP may use DNS servers to cache domain names frequented by its users so the sites load more quickly in a browser. If you leave the *Manually DNS* checkbox unchecked, the CPE will check the first available DNS in the network to resolve the domain name to IP address translation. If you select this checkbox, you can specify a Primary DNS's IP address and a Secondary DNS's IP address.

Figure 4-4: WAN Settings (CAT4)



WAN Settings

Network Mode

WAN Interface LTE

Network Mode NAT

Manually DNS ☐

Primary DNS

Secondary DNS (Optional)

WAN Interface LTE

Network Mode Bridge

Manually DNS ☐

Primary DNS

Secondary DNS

128.104.224.21:2082 says

Please disable L2

Status

Server IP:	192.168.22.52
Server:	Server is not reachable
L2 ID:	0
Status:	L2 is set up
Last Command/Result:	set up/OK
apn1:	APNNAME1 | 100 101 102
apn2:	APNNAME2 | 200 201 202
apn3:	APNNAME3 | 300 301 302
apn4:	APNNAME4 | 400 401 402
Port Mode:	Trunk Mode. Please connect the trunk port of your switch to CPE

4.2.2 WAN Settings (CAT6/7/15)

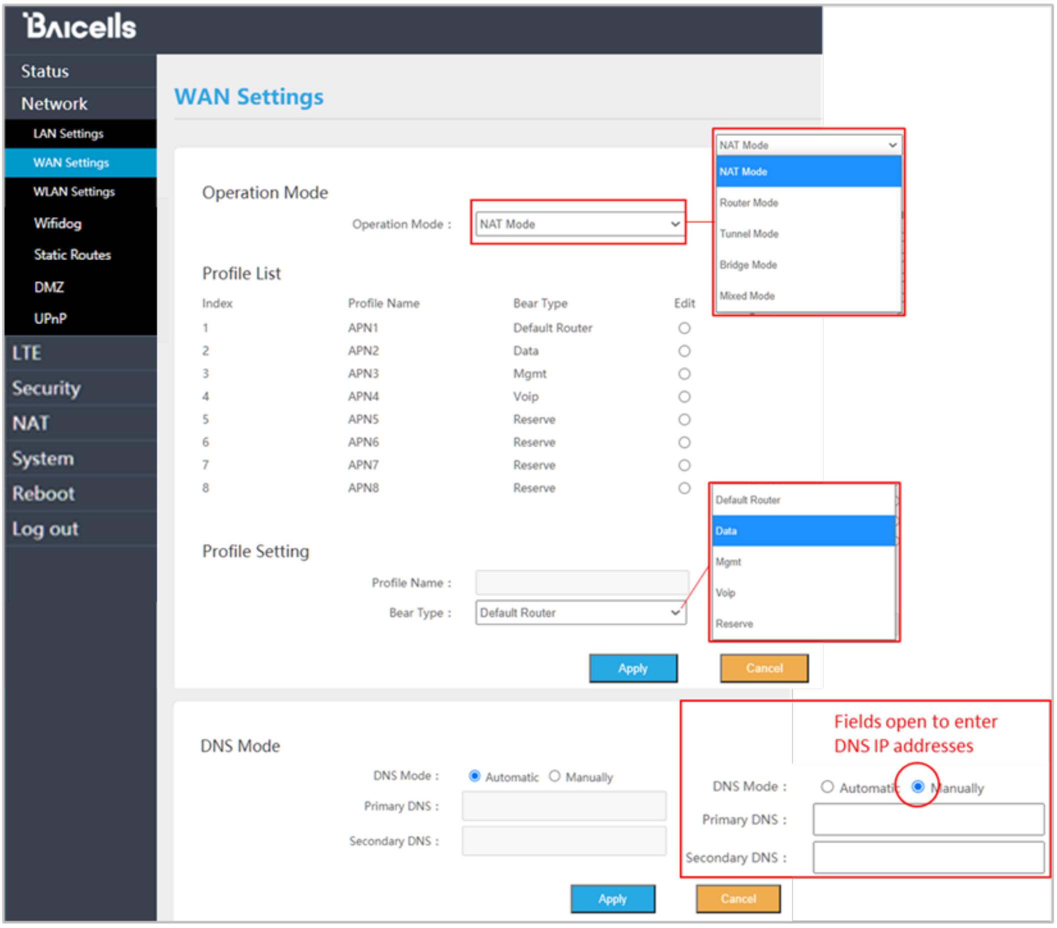
Looking at the CAT6/7/15 *Network* > *WAN Settings* in Figure 4-5 and Figure 4-6, select one of the following for the *Operation Mode*:

- *NAT Mode* - Allows multiple hosts on a private network to access the Internet using a single public IP address. When *NAT* is selected, all eight Access Point Name (APN) gateways can be configured for either Default Router, Data, Mgmt, or Voip. Refer to *section 5.3* concerning APN configurations.
- *Router Mode* - The CPE will dynamically update the router tables
- *Tunnel Mode* - The CPE will support Layer 2 Tunneling Protocol (L2TP) or Generic Routing Encapsulation (GRE) VPN mode. You can set the *Default Route* to *VPN* or *WAN*.
- *Bridge Mode* - The WAN port addresses will bridge to the LAN port; the LAN port will work in trunking mode.
- *Mixed Mode* - Each APN gateway can be configured with a different mode, either *NAT* or *Bridge*, and a different bearer type.

In the list of APNs under *Profile List*, to change the *Bear Type* select the radio button under *Edit* and in *Profile Setting* choose the *Bear Type*. For *DNS Mode*, you can select either *Automatic* or *Manually*. The DNS server translates domain names such as *www.na.baicells.com* into their underlying IP addresses. The ISP may use DNS servers to cache domain names frequented by its users so the sites load more quickly in a browser.

If you select *Automatic*, the CPE will check the first available DNS in the network to resolve the domain name to IP address translation. If you select *Manually*, specify a Primary DNS IP address and a Secondary DNS IP address.

Figure 4-5: WAN Settings (CAT6/7/15) (1 of 2)



WAN Settings

Operation Mode

Operation Mode : NAT Mode

Profile List

Index	Profile Name	Bear Type	Edit
1	APN1	Default Router	○
2	APN2	Data	○
3	APN3	Mgmt	○
4	APN4	Voip	○
5	APN5	Reserve	○
6	APN6	Reserve	○
7	APN7	Reserve	○
8	APN8	Reserve	○

Profile Setting

Profile Name :

Bear Type : Default Router

DNS Mode

DNS Mode : ● Automatic ○ Manually

Primary DNS :

Secondary DNS :

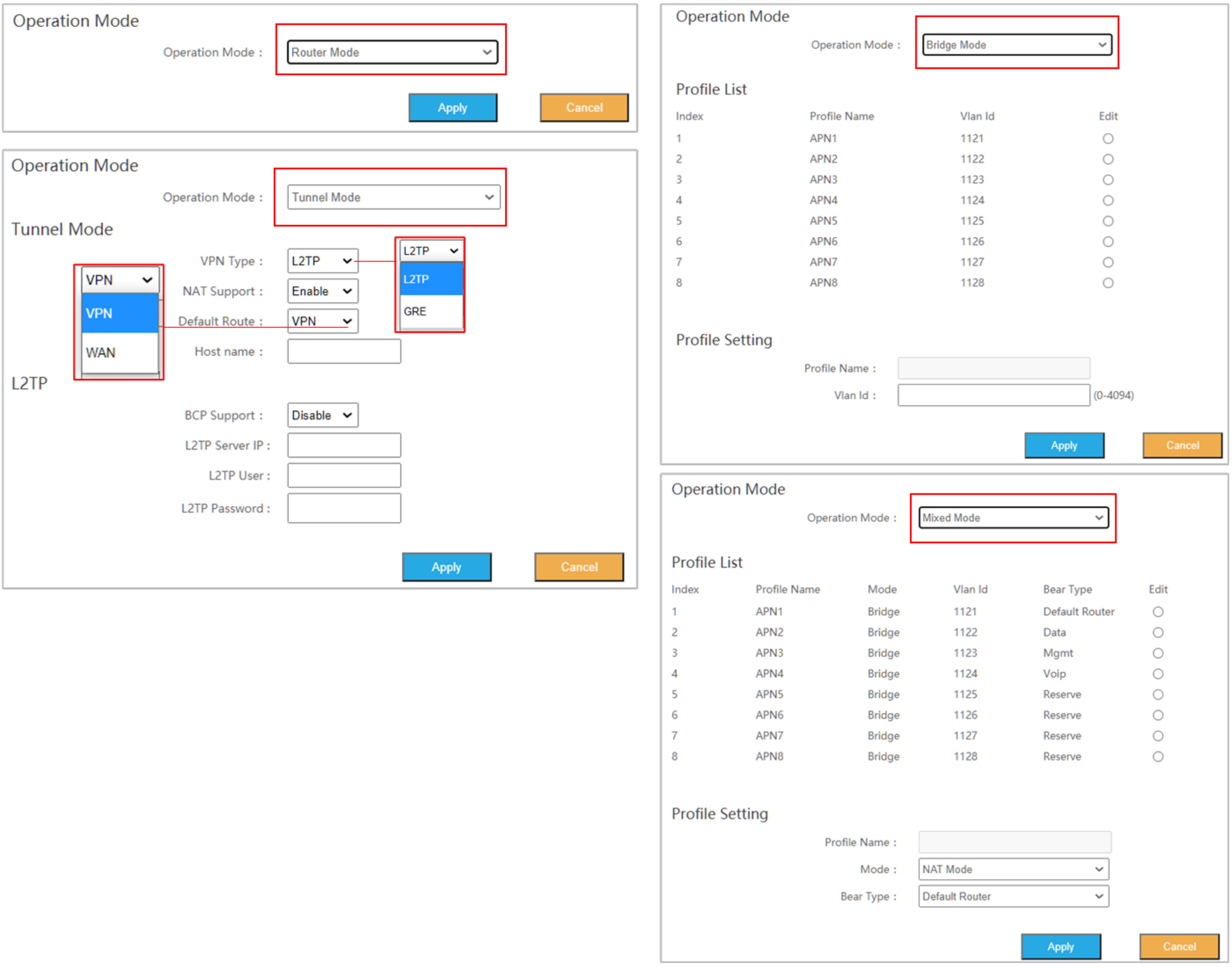
Fields open to enter DNS IP addresses

DNS Mode : ○ Automatic ● Manually

Primary DNS :

Secondary DNS :

Figure 4-6: WAN Settings (CAT6/7/15) (2 of 2)



Operation Mode

Operation Mode : Router Mode

Operation 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 :

L2TP Password :

Operation 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)

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

Table 4-2: WAN Settings

Field Name	Description
Network or Operation Mode	
WAN Interface	CAT4 only. LTE is the only option.
Network Mode or Operation Mode	CAT4: • NAT - Network Address Translation. Allows multiple hosts on a private network to access the Internet using a single public IP address. • Bridge - The WAN port addresses will bridge to the LAN port, and the LAN port will work in trunking mode. If you select *Bridge* mode, the system will prompt you to disable L2 in the *VPN* > *L2* sub-menu. CAT6/7/15: • NAT - Allows multiple hosts on a private network to access the Internet using a single public IP address. • Router - The CPE will dynamically update the router tables. • Tunnel - The CPE will support Layer 2 Tunneling Protocol (L2TP) or Generic Routing Encapsulation (GRE) VPN mode. See field descriptions below*.

Field Name	Description
	- Bridge - The WAN port addresses will bridge to the LAN port, and the LAN port will work in trunking mode. If you select *Bridge* mode, the system will prompt you to disable L2 in the *VPN > L2* sub-menu. - Mixed Mode - Each APN gateway can be configured with a different mode, either NAT or Bridge, and a different bearer type.
Manually DNS	CAT4 only. If left unchecked, the CPE will automatically search the domain name on the first available DNS server. If checked, enter the primary and secondary DNS server IP addresses.
Primary DNS	CAT4 only. If *Manually DNS* checkbox was checked, enter the primary DNS server's IP address for the CPE to check first for domain name resolution.
Secondary DNS	CAT4 only. If *Manually DNS* checkbox was checked, enter the secondary DNS server's IP address for the CPE to check after the primary DNS if the domain name was not resolved.
*Tunnel Mode (CAT6/7/15 Only)	
VPN Type	L2TP or GRE
NAT Support	Enable/Disable NAT on the VPN
Default Route	VPN or WAN
Host name	Optional - enter the default route name
*L2TP (CAT6/7/15 Only)	
BCP Support	Enable/Disable Bridge Control Protocol for L2TP tunneling. If enabled, must be set up on both ends, the CPE/router acting as Point-to-Point Protocol (PPP) client and the PPP server.
L2TP Server IP	IP address of the L2TP server
L2TP User	L2TP server user name
L2TP Password	L2TP server password
DNS Mode (CAT6/7/15 Only)	
DNS Mode	Automatic or Manually. If you select *Automatic*, the CPE will automatically search the domain name on the first available DNS server. If you select *Manually*, enter the primary and secondary DNS server IP addresses.
Primary DNS	If *DNS Mode* was set to *Manually*, enter the primary DNS server's IP address for the CPE to check first for domain name resolution.
Secondary DNS	If *DNS Mode* was set to *Manually*, enter the secondary DNS server's IP address for the CPE to check after the primary DNS if the domain name was not resolved.

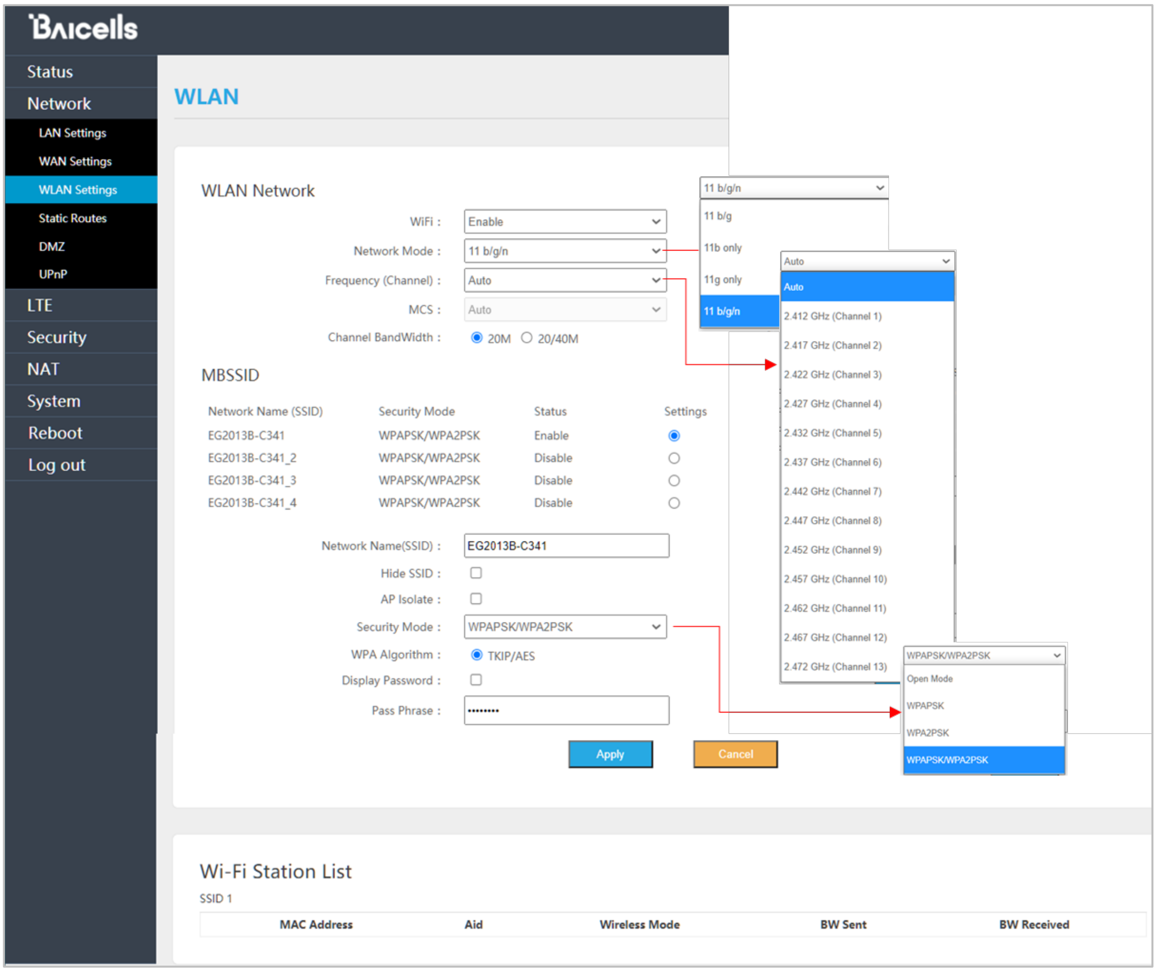
4.3 WLAN Settings

The Baicells Atom ID04 and ID06 CPEs have an embedded Wi-Fi access point, providing converged Wireless LAN (WLAN) and LAN interfaces into one integrated LTE service. The Wi-Fi uses 2.4 GHz unlicensed spectrum and is compliant with IEEE 802.11b/g/n.

You can enable WLAN and configure up to four independent Service Set Identifiers (SSIDs) on the local network. This allows users to customize the settings for each SSID.

An example is shown in Figure 4-7. Refer to the field descriptions in Table 4-3.

Figure 4-7: WLAN Settings



WLAN

WLAN Network

WiFi : Enable

Network Mode : 11 b/g/n

Frequency (Channel) : Auto

MCS : Auto

Channel BandWidth : ● 20M ○ 20/40M

MBSSID

Network Name (SSID)	Security Mode	Status	Settings
EG2013B-C341	WPAPSK/WPA2PSK	Enable	●
EG2013B-C341_2	WPAPSK/WPA2PSK	Disable	○
EG2013B-C341_3	WPAPSK/WPA2PSK	Disable	○
EG2013B-C341_4	WPAPSK/WPA2PSK	Disable	○

Network Name(SSID) : EG2013B-C341

Hide SSID : □

AP Isolate : □

Security Mode : WPAPSK/WPA2PSK

WPA Algorithm : ● TKIP/AES

Display Password : □

Pass Phrase : ••••••••

Wi-Fi Station List

SSID 1

MAC Address	Aid	Wireless Mode	BW Sent	BW Received

Table 4-3: WLAN Settings

Field Name	**Description**
WLAN Network	
WiFi	Enable/Disable the Wi-Fi access point
Network Mode	Select the (802.11) *Network Mode*: 11b/g, 11b only, 11g only, 11g/n, or 11b/g/n
Frequency Channel	Select *Auto* or select a specific channel. If set to Auto, the device will scan the network and start a Wi-Fi association in a clear channel. The channel list will vary according to CPE model.
MCS	Modulation and Coding Scheme supported. Is set to Auto by default and cannot be configured.
Channel Bandwidth	20 MHz or 20/40 MHz channel bandwidth for Wi-Fi
MBSSID	
Network Name (SSID)	Enter a name to identify the SSID
Hide SSID	If the checkbox is selected, the SSID will not be broadcast.
AP Isolate	Isolate the SSID settings from each other. When enabled, traffic on one SSID will not be forwarded to any other SSID.
Security Mode	Select the type of encryption to use: • Open mode - No security settings; anyone within range of your network can access it without a password • WPAPSK - Software based Wi-Fi Protected Access Pre-Shared Key generation between

Field Name	Description
	client devices and the WLAN. Requires the user to enter a password. • WPA2PSK - Hardware based Wi-Fi Alliance variation of the WPAPSK encryption method. Requires the user to enter a password. • WPAPSK/WPA2PSK - Access to the WLAN requires both a PSK and a password
WPA Algorithm	Only TKIP/AES is available at this time. Temporal Key Integrity Protocol keys and rekeys packet content, while Advanced Encryption Standard is a Wi-Fi Alliance certified encryption.
Display Password	Select the checkbox if you want to display the security password in the *Pass Phrase* field.
Pass Phrase	Security password clients must enter to access the LAN. Must be at least eight characters.

4.4 Wifidog (CAT6/7/15)

The feature, Wifidog, is available on Atom UEs and can be used to build wireless hotspots. The feature works in cooperation with a remote authentication server. When Wifidog is enabled, Wi-Fi devices such as guest users will have to be authenticated through the remote authentication server.

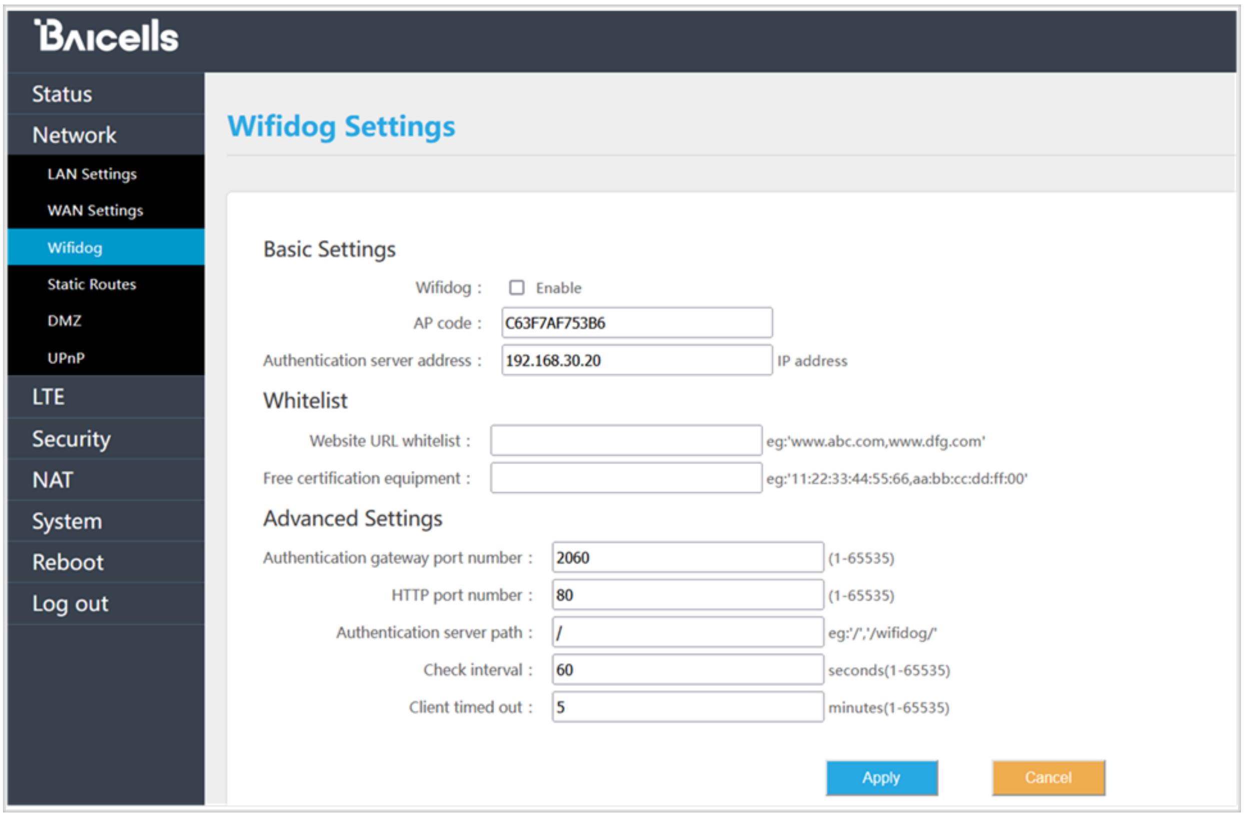
NOTE 1: The feature requires a connection to an authentication server to function.

NOTE 2: Wifidog is not recommended for Baicells UEs using Power over Ethernet (PoE).

You can create a whitelist to identify which website addresses, or URLs, users are allowed to reach. You can also limit the number of times that a user can try to log in within a configured time period before failure to authenticate times out. These settings help to avoid unauthorized use of the network.

In the GUI, go to *Network* > *Wifidog* (Figure 4-8). Notice the three panes in the *Wifidog Settings* window - *Basic Settings*, *Whitelist*, and *Advanced Settings*. In the *Basic Settings* pane, click on the checkbox next to *Enable* to initiate Wifidog, and enter the *AP code* and the *Authentication Server Address*. If you don't want to create a whitelist or configure advanced settings, then click on *Apply*. Otherwise, continue to the additional procedures for these settings before clicking on *Apply*.

Figure 4-8: Wifidog



Wifidog Settings

Basic Settings

Wifidog : □ Enable

AP code : C63F7AF753B6

Authentication server address : 192.168.30.20 IP address

Whitelist

Website URL whitelist : eg:'www.abc.com,www.dfg.com'

Free certification equipment : eg:'11:22:33:44:55:66,aa:bb:cc:dd:ff:00'

Advanced Settings

Authentication gateway port number : 2060 (1-65535)

HTTP port number : 80 (1-65535)

Authentication server path : / eg:'/','/wifidog/'

Check interval : 60 seconds(1-65535)

Client timed out : 5 minutes(1-65535)

In the *Whitelist* pane you can add URL addresses to be whitelisted – that is, allowed – without the user having to authenticate. Separate each URL with a comma (,). For the *Free certification equipment* field, enter the hotspot users' device MAC addresses. Use a comma (,) to separate each one. If you don’t want to configure advanced settings, then click on *APPLY*. Otherwise, continue to the additional procedures for these settings before clicking on *APPLY*.

In the *Advanced Settings* pane, if you want all hotspot users to use the same authentication server and login requirements, enter the server path information and set the *Check interval* field (maximum time, in seconds), for logging in and the *Client timed out* field (maximum amount of time before failure to authenticate times out, in minutes). Click on *APPLY*.

4.5 Static Routes

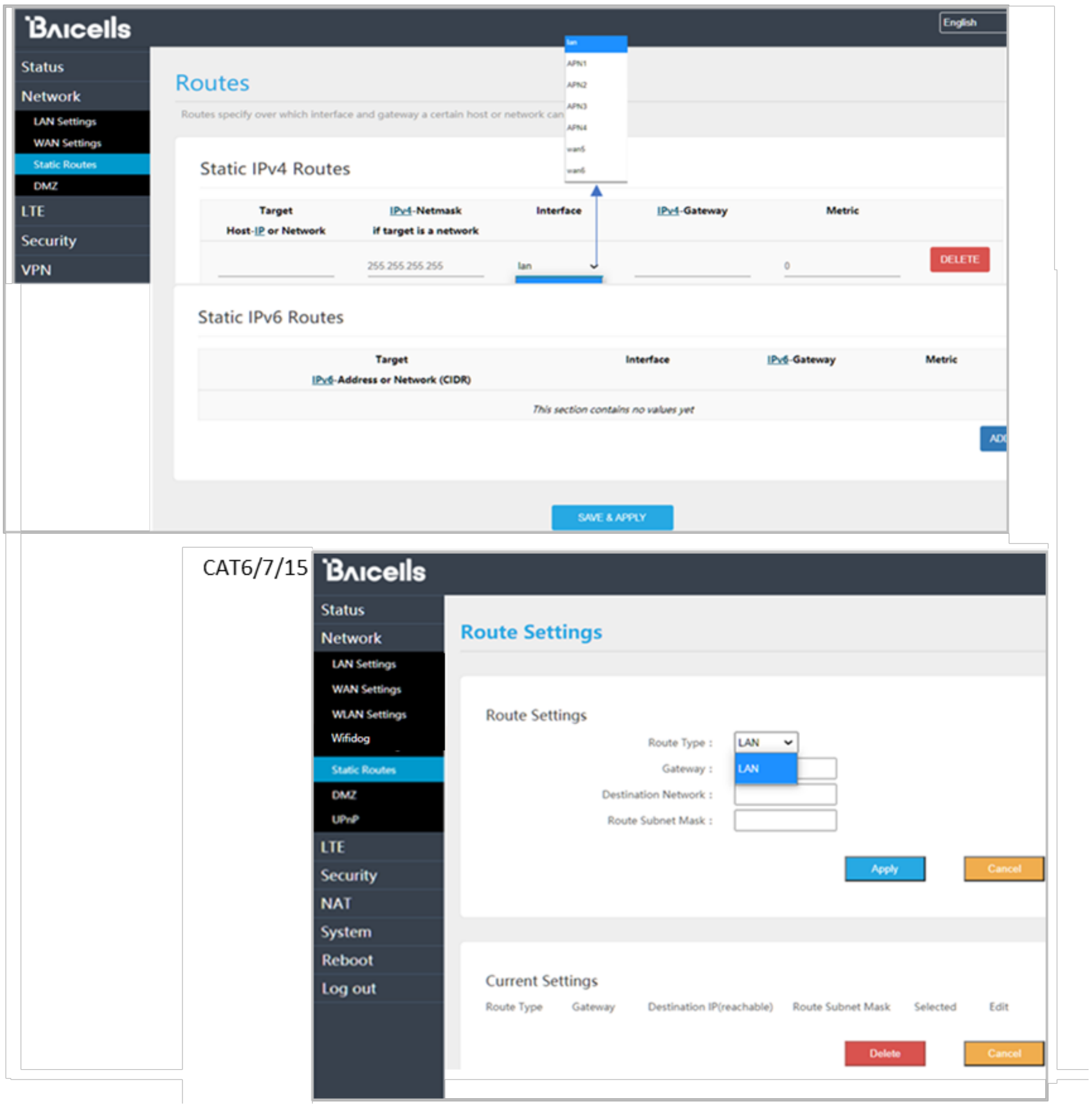
Routes specify over which interface and gateway a certain host or network can be reached. Static routes are typically used in small local networks where the routing table entries are populated manually.

To enable one or more static routes, go to *Network > Static Routes* (Figure 4-9). The CAT4 GUI separates IPv4 and IPv6 routes. To add a static route, enter the Target Host-IP or Network address, the Netmask, the type of Interface (lan, APN1, APN2, APN3, APN4, wan5, or wan6), and the Gateway. Click on *ADD*.

In the CAT6/7/15 GUI, select the route type (LAN), and enter the gateway, destination network, and route subnet mask. The configured routes will display at the bottom of the window.

Figure 4-9: Static Routes

CAT4



Routes

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

Static IPv4 Routes

Target Host-IP or Network	IPv4-Netmask if target is a network	Interface	IPv4-Gateway	Metric	
	255.255.255.255	lan		0	DELETE

Static IPv6 Routes

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

CAT6/7/15

Route Settings

Route Settings

Route Type : LAN

Gateway :

Destination Network :

Route Subnet Mask :

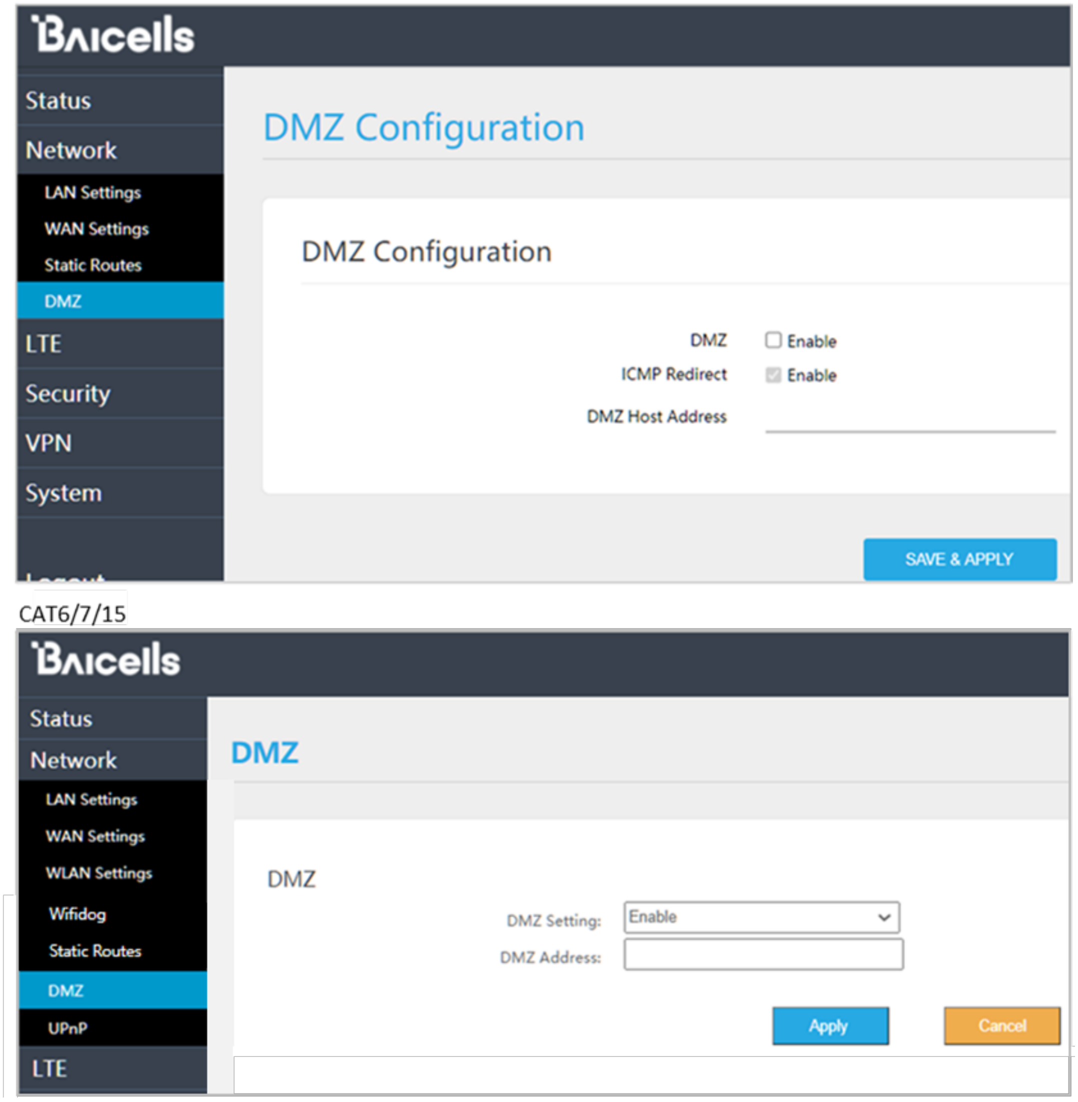
Current Settings

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

4.6 DMZ

The DMZ refers to a firewall between incoming WAN traffic and the LAN to which the CPE is connected. When the LAN has a DMZ server, you can enable DMZ for the CPE so that packets from the WAN are sent directly to the DMZ server. Optionally, in the CAT4 GUI you can enable Internet Control Message Protocol (ICMP) redirect error messages to an ICMP server. Refer to Figure 4-10.

Figure 4-10: DMZ



CAT4

DMZ Configuration

DMZ Configuration

DMZ ☐ Enable

ICMP Redirect ☑ Enable

DMZ Host Address

CAT6/7/15

DMZ

DMZ

DMZ Setting: Enable

DMZ Address:

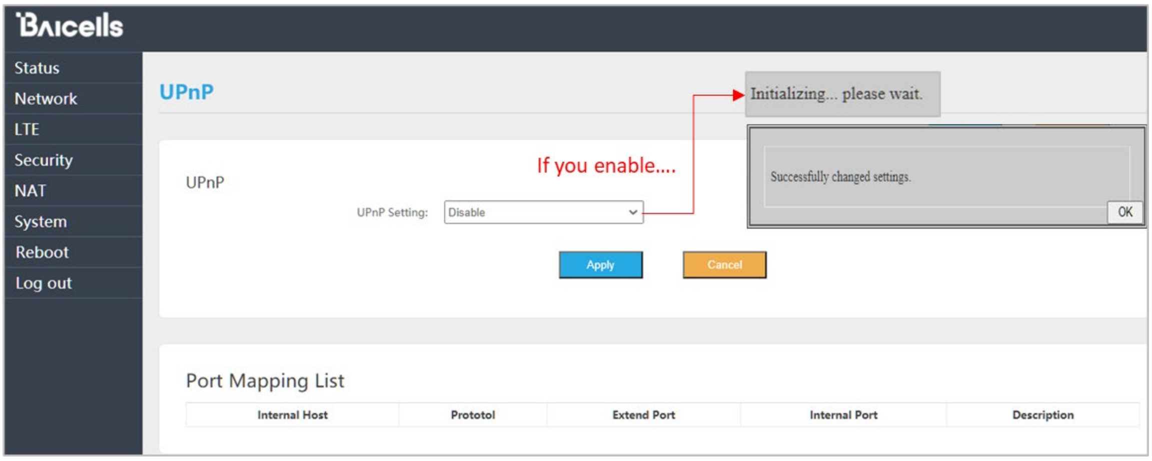
4.7 UPnP (CAT6/7/15)

NOTE: For CAT4, Universal Plug-n-Play (UPnP) is under the *Security* menu (*section 6.12*).

The UPnP function provides a set of networking protocols that allow device-to-device networking on a local network. When UPnP is enabled, devices seamlessly discover each other's presence on the local network and attach dynamically to one another and to network services. Typically, UPnP is reserved for residential or private networks and not used in an enterprise environment as it may consume too many resources in a network with many devices.

When you enable UPnP (Figure 4-11), you will receive a message that the system is initializing, and then it will indicate the change was successful. To remove UPnP, simply select *Disable* and the system will again prompt that it is initializing. Any redirects of traffic will display in the *Port Mapping List* at the bottom of the window, showing the host name, protocol, extended port, internal port, and a description.

Figure 4-11: UPnP (CAT6/7/15)



Initializing... please wait.

Successfully changed settings.

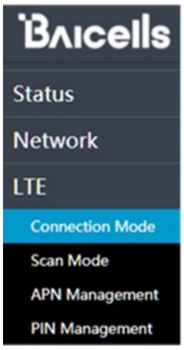
Internal Host	Prototol	Extend Port	Internal Port	Description

5 LTE Menu

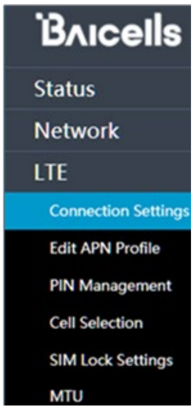
The *LTE* menu for CAT4 and CAT6/7/15 contains sub-menus for how users connect to the network through the CPE, frequency scanning settings, APN management, and PIN management. In addition, CAT6/7/15 also provides Edit APN Profile, SIM Lock Settings, and MTU settings (Figure 5-1). All LTE sub-menus are described in this section.

Figure 5-1: LTE Menu

CAT4



CAT6/7/15

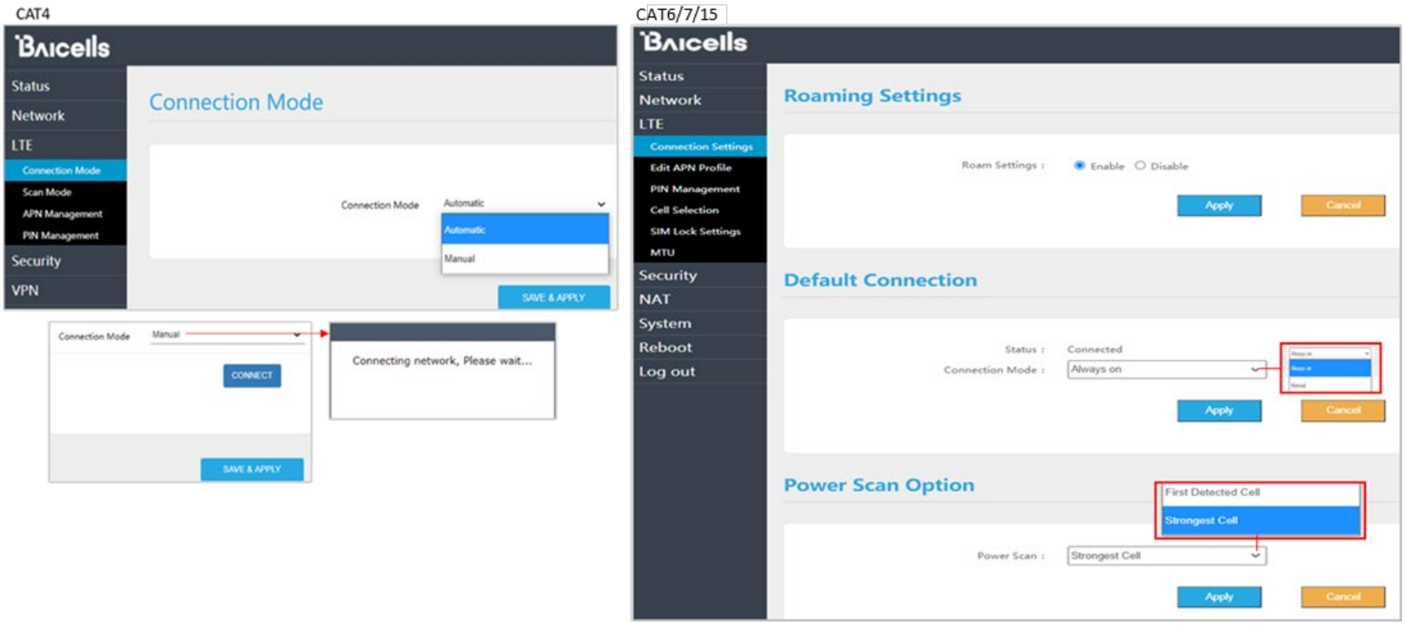


5.1 Connection Mode / Connection Settings

Looking at the top of the CAT4 *Connection Mode* window (Figure 5-2), you can set the CPE connection mode to *Automatic* to connect automatically to the network (assuming the user has inserted a valid SIM card), or you can set the connection mode to *Manual*, where the user has to select *CONNECT* to connect to the network each time.

In the CAT6/7/15 GUI the *Roaming Settings* pane is used to enable roaming for the CPE, allowing the user to access other PLMN networks. When disabled, the CPE accesses the PLMN as programmed on the SIM card. The *Default Connection* pane shows the connection status and mode. The mode can be set to *Always on* or *Manual*. If set as *Manual*, the user will have to manually connect to the network each time. In the *Power Scan Option* pane, select either *First Detected Cell* or with the *Strongest Cell*.

Figure 5-2: Connection Mode/Settings

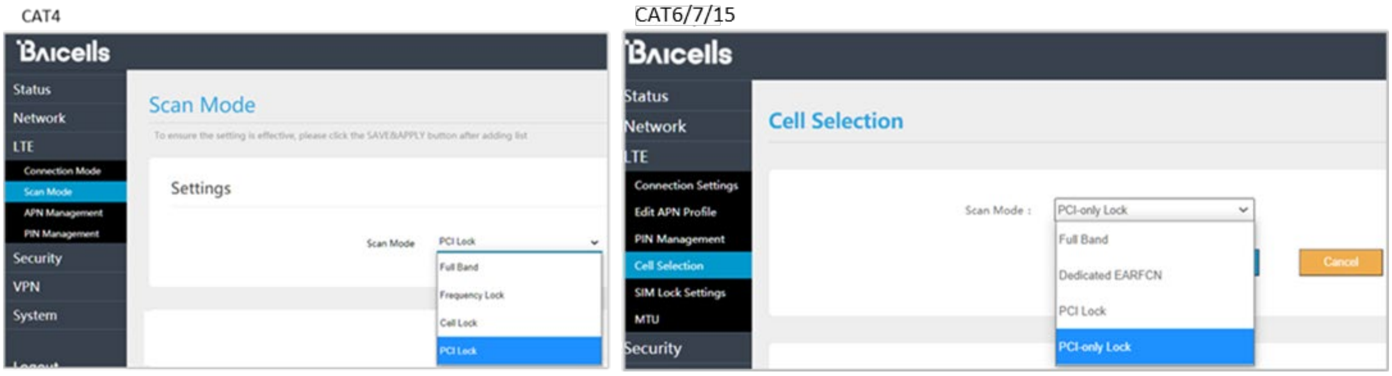


5.2 Scan Mode (CAT4) / Cell Selection (CAT6/7/15)

The *Scan Mode* sub-menu, as it is called in the CAT4 GUI, and *Cell Selection*, the sub-menu name in CAT6/7/15, determines which frequencies the CPE's routine scan of available frequencies will cover. When scanning, the CPE tunes to a specific frequency and measures the simplest signal quality - Received Signal Strength Indication (RSSI).

As part of the cell selection and reselection process, the CPE performs the scan first and then selects a small number of candidate cells to go through the next step of measuring and evaluating signals to select the best eNB to serve it. There are four different scanning options, as shown in Figure 5-3. The mode names vary slightly between CAT4 and CAT6/7/15, but function essentially the same.

Figure 5-3: Scan Mode (CAT4) / Cell Selection (CAT6/7/15)



Each of the modes is explained below.

- ***Full Band*** – Default setting. The CPE will routinely scan all channels in the band, which can make the time it takes to connect to the network longer than the other modes. The band is dependent on the CPE model.
- ***Frequency Lock* or *Dedicated EARFCN*** – You can specify which frequencies or EARFCNs the CPE will

scan when it is first powered on. If the CPE cannot connect to the network after scanning the list, it will scan other supported bands and frequencies. You can add up to 10 EARFCNs or frequencies.

- ***Cell Lock* or *PCI Lock*** - A combination of Physical Cell Identifier (PCI) + EARFCN or frequency. The CPE will scan only the list of eNBs with the PCI and EARFCN combination, which accelerates network access time.
- ***PCI-only Lock*** – You can lock the CPE to a designated PCI or PCI range.

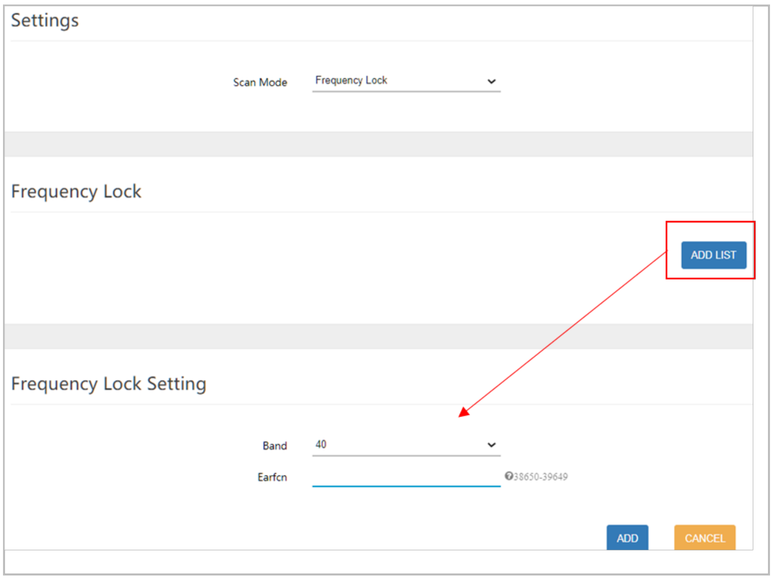
If you wish to leave the scan mode as Full Band, you do not need to make any configuration changes in this menu. The procedures for configuring the other three modes are described for CAT4 and for CAT6/7/15 in the sections that follow.

5.2.1 CAT4

Following are the procedures for configuring Frequency Lock, Cell Lock, and PCI Lock on a CAT4 CPE.

- Frequency Lock (Figure 5-4)
  1. For *Scan Mode*, select *Frequency Lock* from the pull-down menu.
  2. Click on *ADD LIST* to open the *Frequency Lock Setting* pane.
  3. Select the *Band* number, and enter the *Earfcn*.
  4. Click on *ADD*.

Figure 5-4: Frequency Lock (CAT4)



Settings

Scan Mode: Frequency Lock

Frequency Lock

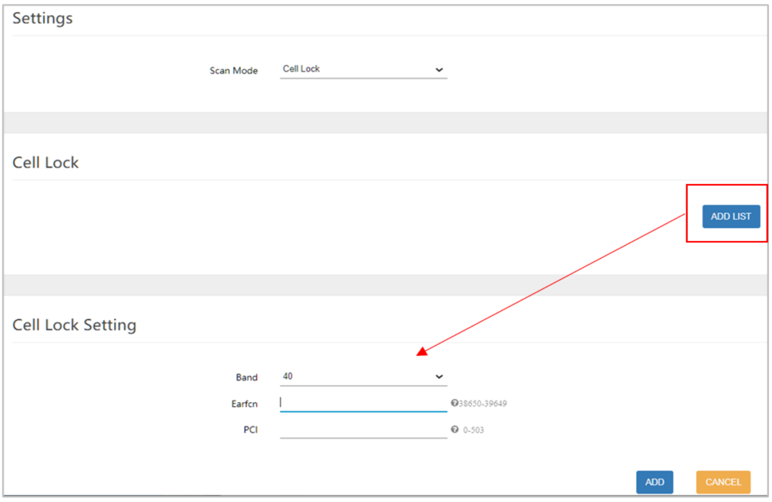
Frequency Lock Setting

Band: 40

Earfcn: 38650-39649

- Cell Lock (Figure 5-5)
  1. For *Scan Mode*, select *Cell Lock* from the pull-down menu.
  2. Click on *ADD LIST* to open the *Cell Lock Setting* pane.
  3. Select the *Band* number, and enter the *Earfcn* and *PCI* number combination.
  4. Click on *ADD*.

Figure 5-5: Cell Lock (CAT4)



Settings

Scan Mode: Cell Lock

Cell Lock

Cell Lock Setting

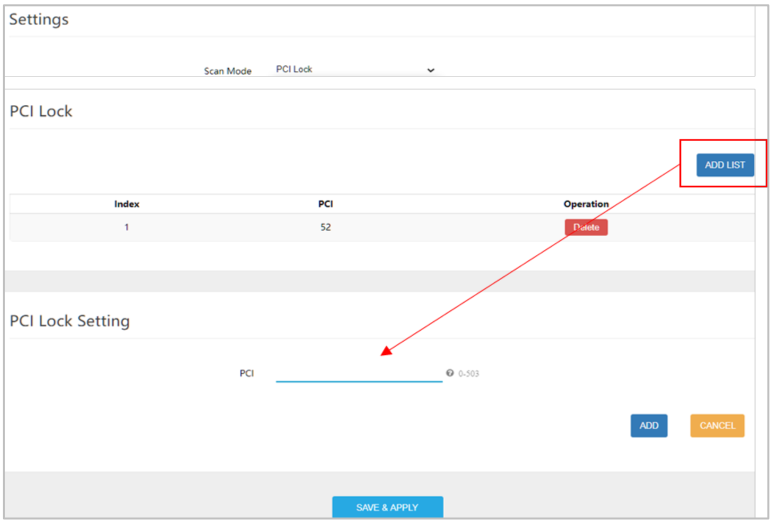
Band: 40

Earfcn: 38650-39649

PCI: 0-503

- PCI Lock (Figure 5-6)
    1. For *Scan Mode*, select *PCI Lock* from the pull-down menu.
    2. Click on *ADD LIST* to open the *PCI Lock Setting* pane.
    3. Enter the *PCI* number.
    4. Click on *ADD*. Then, click *SAVE & APPLY*.

Figure 5-6: PCI Lock (CAT4)



Settings

Scan Mode: PCI Lock

PCI Lock

Index	PCI	Operation
1	52	Delete

PCI Lock Setting

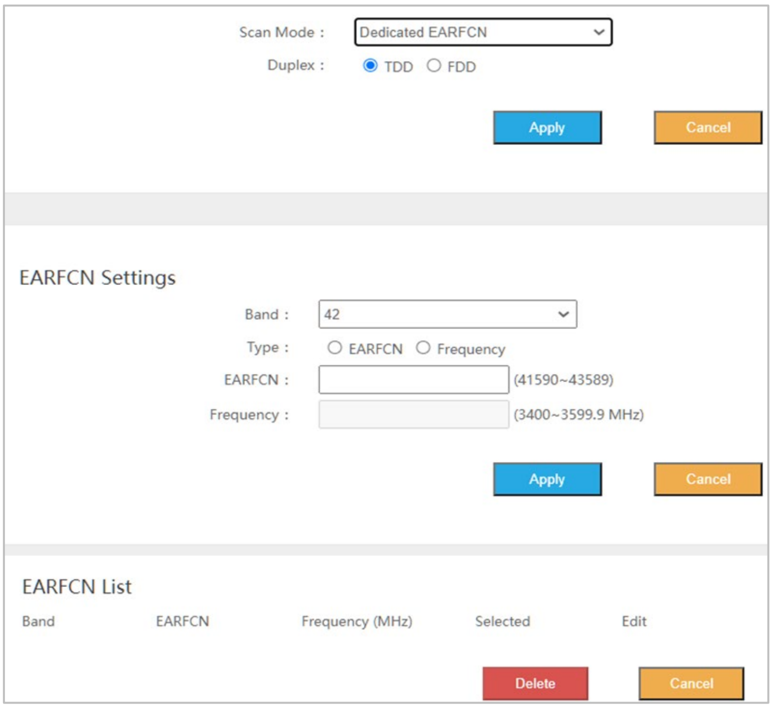
PCI: 0-503

5.2.2 CAT6/7/15

Following are the procedures for configuring Dedicated EARFCN, PCI Lock, and PCI-only Lock on a CAT6/7/15 CPE.

- Dedicated EARFCN (Figure 5-7)
    1. For *Scan Mode*, select *Dedicated EARFCN* from the pull-down menu.
    2. Identify the CPE LTE duplexing mode, *TDD* or *FDD*, and then select *Apply*.
    3. In the *EARFCN Settings* pane, choose the *Band* number from the pull-down menu.
    4. Select either *EARFCN* or *Frequency*, and enter the associated number to identify the EARFCN or frequency.
    5. Click on *Apply*. The configuration will appear in the *EARFCN List* in the bottom pane.

Figure 5-7: Dedicated EARFCN (CAT6/7/15)



Scan Mode : Dedicated EARFCN

Duplex : ● TDD ○ FDD

EARFCN Settings

Band : 42

Type : ○ EARFCN ○ Frequency

EARFCN : (41590~43589)

Frequency : (3400~3599.9 MHz)

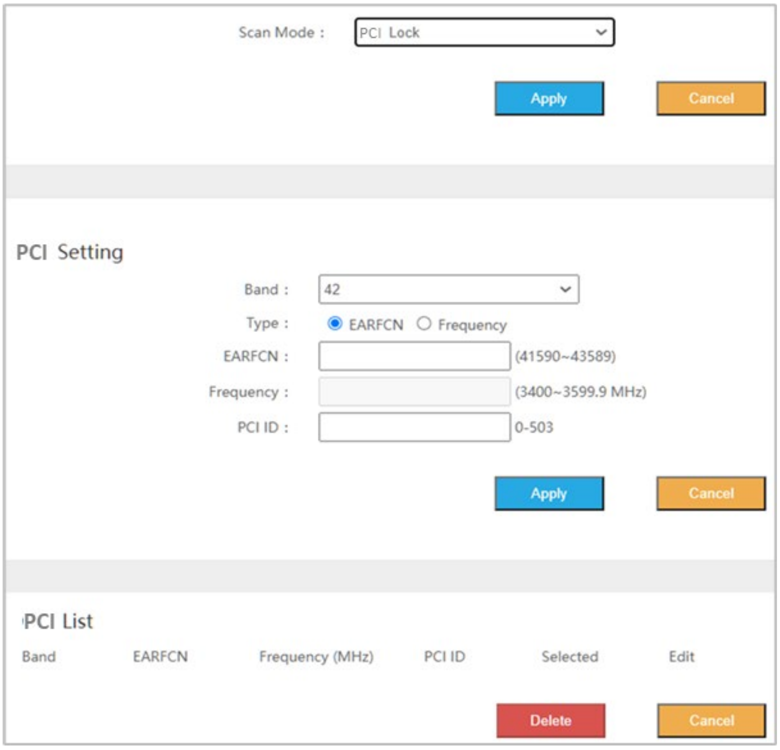
EARFCN List

Band	EARFCN	Frequency (MHz)	Selected	Edit

- PCI Lock (Figure 5-8)

1. For *Scan Mode*, select *PCI Lock* from the pull-down menu, and click on *Apply*.
2. In the *PCI Setting* pane, select the *Band* number from the pull-down menu.
3. For *Type*, choose either *EARFCN* or *Frequency,* and enter the associated number.
4. Enter a *PCI ID* number, (0-503) and click on *Apply*. The configuration will appear in the *PCI List* in the bottom pane.

Figure 5-8: PCI Lock (CAT6/7/15)



Scan Mode : PCI Lock

PCI Setting

Band : 42

Type : ● EARFCN ○ Frequency

EARFCN : (41590~43589)

Frequency : (3400~3599.9 MHz)

PCI ID : 0-503

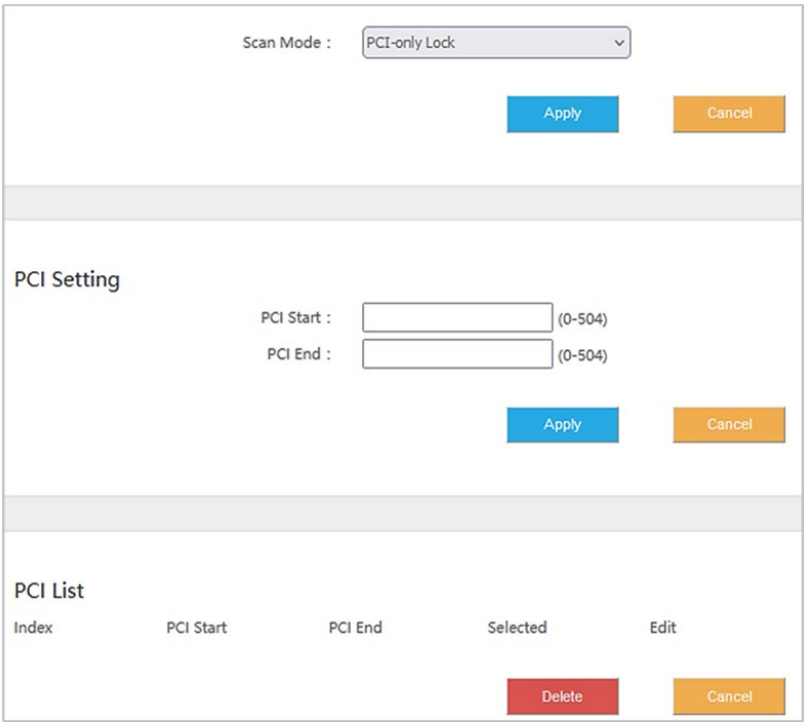
PCI List

Band	EARFCN	Frequency (MHz)	PCI ID	Selected	Edit

- PCI-only Lock (Figure 5-9)

    1. For *Scan Mode*, select *PCI-only Lock* from the pull-down menu, and click on *Apply*.
    2. In the *PCI Setting* pane, enter the *PCI Start* and *PCI End* numbers.
    3. Click on *Apply*. The configuration will appear in the *PCI List* in the bottom pane.

Figure 5-9: PCI-only Lock (CAT6/7/15)



Scan Mode : PCI-only Lock

5.3 APN Management (CAT4) / Edit APN Profile (CAT6/7/15)

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 traffic, voice, data, etc., and may support different services and QoS levels.

The CAT4 CPE supports up to four APN configurations, while CAT6/7/15 supports eight APNs. In both cases, APN1 must be configured when the CPE to eNB communications connect to the Baicells CloudCore using TR-069.

NOTE: If you are using a Local EPC, typically you would configure the APNs in the core.

5.3.1 CAT4

To configure an APN profile on a CAT4 CPE:

1. Go to *LTE > APN Management* (Figure 5-10).
2. Select the *APN Number* - 1, 2, 3, or 4 - to configure, and select the *Enable* checkbox. *NAT* mode is the default. If desired, use the pull-down menu to select *Bridge* mode.
3. Enter an *APN Name* for this gateway.
4. Enter the *MTU* size of a packet that can be sent on this APN. The range is 576-1500 bytes.

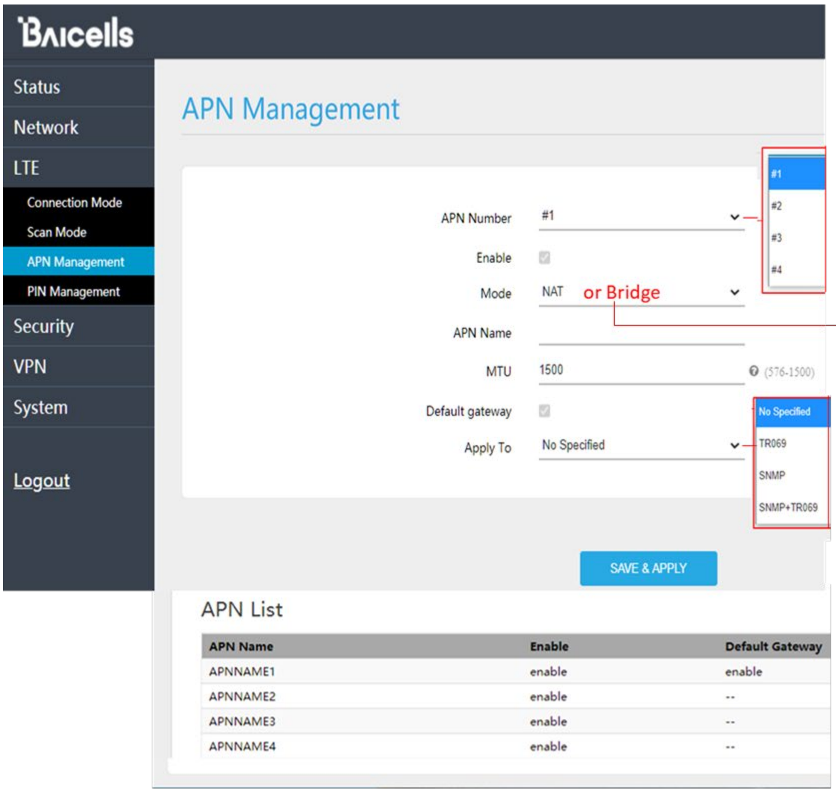
NOTE: For CAT6/7/15, refer to the *LTE > MTU* sub-menu (*section 5.6*).

5. Select the checkbox for *Default gateway* if you want this APN to serve as the default APN for this CPE.

6. In the *Apply To* field, choose either *No Specified*, *TR069*, *SNMP*, or *SNMP+TR069* to indicate which protocol can be used to collect information about the eNBs to which this CPE can connect.

7. Click on SAVE & *APPLY*. The configuration will appear in the *APN List* in the bottom pane.

Figure 5-10: APN Management (CAT4)



APN Management

APN Number: #1

Enable: ☑

Mode: NAT or Bridge

APN Name:

MTU: 1500 (576-1500)

Default gateway: ☑

Apply To: No Specified

APN List

APN Name	Enable	Default Gateway
APNNAME1	enable	enable
APNNAME2	enable	--
APNNAME3	enable	--
APNNAME4	enable	--

NAT mode is the default, so when *Network > WAN Settings* is set to *NAT* the *Mode* field here doesn't display.

When *Network > WAN Settings* is set to *Bridge* the *Mode* field here displays with a pull-down menu *NAT* or *Bridge* option.

5.3.2 CAT6/7/15

To edit and enable an APN profile on a CAT6/7/15 CPE:

Go to *LTE > Edit APN Profile* (Figure 5-11) to display the *APN Profile* window.

1. In the *APN Profile List*, select the radio button under *Edit*. The current settings for that APN will display under *APN Profile Settings*.

2. When you are ready to execute the edits, select the *Enable* checkbox.

3. Enter a *Profile Name* and an *APN* number or description.

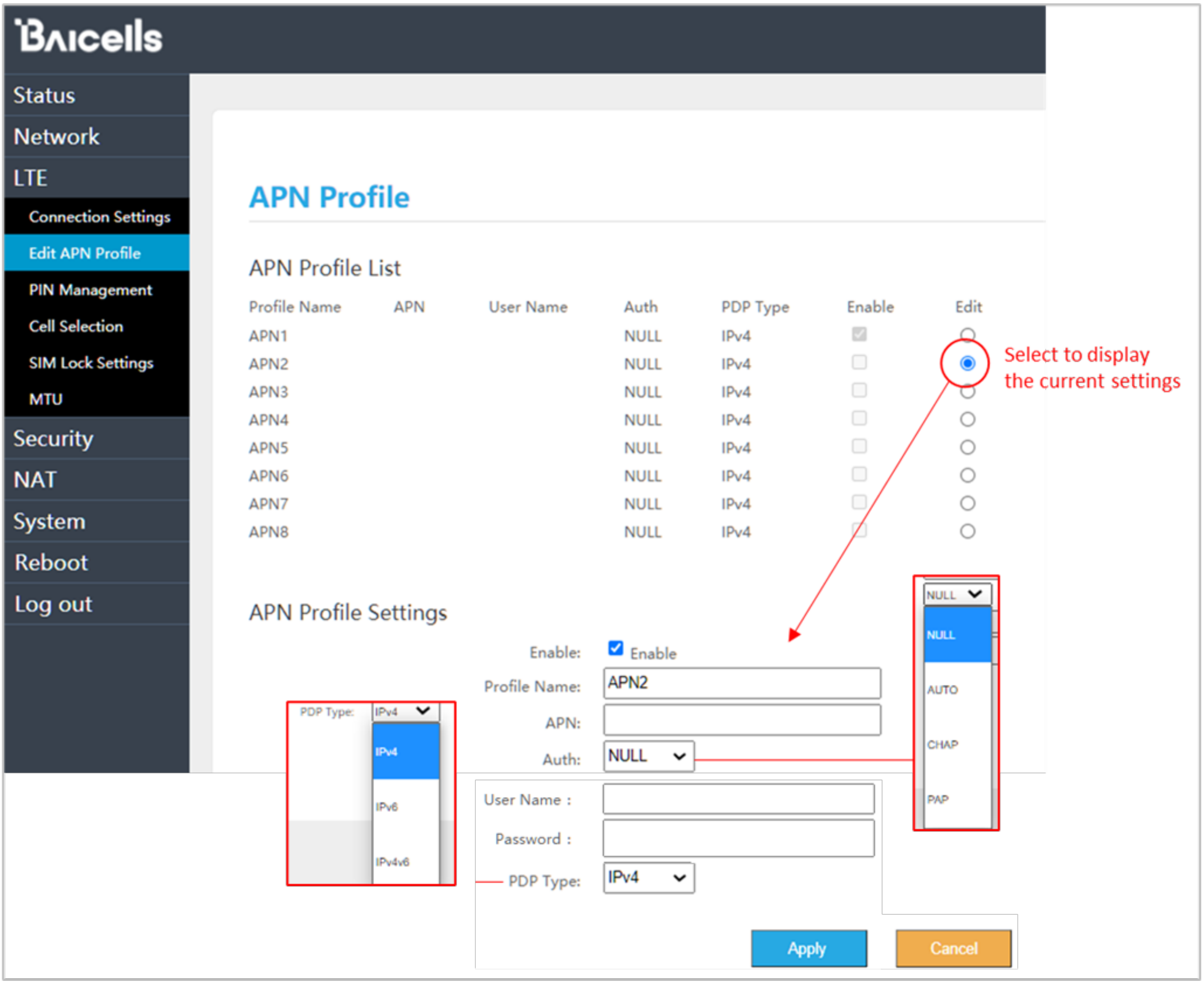
4. For *Auth*, select *NULL*, *AUTO*, *CHAP*, or *PAP* for the type of authentication required to access the APN.

5. Optionally, enter a *User Name* and *Password* to access the APN.

6. Select the *PDP Type*, or type IP addressing - *IPv4*, *IPv6*, or *IPv4v6* - supported on this interface.

7. Click on *Apply* to execute the changes.

Figure 5-11: Edit APN Profile (CAT6/7/15)



APN Profile

APN Profile List

Profile Name	APN	User Name	Auth	PDP Type	Enable	Edit
APN1			NULL	IPv4	☑	○
APN2			NULL	IPv4	□	●
APN3			NULL	IPv4	□	○
APN4			NULL	IPv4	□	○
APN5			NULL	IPv4	□	○
APN6			NULL	IPv4	□	○
APN7			NULL	IPv4	□	○
APN8			NULL	IPv4	□	○

APN Profile Settings

Enable: ☑ Enable
Profile Name: APN2
APN:
Auth: NULL
User Name :
Password :
PDP Type: IPv4

5.4 PIN Management

You can configure a CPE login Personal Identification Number (PIN) using the *LTE > PIN Management* sub-menu. If a user attempts to access the Internet through the CPE but does not have the PIN or enters the wrong PIN, they will be denied access.

The *USIM Status* field indicates if the CPE's SIM card is inserted and available (CAT4), and the *USIM Card Status* field in CAT6/7/15 will indicate if a PIN is enabled or disabled. The USIM card must be available before you can configure a PIN or access the Internet through the CPE.

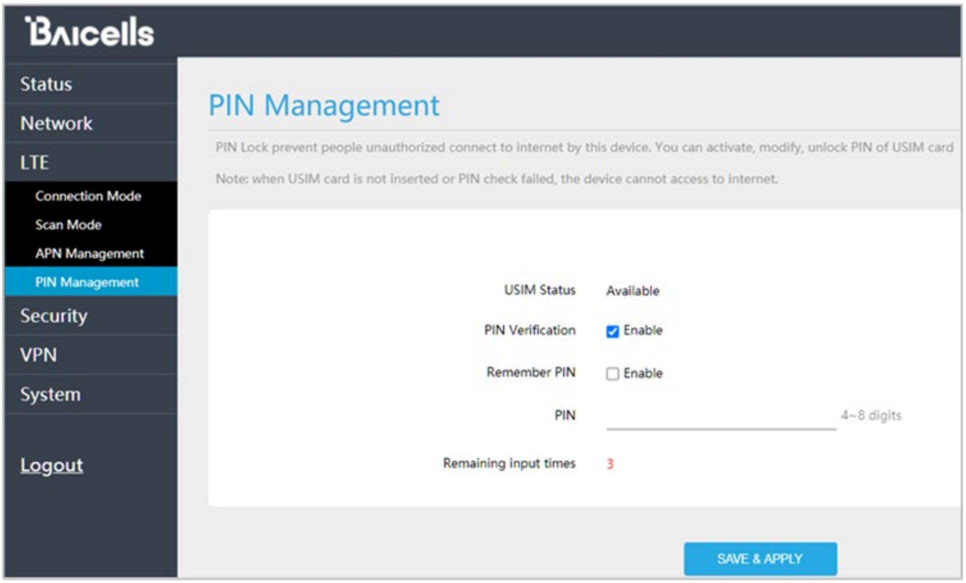
The *PIN Verification* field initially is not enabled. If you click on the checkbox next to *Enable*, it opens up the field where you can enter the PIN number that users will need (Figure 5-12). The PIN number can be four to eight digits, using numbers only. In the CAT4 GUI, you have the option to enable *Remember PIN*.

In CAT6/7/15, the *Remain Attempts* field indicates the maximum number of times (three) that a user can try to enter the correct PIN before getting locked out. If this happens, contact support.

Important: You will need the PIN number before you can modify the PIN Management settings. Be sure to record the PIN that you enter.

Figure 5-12: PIN Management

CAT4



PIN Management

PIN Lock prevent people unauthorized connect to internet by this device. You can activate, modify, unlock PIN of USIM card

Note: when USIM card is not inserted or PIN check failed, the device cannot access to internet.

USIM Status: Available

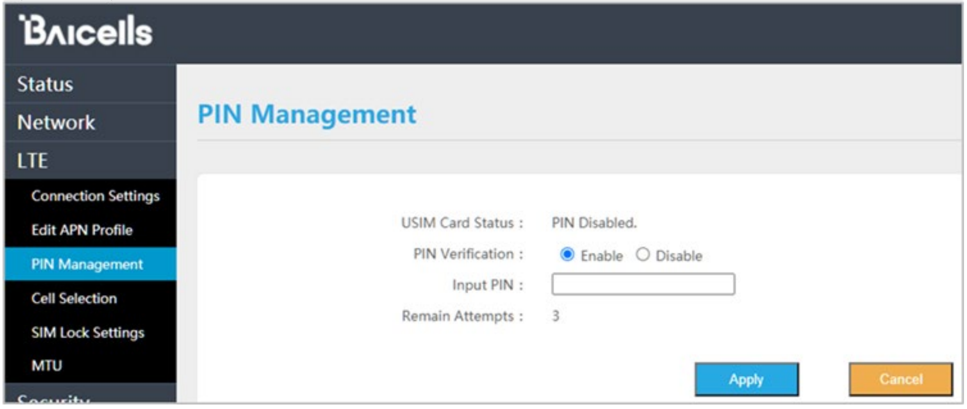
PIN Verification: ☑ Enable

Remember PIN: □ Enable

PIN: 4~8 digits

Remaining input times: 3

CAT6/7/15



PIN Management

USIM Card Status : PIN Disabled.

PIN Verification : ● Enable ○ Disable

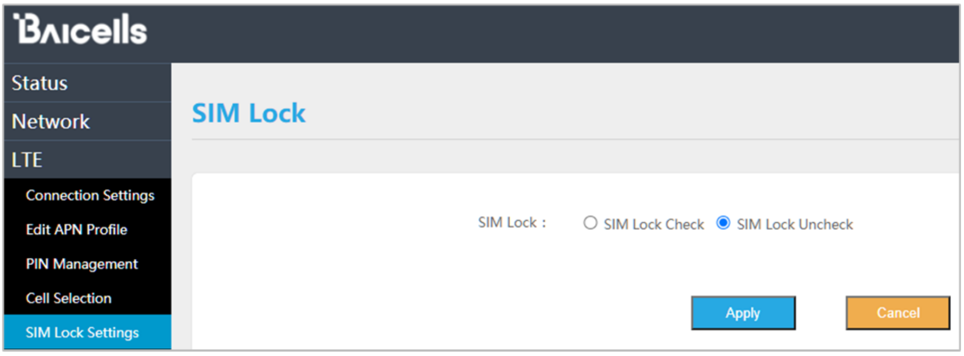
Input PIN :

Remain Attempts : 3

5.5 SIM Lock Settings (CAT6/7/15)

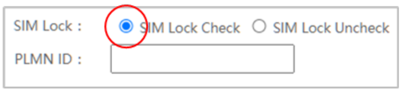
Use the *LTE > SIM Lock Settings* sub-menu to lock the CPE's SIM card to a specific operator's network using the Public Land Mobile Network (PLMN) identification number. By default, the *SIM Lock* is set to *SIM Lock Uncheck*. To enable, select the *SIM Lock Check* radio button, enter the *PLMN ID*, and click *Apply* (Figure 5-13). When enabled, the CPE will be able to attach only to that PLMN operator network.

Figure 5-13: SIM Lock Settings (CAT6/7/15)



SIM Lock

SIM Lock : ○ SIM Lock Check ● SIM Lock Uncheck



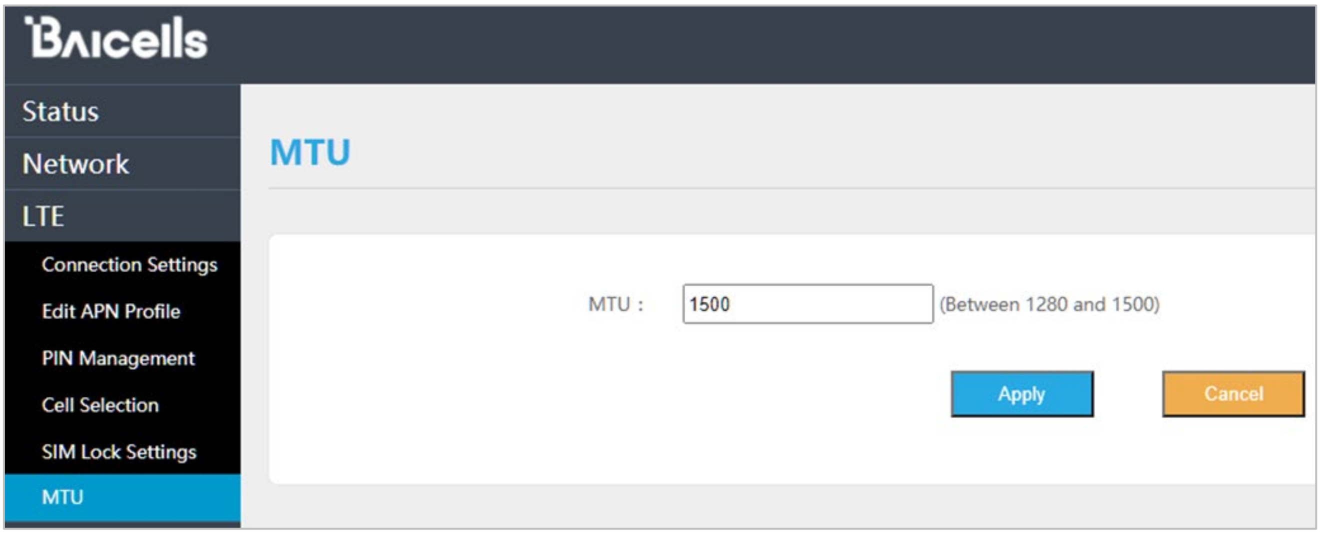
SIM Lock : ● SIM Lock Check ○ SIM Lock Uncheck

PLMN ID :

5.6 MTU (CAT6/7/15)

While the CAT4 GUI contains the MTU setting as part of the APN Management configuration (*section 5.3.1*), in CAT6/7/15 the *MTU* sub-menu is located under the *LTE* menu (Figure 5-14). The MTU pertains to the WAN (LTE) connection, and the range is 1280 to 1500 bytes you can enter to set the maximum data packet size that can be transmitted to/from this CPE.

Figure 5-14: MTU (CAT6/7/15)

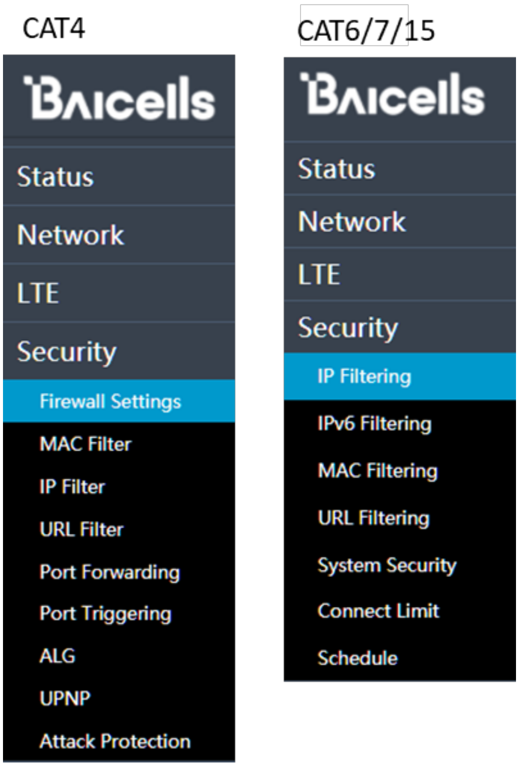


MTU : 1500 (Between 1280 and 1500)

6 Security Menu

The *Security* menu provides several protection feature options, and varies between CAT4 and CAT6/7/15 CPEs (Figure 6-1). Each sub-menu is described in this section.

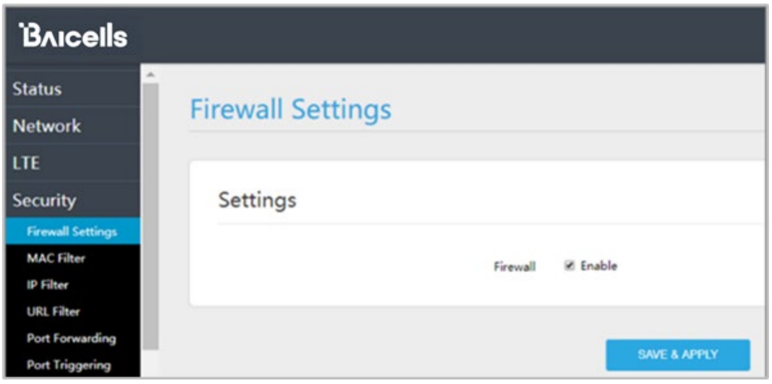
Figure 6-1: Security



6.1 Firewall Settings (CAT4)

When you select the *Security* menu it opens to the *Firewall Settings* window (Figure 6-2). If you enable the firewall by clicking on the checkbox, the other sub-menus under *Security* allow you to configure the firewall's MAC filter, IP filter, and so forth.

Figure 6-2: Firewall Settings (CAT4)

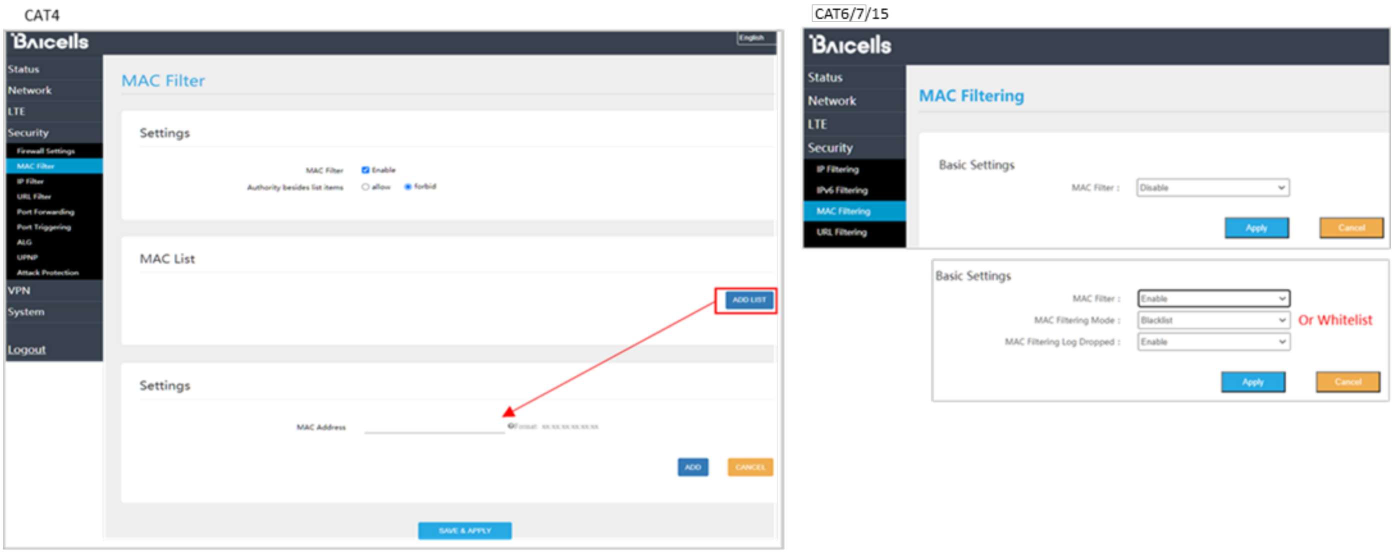


Firewall ☑ Enable

6.2 MAC Filter/Filtering

The Media Access Control Filter (*MAC Filter*) allows you to identify a list of devices either allowed/whitelisted to access or forbidden/blacklisted from accessing the network (Figure 6-3). Refer to the configuration procedure for CAT4 and for CAT6/7/15 in the following two sections.

Figure 6-3: MAC Filter/Filtering



MAC Filter ☑ Enable
Authority besides list items ○ allow ● forbid

MAC Address ________ Format: xx:xx:xx:xx:xx:xx

MAC Filter : Disable

MAC Filter : Enable
MAC Filtering Mode : Blacklist
MAC Filtering Log Dropped : Enable

6.2.1 CAT4

To set up MAC filtering on a CAT4 CPE:

1. Go to the *Security* > *MAC Filter* sub-menu, and select the *Enable* checkbox for *MAC Filter*.
2. For the *Authority besides list items* field, select *allow* if you want to identify the MAC addresses of devices allowed to access the network through the CPE, or *forbid* to enter the MAC addresses of devices that will be denied access.

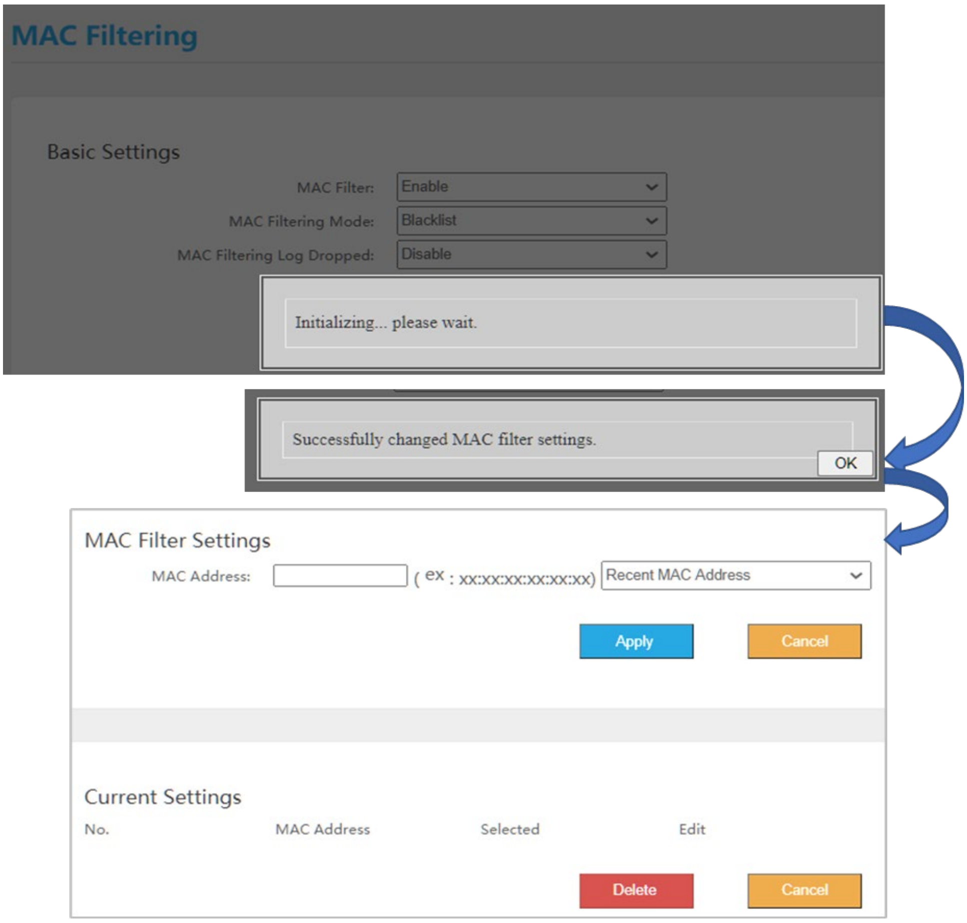
3. In the *MAC List* pane, select *ADD LIST*.
4. In the *Settings* pane, enter the first *MAC Address*, and click on *ADD*. To add more MAC addresses, repeat steps 3 and 4.
5. Click on *SAVE & APPLY* to implement the filtering configuration.

6.2.2 CAT6/7/15

To set up MAC filtering on a CAT6/7/15 CPE:

1. Go to the *Security > MAC Filtering* sub-menu to display the *MAC Filtering* window. Then, select *Enable* for *MAC Filter* in the *Basic Settings* window. Additional fields will appear.
2. For *MAC Filtering Mode*, select *Whitelist* if you want to identify the MAC addresses of devices allowed to access the network through the CPE, or select *Blacklist* to enter the MAC addresses of devices that will be denied access.
3. The *MAC Filtering Log Dropped* field can be used to enable or disable logs pertaining to dropped MAC addresses.
4. Click on *Apply*. The system will indicate it is initializing the changes and then display when the basic filter settings have been successfully changed (Figure 6-4). Click on *OK*.
5. In the *MAC Filter Settings* pane that pops up, enter the first *MAC Address*. Note that you can use the *Recent MAC Address* list to select an address. Click on *Apply*. The added MAC address will appear under the *Current Settings* pane, where you can edit or delete an address.
6. To add more addresses, repeat step 5.

Figure 6-4: MAC Filtering (CAT6/7/15)



MAC Filtering

Basic Settings

MAC Filter: Enable

MAC Filtering Mode: Blacklist

MAC Filtering Log Dropped: Disable

Initializing... please wait.

Successfully changed MAC filter settings.

MAC Filter Settings

MAC Address: (ex : xx:xx:xx:xx:xx:xx)

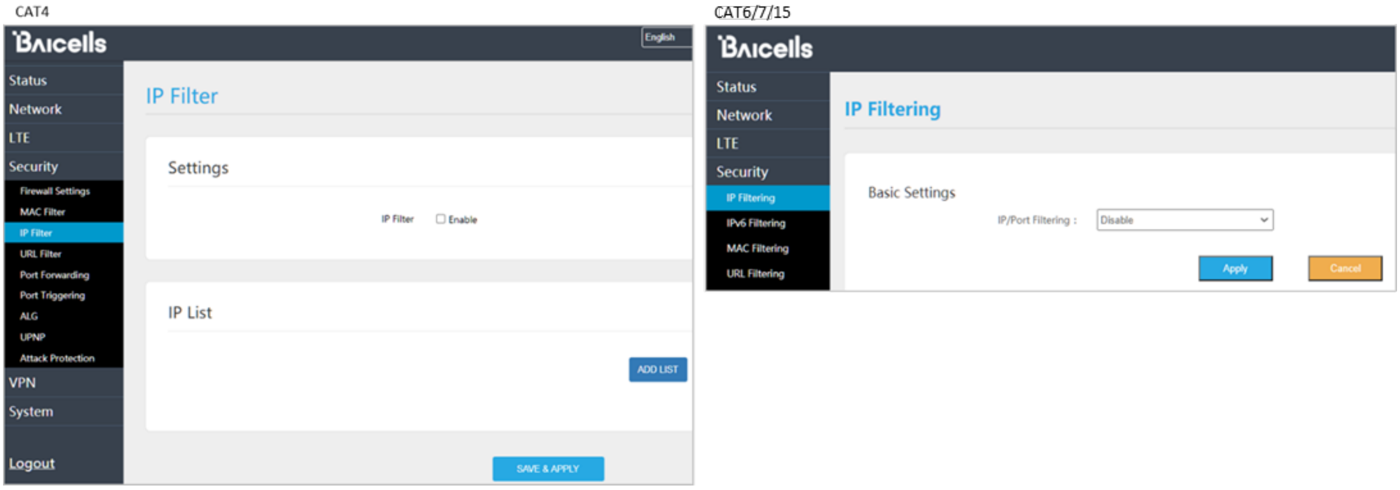
Current Settings

No.	MAC Address	Selected	Edit

6.3 IP Filter/Filtering

When using a firewall server in the local network, invoke this setting to enable the firewall for this CPE. You can define a list of devices either allowed/whitelisted to access or forbidden/blacklisted from accessing the network services (Figure 6-5). Refer to the configuration procedure for CAT4 and for CAT6/7/15 in the following two sections.

Figure 6-5: IP Filter/Filtering



CAT4

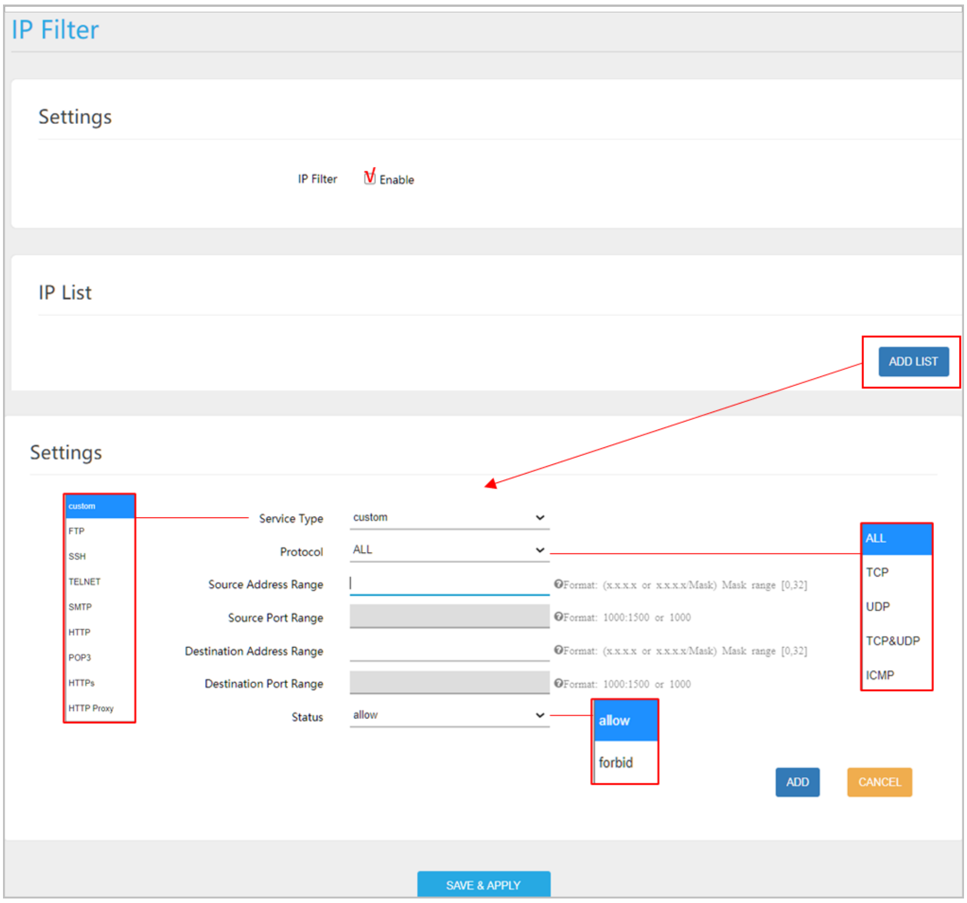
CAT6/7/15

6.3.1 CAT4

To set up IP filtering on a CAT4 CPE (Figure 6-6):

1. Go to the *Security > IP Filter* sub-menu to display the *IP Filter* window. Then, select the *Enable* checkbox for *IP Filter* in the *Settings* pane.
2. In the *IP List* pane, click on *ADD LIST* to open the *Settings* fields.
3. Select a *Service Type*: custom, FTP, SSH, TELNET, SMTP, HTTP, POP3, HTTPs, or HTTP Proxy
4. Select a *Protocol*: ALL, TCP, UDP, TCU&UDP, or ICMP
5. For *Source Address Range*, enter the beginning IP address or subnet mask, for example, x.x.x.x or x.x.x.x/mask.
6. To indicate a range of source addresses, enter the *Source Port Range*: 1000 to 1500, or 1000
7. Repeat steps 5 and 6, but this time enter the *Destination Address Range* and *Destination Port Range*.
8. For the range of addresses that you entered, in the *Status* field select *allow* if you want those services to be allowed through the CPE, or *forbid* if you want to deny those services through the CPE.
9. Click on *SAVE & APPLY* to implement the filtering configuration.

Figure 6-6: Enable IP Filtering on CAT4 CPE



IP Filter

Settings

IP Filter ☑ Enable

IP List

Settings

Service Type: custom

Protocol: ALL

Source Address Range: Format: (x.x.x.x or x.x.x.x/Mask) Mask range [0,32]

Source Port Range: Format: 1000:1500 or 1000

Destination Address Range: Format: (x.x.x.x or x.x.x.x/Mask) Mask range [0,32]

Destination Port Range: Format: 1000:1500 or 1000

Status: allow

6.3.2 CAT6/7/15

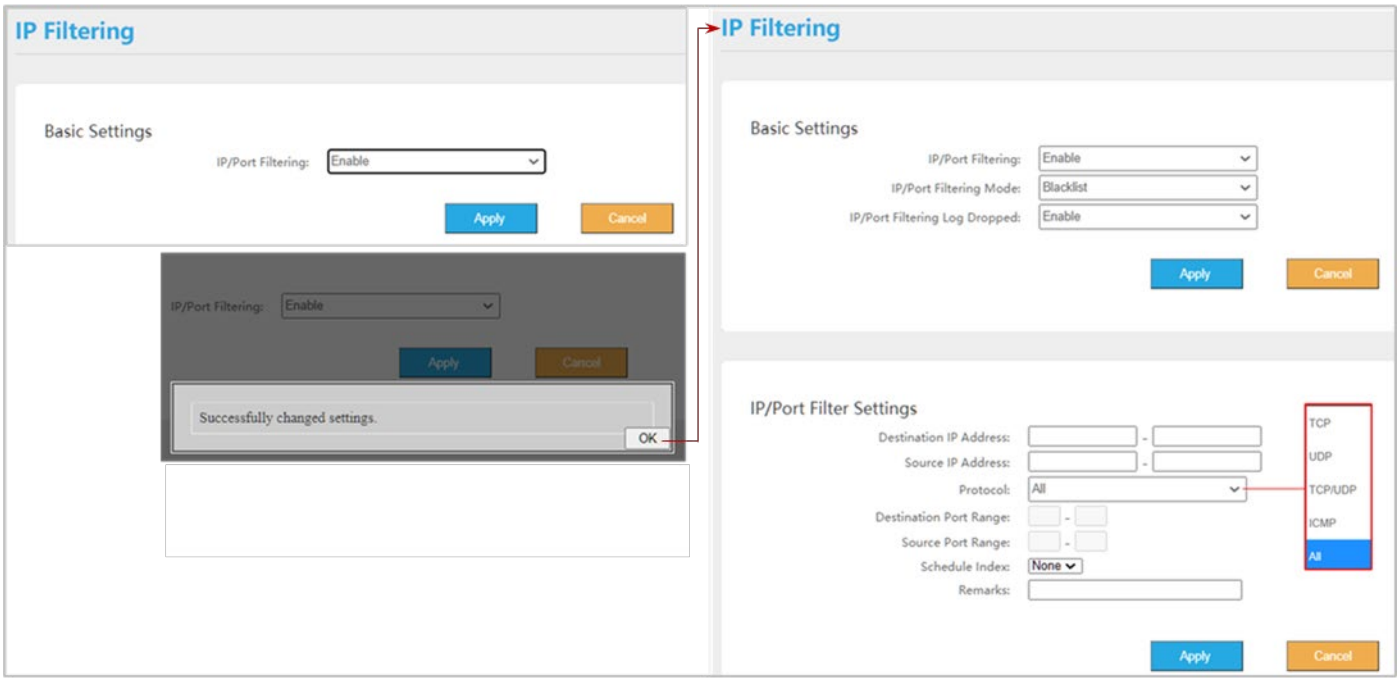
To set up IPv4 filtering on a CAT6/7/15 CPE (Figure 6-7):

NOTE: Refer to *section 6.4* for IPv6 Filtering.

1. Go to the *Security* > *IP Filtering* sub-menu to display the *IP Filtering* window. Then, select *Enable* from the pull-down menu for *IP/Port Filtering* in the *Basic Settings* pane.
2. Click on *Apply*. The system will initialize the setting change, and then display "*Successfully changed settings*". Click on *OK*.
3. In the *Basic Settings* pane, for *IP/Port Filtering Mode* select either *Blacklist* or *Whitelist*. Blacklisting services means they will not be allowed through the CPE. Whitelisting services means they will be allowed through the CPE.
4. In the *Basic Settings* pane, the *IP/Port Filtering Log Dropped* field can be used to enable or disable logs pertaining to dropped IP addresses.
5. In the *IP/Port Filter Settings* pane, enter the *Destination IP Address* range and the *Source IP Address* range.
6. Select the *Protocol* to filter: TCP, UDP, TCU&UDP, ICMP, or ALL
7. Enter the *Destination Port Range* and *Source Port Range* information.
8. The *Schedule Index* field allows you to enter the index number of a time schedule configured in *Security* > *Schedule* (*section 6.11*). Add any notes regarding this configuration in the *Remarks* text box.

9. Click on *Apply* to implement the filtering configuration.

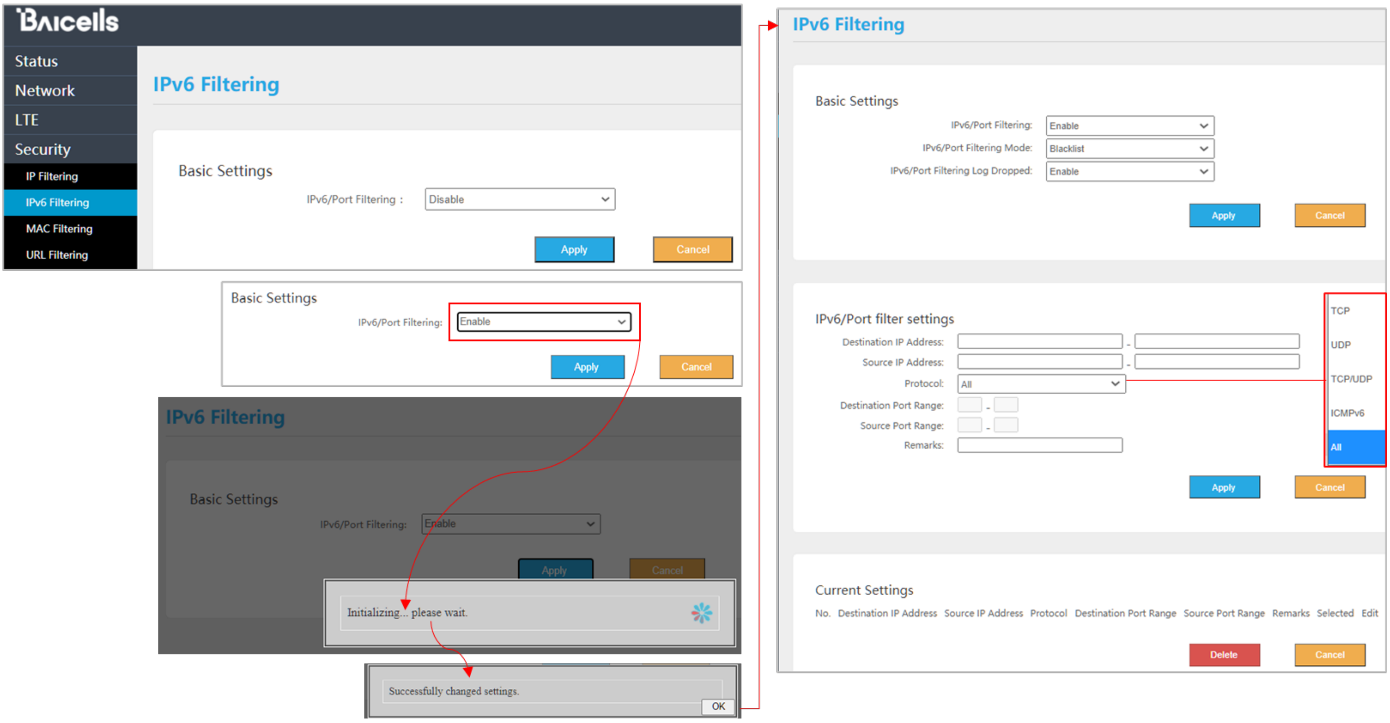
Figure 6-7: Enable IP Filtering on CAT6/7/15 CPE



6.4 IPv6 Filtering (CAT6/7/15)

The *Security > IPv6 Filtering* sub-menu in CAT6/7/15 essentially works the same way as *Security > IP Filtering*, explained in *section 6.3*, except the settings are specific to IPv6 traffic. Please refer to the procedure in *section 6.3*, noting the addition of "IPv6" in some of the *IPv6 Filtering* fields (Figure 6-8).

Figure 6-8: IPv6 Filtering (CAT6/7/15)


Baicells
Status
Network
LTE
Security
IP Filtering
IPv6 Filtering
MAC Filtering
URL Filtering
IPv6 Filtering
Basic Settings
IPv6/Port Filtering : Disable
Apply
Cancel
IPv6/Port Filtering: Enable
Initializing... please wait.
Successfully changed settings.
OK
IPv6 Filtering
IPv6/Port Filtering Mode: Blacklist
IPv6/Port Filtering Log Dropped: Enable
IPv6/Port filter settings
Destination IP Address:
Source IP Address:
Protocol: All
Destination Port Range:
Source Port Range:
Remarks:
TCP
UDP
TCP/UDP
ICMPv6
All
Current Settings
No. Destination IP Address Source IP Address Protocol Destination Port Range Source Port Range Remarks Selected Edit
Delete

6.5 URL Filter/Filtering

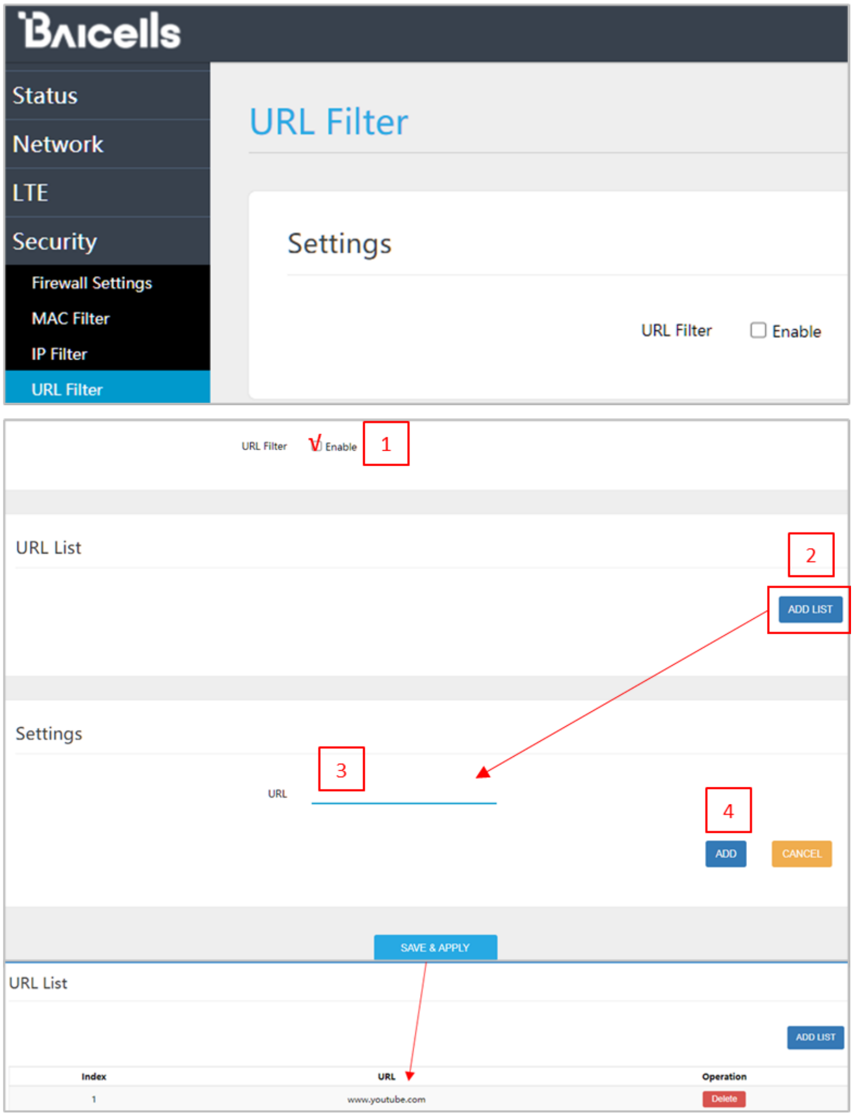
The Uniform Resource Location (URL) Filter allows you to define a list of URL addresses that CPE users are forbidden from accessing. The fields and procedures are slightly different between CAT4 and CAT6/7/15 CPEs. Each is explained in the following sections.

6.5.1 CAT4

To enable URL filtering on a CAT4 CPE (Figure 6-9):

1. Go to *Security* > *URL Filter*, and select the *Enable* checkbox for the *URL Filter* feature in the *Settings* pane.
2. In the top *URL List* pane, select *ADD LIST*.
3. In the *URL Settings* pane, enter the first *URL* address.
4. Click on *ADD*. The URL will be added in the bottom *URL List*. Repeat steps 3 and 4 to add more URLs.
5. When you've added all the desired URLs, then click on *SAVE & APPLY*.

Figure 6-9: URL Filter (CAT4)



URL Filter ✓ Enable

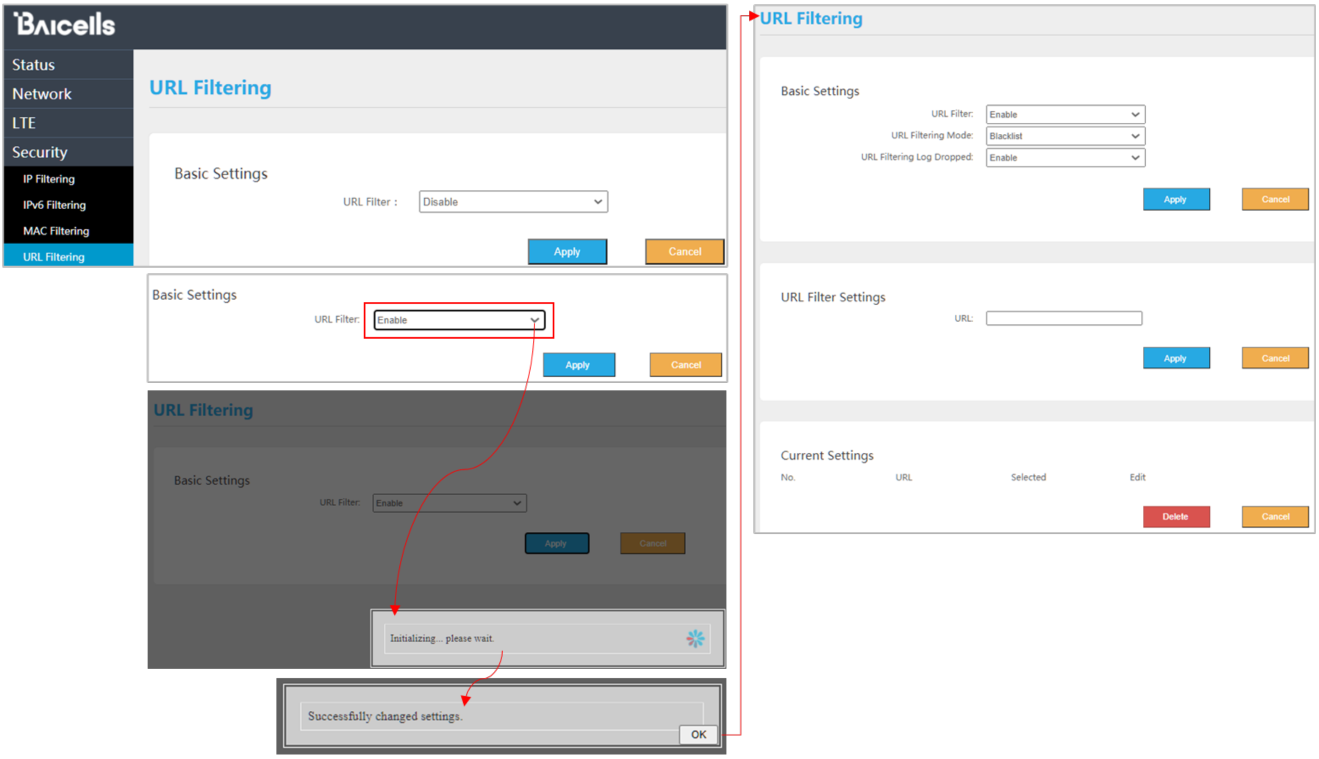
Index	URL	Operation
1	www.youtube.com	Delete

6.5.2 CAT6/7/15

To enable URL filtering on a CAT6/7/15 CPE (Figure 6-10):

1. Go to *Security* > *URL Filtering* to display the *URL Filtering* window. Then, select *Enable* from the pull-down menu for *URL Filter* in the *Basic Settings* pane.
2. Click on *Apply*. The system will initialize the setting change, and then display "*Successfully changed settings.*" Click on *OK*.
3. For *URL Filtering Mode*, select either *Blacklist* or *Whitelist* in the *Basic Settings* pane. Use *Blacklist* to enter the URL addresses that CPE users will not be allowed to access. Use *Whitelist* to identify URL addresses that CPE users will be allowed to access.
4. In the *Basic Settings* pane, the *URL Filtering Log Dropped* field can be used to enable or disable logs pertaining to dropped (allowed or denied) URL addresses.
5. In the *URL Filter Settings* pane, enter the first *URL* address and click on *Apply*. The URL will be added in the *Current Settings* list at the bottom of the *URL Filtering* window.
6. To add more URL addresses, repeat step 5.

Figure 6-10: URL Filtering (CAT6/7/15)



URL Filtering

Basic Settings

URL Filter : Disable

Basic Settings

URL Filter: Enable

Initializing... please wait.

Successfully changed settings.

URL Filtering

Basic Settings

URL Filter: Enable

URL Filtering Mode: Blacklist

URL Filtering Log Dropped: Enable

URL Filter Settings

URL:

Current Settings

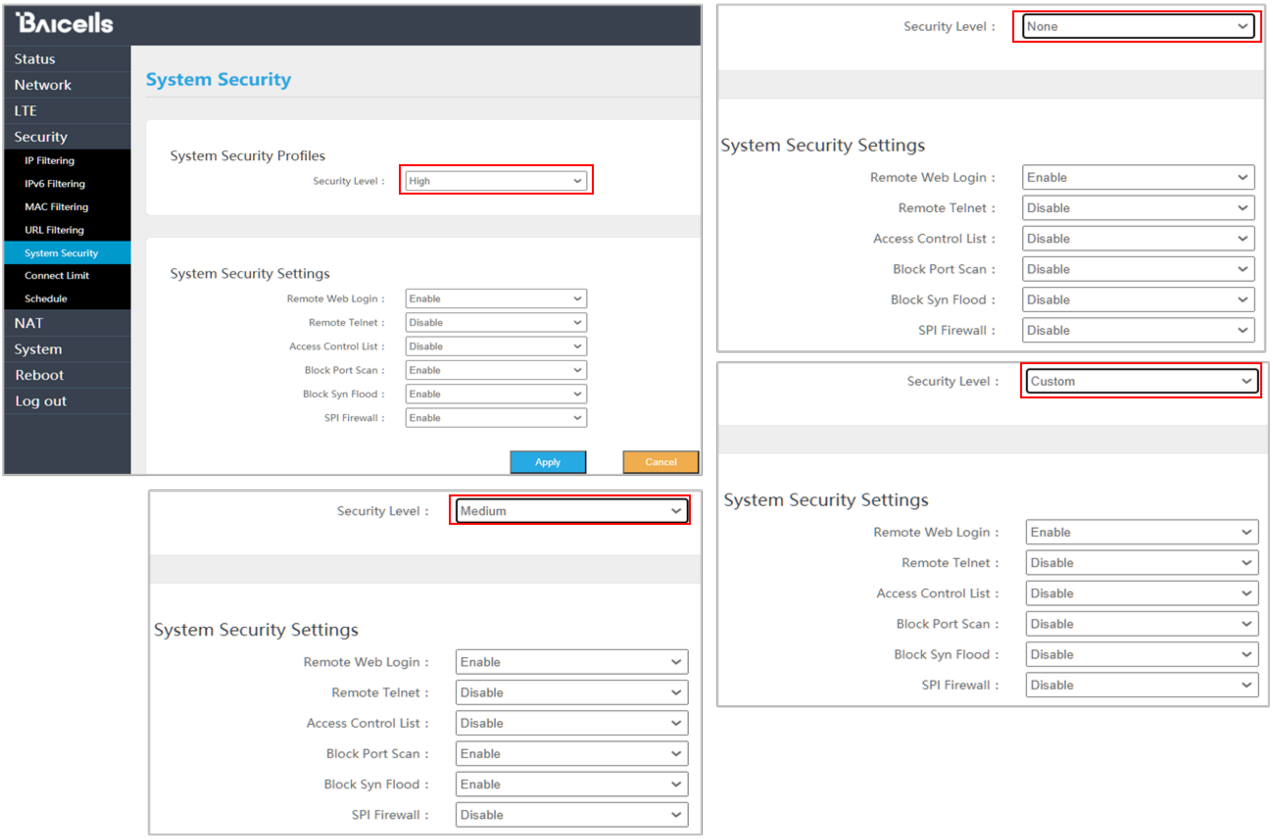
No. URL Selected Edit

6.6 System Security (CAT6/7/15)

The CAT6/7/15 CPE provides two pre-configured security profiles, as well as the option to customize or the option not to use a security profile. The settings determine how the CPE handles remote access and rejects unauthorized use or unrecognized packets. The two pre-configured profiles are referred to as High (default) and Medium. When you change the *Security Level*, the *System Security Settings* in the bottom pane change (Figure 6-11).

If you select *None*, a warning prompt pops up indicating that disabling the Stateful Packet Inspection (SPI) firewall will affect network security (Figure 6-12). If you are sure you want to make the change, select *Yes*. The system will then return a message, "*Successfully changed settings.*" Select *OK* to view the updated fields.

Figure 6-11: System Security (CAT6/7/15)



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

Security Level : None

System Security Settings

Remote Web Login : Enable
Remote Telnet : Disable
Access Control List : Disable
Block Port Scan : Disable
Block Syn Flood : Disable
SPI Firewall : Disable

Security Level : Custom

System Security Settings

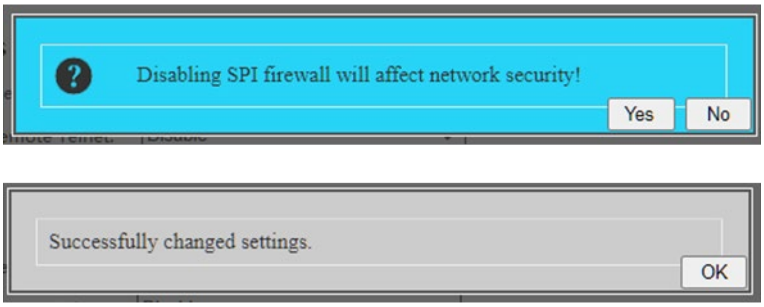
Remote Web Login : Enable
Remote Telnet : Disable
Access Control List : Disable
Block Port Scan : Disable
Block Syn Flood : Disable
SPI Firewall : Disable

Security Level : Medium

System Security Settings

Remote Web Login : Enable
Remote Telnet : Disable
Access Control List : Disable
Block Port Scan : Enable
Block Syn Flood : Enable
SPI Firewall : Disable

Figure 6-12: Security Level = None (CAT6/7/15)

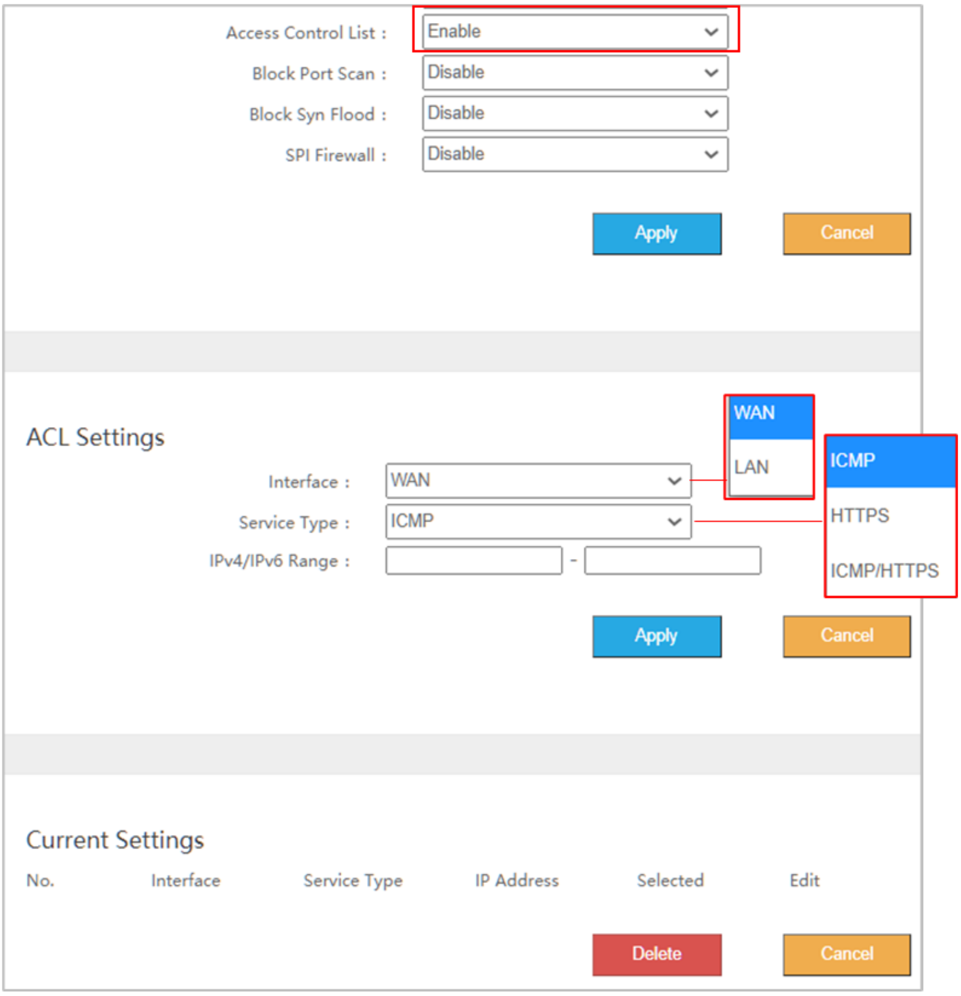


Disabling SPI firewall will affect network security!

Successfully changed settings.

If you enable the Access Control List (ACL) setting, after the warning and successful change prompts the *ACL Settings* pane will appear (Figure 6-13). Enter the *Interface* as *WAN* or *LAN*, the *Service Type* as *ICMP, HTTPS*, or *ICMP/HTTPS*, and the *IPv4/IPv6 Range*. Click on *Apply* to implement the changes. The new settings will appear in the *Current Settings* pane.

Figure 6-13: ACL Enable (CAT6/7/15)



Access Control List : Enable

Block Port Scan : Disable

Block Syn Flood : Disable

SPI Firewall : Disable

ACL Settings

Interface : WAN

Service Type : ICMP

IPv4/IPv6 Range : -

Current Settings

No.	Interface	Service Type	IP Address	Selected	Edit

6.7 Port Forwarding (CAT4)

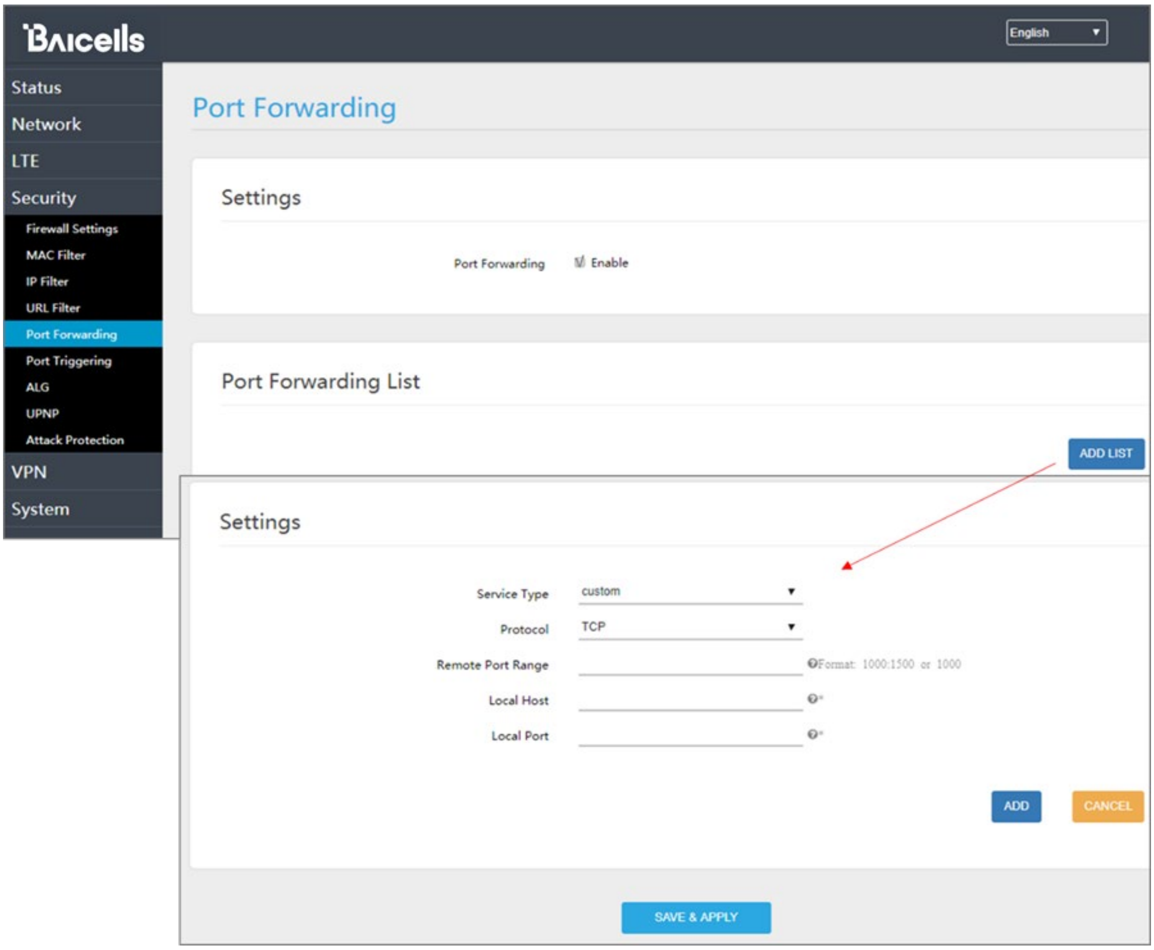
NOTE: For CAT6/7/15, refer to the *NAT > Port Forwarding* function described in *section 7.1*.

When Network Address Translation (NAT) is selected for the *Network > WAN > Network Mode* setting, 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), configuring the *Port Forwarding* settings is required so that all accesses to the external server port from the Internet are redirected to the server on the LAN.

To add a port forwarding rule, click on the checkbox next to *Enable*, and click on *ADD LIST* as shown in Figure 6-14. To add more lists, click on *ADD*. The fields are explained in Table 6-1.

Figure 6-14: Port Forwarding (CAT4)



Port Forwarding

Settings

Port Forwarding ☑ Enable

Port Forwarding List

Settings

Service Type: custom

Protocol: TCP

Remote Port Range: Format: 1000:1500 or 1000

Local Host:

Local Port:

Table 6-1: Port Forwarding (CAT4)

Field Name	Description
Service Type	Select the type of service, either Custom, DNS, FTP, IPSec, POP3, SMTP, PPTP, Realplay, SSH, HTTPs, SNMP, SNMP Trap, Telnet, TFTP, or HTTP NOTE: SNMP is supported on CAT6/7/15 CPEs (see *section 9.9*).
Protocol	Select the type of data protocol, either TCP, UDP, or TCP&UDP
Remote Port Range	Enter the port number range for the remote device in the format of 1000 to 1500
Local Host	Enter the local host IP address. The address must be different from the IP address that is set for the LAN Host Settings parameter, but they must be on the same network segment.
Local Port	Enter the local port number. Range is 1 to 65,535.

6.8 Port Triggering (CAT4)

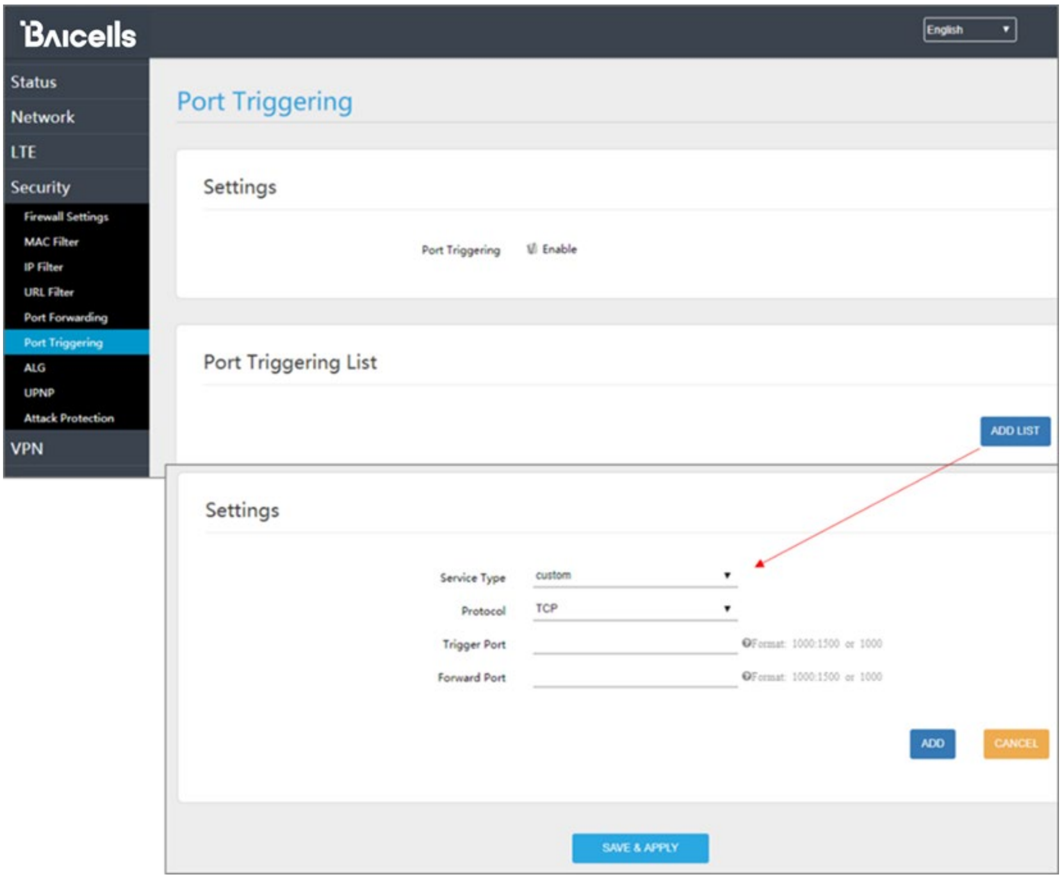
NOTE: For CAT6/7/15, refer to the *NAT > Port Trigger* function described in *section 7.3*.

The *Port Triggering* feature is a configuration option on a router - in this case, the CPE - when its *Network > WAN > Network Mode* setting is Network Address Translation (NAT). When an application uses a trigger port to build a connection, the CPE will forward the data to the forward port.

To enable port triggering (Figure 6-15):

1. Go to *Security > Port Triggering*.
2. Select the *Enable* checkbox and click on *ADD LIST*.
3. Enter the *Service Type*: *custom*, *DNS*, *FTP*, *IPSec*, *SSH*, *TELNET*, *SMTP*, *PPTP*, *Realplay*, *HTTP*, *POP3*, *SNMP*, *SNAP Trap*, *HTTPs*, or *TFTP*.
4. Choose a *Protocol*: *TCP*, *UDP*, or *TCP&UDP*.
5. Click on *SAVE & APPLY*.

Figure 6-15: Port Triggering (CAT4)



Port Triggering ☑ Enable

Service Type: custom

Protocol: TCP

Trigger Port: Format: 1000:1500 or 1000

Forward Port: Format: 1000:1500 or 1000

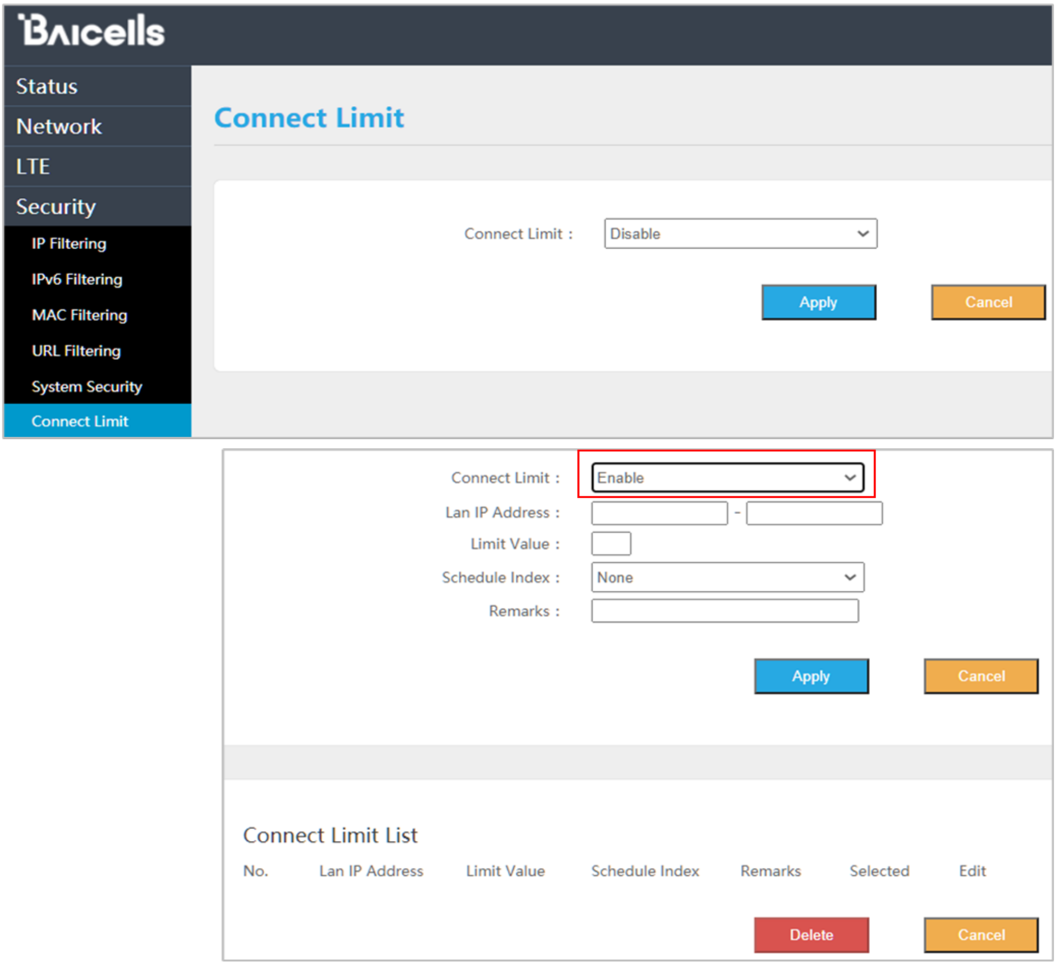
6.9 Connect Limit (CAT6/7/15)

The Connect Limit feature is used to control the number of connections through the CPE 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.

To enable the Connect Limit feature (Figure 6-16):

1. Go to *Security > Connect Limit* and select *Enable*.
2. Enter the *LAN IP Address* range.
3. Enter the *Limit Value*, from 1 to 16.
4. The *Schedule Index* currently is always *None*. Enter any *Remarks* you wish to make concerning this configuration, and click on *Apply*. The configuration will appear in the *Connect Limit List*.

Figure 6-16: Connect Limit (CAT6/7/15)



Connect Limit

Connect Limit : Disable

Connect Limit : Enable

Lan IP Address : -

Limit Value :

Schedule Index : None

Remarks :

Connect Limit List

No.	Lan IP Address	Limit Value	Schedule Index	Remarks	Selected	Edit

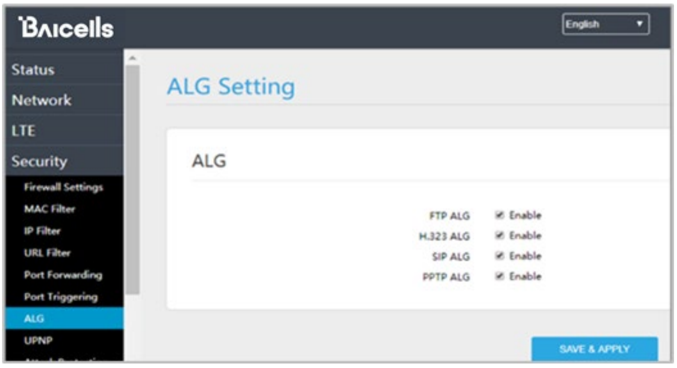
6.10 ALG (CAT4)

NOTE: For CAT6/7/15, refer to the *NAT > ALG Settings* described in *section 7.2*.

The Application Layer Gateway (ALG) function provides a security component that augments a firewall or the Network Address Translation (NAT) mode used by the CPE if *Network > WAN > Network Mode = NAT*. The ALG function allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer control/data protocols such as *FTP ALG*, *H.323 ALG*, *SIP ALG*, and *PPTP ALG*.

You can enable the different types of application protocols by selecting the checkbox next to the protocol name and then clicking on *SAVE & APPLY* (Figure 6-17).

Figure 6-17: ALG (CAT4)



ALG Setting

ALG

FTP ALG ☑ Enable
H.323 ALG ☑ Enable
SIP ALG ☑ Enable
PPTP ALG ☑ Enable

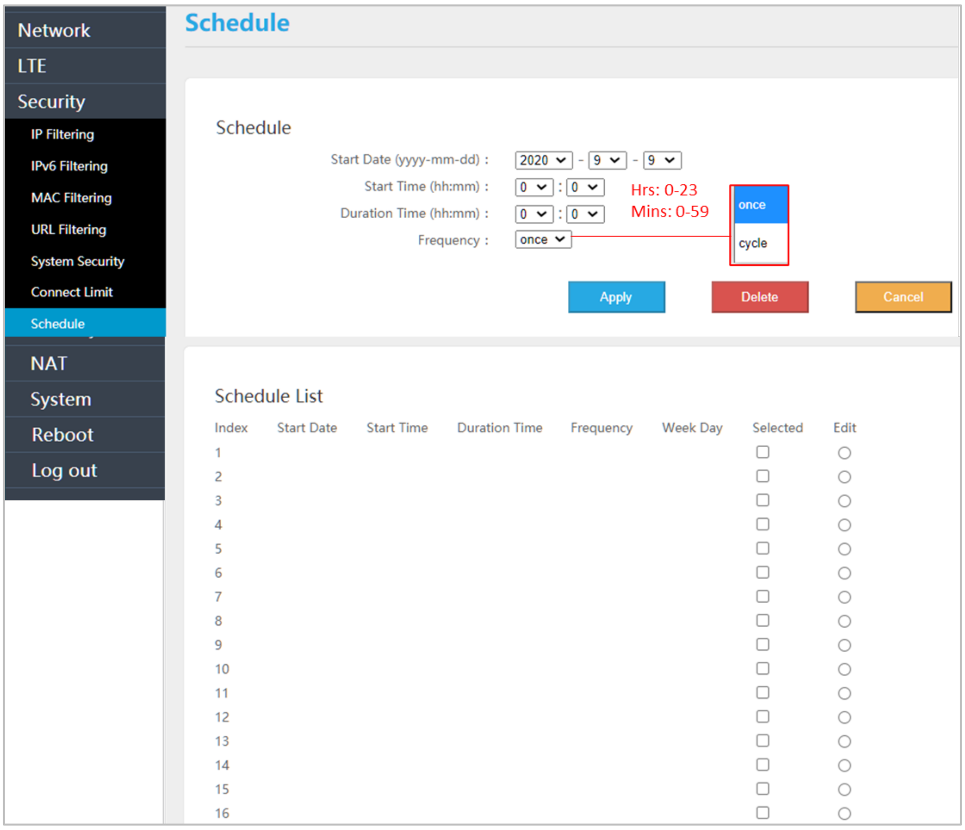
SAVE & APPLY

6.11 Schedule (CAT6/7/15)

The *Security > Schedule* feature can be used in conjunction with the IP Filtering function, where you can select a *Schedule Index* (section 6.3.2) that is configured in this *Security > Schedule* sub-menu. If assigned, the schedule determines when IP/port filtering will occur. You can create up to 16 schedules.

Referring to Figure 6-18, create a schedule by entering the *Start Date*, *Start Time*, *Duration Time*, and *Frequency*, and then click on *Apply*. The schedule will be shown in the *Schedule List* at the bottom of the window, where it is given an index number.

Figure 6-18: Schedule (CAT6/7/15)



Schedule

Schedule

Start Date (yyyy-mm-dd) : 2020 - 9 - 9
Start Time (hh:mm) : 0 : 0
Duration Time (hh:mm) : 0 : 0
Frequency : once

Hrs: 0-23
Mins: 0-59

Schedule List

Index	Start Date	Start Time	Duration Time	Frequency	Week Day	Selected	Edit
1						□	○
2						□	○
3						□	○
4						□	○
5						□	○
6						□	○
7						□	○
8						□	○
9						□	○
10						□	○
11						□	○
12						□	○
13						□	○
14						□	○
15						□	○
16						□	○

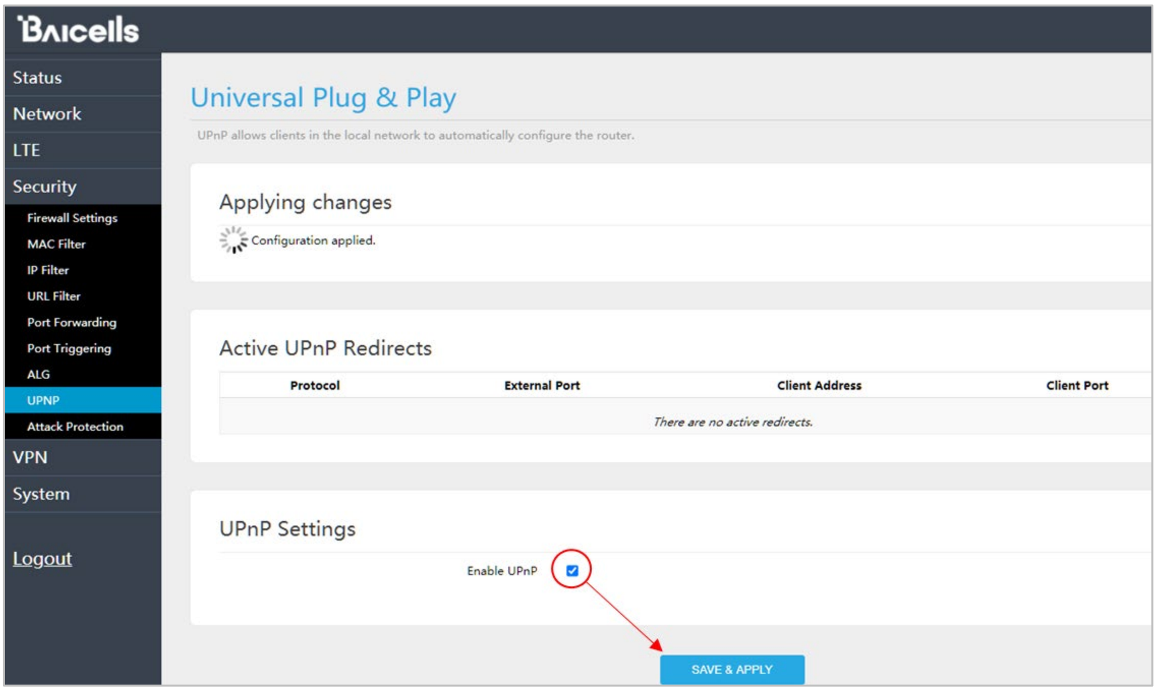
6.12 UPNP (CAT4)

NOTE: For a CAT6/7/15 CPE, the Universal Plug & Play (UPnP) feature is configured in the *Network > UPnP* sub-menu (*section 4.7*).

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

Go to *Security > UPNP > UPNP Settings* and click on the checkbox next to *Enable UPnP*. This action enables the CPE to be searched by other devices (Figure 6-19). The *Universal Plug & Play* window will temporarily display "*Waiting for changes to be applied*" and then "*Configuration applied*". Once enabled, any redirects of traffic will display in the *Active UPnP Redirects* section of the window.

Figure 6-19: UPNP (CAT4)



Universal Plug & Play

UPnP allows clients in the local network to automatically configure the router.

Applying changes

Configuration applied.

Active UPnP Redirects

Protocol	External Port	Client Address	Client Port
There are no active redirects.			

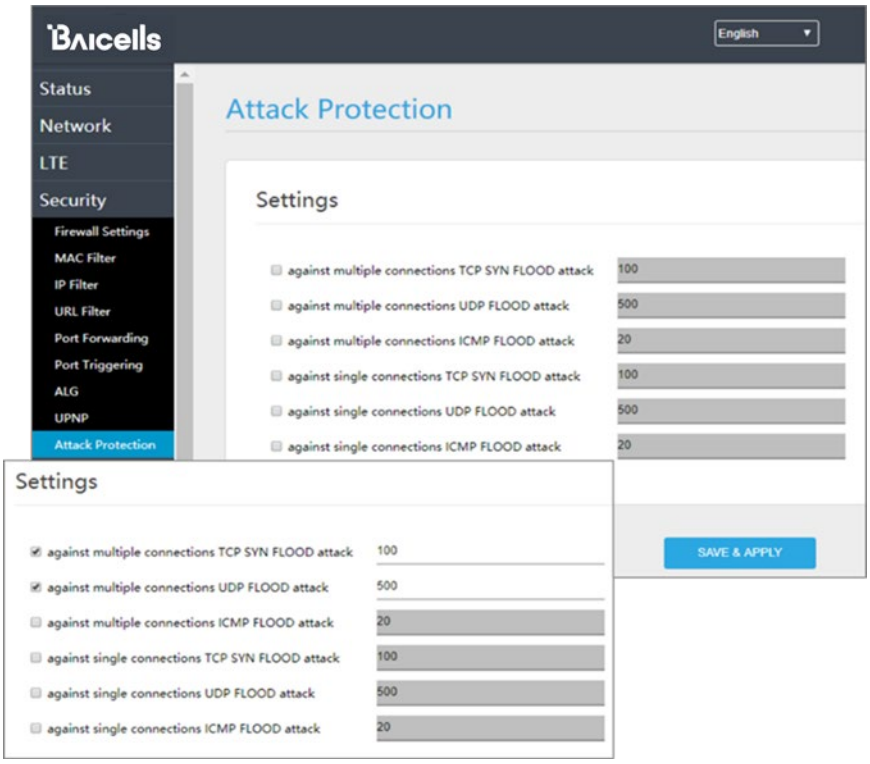
UPnP Settings

Enable UPnP ☑

6.13 Attack Protection (CAT4)

The *Attack Protection* settings provide an additional security measure to help prevent computer hacker attacks such as *TCP SYN FLOOD*, *UDP FLOOD*, and *IMCP FLOOD* for devices connected to the network through the CPE. In the *Security > Attack Protection* window (Figure 6-20), click on the flood protection options you want to enable. When you click the checkbox, the field on the right becomes editable. Accept the default timer value, in seconds, or enter a value for each type of protection.

Figure 6-20: Attack Protection (CAT4)



Attack Protection

Settings

□ against multiple connections TCP SYN FLOOD attack	100
□ against multiple connections UDP FLOOD attack	500
□ against multiple connections ICMP FLOOD attack	20
□ against single connections TCP SYN FLOOD attack	100
□ against single connections UDP FLOOD attack	500
□ against single connections ICMP FLOOD attack	20

Settings

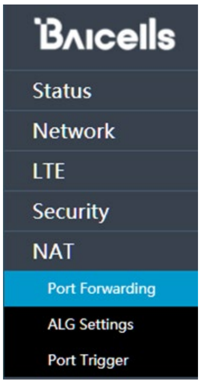
☑ against multiple connections TCP SYN FLOOD attack	100
☑ against multiple connections UDP FLOOD attack	500
□ against multiple connections ICMP FLOOD attack	20
□ against single connections TCP SYN FLOOD attack	100
□ against single connections UDP FLOOD attack	500
□ against single connections ICMP FLOOD attack	20

7 NAT Menu (CAT6/7/15)

The *NAT* menu contains the *Port Forwarding*, *ALG Settings*, and *Port Trigger* functions (Figure 7-1). Each of these is described in the sections that follow.

> NOTE: The CAT4 GUI provides these three functions under the *Security* menu (see *section 6.7*, *section 6.8*, and *section 6.10*).

Figure 7-1: NAT Menu (CAT6/7/15)



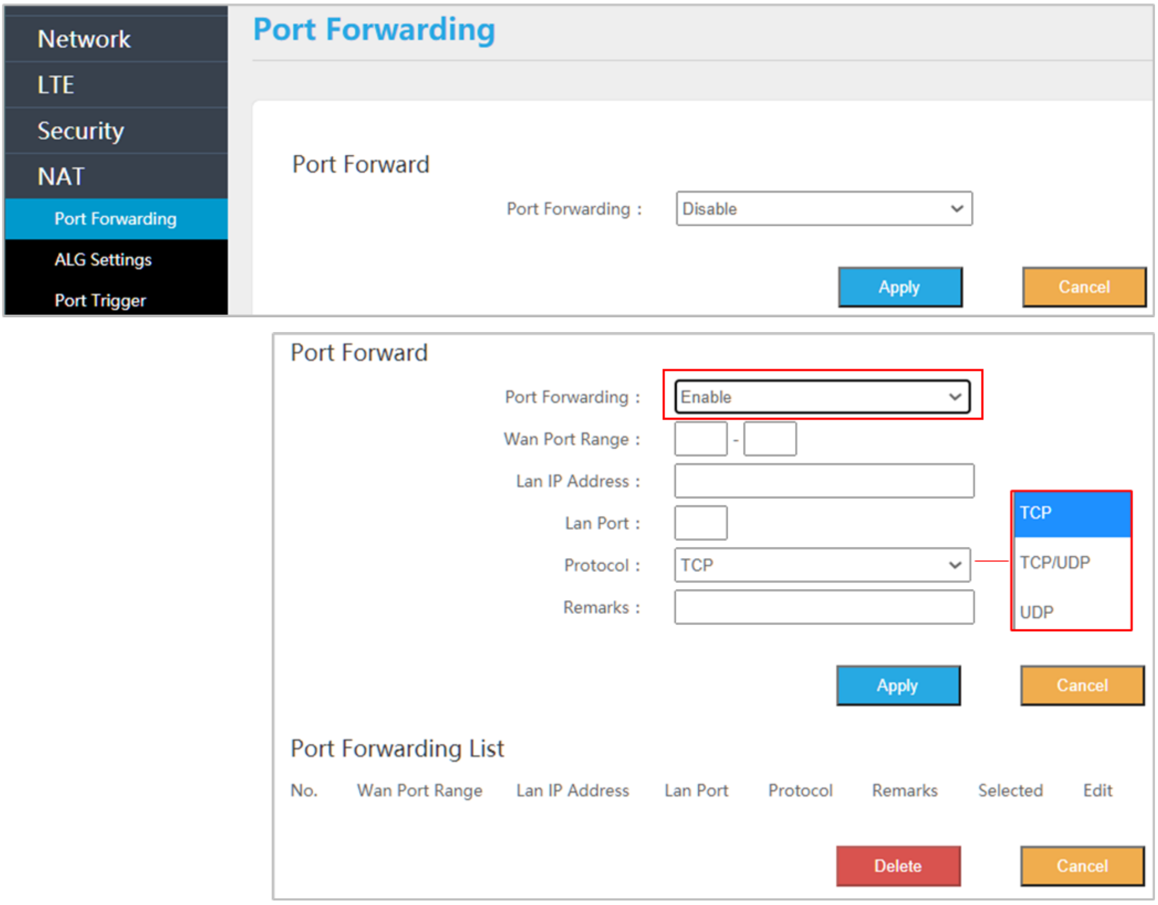
7.1 Port Forwarding (CAT6/7/15)

When Network Address Translation (NAT) is selected for the Network Mode under *Network* > *WAN Settings* (*section 4.2*), 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), configuring the *Port Forwarding* settings is required so that all accesses to the external server port from the Internet are redirected to the server on the LAN.

To add a port forwarding rule (Figure 7-2):

1. Go to *NAT* > *Port Forwarding*, and select *Enable*.
2. Enter the *Wan Port Range* for the remote device in the format of 1000 to 1500.
3. Enter the local host *Lan 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.
4. Enter the local *Lan Port number*. The range is 1 to 65,535.
5. Select a type of data *Protocol*: *TCP*, *TCP/UDP*, or *UDP.*
6. Optionally, enter any *Remarks* you wish to make about this configuration, and then click on *Apply*. The port forwarding rule will be added to the *Port Forwarding List* at the bottom.
7. To add more rules, repeat steps 2-6.

Figure 7-2: Port Forwarding (CAT6/7/15)

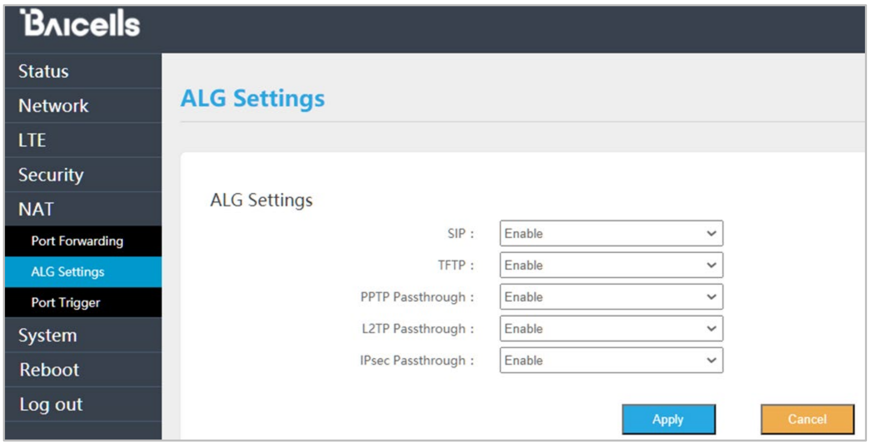


7.2 ALG Settings (CAT6/7/15)

The Application Layer Gateway (ALG) function provides a security component that augments a firewall or the Network Address Translation (NAT) used by the CPE when NAT is configured for the Network Mode under *Network* > *WAN Settings* (*section 4.2*). ALG 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 Passthrough*, *L2TP Passthrough*, and *IPsec Passthrough*.

You can enable the different types of application protocols by clicking on the checkbox next to the protocol name and clicking on *Apply* (Figure 7-3).

Figure 7-3: ALG Settings (CAT6/7/15)



ALG Settings

SIP : Enable

TFTP : Enable

PPTP Passthrough : Enable

L2TP Passthrough : Enable

IPsec Passthrough : Enable

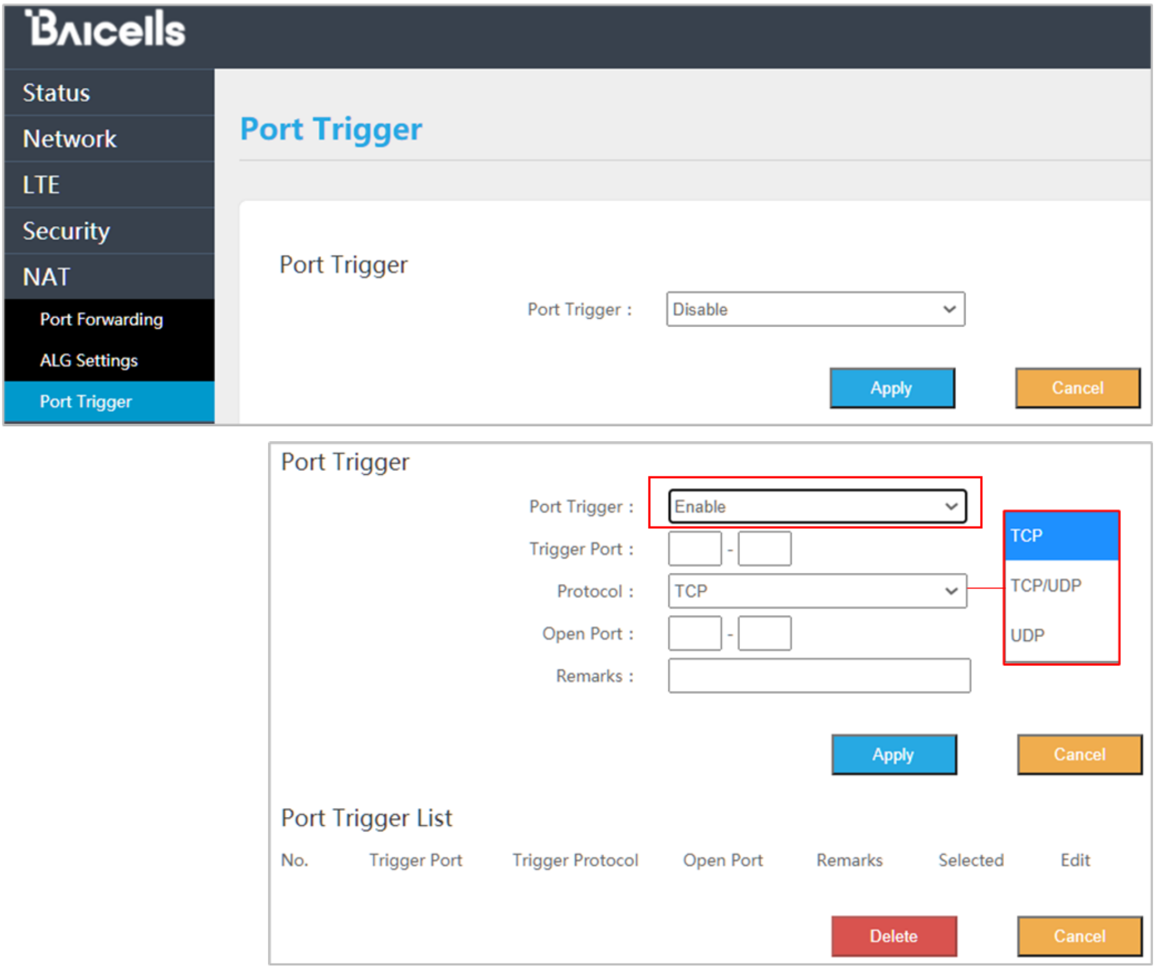
7.3 Port Trigger (CAT6/7/15)

Port triggering is a configuration option on a router - in this case, the CPE - if it is operating in Network Address Translation (NAT) mode for the Network Mode configured under *Network > WAN Settings* (*section 4.2*). When an application uses a trigger port to build a connection, the CPE will forward the data to the forward port.

To create a Port Trigger rule (Figure 7-4):

1. Go to *NAT > Port Trigger*, and select *Enable*.
2. Enter the *Trigger Port* range.
3. Select the type of data *Protocol*: *TCP*, *TCP/UDP*, or *UDP.*
4. Enter the *Open Port* number range.
5. Optionally, enter any *Remarks* you wish to add concerning this configuration, and then click on *Apply*. The rule will be added in the *Port Trigger List*.

Figure 7-4: Port Trigger (CAT6/7/15)



Port Trigger

Port Trigger : Disable

Port Trigger

Port Trigger : Enable

Trigger Port : -

Protocol : TCP

Open Port : -

Remarks :

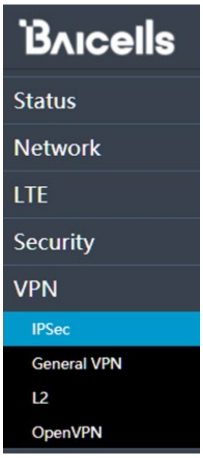
Port Trigger List

No.	Trigger Port	Trigger Protocol	Open Port	Remarks	Selected	Edit

8 VPN Menu (CAT4)

The Virtual Private Network (*VPN*) menu (Figure 8-1) enables you to configure a connection between the CPE and one or more VPNs - for example, to access a corporate network when telecommuting for work. Each sub-menu is described in this section.

Figure 8-1: VPN Menu (CAT4)



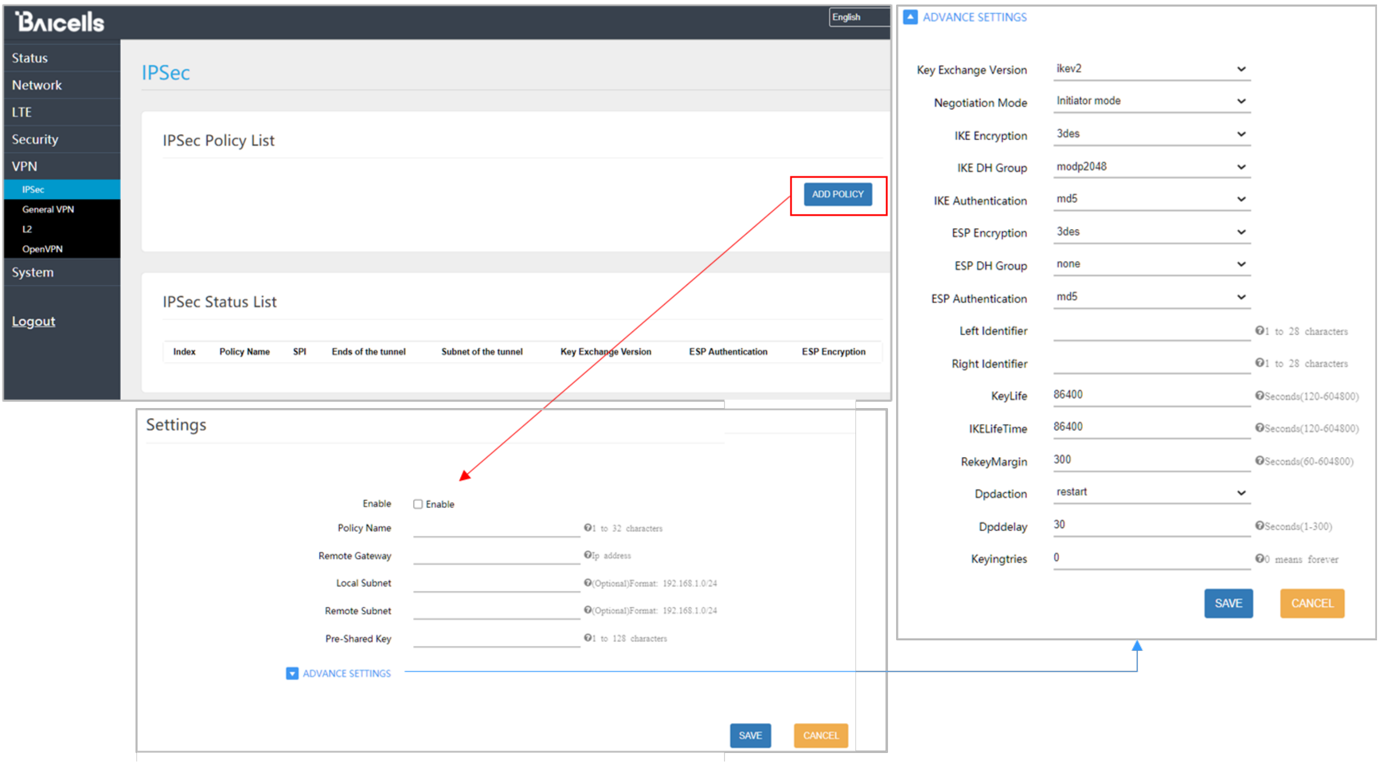
8.1 IPSec (CAT4)

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

To configure an IPSec policy for this CPE (Figure 8-2):

1. Go to *VPN* > *IPSec*, and click on the *ADD POLICY* button.
2. Select the checkbox for *Enable*, and enter a *Policy Name* (1 to 32 characters).
3. Enter the IP address of the *Remote Gateway*, and optionally, the IP address of the *Local Subnet* and *Remote Subnet*.
4. Enter a *Pre-Shared Key* with up to 128 characters for the VPN connection, and click on *SAVE*.
5. The *ADVANCE SETTINGS* offer additional parameters such as key exchange version, IKE encryption method, etc. Refer to Table 8-1 for a description of these fields.

Figure 8-2: IPSec (CAT4)



Index	Policy Name	SPI	Ends of the tunnel	Subnet of the tunnel	Key Exchange Version	ESP Authentication	ESP Encryption

Settings

Enable ☐ Enable
Policy Name ____ 1 to 32 characters
Remote Gateway ____ Ip address
Local Subnet ____ (Optional)Format: 192.168.1.0/24
Remote Subnet ____ (Optional)Format: 192.168.1.0/24
Pre-Shared Key ____ 1 to 128 characters

ADVANCE SETTINGS

Key Exchange Version: ikev2
Negotiation Mode: Initiator mode
IKE Encryption: 3des
IKE DH Group: modp2048
IKE Authentication: md5
ESP Encryption: 3des
ESP DH Group: none
ESP Authentication: md5
Left Identifier: ____ 1 to 28 characters
Right Identifier: ____ 1 to 28 characters
KeyLife: 86400 Seconds(120-604800)
IKELifeTime: 86400 Seconds(120-604800)
RekeyMargin: 300 Seconds(60-604800)
Dpdaction: restart
Dpddelay: 30 Seconds(1-300)
Keyingtries: 0 0 means forever

Table 8-1: IPSec ADVANCE SETTINGS (CAT4)

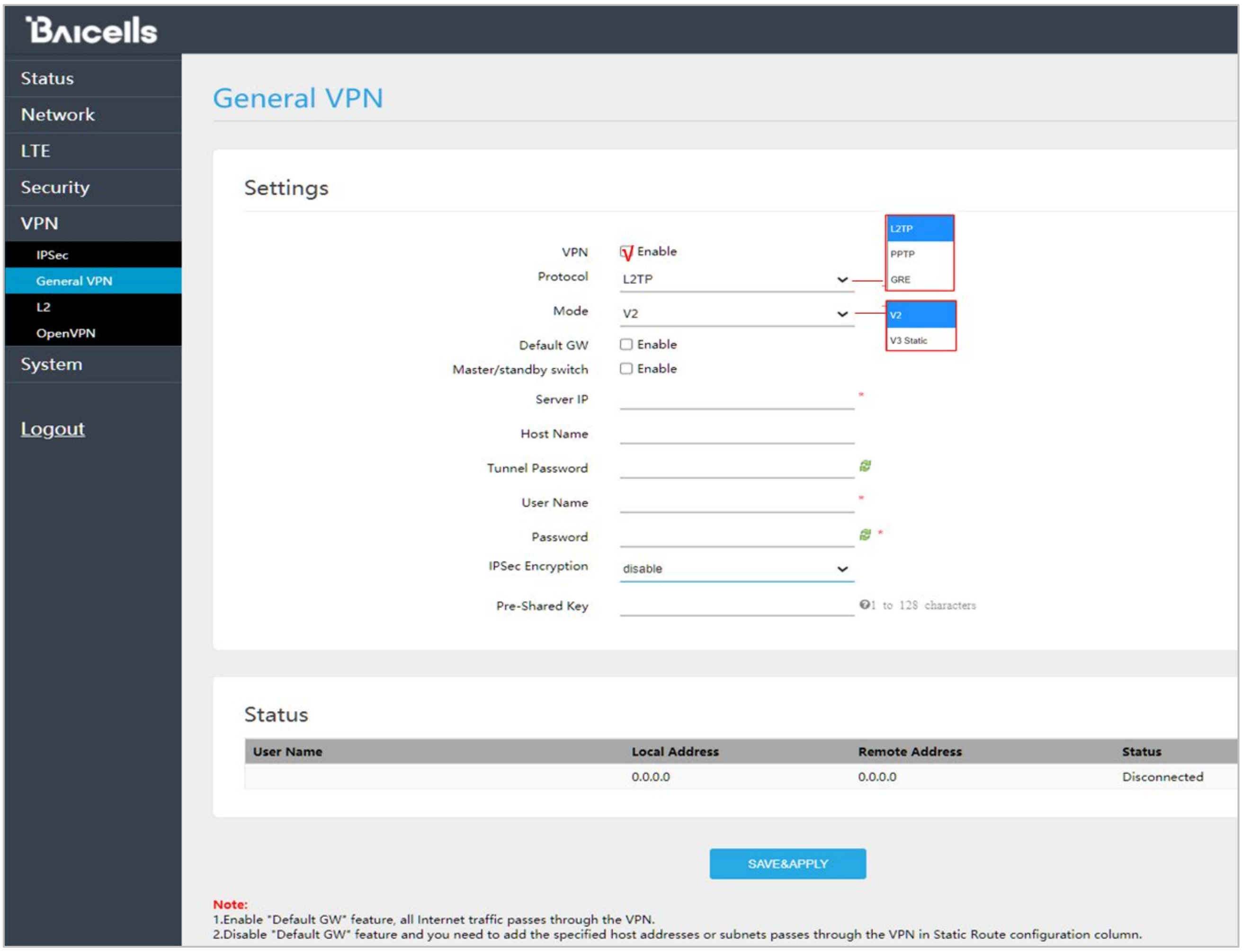
Field Name	Description
Key Exchange Version	Internet Key Exchange (IKE) encryption method version 2 or version 1. IKE is a protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access.
Negotiation Mode	Initiator mode or Responder mode
IKE Encryption	3des, aes128, aes192, or aes256
IKE DH Group	modp768, modp1024, modp1536, modp2048, or modp4096

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

8.2 General VPN (CAT4)

The *VPN > General VPN* sub-menu offers three options for Virtual Private Network (VPN) setup: *L2TP*, *PPTP*, and *GRE* (Figure 8-3). Each method is explained below.

Figure 8-3: General VPN (CAT4)



General VPN

Settings

VPN ☑ Enable
Protocol L2TP
L2TP
PPTP
GRE
Mode V2
V2
V3 Static
Default GW □ Enable
Master/standby switch □ Enable
Server IP *
Host Name
Tunnel Password
User Name *
Password *
IPSec Encryption disable
Pre-Shared Key ❓1 to 128 characters

Status

User Name	Local Address	Remote Address	Status
	0.0.0.0	0.0.0.0	Disconnected

SAVE&APPLY

Note:
1.Enable "Default GW" feature, all Internet traffic passes through the VPN.
2.Disable "Default GW" feature and you need to add the specified host addresses or subnets passes through the VPN in Static Route configuration column.

8.2.1 L2TP (CAT4)

The Layer 2 Tunneling Protocol (L2TP) is a computer networking protocol used by Internet Service Providers (ISPs) for VPN operations. Similar to Layer 2 Data Link layer in the OSI reference model, L2TP is a session layer protocol which provides an unencrypted tunnel between the CPE and the VPN. All Internet traffic including ISP services will pass through the VPN.

A User Datagram Protocol (UDP) port is used for L2TP communications. Because it does not provide any security for the data traffic, such as encryption and confidentiality, an encryption protocol such as IPSec is often used with L2TP.

To configure L2TP VPN, go to *VPN > General VPN* and click on the *Enable* checkbox next to *VPN* (Figure 8-3, above). Refer to Table 8-2 to complete the other fields. When you are finished, click on *SAVE&APPLY*. Any users who access the network through this VPN connection will be listed under *Status* in the bottom pane, showing the user name, local and remote addresses, and their connect/disconnect status.

Table 8-2: L2TP (CAT4)

Field Name	Description
Mode	Select either *LT2P* tunneling protocol version 2 (*V2*) or version 3 static mode (*V3 Static*)
Default GW	Click on the checkbox to enable this as the default gateway. If enabled, all Internet traffic will pass through the VPN.
Master/standby switch	Enable/Disable this VPN as the master server
Server IP	Virtual Private Network server IP address
Host Name	If Default GW setting is Disabled, enter the host addresses or subnets
Tunnel Password	Optionally, enter a tunnel password
User Name	User name required to access the VPN connection
Password	Password required to access the VPN connection
IPSec Encryption	Enable/Disable IPSec encryption on this VPN connection
Pre-Shared Key	1 to 128 character key to be used for authentication between the local and remote connection

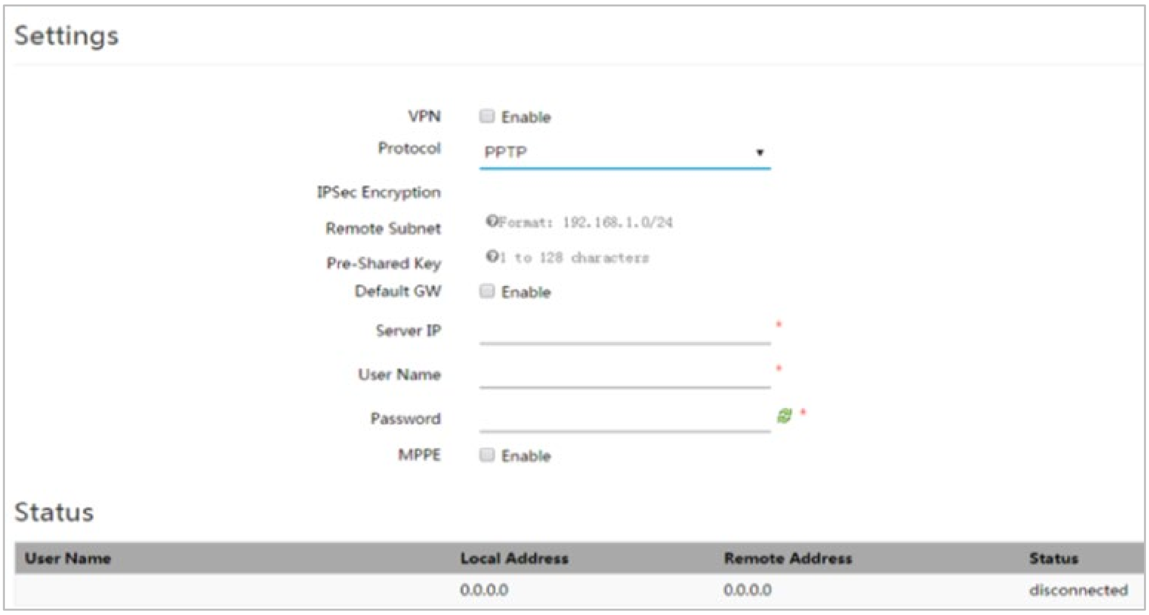
8.2.2 PPTP (CAT4)

Point-to-Point Tunneling Protocol (PPTP) is a network protocol mostly used with Windows computers. Today, PPTP is considered obsolete for use in VPNs because of its many known security deficiencies. Nevertheless, PPTP is still in use in some networks.

PPTP uses a TCP control channel and a generic routing encapsulation (GRE) tunnel to encapsulate PPP packets. Enable VPN using the checkbox (Figure 8-4), and select PPTP for the VPN protocol. Refer to Table 8-3 for a description of each field.

Any users who access the network through this VPN connection will be listed under *Status* in the bottom pane, showing the user name, local and remote addresses, and their connect/disconnect status.

Figure 8-4: PPTP (CAT4)



Settings

VPN	□ Enable
Protocol	PPTP ▾
IPSec Encryption	
Remote Subnet	Format: 192.168.1.0/24
Pre-Shared Key	1 to 128 characters
Default GW	□ Enable
Server IP	*
User Name	*
Password	*
MPPE	□ Enable

Status

User Name	Local Address	Remote Address	Status
	0.0.0.0	0.0.0.0	disconnected

Table 8-3: PPTP (CAT4)

Field Name	Description
VPN	Enable/Disable VPN
Protocol	Select *PPTP*
Default GW	Click on the checkbox to enable this as the default gateway
Server IP	VPN server IP address
User Name	User name required to access the VPN connection
Password	Password required to access the VPN connection
MPPE	Select the checkbox to enable Microsoft Point-to-Point Encryption

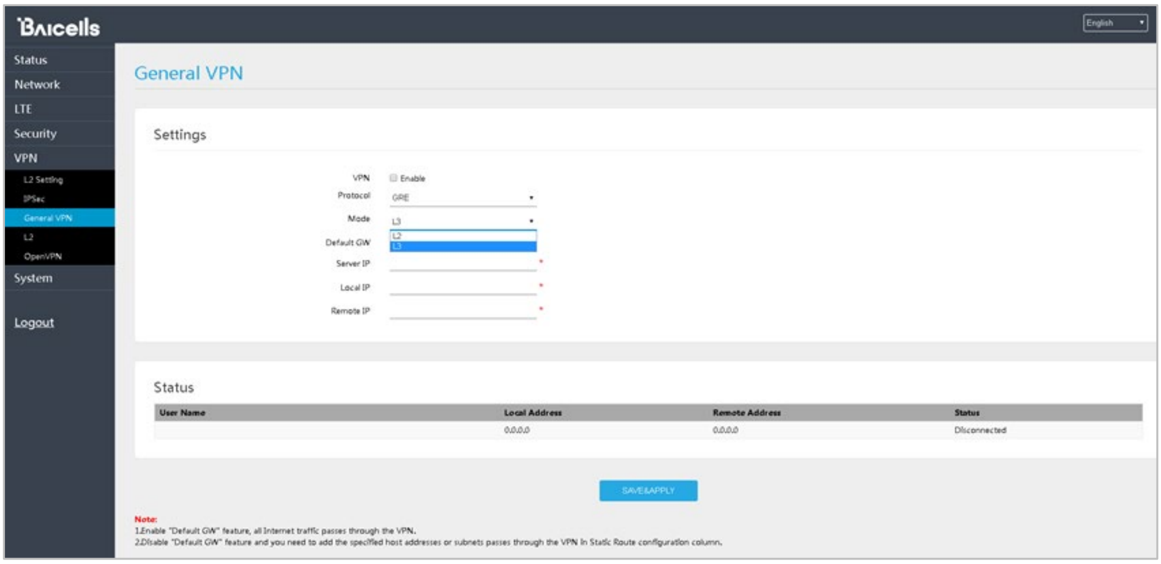
8.2.3 GRE (CAT4)

Generic Routing Encapsulation (GRE) is a communication protocol used to establish a direct, point-to-point connection between network nodes. GRE lets two peers share data they would not otherwise be able to share over the Internet. GRE encapsulates a wide variety of network layer protocols inside virtual point-to-point links over the IP network.

To use GRE VPN, click on the *Enable* checkbox next to *VPN* and select *GRE* as the protocol (Figure 8-5). Complete the parameters per Table 8-4.

Any users who access the network through this VPN connection will be listed under *Status* in the bottom pane, showing the user name, local and remote addresses, and their connect/disconnect status.

Figure 8-5: GRE (CAT4)



General VPN

Settings

VPN □ Enable
Protocol GRE
Mode L3
L2
L3
Default GW
Server IP *
Local IP *
Remote IP *

Status

User Name	Local Address	Remote Address	Status
	0.0.0.0	0.0.0.0	Disconnected

Note:
1.Enable "Default GW" feature, all Internet traffic passes through the VPN.
2.Disable "Default GW" feature and you need to add the specified host addresses or subnets passes through the VPN in Static Route configuration column.

Table 8-4: GRE (CAT4)

Field Name	Description
VPN	Enable/Disable VPN
Protocol	Select *GRE*
Default GW	Click on the checkbox to enable this as the default gateway
Server IP	VPN server IP address
Local IP	Local IP address
Remote IP	Remote IP address

8.3 L2 (CAT4)

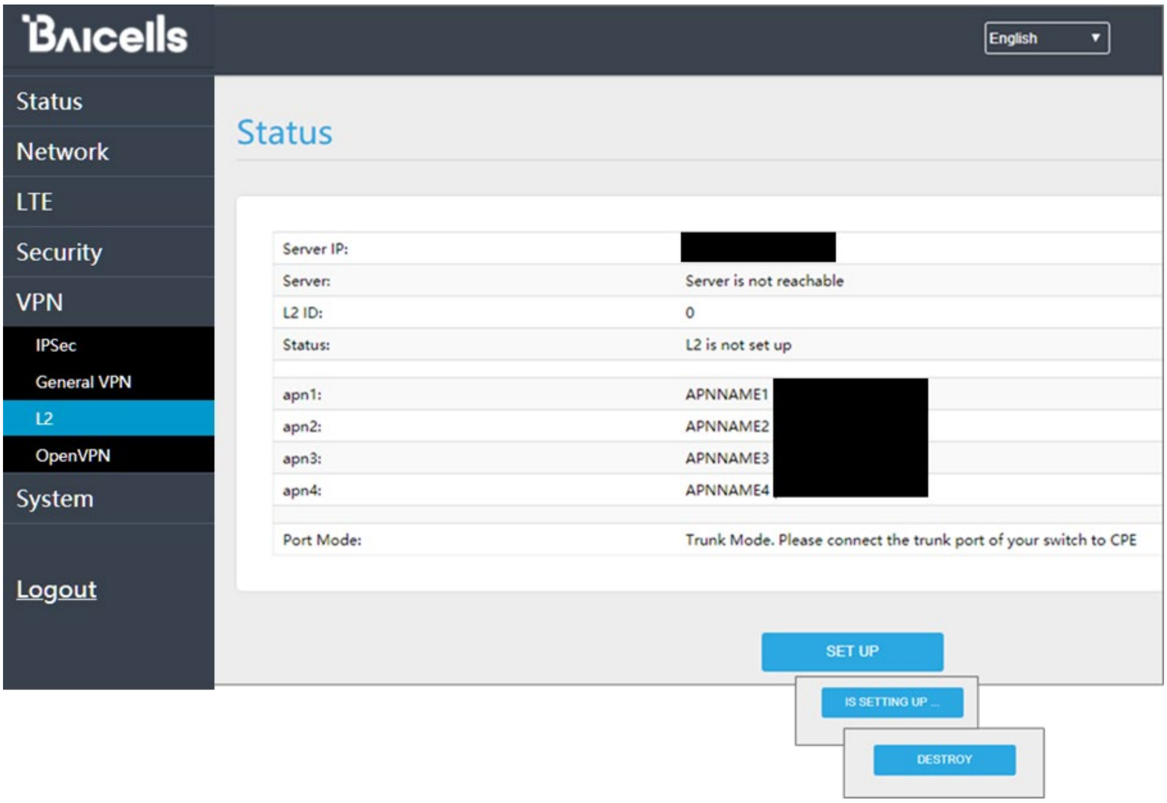
Virtual Extensible Local Area Network (VxLAN) is a network virtualization technology that attempts to address the scalability problems associated with large cloud computing deployments. Baicells's L2 VPN technology is based on VxLAN and must be coordinated with the Baicells CloudCore Evolved Packet Core (EPC). L2 will not work if you are using another vendor's EPC.

To configure L2 VPN, go to *VPN* > *L2* and click on *SET UP* (Figure 8-6). You will receive a message "*Is Setting Up*" to indicate the connection is being established. The resulting screen for a successful connection will show "*Last Command/Result"* or "*set up/OK*".

When the CPE starts an L2 VPN service, all APN services defined under *LTE* > *APN Management* will be activated and the CPE will work like a Layer 2/Layer 3 switch (Figure 8-7).

To release the L2 VPN connection, select *DESTROY*. The screen will report "*Is Destroying*", and then it will return to the *Set Up* screen.

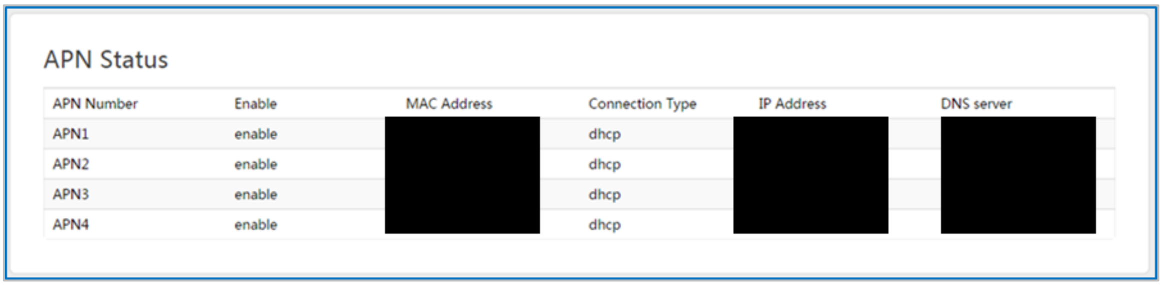
Figure 8-6: Set Up L2 (CAT4)



Status

Server IP:	[redacted]
Server:	Server is not reachable
L2 ID:	0
Status:	L2 is not set up
apn1:	APNNAME1 [redacted]
apn2:	APNNAME2 [redacted]
apn3:	APNNAME3 [redacted]
apn4:	APNNAME4 [redacted]
Port Mode:	Trunk Mode. Please connect the trunk port of your switch to CPE

Figure 8-7: APN Status (CAT4)



APN Status

APN Number	Enable	MAC Address	Connection Type	IP Address	DNS server
APN1	enable	[redacted]	dhcp	[redacted]	[redacted]
APN2	enable	[redacted]	dhcp	[redacted]	[redacted]
APN3	enable	[redacted]	dhcp	[redacted]	[redacted]
APN4	enable	[redacted]	dhcp	[redacted]	[redacted]

8.4 OpenVPN (CAT4)

OpenVPN is an open-source, Virtual Private Network (VPN) encryption protocol. As well as being extremely secure, OpenVPN is highly customizable and can be implemented in a number of ways. For that reason, using this VPN method requires significant networking experience to implement.

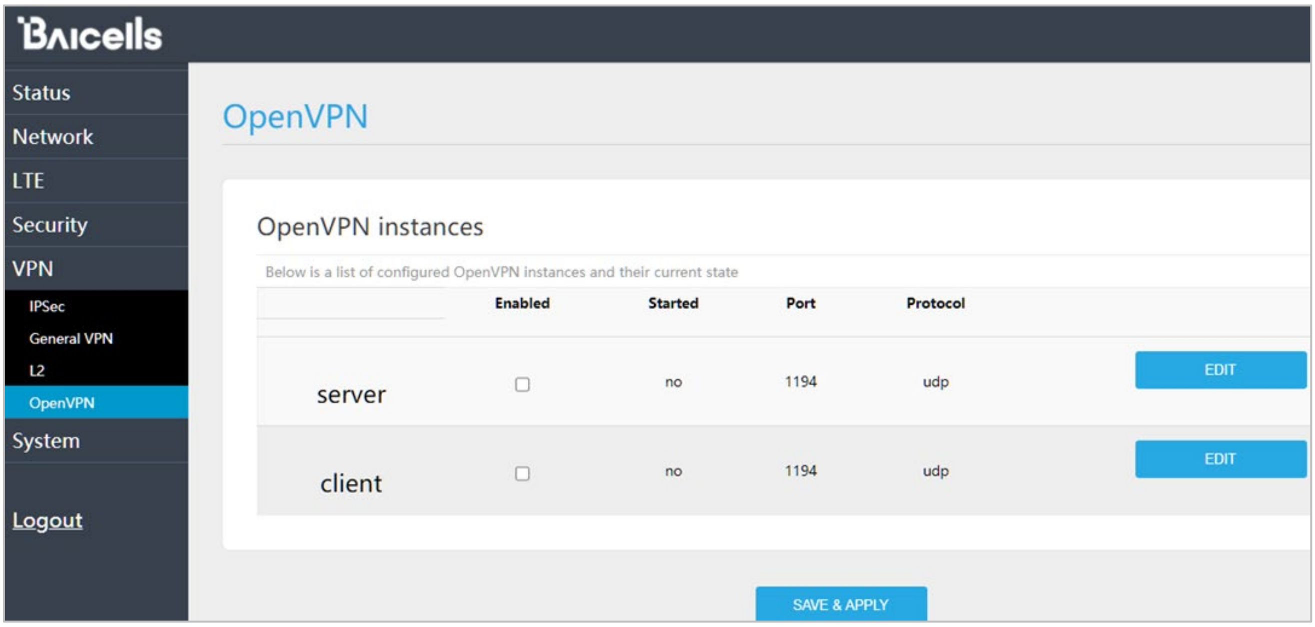
The range of options includes remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions. The remote access solutions support robust capabilities such as load balancing, failover, and more granular access controls, e.g., articles, examples, security overview, and non-English languages.

OpenVPN implements OSI Layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol. It supports flexible client authentication methods based on certificates, smart cards, and/or two-factor authentication.

Using OpenVPN allows user or group-specific access control policies via firewall rules applied to the VPN interface. Setting up OpenVPN involves configuring server and client settings.

To view or change the server and client settings, go to *VPN > OpenVPN* and click on *Edit*. Refer to Figure 8-8 (initial window), Figure 8-9 (Edit server), and Figure 8-10 (Edit client).

Figure 8-8: OpenVPN (CAT4)



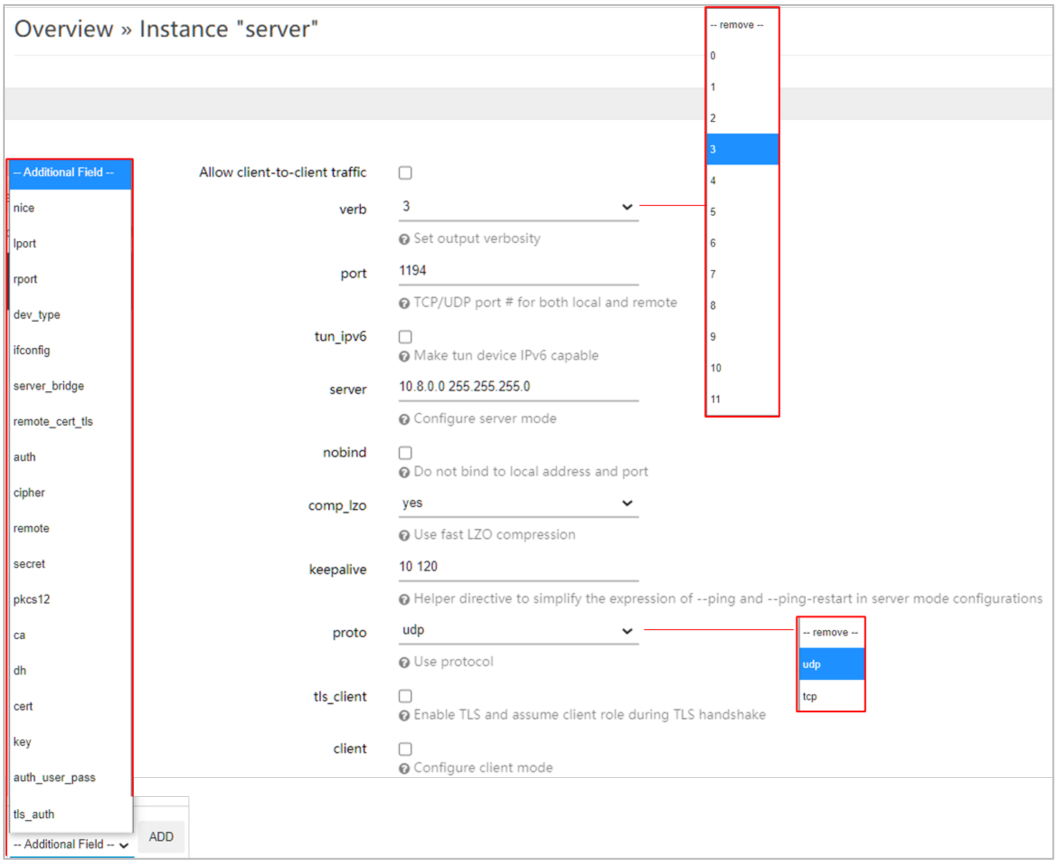
OpenVPN

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

	Enabled	Started	Port	Protocol	
server	□	no	1194	udp	EDIT
client	□	no	1194	udp	EDIT

Figure 8-9: Edit server (CAT4)



Overview » Instance "server"

Allow client-to-client traffic □

verb 3
Set output verbosity

port 1194
TCP/UDP port # for both local and remote

tun_ipv6 □
Make tun device IPv6 capable

server 10.8.0.0 255.255.255.0
Configure server mode

nobind □
Do not bind to local address and port

comp_lzo yes
Use fast LZO compression

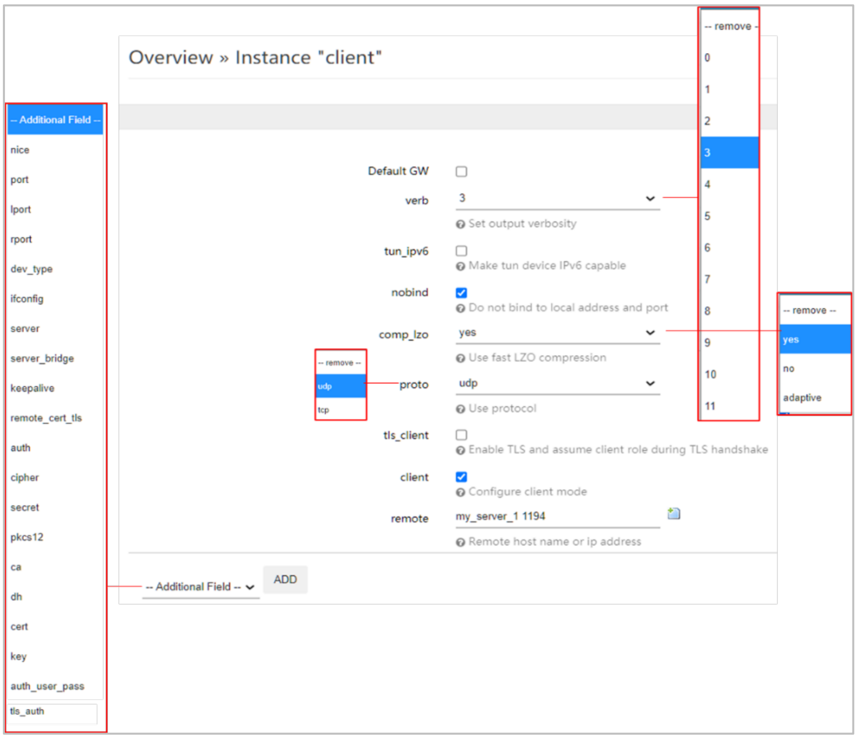
keepalive 10 120
Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations

proto udp
Use protocol

tls_client □
Enable TLS and assume client role during TLS handshake

client □
Configure client mode

Figure 8-10: Edit client (CAT4)



Overview » Instance "client"

Default GW □

verb 3

Set output verbosity

tun_ipv6 □

Make tun device IPv6 capable

nobind ☑

Do not bind to local address and port

comp_lzo yes

Use fast LZO compression

proto udp

Use protocol

tls_client □

Enable TLS and assume client role during TLS handshake

client ☑

Configure client mode

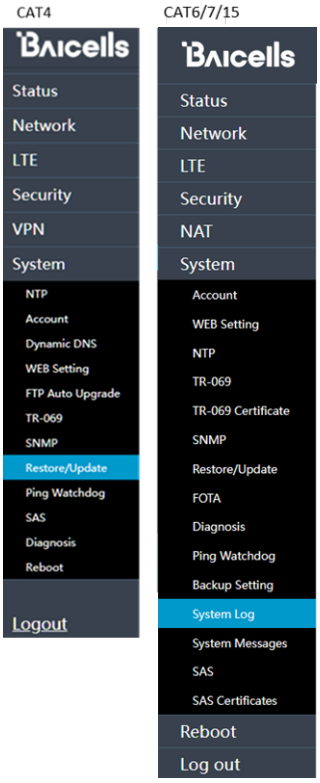
remote my_server_1 1194

Remote host name or ip address

9 System Menu

The *System* menu provides additional options for the CPE features. The sub-menus are different between CAT4 and CAT6/7/15 - some in a different order, some with different names for essentially the same functions, and some that are simply added or missing in comparison of the two *System* menus (Figure 9-1). Each sub-menu for both CAT4 and CAT6/7/15 is explained in the sections that follow.

Figure 9-1: System Menu

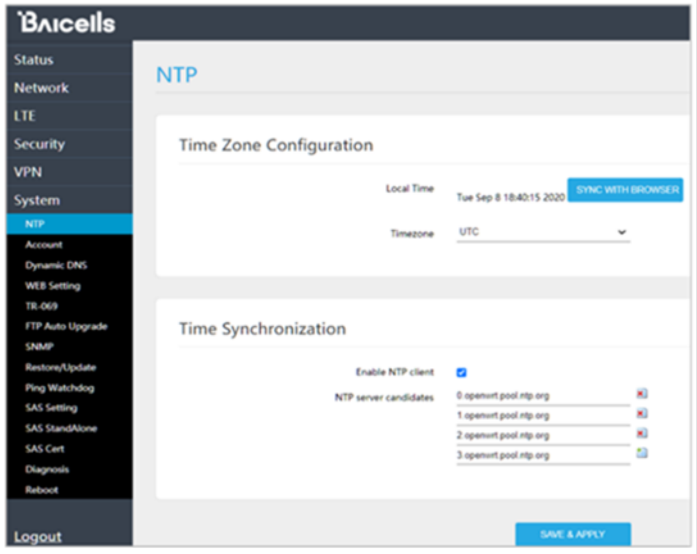


9.1 NTP

The operator can configure up to four NTP servers to provide correct time-of-day to the network devices. In the CPE GUI you can establish the time zone that the CPE is in, and enable NTP client to use any of the defined NTP services or select one or more specific NTP servers the CPE will use for time synchronization with the network (Figure 9-2). In CAT6/7/15, you can set the synchronization mode manually as well. In CAT6/7/15, you can also enable Daylight Saving Time to automatically start and stop on the designated dates. Use the *SYNC WITH BROWSER* button (CAT4) to refresh the local time that is displayed.

Figure 9-2: NTP

CAT4



NTP

Time Zone Configuration

Local Time Tue Sep 8 18:40:15 2020

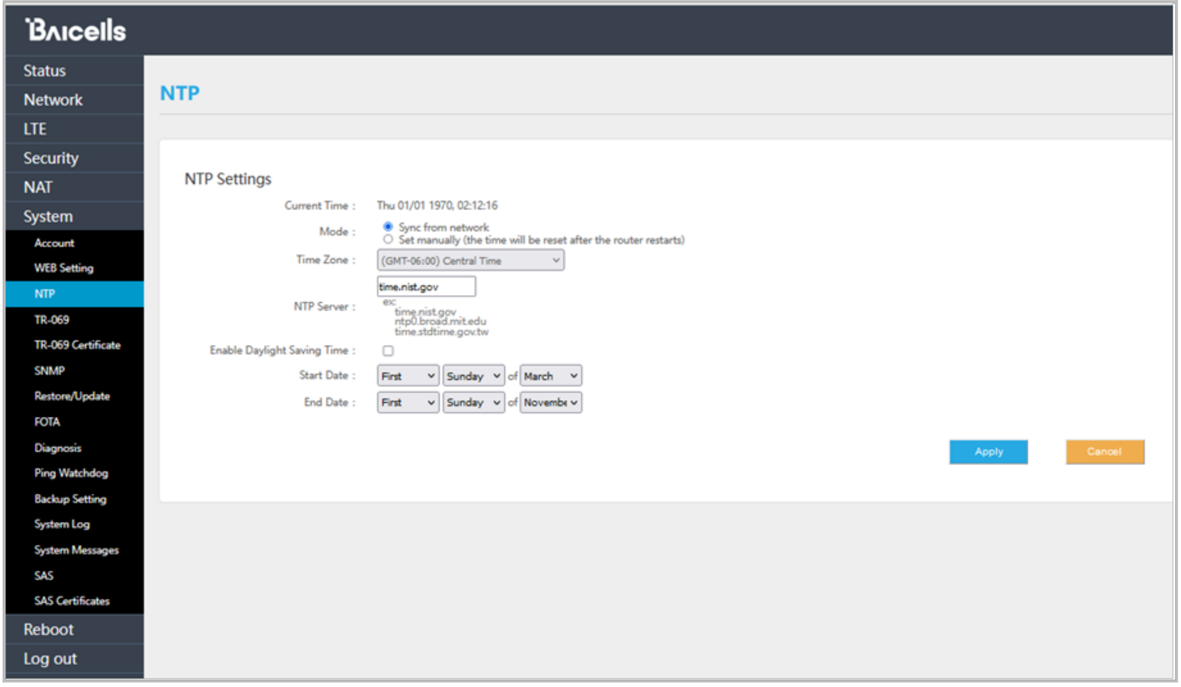
Timezone UTC

Time Synchronization

Enable NTP client ☑

NTP server candidates
0.openwrt.pool.ntp.org
1.openwrt.pool.ntp.org
2.openwrt.pool.ntp.org
3.openwrt.pool.ntp.org

CAT6/7/15



NTP

NTP Settings

Current Time : Thu 01/01 1970, 02:12:16

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

Time Zone : (GMT-06:00) Central Time

NTP Server : time.nist.gov
exc
time.nist.gov
ntp0.broad.mit.edu
time.stdtime.gov.tw

Enable Daylight Saving Time : □

Start Date : First Sunday of March

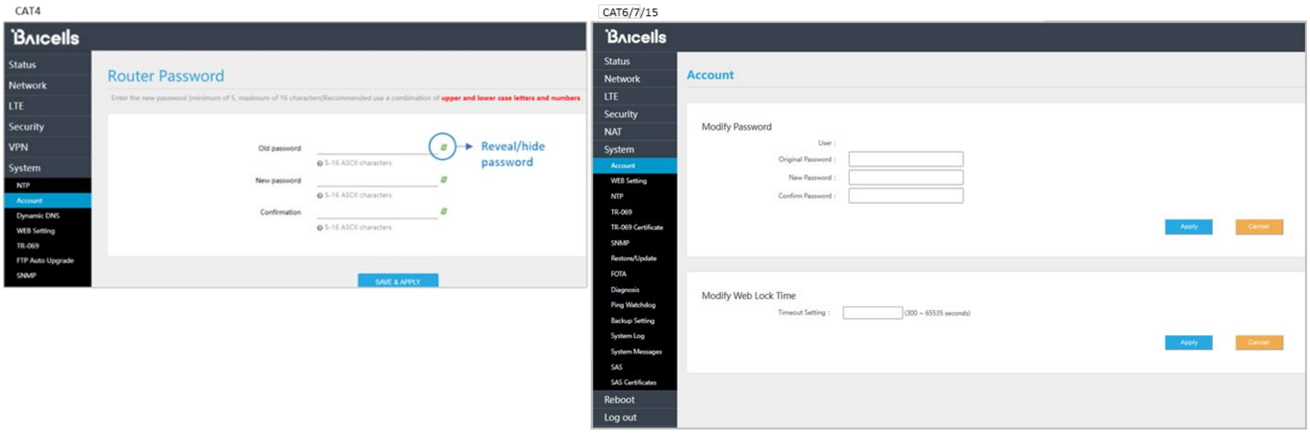
End Date : First Sunday of Novembe

9.2 Account

The *System > Account* sub-menu is used to change the CPE administrative user's login password (Figure 9-3). The password must be five to 12 characters. Baicells recommends using a combination of upper- and lower-case letters and numbers. The new password must be re-entered to confirm it.

In the CAT6/7/15 GUI, you can also set a Web Lock Time which will force a logout of users after that period of time. Enter 0 to 65535 (default) seconds.

Figure 9-3: Account



CAT4

Router Password

Enter the new password (minimum of 5, maximum of 16 characters)Recommended use a combination of upper and lower case letters and numbers.

Old password
5-16 ASCII characters
New password
5-16 ASCII characters
Confirmation
5-16 ASCII characters

Reveal/hide password

CAT6/7/15

Account

Modify Password
User :
Original Password :
New Password :
Confirm Password :

Modify Web Lock Time
Timeout Setting : (300 ~ 65535 seconds)

9.3 Dynamic DNS (CAT4)

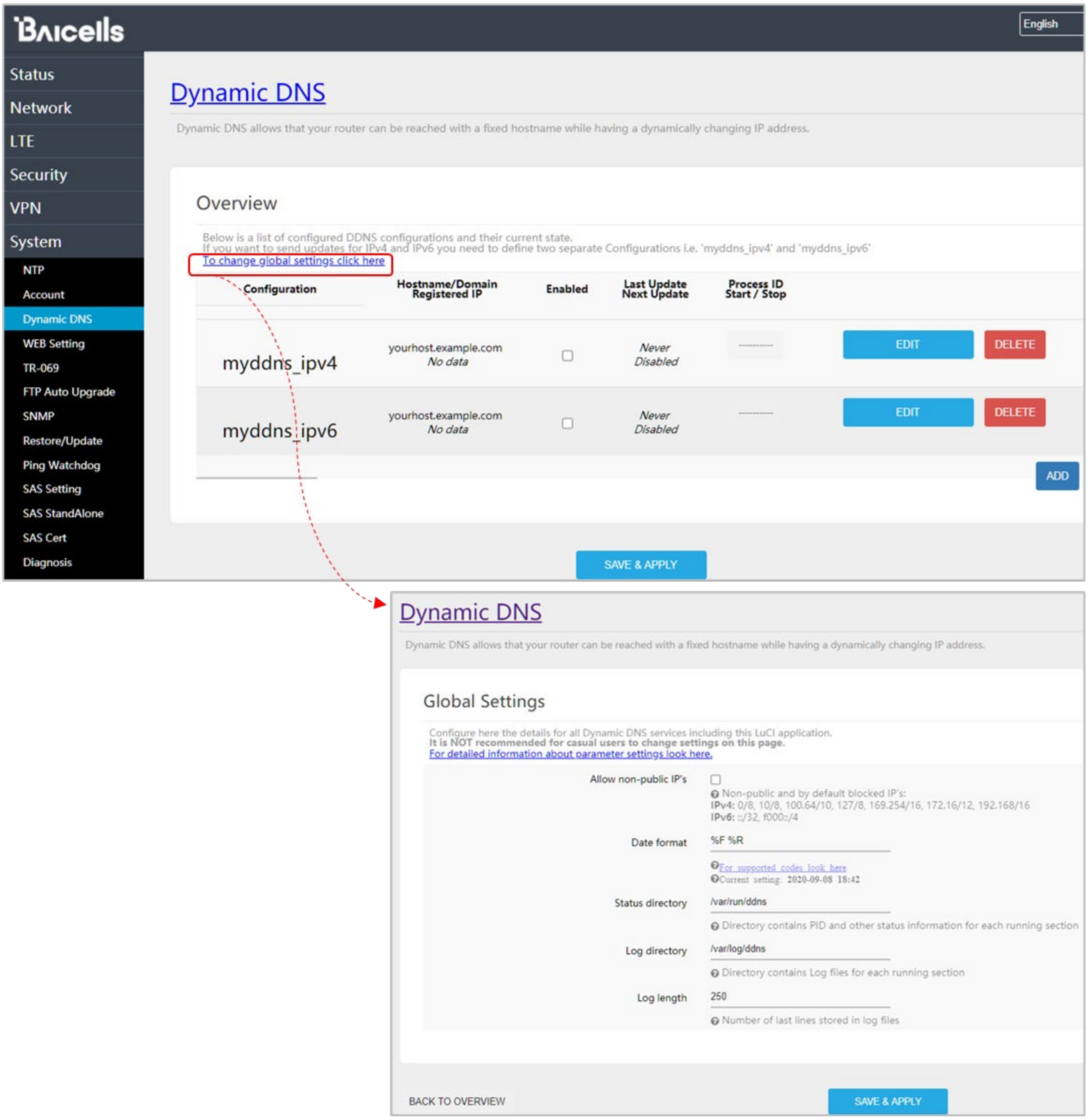
Caution: Baicells recommends that only experienced IP networking professionals change or configure the Dynamic DNS settings. It is not recommended for casual users.

Typically the CPE, functioning as a router, changes the IP address of connected devices periodically. The Dynamic Domain Name System (DNS) is a service that assigns the CPE a fixed domain name even when it is using a dynamic IP address. It makes a dynamic IP address act as though it is static.

This feature is based on the OpenWRT Project, a Linux OS based application. For more information on OpenWRT and client configuration options, please visit *https://openwrt.org*.

To view the global Dynamic DNS settings, click on the link in the *Overview* window that says "*To change global settings, click here*" as shown in Figure 9-4. This opens a *Global Settings* window where you can enter or change the settings that will affect IPv4 and IPv6 traffic.

Figure 9-4: Dynamic DNS (CAT4)



Dynamic DNS

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

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	Hostname/Domain 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

Dynamic DNS

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

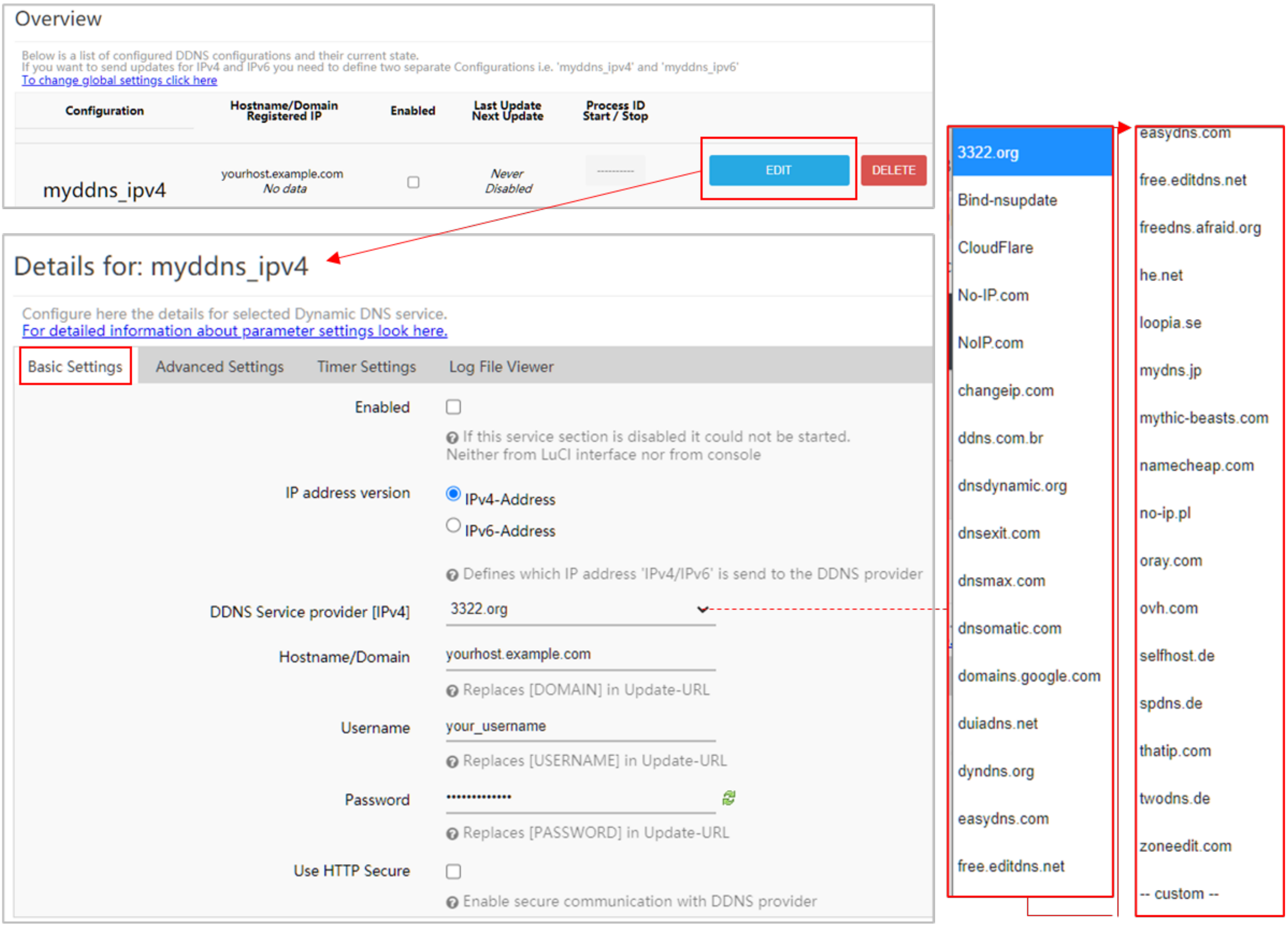
Global Settings

Configure here the details for all Dynamic DNS services including this LuCI application.
It is NOT recommended for casual users to change settings on this page.
For detailed information about parameter settings look here.

Allow non-public IP's	□ Non-public and by default blocked IP's: **IPv4:** 0/8, 10/8, 100.64/10, 127/8, 169.254/16, 172.16/12, 192.168/16 **IPv6:** ::/32, f000::/4
Date format	%F %R For supported codes look here Current setting: **2020-09-08 18:42**
Status directory	/var/run/ddns Directory contains PID and other status information for each running section
Log directory	/var/log/ddns Directory contains Log files for each running section
Log length	250 Number of last lines stored in log files

To edit the existing *myddns_ipv4* or *myddns_ipv6* Dynamic DNS settings, in the *Overview* window click on *Edit*. The *Details* page will show four tabs: *Basic Settings*, *Advanced Settings*, *Timer Settings*, and *Log File Viewer* (Figure 9-5). The other tabs are shown in Figure 9-6, Figure 9-7, and Figure 9-8. The examples are for *myddns_ipv4*.

Figure 9-5: Edit - Basic Settings Tabs (CAT4)



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	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
myddns_ipv4	yourhost.example.com *No data*	□	*Never* *Disabled*	----------	EDIT DELETE

Details for: myddns_ipv4

Configure here the details for selected Dynamic DNS service.
For detailed information about parameter settings look here.

Basic Settings | Advanced Settings | Timer Settings | Log File Viewer

Enabled □
If this service section is disabled it could not be started. Neither from LuCI interface nor from console

IP address version ● IPv4-Address ○ IPv6-Address
Defines which IP address 'IPv4/IPv6' is send to the DDNS provider

DDNS Service provider [IPv4]: 3322.org

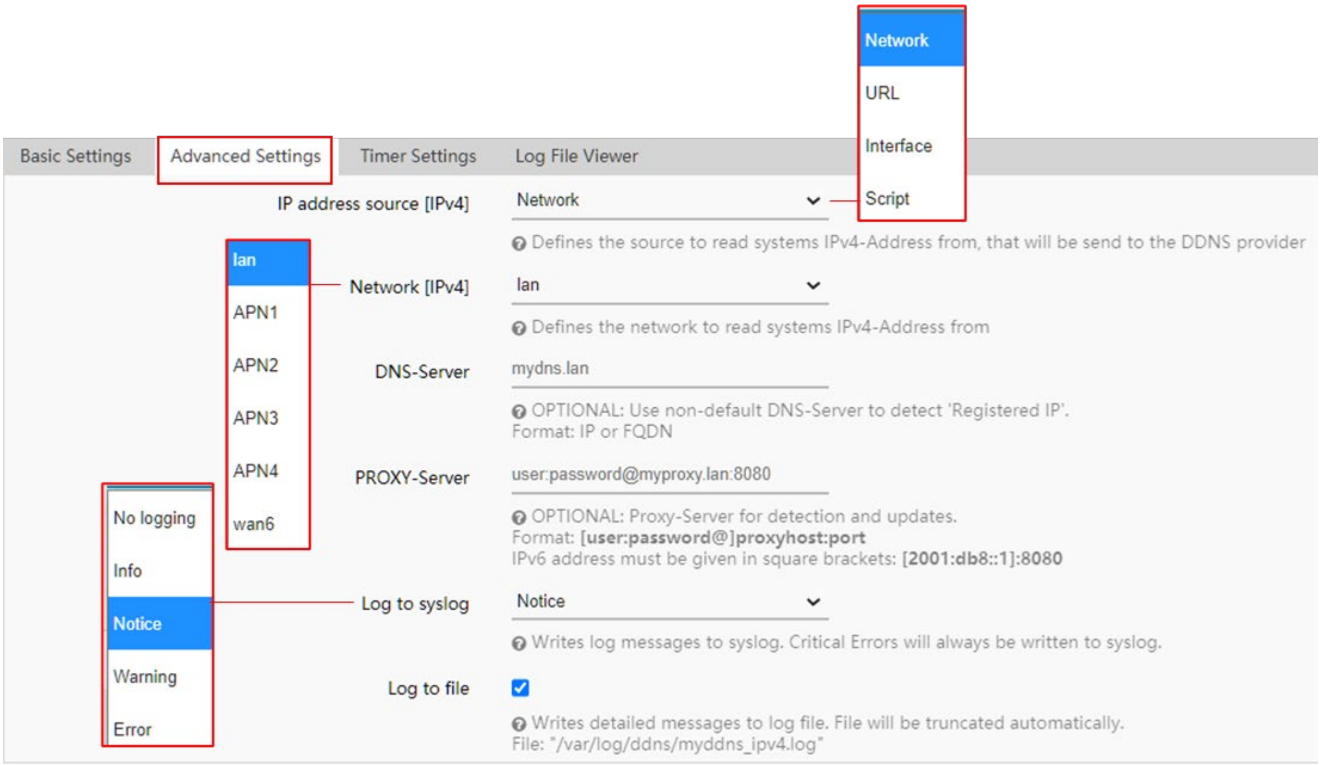
Hostname/Domain: yourhost.example.com
Replaces [DOMAIN] in Update-URL

Username: your_username
Replaces [USERNAME] in Update-URL

Password: ••••••••••••
Replaces [PASSWORD] in Update-URL

Use HTTP Secure □
Enable secure communication with DDNS provider

Figure 9-6: Advanced Settings (CAT4)



Basic Settings | Advanced Settings | Timer Settings | Log File Viewer

IP address source [IPv4]: Network
Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider

Network [IPv4]: lan
Defines the network to read systems IPv4-Address from

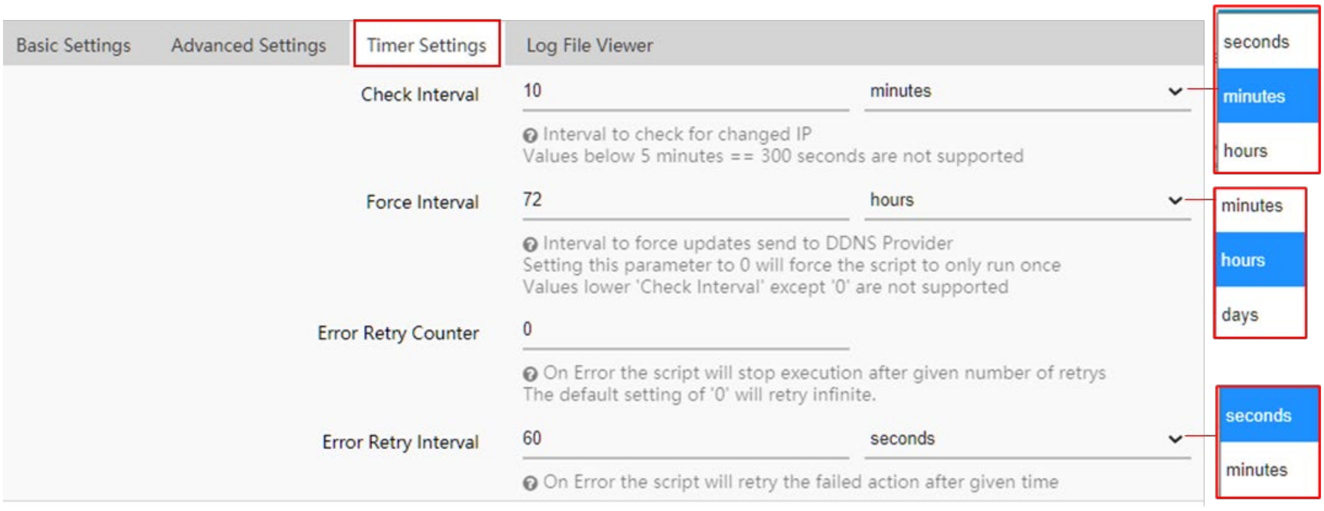
DNS-Server: mydns.lan
OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'.
Format: IP or FQDN

PROXY-Server: user:password@myproxy.lan:8080
OPTIONAL: Proxy-Server for detection and updates.
Format: **[user:password@]proxyhost:port**
IPv6 address must be given in square brackets: **[2001:db8::1]:8080**

Log to syslog: Notice
Writes log messages to syslog. Critical Errors will always be written to syslog.

Log to file ☑
Writes detailed messages to log file. File will be truncated automatically.
File: "/var/log/ddns/myddns_ipv4.log"

Figure 9-7: Timer Settings (CAT4)



Check Interval: 10 minutes

Interval to check for changed IP
Values below 5 minutes == 300 seconds are not supported

Force Interval: 72 hours

Interval to force updates send to DDNS Provider
Setting this parameter to 0 will force the script to only run once
Values lower 'Check Interval' except '0' are not supported

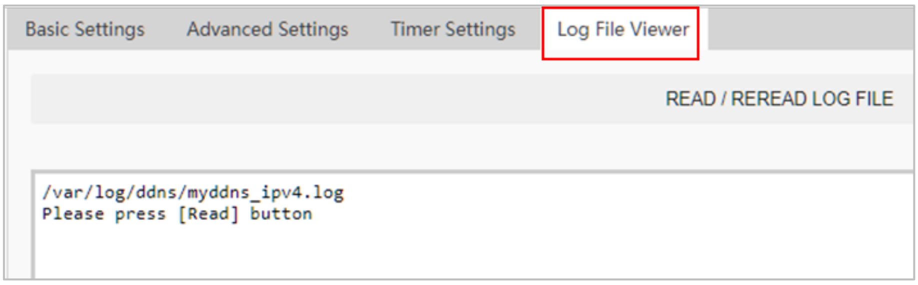
Error Retry Counter: 0

On Error the script will stop execution after given number of retrys
The default setting of '0' will retry infinite.

Error Retry Interval: 60 seconds

On Error the script will retry the failed action after given time

Figure 9-8: Log File Viewer (CAT4)

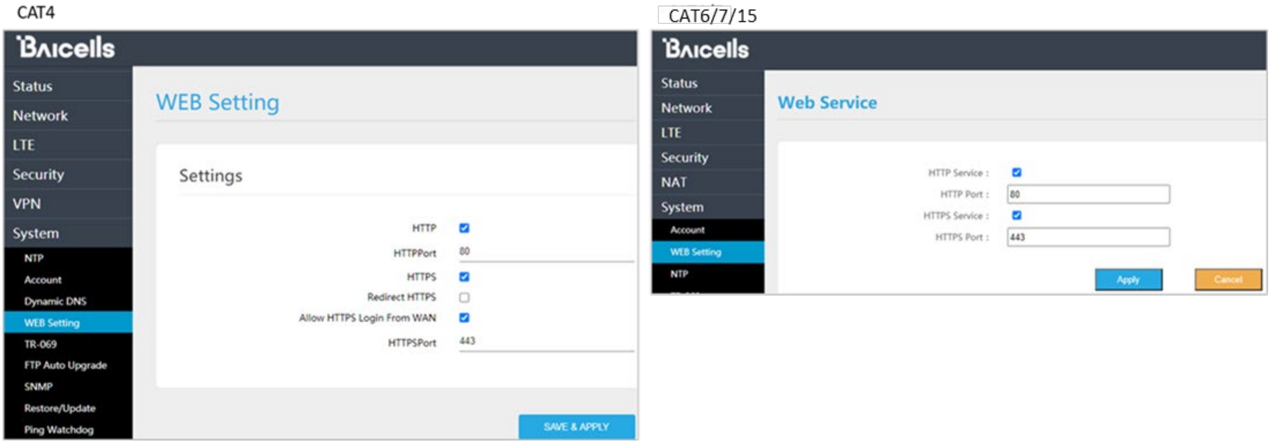


```
/var/log/ddns/myddns_ipv4.log
Please press [Read] button
```

9.4 WEB Setting

The *WEB Setting* is used to enable remote Web access to the CPE. This is especially necessary for support technicians who are troubleshooting issues. Refer to Figure 9-9 to see the CAT4 and CAT6/7/15 fields, and to Table 9-1 for a description of each field.

Figure 9-9: WEB Setting



CAT4

WEB Setting

Settings

HTTP ☑
HTTPPort 80
HTTPS ☑
Redirect HTTPS □
Allow HTTPS Login From WAN ☑
HTTPSPort 443

CAT6/7/15

Web Service

HTTP Service : ☑
HTTP Port : 80
HTTPS Service : ☑
HTTPS Port : 443

Table 9-1: WEB Setting

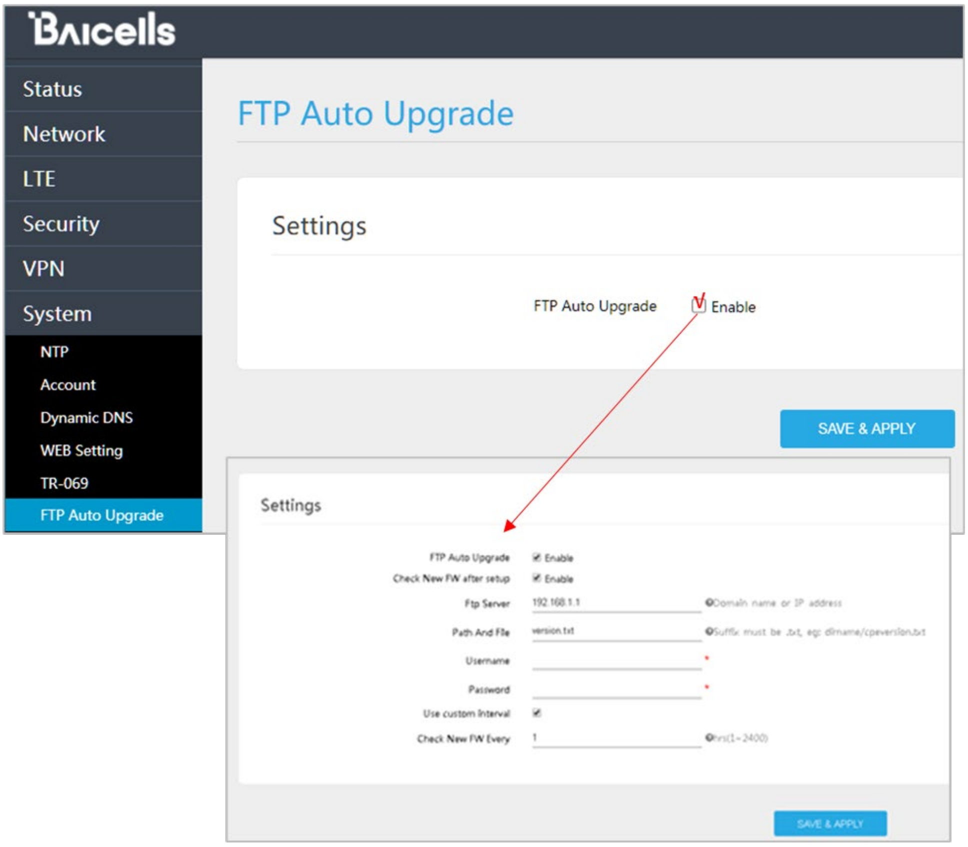
Field Name	Description
HTTP or HTTP Service	Select the checkbox to enable the ability to log in to the CPE through an HTTP Web address
HTTPPort	Enter the HTTP port number to be used. Range is 80 to 65,535. Default is port 80.
HTTPS or HTTP Service	Select the checkbox to enable the ability to log in to the CPE through an HTTPS Web address
Redirect HTTPS	Select the checkbox to allow HTTP addresses to be redirected to more secure HTTPS addresses
Allow HTTPs Login From WAN	Select the checkbox next to *Enable* to log in to an HTTPs Web address from the WAN
HTTPS Port	Enter the HTTPS port number to be used. Range is 80 to 65,535. Default is port 443.

9.5 FTP Auto Upgrade (CAT4)

FTP Auto Upgrade is an optional feature that can be used for Over-The-Air (OTA) firmware upgrades. The CPE will detect a new version of firmware on the dedicated FTP server and will automatically upgrade to the latest version.

Looking at Figure 9-10, select the *Enable* checkbox next to the *FTP Auto Upgrade* field. This will open additional settings. Enable *Check New FW after setup*, and enter the *Ftp Server* domain name or IP address and the *Path And File* text suffix. If login permissions are required to access the server, enter the *Username* and *Password*. To configure a set interval for the CPE to check the server for new firmware, select the checkbox next to *Use custom Interval* and enter the interval time, in hours. The range is 1-2400 hours.

Figure 9-10: FTP Auto Upgrade (CAT4)



FTP Auto Upgrade

Settings

FTP Auto Upgrade ☑ Enable

SAVE & APPLY

Settings

FTP Auto Upgrade ☑ Enable

Check New FW after setup ☑ Enable

Ftp Server 192.168.1.1 Domain name or IP address

Path And File version.txt Suffix must be .txt, eg: dirname/cpeversion.txt

Username *

Password *

Use custom Interval ☑

Check New FW Every 1 hrs(1~2400)

SAVE & APPLY

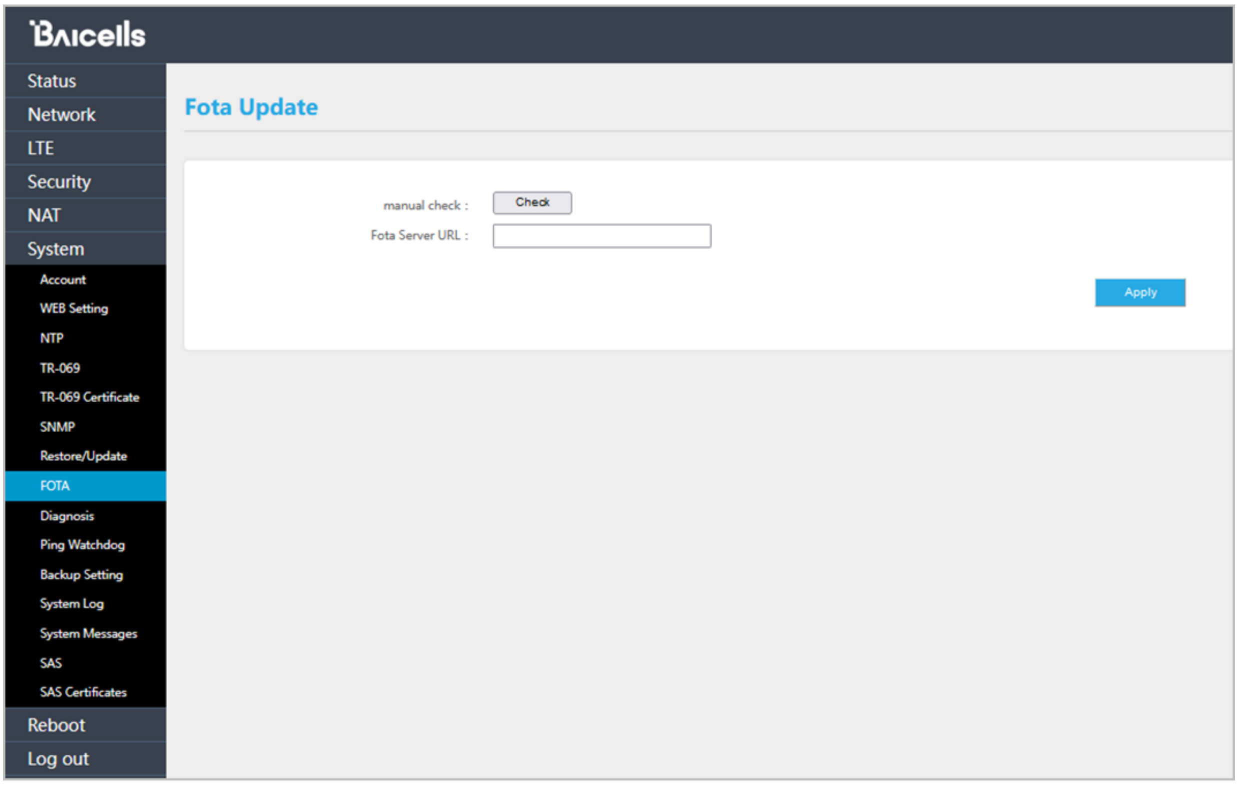
9.6 FOTA (CAT6/7/15)

The *System* > *FOTA* sub-menu is used to upgrade Firmware Over-The-Air (FOTA) (Figure 9-11). The CPE will detect a new version of firmware on the dedicated FTP server and will automatically upgrade to the latest version.

In the *Fota Update* window, select *Check*. If an upgraded firmware file is available, the Fota Server URL will display the file path. To apply the upgraded firmware, click *Apply*.

If no upgraded firmware file is found, the system will return a message, "*[FOTA] No new version available.*" Select *OK* to close the system message window.

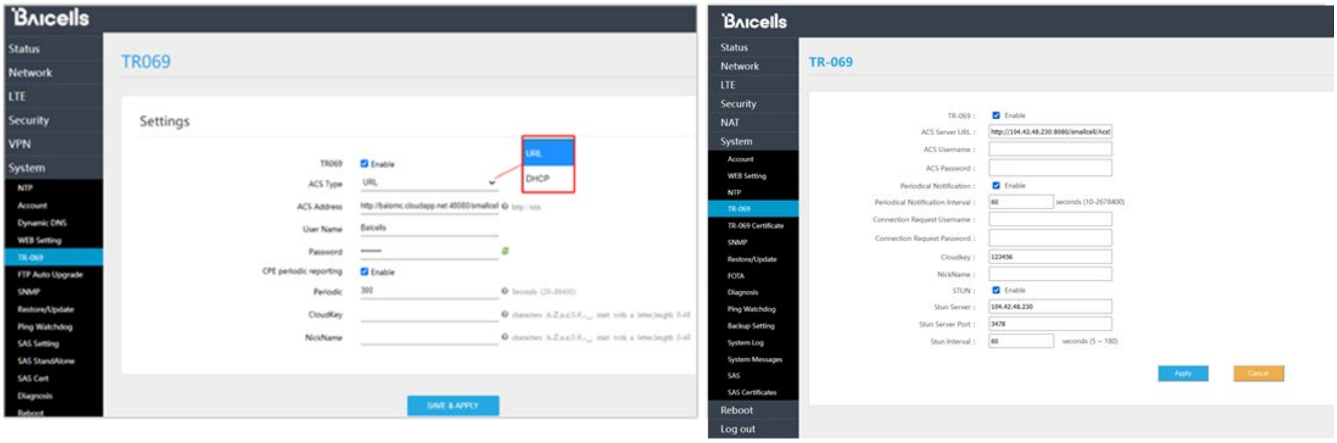
Figure 9-11: FOTA (CAT6/7/15)



9.7 TR-069

The network devices use a TR-069 connection to an Automatic Configuration Server (ACS), in most cases, the Baicells CloudCore Operations Management Console (OMC) or a Local OMC. Refer to Figure 9-12 and Table 9-2 (CAT4) or Table 9-3 (CAT6/7/15) to configure the settings.

Figure 9-12: TR-069



CAT4

TR069

Settings

TR069: ☑ Enable

ACS Type: URL

ACS Address: http://baiomc.cloudapp.net:48080/smallcel

User Name: Baicells

Password: ••••••

CPE periodic reporting: ☑ Enable

Periodic: 300

CloudKey:

NickName:

CAT6/7/15

TR-069

TR-069 : ☑ Enable

ACS Server URL : http://104.42.48.230:8080/smallcell/Acs

ACS Username :

ACS Password :

Periodical Notification : ☑ Enable

Periodical Notification Interval : 60 seconds (10-2678400)

Connection Request Username :

Connection Request Password :

Cloudkey : 123456

NickName :

STUN : ☑ Enable

Stun Server : 104.42.48.230

Stun Server Port : 3478

Stun Interval : 60 seconds (5 ~ 180)

Table 9-2: TR-069 (CAT4)

Field Name	Description
TR069	Select the checkbox next to *Enable* to enable a TR-069 automatic configuration service (ACS)
ACS Type	Select *URL* or *DHCP* to identify the source of the ACS service. When you select *URL*, the next field (*ACS Address*) appears.
ACS Address	Enter the server Web address, typically the Baicells CloudCore OMC or a Local OMC. • CloudCore OMC: *http://baiomc.cloudapp.net:48080/smallcell/AcsService* • Local OMC: http://xx.xx.xx.xx:8080/smallcell/AcsService
User Name	Enter the user name to access the ACS server
Password	Enter the password to access the ACS server
CPE periodic reporting	Select the checkbox next to *Enable* to enable the CPE to periodically check with the ACS server for new software
Periodic	If you enabled CPE periodic reporting, input how often the CPE should check the ACS server for current information. The range is 20 to 86,400 seconds.
CloudKey	Enter the operator's unique CloudKey . When the device powers up the first time it will automatically be added to the operator's CloudCore account.
NickName	Optional – enter a nickname to identify the server

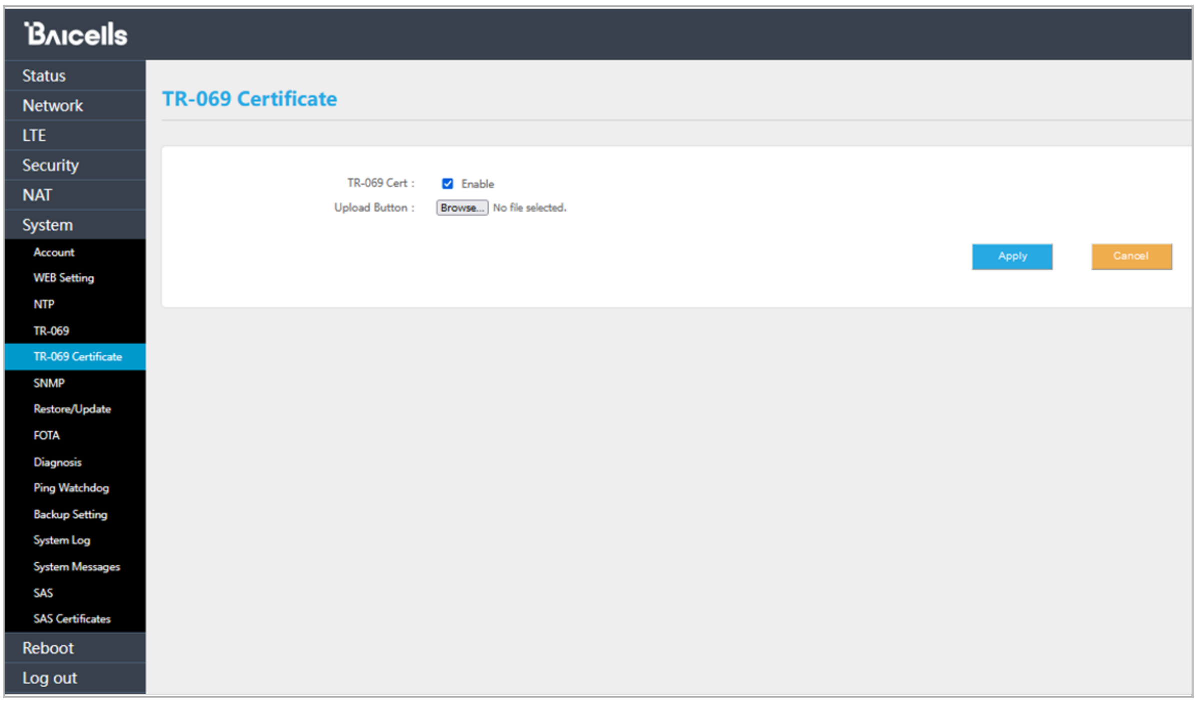
Table 9-3: TR-069 (CAT6/7/15)

Field Name	Description
TR069	Select the checkbox next to *Enable* to enable a TR-069 automatic configuration service (ACS)
ACS Server URL	Enter the server Web address, typically the Baicells CloudCore OMC or a Local OMC. • CloudCore OMC: *http://baiomc.cloudapp.net:48080/smallcell/AcsService* • Local OMC: http://xx.xx.xx.xx:8080/smallcell/AcsService
ACS Username	Enter the user name to access the ACS server
ACS Password	Enter the password to access the ACS server
Periodical Notification	Select the checkbox next to *Enable* to enable the CPE to periodically check with the ACS server for new software
Periodical Notification Interval	If you enabled CPE periodic reporting, input how often the CPE should check the ACS server for current information. The range is 10 to 2,678,400 seconds.
Connection Request Username	If you are using a third-party ACS server, they may require a connection request username. If so, enter that username in this field.
Connection Request Password	If you are using a third-party ACS server, they may require a connection request password. If so, enter that password in this field.
Cloudkey	Enter the operator's unique CloudKey . When the device powers up the first time it will automatically be added to the operator's CloudCore account.
NickName	Optional – enter a nickname to identify the server
STUN	Select the checkbox next to *Enable* to enable a Session Traversal Utilities for NAT (STUN) server
STUN Server	Enter the STUN server IP address
STUN Server Port	Enter the STUN server port number
STUN Interval	If you enabled STUN, input how often the CPE should check the STUN server for current information. The range is 5 to 180 seconds.

9.8 TR-069 Certificate (CAT6/7/15)

The *System > TR-069 Certificate* sub-menu is used to upload the TR-069 authorization certificate for this CPE (Figure 9-13). In the *TR-069 Certificate* window, select the *Enable* checkbox next to *TR-069 cert*. Then, next to *Upload Button* click on *Browse…*. Navigate to the certificate file, select it, and click on *Apply*.

Figure 9-13: TR-069 Certificate (CAT6/7/15)



TR-069 Certificate

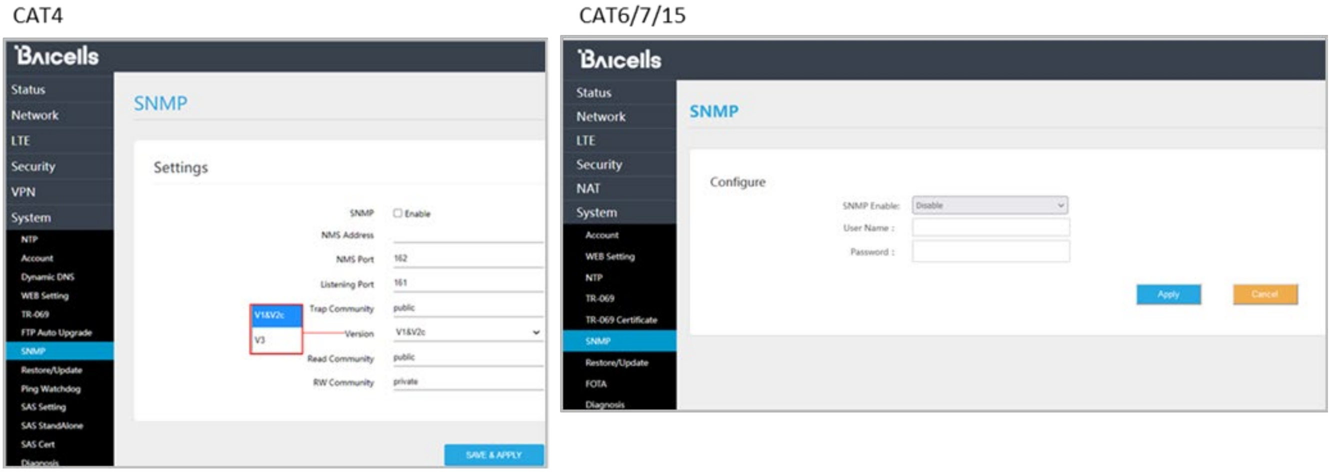
TR-069 Cert : ☑ Enable

Upload Button : Browse... No file selected.

9.9 SNMP

The Simple Network Management Protocol (SNMP) is used for connecting a device with a Network Management System (NMS) server. When enabled, the operator's NMS can monitor and control the connected CPE. The NMS will be able to collect event logs, alarm logs, and other data from the CPE. Refer to Figure 9-14 and to Table 9-4 (CAT4) or Table 9-5 (CAT6/7/15) for a description of each field to configure SNMP.

Figure 9-14: SNMP



CAT4

SNMP

Settings

SNMP ☐ Enable

NMS Address

NMS Port 162

Listening Port 161

Trap Community public

Version V1&V2c

Read Community public

RW Community private

CAT6/7/15

SNMP

Configure

SNMP Enable: Disable

User Name :

Password :

Table 9-4: SNMP (CAT4)

Field Name	Description
SNMP	Enable Simple Network Management Protocol by clicking the checkbox.
NMS Address	NMS server IP address
NMS Port	NMS server port number
Listening Port	Peer port number for the CPE to listen to packets from the NMS

Field Name	Description
Trap Community	Public or private - select read/write permissions for data from the CPE to the NMS
Version	Select the SNMP protocol version to use- V1&V2c (for SNMPv1+SNMPv2c) or V3 (for SNMPv3)
Read Community	Public or private. Read-only community name.
RW Community	Public or private. Read/Write community name.

Table 9-5: SNMP (CAT6/7/15)

Field Name	Description
SNMP	Enable Simple Network Management Protocol by clicking the checkbox.
User Name	Enter the user name to access the NMS server via SNMP
User Password	Enter the user password to access the NMS server via SNMP

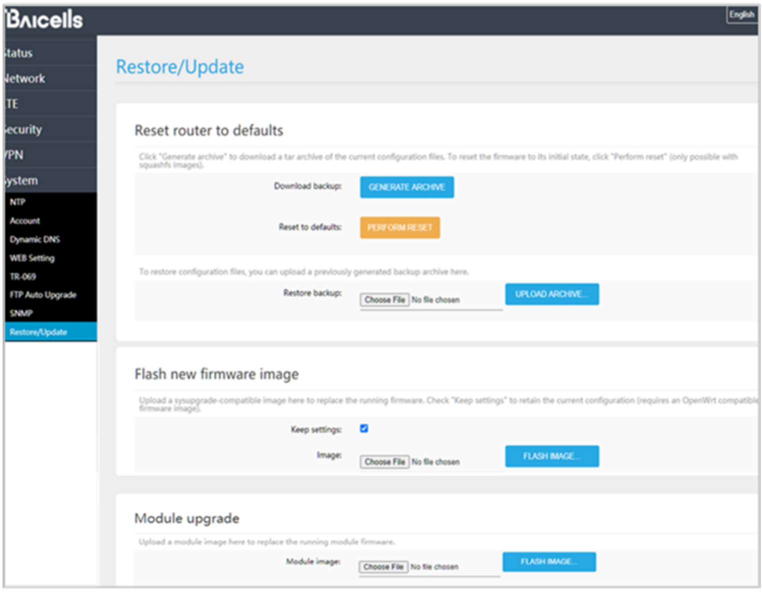
9.10 Restore/Update (CAT4/6/7/15) and Backup Setting (CAT6/7/15)

Baicells periodically issues new firmware to introduce new features, enhance existing features, and fix any bug issues. New firmware availability is announced in the OMC. The *System > Restore/Update* sub-menu is used to update the firmware or to restore all of the GUI settings to their default values. In the case of CAT4, the sub-menu also includes the ability to download/export or restore/import a backup file of the configuration settings; the same function is available on CAT6/7/15 but is in a separate sub-menu: *System > Backup Setting*. Refer to Figure 9-15. The procedure for each function is in the sections that follow.

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

Figure 9-15: Restore/Update (CAT4/6/7/15) and Backup Setting (CAT6/7/15)

CAT4



Restore/Update

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:

Reset to defaults:

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

Restore backup: No file chosen

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: ☑

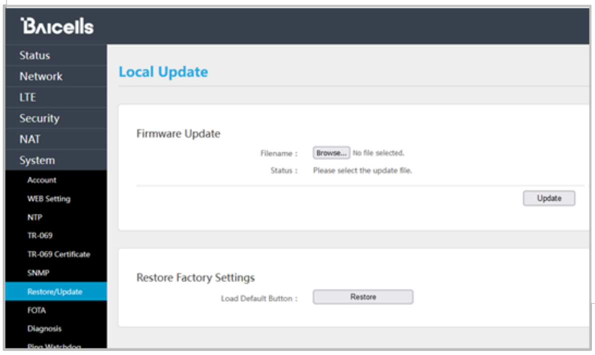
Image: No file chosen

Module upgrade

Upload a module image here to replace the running module firmware.

Module image: No file chosen

CAT6/7/15 Restore/Update



Local Update

Firmware Update

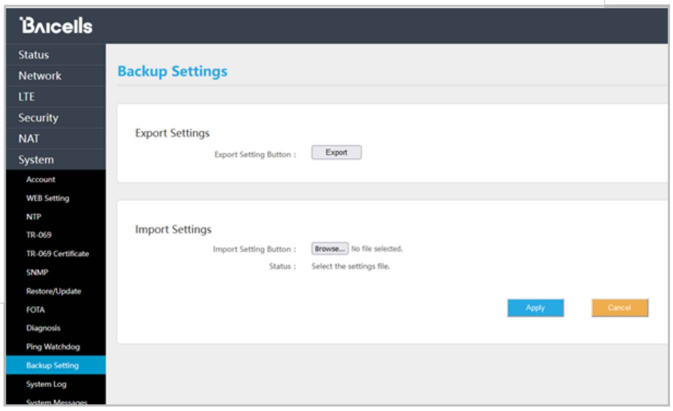
Filename : No file selected.

Status : Please select the update file.

Restore Factory Settings

Load Default Button :

CAT6/7/15 Backup Setting



Backup Settings

Export Settings

Export Setting Button :

Import Settings

Import Setting Button : No file selected.

Status : Select the settings file.

9.10.1 Backup and Restore

You can back up and save the current GUI settings in the event you might need to restore the data on the CPE at a later time. In the CAT4 GUI, go to *System > Restore/Update* and under the *Reset router to defaults* pane click on *GENERATE ARCHIVE*. To initiate a Restore action, in the *Reset router to defaults* pane click on *Choose File* in the *Restore backup* field, navigate to the backup file and, once selected, click on *UPLOAD ARCHIVE*.

In the CAT6/7/15 GUI, to back up the configuration go to *System > Backup Setting* and in the *Export Settings* pane select *Export*. To restore a backup file, under the *Import Settings* pane click on *Choose File*, navigate to and select the file, and click on *Apply*.

9.10.2 Restore Default Settings

To restore the default configuration values in the GUI, for CAT4 go to *System > Restore/Update* and select the *PERFORM RESET* button. In the CAT6/7/15, under the *Restore Factory Settings* pane, click on *Restore*.

9.10.3 Update Firmware

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

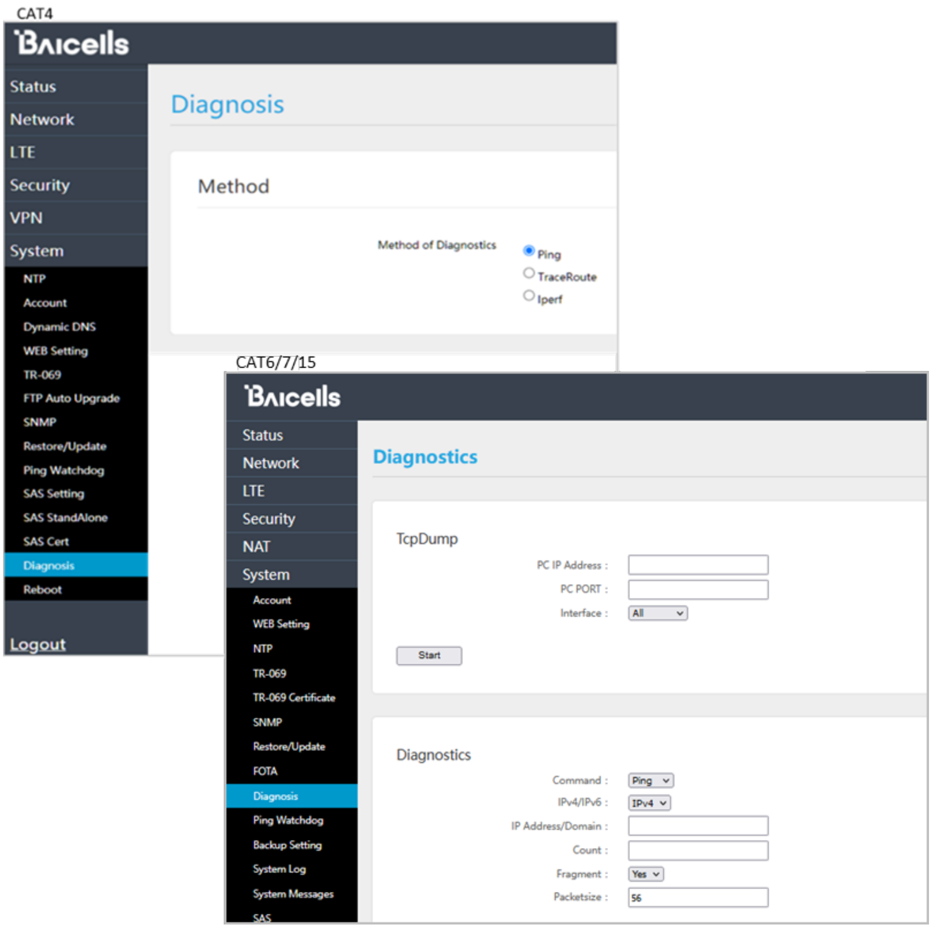
In the CAT4 *Flash new firmware image* pane, select the *Keep settings* checkbox if you want to retain the current configuration settings on the new firmware. Then, select *Choose File* and navigate to the firmware image file. Once you select the file, click on *FLASH IMAGE*. Use the *Module upgrade* function, if directed to do so by Baicells, to upgrade a specific module within the CPE.

In the CAT6/7/15 *Firmware Update* pane, select *Browse…* to navigate to the firmware image file and once the file is selected, click on *Update*. In CAT6/7/15 the current configuration settings are automatically saved.

9.11 Diagnosis

The *System > Diagnosis* sub-menu provides diagnostic tests that can be used for monitoring and troubleshooting connection issues. On the CAT4, there are three diagnostic tests available: *Ping*, *TraceRoute*, and *Iperf* (Figure 9-16). The CAT6/7/15 supports *TcpDump*, *Ping*, and *Trace*. Each type of test is explained in the following sections.

Figure 9-16: Diagnosis



Diagnosis

Method

Method of Diagnostics ● Ping ○ TraceRoute ○ Iperf

Diagnostics

TcpDump

PC IP Address :
PC PORT :
Interface : All

Diagnostics

Command : Ping
IPv4/IPv6 : IPv4
IP Address/Domain :
Count :
Fragment : Yes
Packetsize : 56

9.11.1 Ping

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

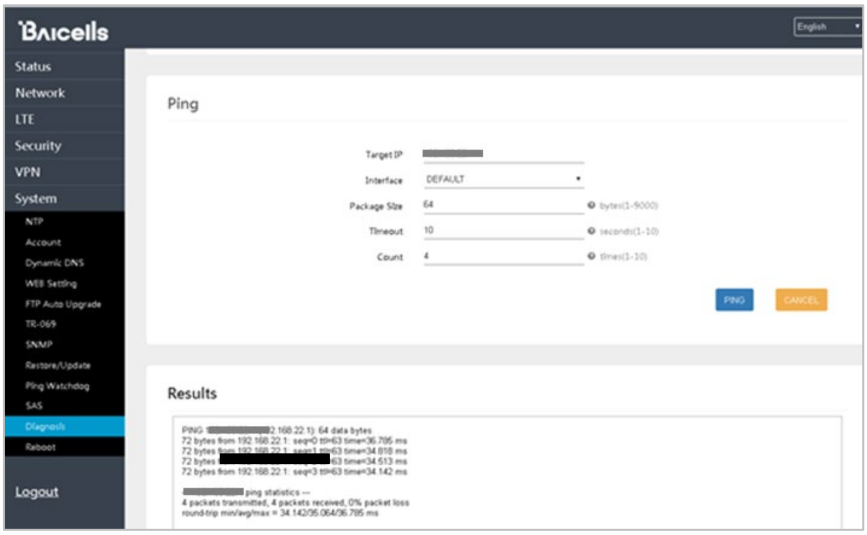
9.11.1.1 CAT4

To initiate a ping test on a CAT4 CPE (Figure 9-17):

1. Go to *System* > *Diagnosis*, and select the *Ping* radio button as the *Method of Diagnostics*.
2. *Target IP*: Enter the device IP address for the CPE to ping.
3. *Interface*: Select which interface the CPE should use (either *DEFAULT*, *APN1*, *APN2*, *APN3*, or *APN4)*.
4. *Package Size*: Enter the data packet size to be sent to the target IP address. Range: 1-9000 bytes.
5. *Timeout*: Set a timeout period. Range: 1-10 seconds.
6. *Count*: Enter the number of times you want the ping test to execute. Range: 1-10 times.
7. Click on the *PING* button. The test will start immediately.

Results of the ping test will appear at the bottom of the window, showing the target IP address, the number of data bytes sent, the number of packets transmitted, the number of packets received, and the percentage of packets lost.

Figure 9-17: CAT4 Ping



Ping

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

Results

```
PING 1[redacted]2.168.22.1): 64 data bytes
72 bytes from 192.168.22.1: seq=0 ttl=63 time=36.785 ms
72 bytes from 192.168.22.1: seq=1 ttl=63 time=34.818 ms
72 bytes [redacted]63 time=34.513 ms
72 bytes from 192.168.22.1: seq=3 ttl=63 time=34.142 ms

[redacted] ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 34.142/35.064/36.785 ms
```

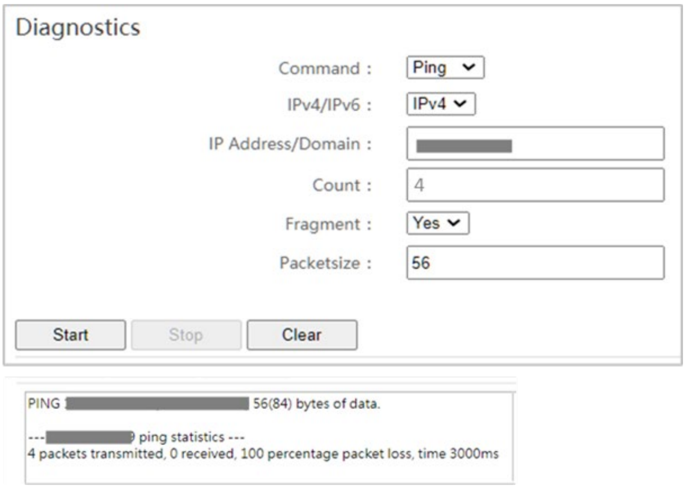
9.11.1.2 CAT6/7/15

To initiate a ping test on a CAT6/7/15 CPE (Figure 9-18):

1. Go to *System* > *Diagnosis*, and at the *Command* field in the *Diagnostics* pane select *Ping* from the pull-down menu.
2. *IPv4/IPv6*: Select if you want to use *IPv4* or *IPv6* packets.
3. *IP Address/Domain*: Enter the target device's IP address or a domain name for the CPE to ping.
4. *Count*: Enter the number of times you want the ping test to execute. Range: 1-10 times.
5. *Fragment*: Allow IP fragments, *Yes* or *No*.
6. *Packetsize*: Enter the data packet size to be sent to the target IP address. Range: 1-9000 bytes.
7. Click on the *Start* button. The test will start immediately.

Results of the ping test will appear at the bottom of the window, showing the IP address to which the pings were sent; the number of data bytes sent; the number of packets transmitted; the number of packets received; the percentage of packets lost; and the amount of time, in milliseconds.

Figure 9-18: CAT6/7/15 Ping



Diagnostics

Command : Ping

IPv4/IPv6 : IPv4

IP Address/Domain : [redacted]

Count : 4

Fragment : Yes

Packetsize : 56

```
PING [redacted] 56(84) bytes of data.

---[redacted] ping statistics ---
4 packets transmitted, 0 received, 100 percentage packet loss, time 3000ms
```

9.11.2 TraceRoute

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

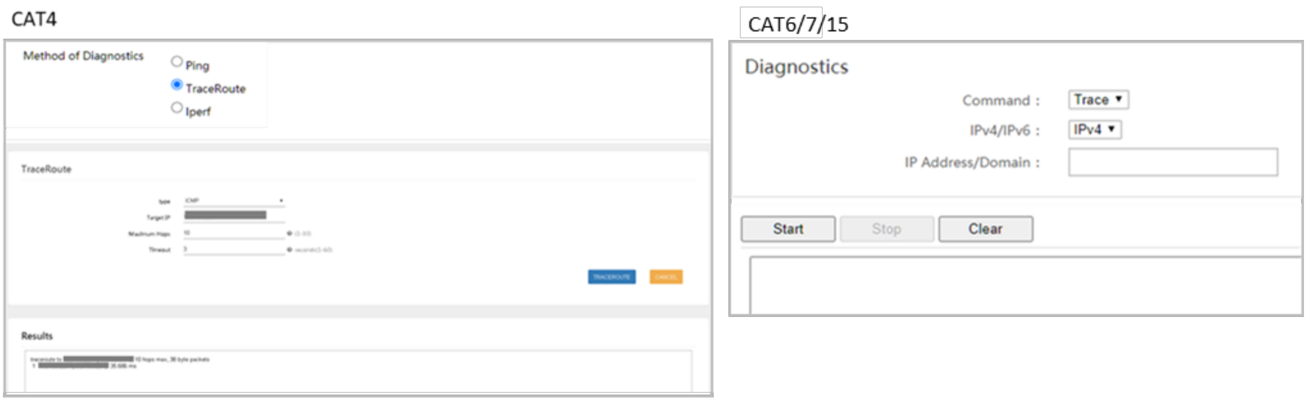
The fields for TraceRoute vary slightly between CAT4 and CAT6/7/15 (Figure 9-19). The procedure below is for CAT4. The CAT6/7/15 fields only require you to select *Trace* as the command, select *IPv4* or *IPv6* type packets, and enter the target device IP address or domain name. When you press *Start*, the test will run immediately and the results will appear in the bottom pane.

To initiate a TraceRoute on a CAT4 CPE:

1. Go to *System* > *Diagnosis*, and select the *TraceRoute* radio button.
2. *Type*: Leave the default Internet Control Message Protocol (*ICMP*).
3. *Target IP*: Enter a target device's IP address or domain name to which the CPE is to send packets.
4. *Maximum Hops*: Enter the maximum number of hops between network nodes you want the packets that the CPE sends to take to reach the target address. If the TraceRoute hits that number, the test will end. Range: 1-30.
5. *Timeout*: Enter a timeout period, in seconds. Range: 1-60 seconds.
6. Click on the *TRACEROUTE* button. The test will start immediately.

Results of the TraceRoute will appear at the bottom of the window, showing the target IP address, the number of hops that it took from the CPE to the target IP, the packet size (bytes), and the average time between hops (milliseconds).

Figure 9-19: TraceRoute



CAT4

Method of Diagnostics ○ Ping ● TraceRoute ○ Iperf

TraceRoute

Type: ICMP

Target IP: [redacted]

Maximum Hops: 10 (1-10)

Timeout: 3 seconds(1-60)

Results

```
traceroute to [redacted] 10 hops max, 38 byte packets
 1  [redacted] 35.606 ms
```

CAT6/7/15

Diagnostics

Command : Trace

IPv4/IPv6 : IPv4

IP Address/Domain :

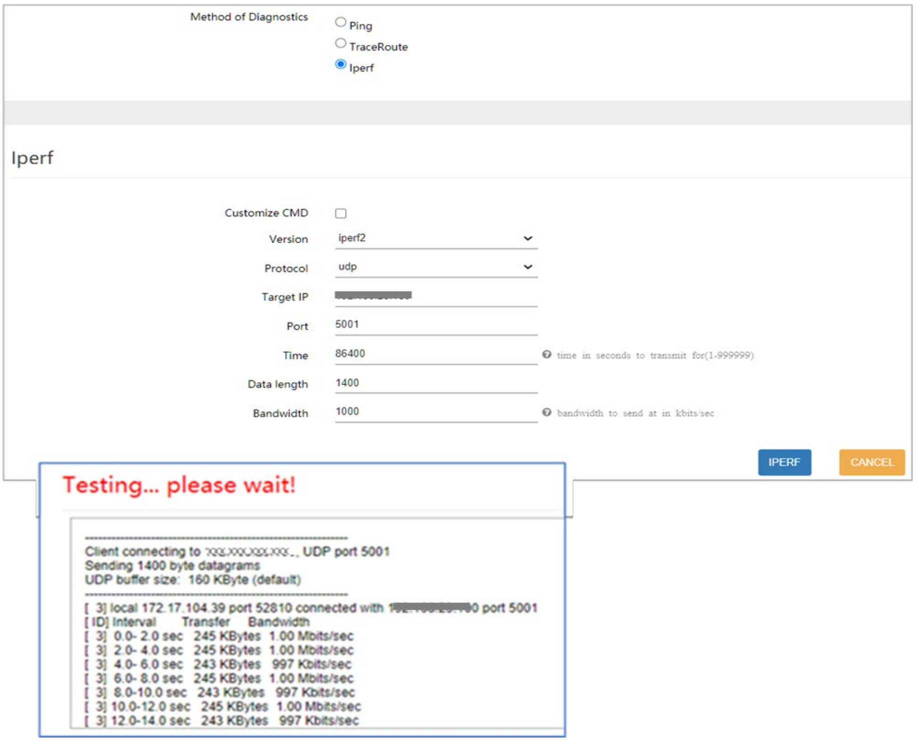
9.11.3 Iperf (CAT4)

The *Iperf* tool under *System* > *Diagnosis* measures the throughput of either Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets between the CPE and a target IP address. The results are useful for assessing network performance and for troubleshooting issues.

Referring to Figure 9-20, to run the Iperf test select the *Method of Diagnostics* by clicking on the radio button next to *Iperf*. Enter the Iperf settings per the field descriptions in Table 9-6. When finished, click on the *IPERF* button. The test will run immediately. The results will appear at the bottom of the screen, showing data throughput on the uplink and downlink.

NOTE: The Iperf server/client needs to be running on the other end point for the Iperf test to complete and be successful.

Figure 9-20: Iperf (CAT4)



Method of Diagnostics ○ Ping ○ TraceRoute ● Iperf

Iperf

Customize CMD □

Version: iperf2

Protocol: udp

Target IP: [redacted]

Port: 5001

Time: 86400 — time in seconds to transmit for(1-999999)

Data length: 1400

Bandwidth: 1000 — bandwidth to send at in kbits/sec

Testing... please wait!

```
------------------------------------------------------------
Client connecting to xxx.xxx.xxx.xxx., UDP port 5001
Sending 1400 byte datagrams
UDP buffer size:  160 KByte (default)
------------------------------------------------------------
[  3] local 172.17.104.39 port 52810 connected with [redacted] port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0- 2.0 sec   245 KBytes  1.00 Mbits/sec
[  3]  2.0- 4.0 sec   245 KBytes  1.00 Mbits/sec
[  3]  4.0- 6.0 sec   243 KBytes   997 Kbits/sec
[  3]  6.0- 8.0 sec   245 KBytes  1.00 Mbits/sec
[  3]  8.0-10.0 sec   243 KBytes   997 Kbits/sec
[  3] 10.0-12.0 sec   245 KBytes  1.00 Mbits/sec
[  3] 12.0-14.0 sec   243 KBytes   997 Kbits/sec
```

Table 9-6: Iperf (CAT4)

Field Name	Description
Customize CMD	Select this option if you wish to customize the Iperf test parameters
Version	Select which version of Iperf to use, either *iperf2* or *iperf3*
Protocol	Select the data packet protocol type, either *TCP* or *UDP*, for the test
Target IP	The target, reachable IP address. Default is 192.168.23.100.
Port	The target port number. Range is 1024 to 65,535. Default is 5001.
Time	Enter the amount of time (in seconds) for the Iperf tool to measure the data throughput. Range: 1 to 999999 seconds.
Data Length	Data length, measured in bytes
Bandwidth	Send/receive data rate, in kbps

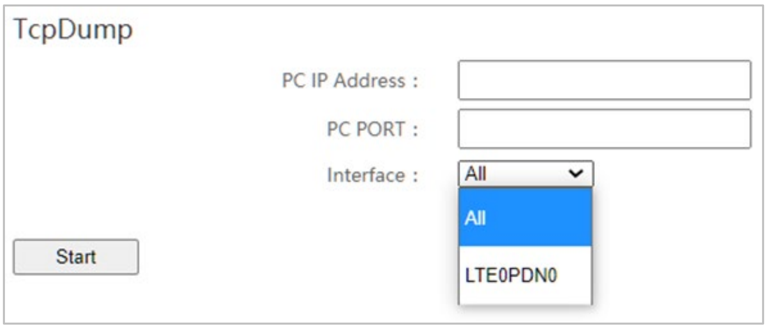
9.11.4 TcpDump (CAT6/7/15)

TcpDump is an open-source command-line packet analysis tool (Figure 9-21). In the CAT6/7/15, TcpDump is included as a diagnostic tool. When the tool is initiated and runs, it will capture contents of TCP/IP and other packets that are being transmitted or received over the network.

The content is typically captured in a packet capture (pcap) file, which can be opened, viewed, and even manipulated through third-party software such as Wireshark. The information is useful for monitoring or troubleshooting network activity. An example of a "dump" output using Wireshark is shown in Figure 9-22.

To use TcpDump, enter the computer's IP address and port number - for example, the port on a Windows PC is called WinDump. Next, select the type of *Interface*: *ALL* or *LTE0PDN0* (*APN0*), meaning all traffic or only LTE traffic. When you click on *Start*, the tool will begin "dumping" the information in the command line on the computer. Be sure to select *Stop* to end the TcpDump.

Figure 9-21: TcpDump



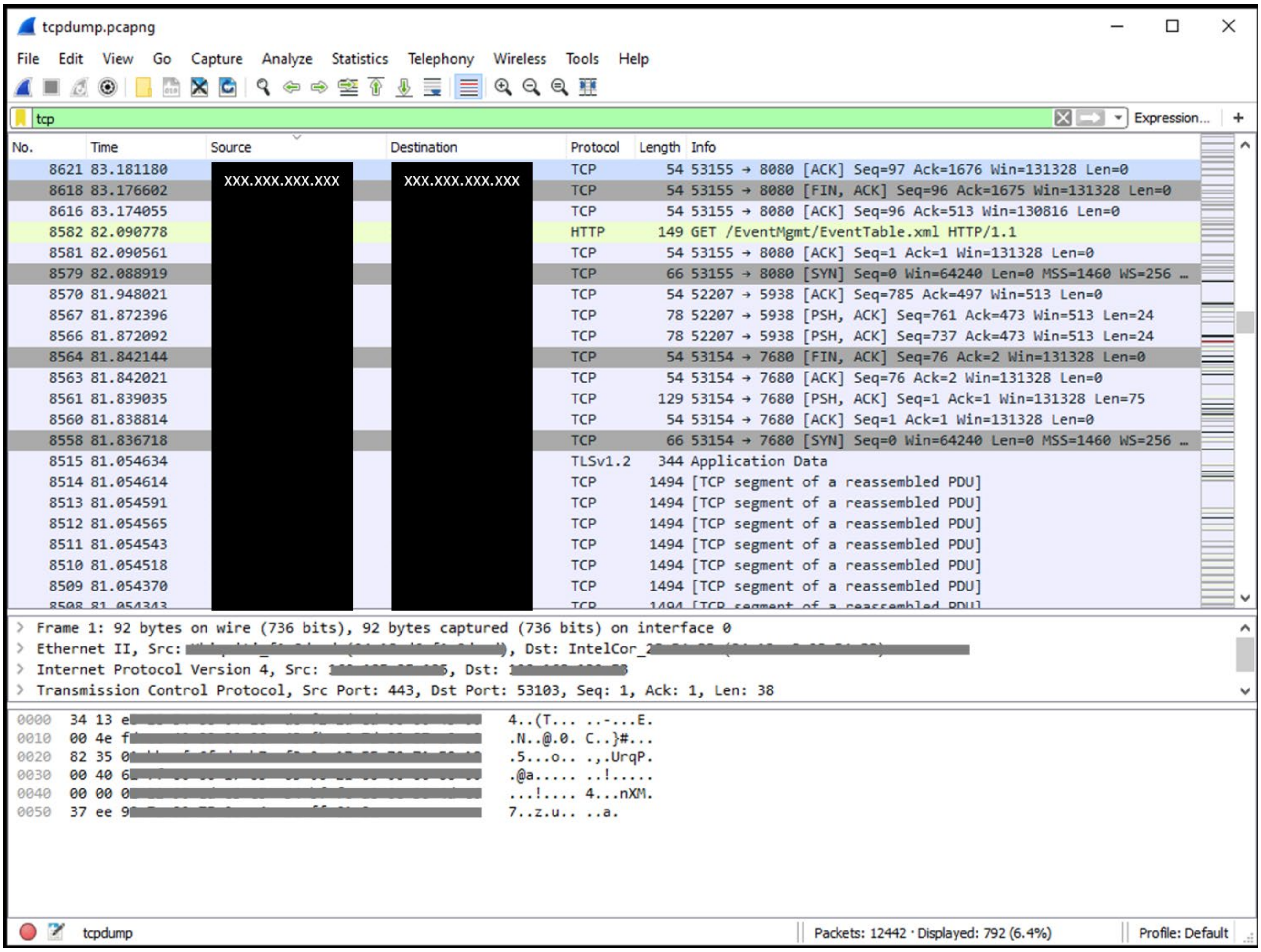
TcpDump

PC IP Address :

PC PORT :

Interface : All

Figure 9-22: TcpDump Example



tcpdump.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp
Expression...

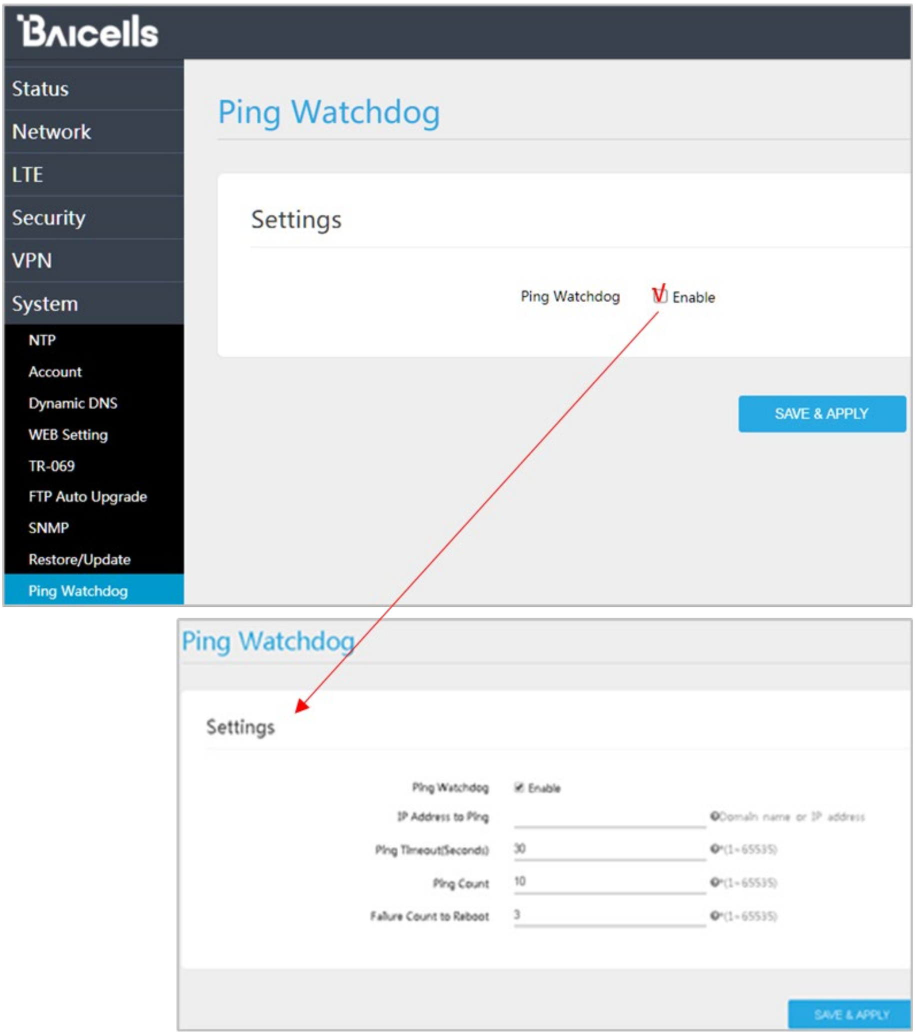
```
No.   Time       Source            Destination       Protocol Length Info
 8621 83.181180  xxx.xxx.xxx.xxx   xxx.xxx.xxx.xxx   TCP        54 53155 → 8080 [ACK] Seq=97 Ack=1676 Win=131328 Len=0
 8618 83.176602  [redacted]        [redacted]        TCP        54 53155 → 8080 [FIN, ACK] Seq=96 Ack=1675 Win=131328 Len=0
 8616 83.174055                                      TCP        54 53155 → 8080 [ACK] Seq=96 Ack=513 Win=130816 Len=0
 8582 82.090778                                      HTTP      149 GET /EventMgmt/EventTable.xml HTTP/1.1
 8581 82.090561                                      TCP        54 53155 → 8080 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 8579 82.088919                                      TCP        66 53155 → 8080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 …
 8570 81.948021                                      TCP        54 52207 → 5938 [ACK] Seq=785 Ack=497 Win=513 Len=0
 8567 81.872396                                      TCP        78 52207 → 5938 [PSH, ACK] Seq=761 Ack=473 Win=513 Len=24
 8566 81.872092                                      TCP        78 52207 → 5938 [PSH, ACK] Seq=737 Ack=473 Win=513 Len=24
 8564 81.842144                                      TCP        54 53154 → 7680 [FIN, ACK] Seq=76 Ack=2 Win=131328 Len=0
 8563 81.842021                                      TCP        54 53154 → 7680 [ACK] Seq=76 Ack=2 Win=131328 Len=0
 8561 81.839035                                      TCP       129 53154 → 7680 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=75
 8560 81.838814                                      TCP        54 53154 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
 8558 81.836718                                      TCP        66 53154 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 …
 8515 81.054634                                      TLSv1.2   344 Application Data
 8514 81.054614                                      TCP      1494 [TCP segment of a reassembled PDU]
 8513 81.054591                                      TCP      1494 [TCP segment of a reassembled PDU]
 8512 81.054565                                      TCP      1494 [TCP segment of a reassembled PDU]
 8511 81.054543                                      TCP      1494 [TCP segment of a reassembled PDU]
 8510 81.054518                                      TCP      1494 [TCP segment of a reassembled PDU]
 8509 81.054370                                      TCP      1494 [TCP segment of a reassembled PDU]
 8508 81.054343                                      TCP      1494 [TCP segment of a reassembled PDU]

> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
> Ethernet II, Src: [redacted]), Dst: IntelCor_[redacted]
> Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
> Transmission Control Protocol, Src Port: 443, Dst Port: 53103, Seq: 1, Ack: 1, Len: 38

0000  34 13 [redacted]   4..(T... ..-...E.
0010  00 4e [redacted]   .N..@.0. C..}#...
0020  82 35 [redacted]   .5...o.. .,.UrqP.
0030  00 40 [redacted]   .@a..... ..!.....
0040  00 00 [redacted]   ...!.... 4...nXM.
0050  37 ee [redacted]   7..z.u.. ..a.
```

9.12 Ping Watchdog

Ping Watchdog is a feature used for detecting the Internet connection state of the CPE. If the CPE cannot connect to the Internet and if this feature is enabled, it will reset the LTE module in the CPE firmware or reboot the CPE in an attempt to recover the connection. To enable the watchdog function (Figure 9-23 [CAT4] and Figure 9-24 [CAT6/7/15]):

1. Go to *System > Ping Watchdog*, and select the *Enable* checkbox next to *Ping Watchdog*.
2. In the *Settings* (CAT4) or *Ping Watchdog* (CAT6/7/15)window that opens, enter the *IP Address to Ping* (CAT4) or *Enter IP address or URL to Ping* (CAT6/7/15). The address must be reachable via the Internet for the CPE to try to ping it.
3. Set the *Ping Timeout*, in seconds, which determines how long the CPE will continue to try to ping the address. The range is 1-65535 seconds.
4. Enter the *Ping Count*, or number of times to try to ping the address, in the range of 1-65535 times.
5. For *Failure Count to Reboot*, enter the maximum number of times the CPE can try the ping but fail before the CPE initiates a reboot. The range is 1-65535 times.

Figure 9-23: Ping Watchdog (CAT4)



Ping Watchdog

Settings

Ping Watchdog ☑ Enable

Ping Watchdog

Settings

Ping Watchdog ☑ Enable

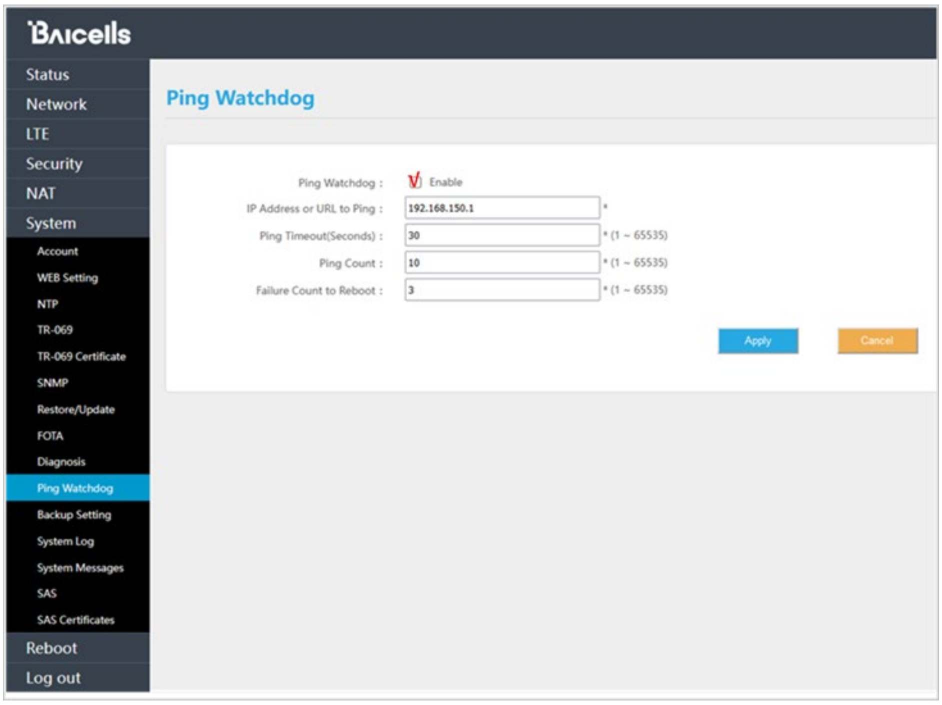
IP Address to Ping ____ Domain name or IP address

Ping Timeout(Seconds) 30 *(1~65535)

Ping Count 10 *(1~65535)

Failure Count to Reboot 3 *(1~65535)

Figure 9-24: Ping Watchdog (CAT6/7/15)



Ping Watchdog

Ping Watchdog : ☑ Enable

IP Address or URL to Ping : 192.168.150.1 *

Ping Timeout(Seconds) : 30 * (1 ~ 65535)

Ping Count : 10 * (1 ~ 65535)

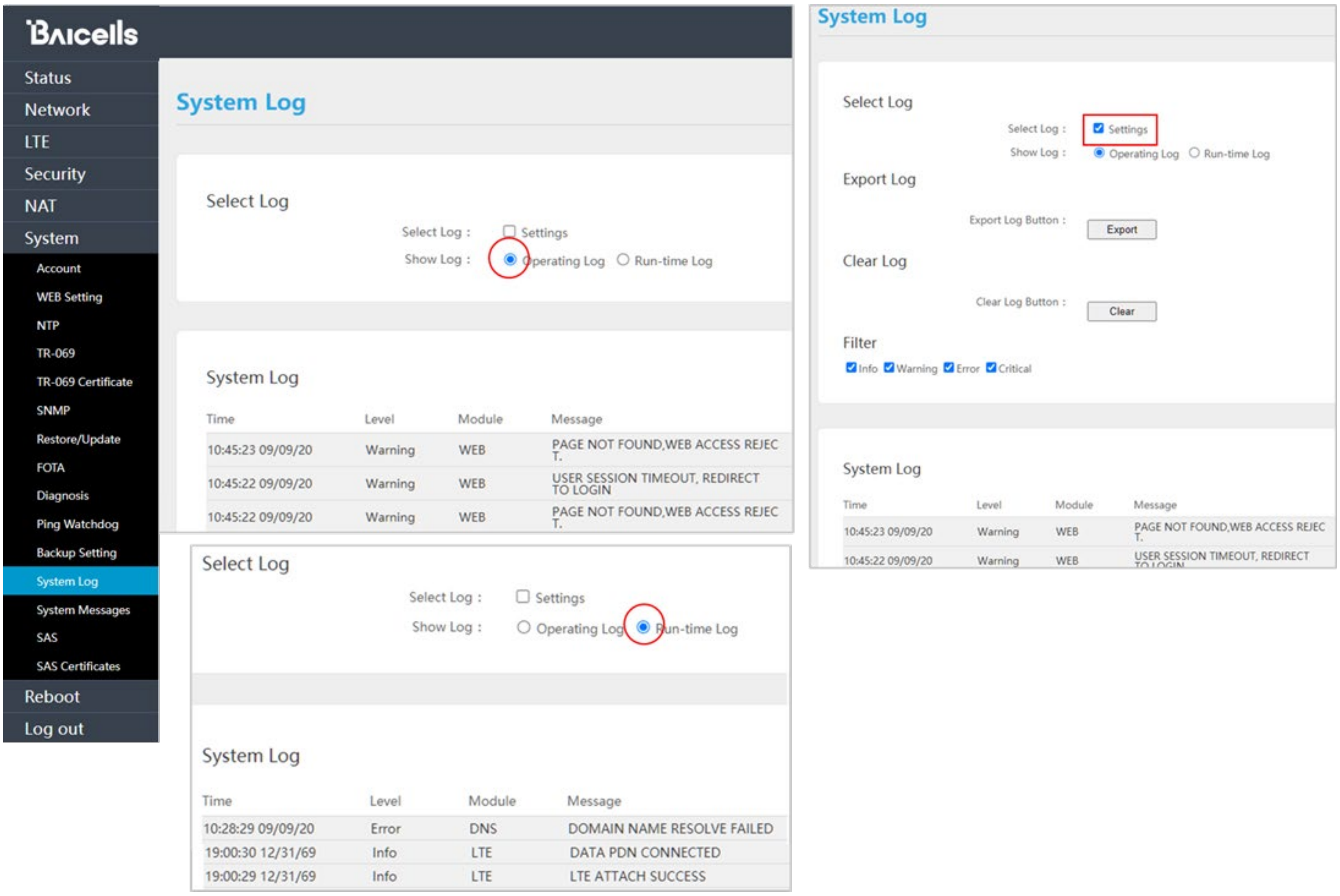
Failure Count to Reboot : 3 * (1 ~ 65535)

9.13 System Log (CAT6/7/15)

System logs provide the debug information that can be used when monitoring or troubleshooting the CPE. The CPE collects operating logs and run-time logs.

Looking at the *System* > *System Log* sub-menu in the CAT6/7/15 GUI (Figure 9-25), the *Select Log* pane offers a *Settings* checkbox, which will allow you to select either *Operating Log* or *Run-time Log*, and to *Filter* the list of logs by alarm severity level: *Info*, *Warning*, *Error*, and/or *Critical*. You can then *Export Log* to save the log file for analysis. Use *Clear Log* to clear the list of current log files.

Figure 9-25: System Log (CAT6/7/15)



System Log

Select Log

Select Log : □ Settings

Show Log : ● Operating Log ○ Run-time Log

System Log

Time	Level	Module	Message
10:45:23 09/09/20	Warning	WEB	PAGE NOT FOUND,WEB ACCESS REJEC T.
10:45:22 09/09/20	Warning	WEB	USER SESSION TIMEOUT, REDIRECT TO LOGIN
10:45:22 09/09/20	Warning	WEB	PAGE NOT FOUND,WEB ACCESS REJEC T.

Select Log

Select Log : □ Settings

Show Log : ○ Operating Log ● Run-time Log

System Log

Time	Level	Module	Message
10:28:29 09/09/20	Error	DNS	DOMAIN NAME RESOLVE FAILED
19:00:30 12/31/69	Info	LTE	DATA PDN CONNECTED
19:00:29 12/31/69	Info	LTE	LTE ATTACH SUCCESS

System Log

Select Log

Select Log : ☑ Settings

Show Log : ● Operating Log ○ Run-time Log

Export Log

Export Log Button : Export

Clear Log

Clear Log Button : Clear

Filter

☑ Info ☑ Warning ☑ Error ☑ Critical

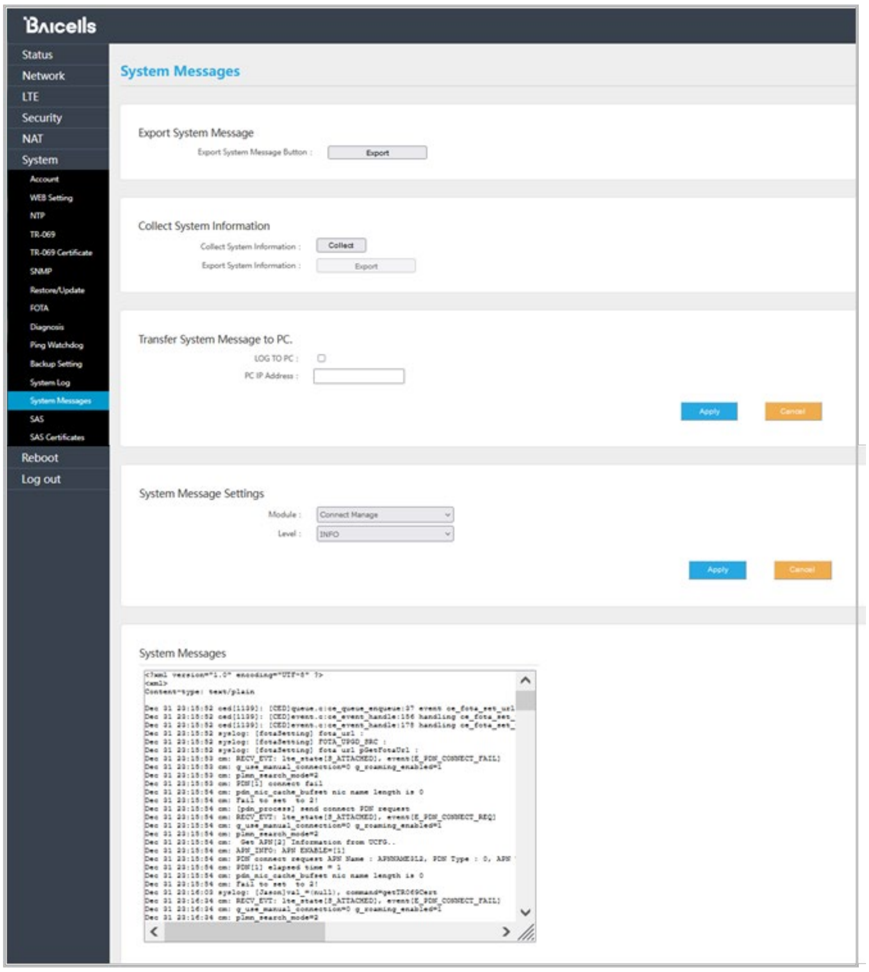
System Log

Time	Level	Module	Message
10:45:23 09/09/20	Warning	WEB	PAGE NOT FOUND,WEB ACCESS REJEC T.
10:45:22 09/09/20	Warning	WEB	USER SESSION TIMEOUT, REDIRECT TO LOGIN

9.14 System Messages (CAT6/7/15)

When remote Web access has been enabled in *System* > *WEB Setting*, you can use the *System* > *System Messages* sub-menu to export the messages, collect real-time system information, or transfer system messages to your computer. You can configure system message settings for the preferred module (*Connect Manage*, *SAS*, *LTE Deamon*, or *All*), and you can select the message level (*INFO*, *EMERG*, *ALERT*, *CRIT*, *ERR*, *WARN*, *NOTICE*, *INFO*, or *DEBUG*). The messages will appear in the *System Messages* pane, as shown in Figure 9-26. Like system logs, the message content can be used to monitor or troubleshoot the CPE.

Figure 9-26: System Messages (CAT6/7/15)



System Messages

Export System Message

Export System Message Button : Export

Collect System Information

Collect System Information : Collect

Export System Information : Export

Transfer System Message to PC.

LOG TO PC : □

PC IP Address :

Apply Cancel

System Message Settings

Module : Connect Manage

Level : INFO

Apply Cancel

System Messages

```
<?xml version="1.0" encoding="UTF-8" ?>
<xml>
Content-type: text/plain

Dec 31 23:15:52 ced[1139]: [CED]queue.c:ce_queue_enqueue:37 event ce_fota_set_url
Dec 31 23:15:52 ced[1139]: [CED]event.c:ce_event_handle:156 handling ce_fota_set_
Dec 31 23:15:52 ced[1139]: [CED]event.c:ce_event_handle:178 handling ce_fota_set_
Dec 31 23:15:52 syslog: [fotaSetting] fota_url :
Dec 31 23:15:52 syslog: [fotaSetting] FOTA_UPGD_SRC :
Dec 31 23:15:52 syslog: [fotaSetting] fota url pGetFotaUrl :
Dec 31 23:15:53 cm: RECV_EVT: lte_state[S_ATTACHED], event[E_PDN_CONNECT_FAIL]
Dec 31 23:15:53 cm: g_use_manual_connection=0 g_roaming_enabled=1
Dec 31 23:15:53 cm: plmn_search_mode=2
Dec 31 23:15:53 cm: PDN[1] connect fail
Dec 31 23:15:54 cm: pdn_nic_cache_bufset nic name length is 0
Dec 31 23:15:54 cm: fail to set  to 2!
Dec 31 23:15:54 cm: [pdn_process] send connect PDN request
Dec 31 23:15:54 cm: RECV_EVT: lte_state[S_ATTACHED], event[E_PDN_CONNECT_REQ]
Dec 31 23:15:54 cm: g_use_manual_connection=0 g_roaming_enabled=1
Dec 31 23:15:54 cm: plmn_search_mode=2
Dec 31 23:15:54 cm:  Get APN[2] Information from UCFG..
Dec 31 23:15:54 cm: APN_INFO: APN ENABLE=[1]
Dec 31 23:15:54 cm: PDN connect request APN Name : APNNAME312, PDN Type : 0, APN
Dec 31 23:15:54 cm: PDN[1] elapsed time = 1
Dec 31 23:15:54 cm: pdn_nic_cache_bufset nic name length is 0
Dec 31 23:15:54 cm: fail to set  to 2!
Dec 31 23:16:03 syslog: [Jason]val_=(null), command=getTR069Cert
Dec 31 23:16:34 cm: RECV_EVT: lte_state[S_ATTACHED], event[E_PDN_CONNECT_FAIL]
Dec 31 23:16:34 cm: g_use_manual_connection=0 g_roaming_enabled=1
Dec 31 23:16:34 cm: plmn_search_mode=2
```

9.15 SAS

Reference: *SAS Deployment Guide*

9.15.1 Introduction

Citizens Broadband Radio Service (CBRS) Spectrum Access System (SAS) is a USA solution based on the 3.55-3.7 GHz band. What makes this solution different is the way the band is accessed. CBRS SAS is based on the concept of shared spectrum, where spectrum is dynamically assigned and released on an as-needed basis.

CBRS Service Devices (CBSD) such as the Baicells eNBs and CPEs must go through certification, and all CBSDs must be installed by a Certified Professional Installer (CPI) in order to lawfully operate within the designated spectrum of CBRS. If you are not sure if the CPE you are working with is certified, please check with your Baicells sales representative.

The Baicells OMC acts as a Domain Proxy (DP) between the CBSDs and the SAS vendor. Both Baicells CloudCore OMC and Local OMC support DP functionality. You will need at least one Certified Professional Installer's (CPI) credentials when configuring an eNB, CPE and the OMC.

The *SAS Deployment Guide* provides a full overview and procedures for implementing CBRS SAS operation across all of the Baicells components. The information in this section pertains only to enabling the CPE as a CBSD.

NOTE: The first generation (Gen 1) Baicells CPEs do not support SAS.

9.15.2 Enable SAS

9.15.2.1 Prerequisites

9.15.2.1.1 Import CBSD in SAS Portal

The Baicells CPE model must be a CBRS SAS certified CBSD. Before enabling SAS on the CPE, you must import the CBSD information in the SAS vendor's portal.

9.15.2.1.2 Verify OMC/ACS Setting

Since the OMC functions as a domain proxy (DP) between CBSDs and the SAS, the CPE must be configured to connect with the OMC. Because the OMC functions as an Automatic Configuration Server (ACS), the field for "pointing" the CPE to the OMC is called *ACS Address*.

Verify that the OMC/ACS URL has been entered correctly, as follows:

1. Go to *System* > *TR-069*, and ensure the *ACS Address* field is configured correctly.
    a. For the CloudCore OMC, enter

       http://baiomc.cloudapp.net:48080/smallcell/AcsService

    b. For a Local OMC, enter the Local OMC server URL, e.g., **http://xx.xx.xx.xx:8080/smallcell/AcsService**
2. If using the Baicells CloudCore OMC, enter the operator's unique CloudKey shown at the top of the CloudCore account window. (The CloudKey is not required for Local OMC.)

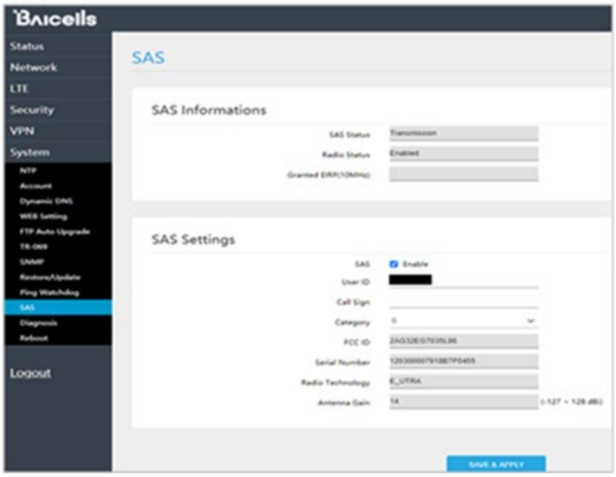
9.15.2.2 Configure SAS in the CAT4 CPE GUI

To enable SAS operation on a certified CAT4 CPE device (Figure 9-27):

1. Go to *System* > *SAS*, and enter the *User ID* provided by the SAS vendor.
2. Optional: Enter the *Call Sign*, which is a parameter that is useful to identify the PAL license under which the operator is deploying a CPE. The parameter is not necessary to configure for the GAA spectrum (3550 – 3700 MHz). Range is 0 to 256 characters (using upper-case letters A-Z, lower-case letters a-z, and digits 0-9).
3. For the *Category* field, which refers to the CBRS equipment category, if this is an indoor CPE leave the default setting of *A*. If this is an outdoor CPE, leave the default setting of *B*. If you need further assistance, see the Baicells CBSD Product Information table in the *SAS Deployment Guide*.
4. All of the other fields will either be (a) auto-filled based on the model of CPE you have, or (b) are the CPE SAS status indications.
5. When you are ready for this CPE to operate in SAS mode, click on the *Enable* checkbox.
6. Click on *SAVE & APPLY*.

Figure 9-27: SAS (CAT4)

CAT4



SAS

SAS Informations

SAS Status: Transmission

Radio Status: Enabled

Granted EIRP(10MHz):

SAS Settings

SAS: ☑ Enable

User ID: [redacted]

Call Sign:

Category: 0

FCC ID: 2AG32EG7035L96

Serial Number: 120300007910B7P0455

Radio Technology: E_UTRA

Antenna Gain: 14 (-127 ~ 128 dB)

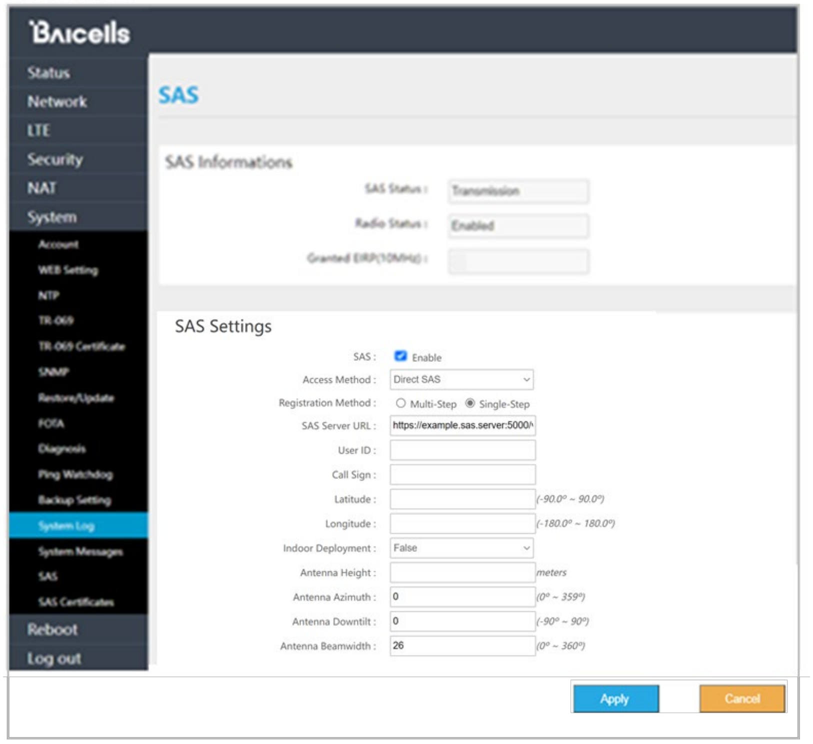
9.15.2.3 Configure SAS in the CAT6/7/15 CPE GUI

To enable SAS operation on a certified CAT6/7/15 CPE device (Figure 9-28):

1. Go to *System* > *SAS*, and select *Access Method* (*Domain Proxy* or *Direct SAS*) from the pull-down menu. If you choose *Domain Proxy*, go to *step 2*. If you choose *Direct SAS*, go to *step 3*.
2. When you choose *Domain Proxy*, the *Registration Method* will default to *Multi-Step* and the *SAS Server URL* will auto-fill to CloudCore OMC URL (***http://baiomc.cloudapp.net:48080/smallcell/AcsService***). Proceed to *step 14*.
3. When you choose *Direct SAS*, you can select the *Single-Step* radio button for the *Registration Method* and configure the remaining fields in the GUI. Proceed to *step 4*.
4. Enter the *SAS Server URL* that has been provided by the SAS vendor.
5. Enter the *User ID* provided by the SAS vendor.
6. Optional: Enter the *Call Sign*, which is a parameter that is useful to identify the PAL license under which the operator is deploying a CPE. The parameter is not necessary to configure for the GAA spectrum (3550 – 3700 MHz). Range is 0 to 256 characters (using upper-case letters A-Z, lower-case letters a-z, and digits 0-9).
7. Enter the *Latitude* of CPE's location (range is -90.0° to 90.0°).
8. Enter the *Longitude* of CPE's location (range is -180.0° to 180.0°).
9. Select *True* or *False* from the pull-down menu to indicate *Indoor Deployment*.
10. Enter the *Antenna Height* in meters.
11. Enter the *Antenna Azimuth* in degrees (range is 0° to 359°, and the default is 0).
12. Enter the *Antenna Downtilt* in degrees (range is -90° to 90°, and the default is 0).
13. Enter the *Antenna Beamwidth* in degrees (range is 0° to 360°, and the default is 26).
14. When you are ready for this CPE to operate in SAS mode, click on the *Enable* checkbox.
15. Click on *APPLY*.

Figure 9-28: SAS (CAT6/7/15)

CAT6/7/15



SAS

SAS Informations

SAS Status : Transmission

Radio Status : Enabled

Granted EIRP(10MHz) :

SAS Settings

SAS : ☑ Enable

Access Method : Direct SAS

Registration Method : ○ Multi-Step ● Single-Step

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

User ID :

Call Sign :

Latitude : (-90.0° ~ 90.0°)

Longitude : (-180.0° ~ 180.0°)

Indoor Deployment : False

Antenna Height : meters

Antenna Azimuth : 0 (0° ~ 359°)

Antenna Downtilt : 0 (-90° ~ 90°)

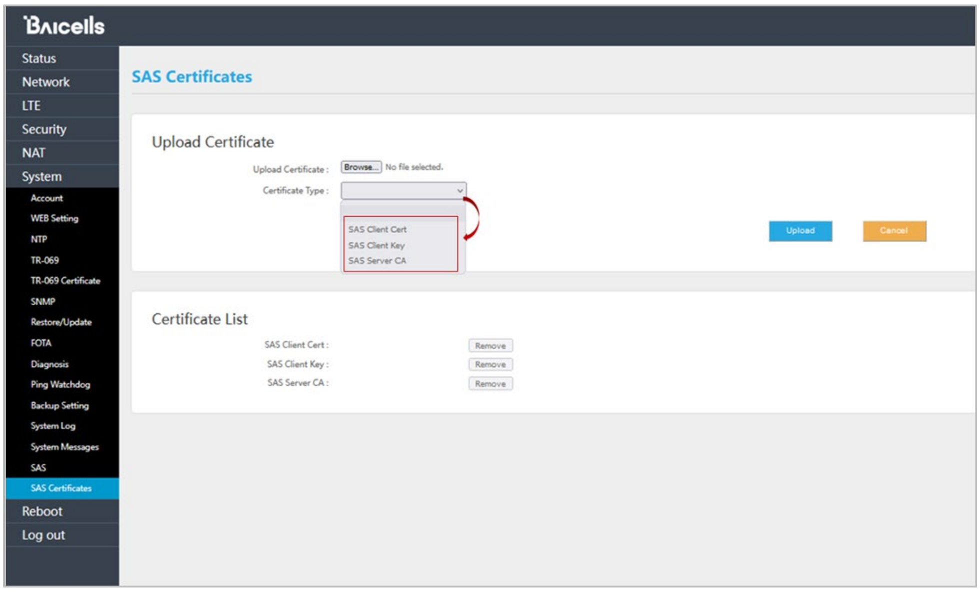
Antenna Beamwidth : 26 (0° ~ 360°)

9.16 SAS Certificates (CAT6/7/15)

The *System* > *SAS Certificates* sub-menu is used to upload and manage SAS certificates (Figure 9-29).

In the *SAS Certificates* window, select the *Certificate Type* from the pull-down menu (*SAS Client Cert*, *SAS Client Key*, or *SAS Server CA*) in the *Upload Certificate* pane. Then, click *Browse…* to navigate to the desired file and click on *Upload*. The certificates already uploaded can be viewed in the *Certificate List* pane. You can use the *Remove* button next to an uploaded certificate you would like to delete from the CPE.

Figure 9-29: SAS Certificates (CAT6/7/15)



SAS Certificates

Upload Certificate

Upload Certificate : Browse... No file selected.

Certificate Type :

SAS Client Cert
SAS Client Key
SAS Server CA

Certificate List

SAS Client Cert : Remove

SAS Client Key : Remove

SAS Server CA : Remove

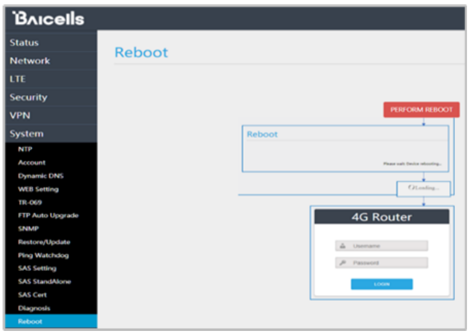
10 Reboot

Use the *Reboot* menu to perform a reboot of the CPE, as shown in Figure 10-1. 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 CPE service.

Figure 10-1: Reboot

CAT4

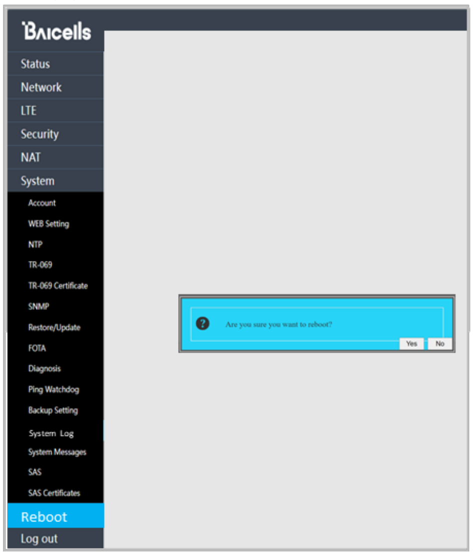


Reboot

Please wait. Device rebooting...

Loading...

CAT6/7/15

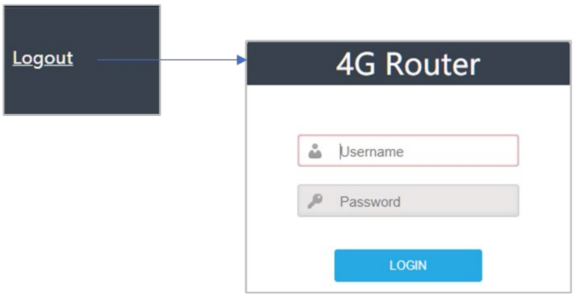


Are you sure you want to reboot?

11 Logout

When you click on the *Logout* menu, you are automatically logged out of the CPE and returned to the *LOGIN* screen (Figure 11-1).

Figure 11-1: Logout


Logout
4G Router
Username
Password
LOGIN