

LTE Router BaiCE_BQ_2.0.x 5G User Manual

Document version: 01

All rights reserved © Baicells Technologies Co., Ltd.



About This Document

This document introduces the GUI and configuration operation of Atom CPE version BaiCE_BQ_2.0.x.

Copyright Notice

Baicells Technologies, Inc., copyrights the information in this document. No part of this document may be reproduced in any form or means without the prior written consent of Baicells Technologies, Inc. The Baicells logo is a proprietary trademark of Baicells Technologies, Inc. Other trademarks mentioned in this document belong to their owners.

Disclaimer

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

Revision Record

Date	Version	Description
December 30, 2022	01	Initial Released.

Contact Us

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

Contents

1. GUI Int	troduction	1
1.1	Computer Requirements	1
1.2	CPE Software	1
1.3	Applicable CPE Model	1
1.4	Log In	2
2. Configu	uration	3
2.1	Status Menu	3
2.1.1	Overview	3
2.1.2	Routes	10
2.2	Network Menu	11
2.2.1	LAN Settings	11
2.2.2	WAN Settings	12
2.2.3	WLAN Settings	15
2.2.4	Static Routes	17
2.2.5	DMZ	17
2.3	Cellular Menu	19
2.3.1	Scan Mode	19
2.3.2	APN Management	22
2.3.3	PIN Management	23
2.4	Security Menu	24
2.4.1	Firewall Settings	24
2.4.2	MAC Filter	25
2.4.3	IP Filter	26
2.4.4	URL Filter	27
2.4.5	Port Forwarding	28
2.4.6	Port Triggering	29
2.4.7	ALG	30

BAICells

	DAIVOIS
2.4.8	UPnP
2.4.9	Attack Protection
2.5	VPN Menu
2.5.1	IPSec
2.5.2	OpenVPN
2.6	System Menu 37
2.6.1	NTP
2.6.2	Account
2.6.3	Dynamic DNS 39
2.6.4	WEB Setting
2.6.5	FTP Auto Upgrade 43
2.6.6	TR-069
2.6.7	SNMP
2.6.8	Restore/Update 47
2.6.9	Ping Watchdog 49
2.6.10	SAS
2.6.11	SAS Certificates
2.6.12	System Messages
2.6.13	Diagnosis
2.6.14	Reboot
2.7	Logout 59
Appendix: R	egulatory Compliance60

Figures

Figure 1-1 Login	2
Figure 2-1 Overview	4
Figure 2-2 Routes	. 11
Figure 2-3 LAN host settings	. 11
Figure 2-4 DHCP settings	.12
Figure 2-5 Bundled Address List	.12
Figure 2-6 WAN Settings	.13
Figure 2-7 Tunnel Mode	.14
Figure 2-8 Bridge Mode	.15
Figure 2-9 WLAN Overview	.15
Figure 2-10 WLAN Settings	.16
Figure 2-11 Static Routes	.17
Figure 2-12 DMZ Examples	. 18
Figure 2-13 DMZ	.19
Figure 2-14 Scan Mode	.19
Figure 2-15 Full Band	.20
Figure 2-16 Cell Lock	.21
Figure 2-17 Band Lock	.22
Figure 2-18 APN Management	.23
Figure 2-19 PIN Management	.24
Figure 2-20 Firewall	.25
Figure 2-21 MAC Filter	.25
Figure 2-22 IP Filter	.26
Figure 2-23 URL Filter	.28
Figure 2-24 Port Forwarding	.29
Figure 2-25 Port Triggering	.30
Figure 2-26 ALG	.31
Figure 2-27 UPnP	.32

Figure 2-28 Attack Protection	32
Figure 2-29 VPN Menu	33
Figure 2-30 IPSec	33
Figure 2-31 IPSec	34
Figure 2-32 OpenVPN	36
Figure 2-33 Server	36
Figure 2-34 Client	37
Figure 2-35 NTP	38
Figure 2-36 Account	39
Figure 2-37 Dynamic DNS Overview	39
Figure 2-38 Dynamic DNS Global Settings	40
Figure 2-39 IPv4 DDNS configuration	41
Figure 2-40 IPv6 DDNS configuration	42
Figure 2-41 WEB Setting	43
Figure 2-42 FTP Auto Upgrade	44
Figure 2-43 TR-069	45
Figure 2-43 TR-069	45 46
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update	45 46 48
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog	45 46 48 49
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu	45 46 48 49 50
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS	45 46 48 49 50 51
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-49 SAS Settings	45 46 48 49 50 51 51
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-49 SAS Settings Figure 2-50 Antenna Parameters	45 46 48 49 50 51 51 52
 Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-49 SAS Settings Figure 2-50 Antenna Parameters Figure 2-51 CPI Settings 	45 46 49 50 51 51 52 53
 Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-49 SAS Settings Figure 2-50 Antenna Parameters Figure 2-51 CPI Settings Figure 2-52 SAS Certificates 	45 46 49 50 51 51 52 53 54
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-49 SAS Settings Figure 2-50 Antenna Parameters Figure 2-51 CPI Settings Figure 2-52 SAS Certificates Figure 2-53 System Messages	45 48 49 50 51 51 52 53 54 54
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-49 SAS Settings Figure 2-50 Antenna Parameters Figure 2-51 CPI Settings Figure 2-52 SAS Certificates Figure 2-53 System Messages Figure 2-54 Diagnosis	45 48 49 50 51 51 52 53 54 54 55
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-48 Automatic SAS Figure 2-49 SAS Settings Figure 2-50 Antenna Parameters Figure 2-51 CPI Settings Figure 2-52 SAS Certificates Figure 2-53 System Messages Figure 2-54 Diagnosis Figure 2-55 Ping Diagnosis Settings	45 46 49 50 51 51 52 53 54 55 55
Figure 2-43 TR-069 Figure 2-44 SNMP Figure 2-45 Restore/Update Figure 2-46 Ping Watchdog Figure 2-47 SAS Menu Figure 2-48 Automatic SAS Figure 2-48 Automatic SAS Figure 2-49 SAS Settings Figure 2-50 Antenna Parameters Figure 2-50 Antenna Parameters Figure 2-51 CPI Settings Figure 2-52 SAS Certificates Figure 2-53 System Messages Figure 2-54 Diagnosis Figure 2-55 Ping Diagnosis Settings Figure 2-56 Trace Diagnosis Settings	45 46 49 50 51 51 52 53 54 55 55 56 57

BAICells

Figure 2-58 Reboot	59
Figure 2-59 Logout	

Tables

Table 1-1 Computer Requirements	1
Table 1-2 CPE Model List	1
Table 2-1 Status	8
Table 2-2 WLAN Settings Parameters	16
Table 2-3 IP Filter	27
Table 2-4 Port Forwarding	29
Table 2-5 IPSec	34
Table 2-6 WEB Setting	43
Table 2-7 TR-069	45
Table 2-8 SNMP	47
Table 2-9 SAS Info field description	50
Table 2-10 SAS Settings	52
Table 2-11 Antenna Parameters	52
Table 2-12 Ping Diagnosis parameters	56
Table 2-13 Trace Diagnosis parameters	57
Table 2-14 Iperf Diagnosis parameters	58

1. GUI Introduction

Baicells provides a GUI to configure CPE devices.

1.1 **Computer Requirements**

The computer you use to connect with the CPE GUI must meet the requirements shown in Table 1-1.

Item	Description				
CPU	Pentium 500 MHz or higher				
Memory	128 MB RAM or higher				
Hard Disk	50MB available space				
Operating System	Microsoft: Windows XP, Windows 7 or higher				
	Mac: MacOSX 10.6 or higher				
Screen Resolution	1024 x 768 pixels or higher				
Browser	Google Chrome 22 or later				
	Internet Explorer 8.0 or later				
	Mozilla Firefox 18.0 or later				
	Safari 5.1 or later				

Table 1-1 Computer Requirements

1.2 CPE Software

The firmware of the CPE should be BaiCE_BQ_2.0.x or above, if the CPE is not running this version, please contact Baicells support to get the corresponding software version.

1.3 Applicable CPE Model

The GUI is matched with the software version of CPE products and is applicable to all models of CPE products with the same software version.

The CPE product model of software version BaiCE_BQ_2.0.x is shown in Table 1-2.

Table 1-2 CPE Model List

Indoor / Outdoor	Product Model			
Indoor	EG3661M-NR6			

1.4 **Log In**

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

The user name and password for the initial login are **admin admin**.

Figure 1-1 Login

,	Bricells
	User Login
	Username
	Password
	line

2. Configuration

2.1 Status Menu

2.1.1 Overview

After logging in, the GUI opens to the Status > Overview page (Figure 2-1). This page is a dashboard of key information regarding the CPE.

Figure 2-1 Overview

Bucella								Second press
S - Status	1	B tractions	6					
-		Seen Indo	and the second second			*1111	Celvie	August (Darminet)
		Walter Street	August 100 March 100				-	Real Property of the
0 Address	1.00		AND THE REPORT OF	The firm		51		
* Letter		21	0010000001100/04 0010110100000	No. 1 mar			wws.15	
0. boury		WE CARL			1000		- 211	
1.114	-	40000 10000	10001000010014 (1000)		N.N. 11		111	
the second	-	And and a second second	Approximation of the local sectors of the local sec				1	1. 218 King The Rel State in the State
0.1499		-						the second second
			1.56 Sett.(01,5710,56 ivelane Struct allows then		er en Geldt, Rit, 11 mit Datherfer Franz 12 min, 12 min		anna An Cher	nen a And Thomas an Ad An And Commence
		CLAR Color	NUMBER OF	and Agency at the second secon	(14).295.295 x	100.00		Noracle State 1
		12 Propriet						

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

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

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

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

Wifi Config 🔽		
SSID1	EG3015M-62-10-2.4G,	
SSID2	Closed	
5GSSID1	EG3015M-62-10-5G.ps	
5GSSID2	Closed	
E Ne	twork / WLAN Settings	
•	Wireless Overview	
	Generic Atheros 802.11anac (wifi0)	
	SSID: EG3015M-82-10-5G Mode: Master BSSID: 48:BF:74:10:82:30 Encryption: psk2+comp	
	SSID: EG3015M-62-10-5G1 Mode: Master Enable Settings Wireless is disabled or not associated	
	SSID: EG3015M-82-10-5G2 Mode: Master Enable Settings Wireless is disabled or not associated	
	SSID: EG3015M-82-10-5G3 Mode: Master Enable Settings. Wireless is disabled or not associated	

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

Carlain	Sugarata Delasta						
Centralia	Augurate (PCC)						
				(THE PART	An example	1999	NUM YOU WANTED IN THE
1.1			1113.004	Calls An Amate	1112-611	(1012)	001040341240294
				P2404	4041	Di Preparez	2000.0.9446
1	12	and second second	22.2.274	10.	201	St.Femaletter	2008.0 4941
-				144.00		10000	04.61 (63.71) 71(5) -64
2.			S	948.02	218432	10.0412	-881-871-681-63
and and	_			ENN'SS	40145	100	
			16.2 67.8				

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



days.

•

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

Desica Heatth					
CPN Transa	2.2%	menty thept	40.3%	Histories, Verson 1	VER C
Fortune Vacant	BACE_BO_1112_NA	Multiply hereine	DeCK_DQ_18.98.1	FARMORS IIANA UNA	Aug 18 2002 22:52.10
LUM Steller	Available	Convention State	Connected	1000	400010000881181
Syrphon (1) Total	19 Hours, 42 Here. 10 pecti	Convention Steel	1 kast, 22 mins, 52 pect		

• The *LAN Status* pane shows LAN settings information, such as IP Address, IPv4 Netmask, IPv6 Prefix, etc.

ELLAN Status					
dfiel katatriess	182 168 150 1	(Pol National	255.255.255.0	UND-Aldren	503# ##70.8d20 1
1PV6-P1600	102e-es70 8620	1Poll Profit Last	60		

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

		_		1 I B Annu Marganese
I Method				2 Settings
Burner of Timpestee				Ping Weenhood
a loss of Taxation of				C Evalue
a reg () marine ()				
El Prez				
Target IF	Interface		Chickeya Sina	See 1
Control	107447			
			Witcher (1999)	
	Gam			
Tress				
19				

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

Postile Water	Pv4.Address	IPv4 DNS	Pv5 Address	IPVICONS.	
AP141	10.00.10.228	1141141141143888			

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

Diversion Martin	MAC Address	il' Address	Lease Time	Type
KC	00414910-0099	182,184,150,08	+1	LAN SHOT
12	AD-76-28-88-64-24	102.188.184.122		Land State

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

Ξw	Fi Axeocuted Stations					
1.03	entertaine					
	LND	MAC Address	IP Address	Rignal	Rofee	R.E. Rote
Ψ.	\$100118W-8219-2.+0	00.41.0812.80.95	192;188,181;84	disti-	-0549-	195.0 1041
100						*

Refer to Table 2-1 for a description of the Status fields.

Table 2-1 Status	
Field Name	Description
Basic Info	
Product Model	CPE model number
Market Name	Market name of CPE products
Module Name	Type of LTE module in the CPE
LAN MAC	The MAC address of the LAN port. The same as the MAC on the
	label.
IMEI	International Mobile Equipment Identity is like a serial number for
	the SIM card
SN	Serial Number
Wifi Config	
SSID	2.4G service set ID
5GSSID	5G service set ID
Cellular Signals	
USIM Status	The Universal Subscriber Identity Module, or SIM, card status is
	either available or not ready in the CPE
IMSI	The unique International Mobile Subscriber Identity (IMSI) number
	associated with the SIM card in the subscriber's CPE. The IMSI
	must be identifiable by the operator's LTE network in order to
	access it.
LTE Mode	The LTE network operates with either Time Division Duplexing
	(TDD) or Frequency Division Duplexing (FDD)
IMEI	International Mobile Equipment Identity is like a serial number for
	the SIM card
PLMN	The Public Land Mobile Number (PLMN), or operator network ID,
	to which the CPE is connected
Band	The range of frequencies within the band the CPE may use for
	wireless communications with an eNB, expressed in MHz
Cell ID	The operator's cell site ID to which the CPE is connected. A cell
	site may comprise more than one eNB. Each eNB is given a PCI
	to identify it.
RSRQ	Reference Signal Receiving Quality indicates the quality of the
	wireless signal
eNB ID	The operator's cell site ID to which the CPE is connected. A cell
	site may comprise more than one eNB. Each eNB is given a PCI
	to identify it.
EARFCN	The E-UTRA Absolute Radio Frequency Channel Number (band
	and frequency) within which the CPE operates
PCI	The Physical Cell Identifier (PCI) unique to each eNB. PCI
	indicates to which eNB the CPE is connected. An operator can
	have multiple eNBs serving the same cell.

Field Name	Description
DL Frequency	The frequency, in MHz, being used in the downlink (eNB to CPE).
	In LTE, the carrier frequency in the uplink and downlink is
	designated by the EARFCN, which identifies the LTE band and
	carrier frequency.
UL Frequency	The frequency, in MHz, that the CPE is using in the uplink (CPE
	to eNB). In LTE, the carrier frequency in the uplink and downlink
	is designated by the EARFCN, which identifies the LTE band and
	carrier frequency.
CINR	The Channel Signal-to-Interference-plus-Noise Ratio reflects the
	signal strength of the signal received from the two antennas in the
	eNB, expressed in decibels (dB)
	NOTE: Additional SINR values are reported when a transmitting
	device is using more than two antennas.
RSRP1 ~ RSRP4	The Signal-to-Interference-plus-Noise Ratio reflects the signal
	strength of the signal received from the two antennas in the eNB,
	expressed in decibels (dB)
	NOTE: Additional SINR values are reported when a transmitting
	device is using more than two antennas.
WAN Throughputs	
DL	The current downlink data throughput rate, in Kbps
UL	The current uplink data throughput rate, in Kbps
Average	The average DL and UL data throughput rates, in Kbps, for this
	CPE in the last 2 minutes
Peak	The peak DL and UL data throughput rates, in Kbps, for this CPE
	in the last 2 minutes
Sum	The total (sum) DL and UL data throughput rates, in Mb
Device Health	
CPU Usage	CPU real-time usage rate, updated every 3s
Memory Usage	The memory usage rate of CPE, updated every 3s
USIM Status	The Universal Subscriber Identity Module, or SIM, card status is
	either available or not ready in the CPE
Connection State	Connection status between the CPE and the network –Checking
	SIM, Scanning, Registering, Acquiring IP, Connected,
	Disconnected.
IMSI	The unique International Mobile Subscriber Identity (IMSI) number
	associated with the SIM card in the subscriber's CPE. The IMSI
	must be identifiable by the operator's LTE network in order to
	access it.
System Up Time	CPE start time
Connection Time	Network access success time
Firmware Version	Version number of the module
Firmware Build	Software version compilation time
Time	

Field Name	Description
Hardware Version	CPE hardware version
Module Version	CPE LTE module firmware version
LAN Status	
IPv4 Address	The IPv4 address of the LAN device
IPv4 Netmask	The subnet mask of the LAN device
IPv6 Address	The IPv6 address of the LAN device
IPv6 Prefix	IPv6 address prefix of LAN device
IPv6 Prefix Len	Length of IPv6 address prefix of LAN device
Diagnosis	
Ping	Ping diagnosis results
Traceroute	Traceroute diagnosis results
Ping Watchdog	Ping Watchdog configuration result
WAN Connections	
Profile Name	APN Number
IPv4 Address/	IPv4or IPv6 address of the APN gateway
IPv6 Address	
IPv4 DNS/ IPv6	IPv4 or IPv6 DNS
DNS	
LAN Connections	
Device Name	The name of each smart device connected through the CPE
MAC Address	The MAC address of each smart device connected through the
	CPE
IP Address	The IP address of each device connected through the CPE
Lease Time	Amount of time a smart device's IP address has been leased
Туре	Type of smart device connection
WiFi Associated Sta	ations
SSID	WIFI SSID
MAC Address	MAC address of the device accessing the SSID
IP Address	IP address of the device accessing the SSID
Signal	The signal strength of the connected device
Noise	WiFi signal noise
RX Rate	Wi-Fi real-time receiving rate
TX Rate	Wi-Fi real-time transmission rate

2.1.2 Routes

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

Figure 2-2 Routes

240	datama	Mac Address		interlace
VIANA	rm.rid	webs mitting for		1000 1107
102100	102.508	100 (0.47-00.467)		brini.
101.71	11110	Ballio 76 81 (talie)		u88.1121
112.14	1014	Sarba 2005 Made		10000000000
1/6-	ut.14	Barle Withiald		-488 1127
194.411	191194	Nother Party label		1111.044
1.0.0	ALOF .	Barley W. Britadak		united Vices
1Pv4-Routes				
IPv4-Routes	Target	P.2 Gatmany	Nerv	Tate
IPv4-Routes	Target	<u>Pat</u> fairning	News.	Take Selection
tiPy4-Routes	Targat BBAANS FBE23418010	<u>Pri-</u> Calmany	Mores 0 0	Takk Sainbin Databin
IPv4-Routes	Target NANANS FEE23410000 NEE1461500000	Put Galance	Norris 0 9 0	Taba Salahin Dalahin Salahin
IPv4-Routes menet and and and and	Target Ritkonet HELZIA LOUIA Hag Hag Hackbook	Post Galaxies	Norris 0 0 0 0	Table Columbus Datables Columbus Agentical
IPv4-Routes ment and and and and and and	Target NALANA HELTIA 1904 HELTIA 1904 HELTIA 1904	P.4- Gatmany	Nore: 0 0 0 0 0 0	Table Salarbia Datablia Salarbia Agentatal Agentatal
IPy4-Routes Mercent and and and and and and and and and and	Terget Interaction Hitchini (HICCIA) Hitchini (HICCIA) HITCHINI (HICCIA) HITCHINI (HICCIA) HITCHINI (HICCIA)	<u>Pr</u> ∔ fairnag	North B B B B B B B B B B B B B B B B B B B	Table Salarbin Datarbin Salarbin Aprilated Aprilated
IPy4-Routes menore and and and and and and and and	Target Bitanall HELDA 1904 Hall National HELDA 1904 HELDA 1904 HELDA 1904 HELDA 1904 HELDA 1904	<u>Pi</u> t fainnig	Nores 8 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9 9	Table Saladhin Datadhin Datadhin Agarthalat Agarthalat Agarthalat Agarthalat
IPy4-Routes moved and and and and and and and an	Target Bitchell HELZIA 19004 HELZIA 19004 HELZIA 19004 HELZIA 19004 HELZIA 19004 HELZIA 19004	<u>n</u> ,÷trinog	Norm 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Table Saintein Dataffer Dataffer Apriliatei Apriliatei Apriliatei april
IPy4-Routes mover and and and and and and and and	Targari Bibliosoff HEL254 19004 HEL254 19004 HEL254 19004 HEL254 19004 HEL254 19004 HEL254 19004 HEL254 19004	<u>n</u> ,÷trinog	Norm 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Table Sainten Denden Santan Aprilatei Aprilatei Sant Sant Sant Sant Sant Sant Sant Sant

2.2 Network Menu

2.2.1 LAN Settings

Enter the Network > LAN Settings, it shows host IP address, subnet mask, and the Maximum Transmission Unit (MTU) size, in bytes (Figure 2-3). The range is 1000-1500 bytes. The default is 1500 bytes.

Figure 2-3 LAN host settings

LAN Host Settings			
IP Address	Suboet Mask	MTU	
162.162.152.1	265.255.255.0	1500	
		@range 1005-1100	

You can enable or disable the DHCP server (Figure 2-4). If enabled, enter the start and end IP addresses, and the lease time for IP address use - from 10 minutes to 720 hours. Optionally, you can enter one or two DNS server IP addresses, and one to three option 138 connection IP addresses for connecting to a Control and Provisioning of Wireless Access Points (CAPWAP) server. When using option 138, the device will connect with the server's LAN port and get an Access Controller (AC) IP address.

Figure 2-4 DHCP settings

DHCP Settings		
DHCP Server		
Enable		
Start IP Address	End IP Address	Lease Time
192 108 100 100	142 108 100 200	121
		O Rangel, 10m-7205
DNS1	0%52	Option-43
11K.114.154.154	8.8.8.8	
(deniame)	● (Optianal)	© Here
Option138	Option138	Option 138
0 p address	e ip address	Ø o address

The *DHCP Reservations* may be used to bind an IP address to a specific MAC address (Figure 2-5). In the bottom half of the pane, enter the IP address and the MAC address, and click on *ADD*. The IP address must be within the range of DHCP addresses. Any configured bindings will appear at the top of the window.

Figure 2-5	Bundled	Address	List
------------	---------	---------	------

Settings		
P Address	MAC Address	
	9 Format serve several	10

2.2.2 WAN Settings

2.2.2.1 NAT Mode

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

Figure 2-6 WAN Settings

Operation Mode					
Operation Mude					
NAT Made	Ŷ				
Profile Setting					
APN Number		Bear Type			
#1	÷	Deta	×		
APN List					
APN Number	APN Name	Enable		Bear Type	
=1		Enable		Data	
DN\$ Mode					
Manually DRS		Primary GNS		Secondary DRS	
Ö					

DNS Mode set how to get DNS server IP:

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

2.2.2.2 Tunnel Mode

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

igure 2-7 Tunne	l Mode			
Operation Mode				
Operation Wode				
Tarout Basis	~			
🖸 Tunnel Mode				
VPN Type				
ane	~			
USE TYPE	2	Next Support		
February a	, i i	- Property		
S Profile Setting				
APN Number	3221	Bear Type		
10	Ŷ	Dee		
Tunnai IF Address		Tunnel Subner Mask	Destination #	
	•		1	
APN List				
AFN Number	APN Name	Enable	Bear Type	
*1		Enable	Data	
ONS Mode				
Matually DNS		Primary DNS	Secondary DNS	
			Idenared .	

2.2.2.3 Bridge Mode

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



Figure 2-8 Bridge Mode

Operation Mode					
Simple Under	*				
Profile Setting					
APN Number		Bear Type			
at .	~	Detta	~		
Vian ID		Sind MAC Address			
10120 L 10-1011 02	102*	@7armat economics			
APN List					
APN Number	APN Name	Enable	Bear Typ		
MI.		Ensible	Data		
DNS Mode					
DNS Mode		Primary DNG		Secondary DNS	

2.2.3 WLAN Settings

Select Network > WLAN Settings, and set the WLAN Network.

Figure 2-9 WLAN Overview

E financial	1,14 Setting	
🖂 Wirele	as Overview	
2	Owneric Athenes 592,11anac (willid)	
	1510: E03015W-02-10-50 Mode: Master B1510: 45: 5F 74:10:62:30 Energytion: px42+comp	Service Service
	SSID: EG3D15M-92+10-501 - Made: Warrer Wireless is disabled or not associated	Eleter Setter
	834D: EGS010M-03-10-003 / Made: Master Wireless is disabled or not essociated	Evalue Sectory
	35:D: EG3511M-42-13-6G3 / Mode: Warrer Wookeen is disabled or not addociated	Contra Derivation

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

Click the "SETTINGS" button to enter the network settings page. As shown in Figure 2-10.



Figure 2-10 WLAN Settings

Device Configuration

General Setup			
	Status	Mode: Master SSID: B BSSID: 48:8F:74:18:08:3	alcellsCPE5G-tangrul 0 Frequency: 5.300 GHz
	Network Mode	902.11a/an/ac/ax	¥
	Country Code	China	~
	Channel	auto	*
	Band Width	BOMHZ	v
	Transmit Power	20 dBm (100 mW)	*

Interface Configuration

	ESSID	BaicellsCPESG-tangrui		
	holding			
	Mode	Access Point	÷	
	Encryption	WPA2-PSK	्र	
	Cipher	Force CCMP (AES)		
Key Renew	al Interval(seconds)		_	
				<i>i</i>

Table 2-2 WLAN Settings Parameters

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



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

2.2.4 Static Routes

Select Network > Static Routes, and set the Static Routes.

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

Figure 2-11 Static Routes

Target Heat (2) of Hereord	(Fight Materials) (Fileger 16 a televite	interface	(All summer	Matrix
	00.00.00.00		1.0	
utto IPvil Raules		АРНЛ АРН2 АРН2 АРН3 АРН4		
-	Tangal (Address or Molecula (2009)	10000	the latera	. Barro
		The sector orders as using all		

2.2.5 DMZ

In technology, the DMZ refers to a firewall between incoming WAN traffic and the LAN to which the CPE is connected. Two basic DMZ methods are (a) using a single firewall, also known as the three-legged model, and (b) using dual firewalls (Figure 2-12). These architectures can be expanded to create complex architectures depending on the network requirements.

Figure 2-12 DMZ Examples



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

Bricells

DMZ	ICMP Reduct	DMZ Host Address
LINE.	TOWN RECEDU	a was to out to an out to
 Enable 	 ER\$5(e) 	

2.3**Cellular Menu**

2.3.1 Scan Mode

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

As part of the cell selection and reselection process, the CPE performs the scan first and then selects a small number of candidate cells to go through the next step of measuring and evaluating signals to select the best eNB that can serve it. The CPE frequently (milliseconds) performs the scan to ensure it has the best possible connection to the network. Refer to Figure 2-14.

Bricells			Weicomeusdmin 🖂	English
💮 Status	4	🔚 Celhillar / Scan Mo	da	
S Network	×.	🕞 Scan Mode		
10 Cellular	~	Scan Mode		
a constraint a	1.1	Full Band	*	
Scan Mode		Full Band Cell Lock		
	Sie -	Band Lock		
APIS Manageme	ITTE		Baxe & Apply	
PIN Managemen	nt			

Figure 2-14 Scan Mode

Select one of the following options:

- Full Band (default) All channels in the band. (Figure 2-15)
 - The CPE will routinely scan all channels in the band, increasing the time it takes to connect compared to the other modes. The band is dependent on the CPE model.

Figure 2-15 Full Band

- Cell Lock Specific cell only. (Figure 2-16)
 - The CPE will scan the list of eNBs with the specified cells when accessing the network. Using this mode can accelerate network access time. 5G CPE supports access to LTE and NR networks, and the locked frequency can be specified according to the accessed network.

Cancel
Property and a second

- Band Lock- Specific band only.
- Scan the specified band when accessing the network. 5G CPE supports access to LTE, SA and NSA networks, and the locked frequency can be specified according to the accessed network. (Figure 2-17)

🔄 Scan Mode					
Scan Mode					
Band Lock	~				
Band Lock					
Add List					
Band Lock Setting					
Band Lock Setting		Band			
Band Lock Setting Rat LTE	*	Band			
Band Lock Setting Rat LTE LTE GA	*	Band 1			
Band Lock Setting Rat LTE LTE SA NSA	Ŷ	Band 1			
Band Lock Setting Rat LTE LTE SA NSA	~	Band 1	Car	icel	
Band Lock Setting Rat LTE LTE SA NSA	~	Band 1 Add	Can	cel	
Band Lock Setting Rat LTE LTE SA NSA	*	Band 1 Add	Car	icel	

After selecting an option, enter the required information.

2.3.2 APN Management

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

The CPE supports 4 APN configurations. At least one APN (TR-069) must be configured when the CPE/eNB connect to the Baicells CloudCore. In the window (Figure 2-18) you will select the APN number (1-4), enable it, enter an APN Name, select Authentication Type, select the type of IP addressing (IPv4), and set the MTU value for the APN.

Figure 2-18 APN Management

1	Bricells					Wescome and	Erglisht -
8	Status	*	E Calbbar / APN Management				_
0	Network	ŝ	APN Management				
	Cellular	5	APN Number #1	v			
	Scar Mode						
	ATH Management		Enable				
	Pik Nanagement						
0	Security	\approx	APM Name		Authenticat	юо Туре	
					NONE		
Ξ	VPN				AUTO		
0	Bystem	2	Internet Protocol		CHAP		
G	Logout		1714	٠	1900 (1200)	(626)	
	0.000.000				W. (1422)	110-92	
				Sere 6	nom		
			APN List				
			APH Name	Internet	Pretocol	Exable	
				IPv4		enable	

2.3.3 PIN Management

Use the PIN Management feature if you want to require users to enter a PIN code before they can use the CPE to access the network (Figure 2-19). Once the PIN is enabled, you will need to remember it if you want to later modify the number. You are limited to 3 tries to enter the correct PIN code before getting locked out. If this happens, contact your service provider (end-users) or Baicells support (service providers).

Figure 2-19 PIN Management

tatus etwork eilular	B 2 2 4	Cuthitar / PON Management
etwork ellular		PIN Management
ellular	~	
		Available
ican Mode		
VPN Management		PIN Verification
SN Management		
ecurity	-	Remember PIN
PN	5	
ystem	÷	PIN
ogout		4-8 digits
		Remaining input times
		3
F	PN ystem ogout	PN ∽ vstem ∽

2.4 Security Menu

2.4.1 Firewall Settings

When using a firewall server in the local network, invoke this setting to enable or disable the firewall for this CPE (Figure 2-20).

Figure 2-20 Firewall



2.4.2 MAC Filter

Media Access Control (MAC) Filtering allows you to identify a list of devices either allowed to access or forbidden from accessing the network through the CPE (Figure 2-21). Select *Enable* to enable MAC filtering, and then determine whether you will allow or forbid the defined MAC addresses to access the network.

Figure 2-21 MAC Filter

ĩ	Bricells			
63	Status		E Security (MAC Filter	
Ģ	Network:	÷	🖂 Settings	
6	Cellular		MAC Filter	Authority besides tot dama
Q	Security			
	Firewall Settings		MAC List	
	MAD FIRM		Add Los	
	IP Filter		MAC Address	
	UHL Filler			
	Part Forwarding		@Fprmat as an or on an	
	Port Trippering		All Canad	
	ALG		- 1	
	Unit			Care & Apply

2.4.3 IP Filter

Internet Protocol (IP) Filtering allows you to filter services based on the IP address of the source device that is using the CPE to access the network (Figure 2-22). You can define a list of devices either allowed or forbidden from accessing the destination address range or port number range you enter.

To use this feature, select the *Enable* check box and then click on ADD LIST to open the settings window. Enter the source devices' IP addresses. Refer to Table 2-3 for a description of each field.

ĩ	Bricells						williams above
-	Status	*	E Security (Print				
0	Netzezek	÷.	🗇 Bettings				
4	Cellular	*	IP Piller		Filler Mode		
-	Security.	2					
	French Settings		E IP Last				
_	MAG Filler		and the second se				
	HOME:		Sarvisa Tope		Planat		Dalety Address Garge
	1001 Pillar		5.000	٠	(all	÷	
	Part Forwarding						Giurner is can ar a standiami
	Part Triggering		Daris Put Range		Gestmation Address Range		Destination Part Range
	#L0						
	MP-off		0707009 (10011005 at 1001		Wate large [[.52]	92.7	Grammer, spectrum or spec
	Billack Permetters						
11	VPN	8	And Carvel				
8	Tysine	÷			Saw Brazy		

Figure 2-22 IP Filter

Table 2-3 IP Filter				
Field Name	Description			
Service Type	Select the type of service, either custom, FTP, SSH, TELNET, SMTP, HTTP, POP3, HTTPs, or HTTP Proxy, the CPE will be allowed or forbidden to use			
Protocol	Select the type of data protocol, either ALL, TCP, UDP, TCP&UDP, or ICMP the CPE will be allowed or forbidden to use			
Source Address Range	Enter the IP address range for the source device(s) in the format of x.x.x.x or x.x.x/mask. The mask value may be 0 or 32.			
Source Port Range	Enter the port number range for the source device(s) in the format of 1000 to 1500, or 1000.			
Destination Address Range	Enter the IP address range for the destination device(s) to be filtered, in the format of x.x.x.x or x.x.x/mask. The mask value may be 0 or 32.			
Destination Port Range	Enter the port number range for the destination device(s) to be filtered, in the format of 1000 to 1500, or 1000.			

2.4.4 URL Filter

The Uniform Resource Location Filter (*URL Filter*) allows you to define a list of URL addresses users are forbidden from accessing. When you enable the filter, a *Settings* window appears. Enter the specific URL address users cannot access, as shown in Figure 2-23. To add more URL addresses, click on *ADD*. After entering the addresses and saving, the URL(s) you enter will appear in the URL List.



Figure 2-23 URL Filter

T	Bricells		Welcome;admin
8	Status		E Security/URL Filter
Ð	Network	×.	E Settings
di.	Cellular	÷	URL Filter
0	Security		
	Firewall Settings		
	MAC Filter		Add List
	iP Filter		101
	CONT. FILME		UNL
	Port Forwarding		
	Port Triggering		
	ALG		Canosi
	UPn₽		Contraction of the local data

2.4.5 Port Forwarding

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

To add a port forwarding rule, select the *Enable* check box and click on *ADD LIST* (Figure 2-24). Enter the parameters per the field descriptions in Table 2-4.

Figure 2-24 Port Forwarding

Ĩ	Bricells					Theorem advect
8	Status	۰.	E Supplements			
0	Bataork		E Settings			
4	GeRular	e.	⇒jet forwarding ⊖ Ecolor			
10	Security					
	Frendl Artinge		E Port List			
	MAG FIRM		And and			
	17 Films		Name of Street		Robert	And the second second
	1015-12160		ant	÷	100	 And the second sec
	PeriTreasuring					Grand states a loss
	Part Crapeting		Locar House		Lical Part	
	ALC .		0.		0	
	Linut.					
	Atlant Promision					
10	VPN		the lines			
4	System				Ten Link	

Table 2-4 Port Forwarding

5			
Field Name	Description		
Service Type	Select the type of service, either Custom, DNS, FTP, IPSec, POP3, SMTP, PPTP, Realplay, SSH, HTTPs, SNMP, SNMP Trap, Telnet, TFTP, or HTTP		
Protocol	Select the type of data protocol, either TCP, UDP, or TCP&UDP		
Remote Port Range	Enter the port number range for the remote device in the format of 1000 to 1500. Value range is 0~65535.		
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.		

2.4.6 Port Triggering

Port Triggering is a configuration option on a router - in this case, the CPE - if it is operating in NAT mode as the WAN interface type (<u>section 2.2.2</u>). When an application uses a trigger port to build a connection, the CPE will forward the data to the forward port.

To configure the feature, click on the check box next to *Enable* and then click on *ADD LIST* to enter the service type, protocol, trigger port, and forward port (Figure 2-25).

Figure 2-25 Port Triggering

ĩ	Aicells				
55	Status		E Second Per Negaring		
G	Network	-	E Settings		
ŝ	Cellular	æ	Port Trippering		
9	Security	1			
	Firewall Sattings		Port List		
	MAC Filter		Avent Link		
	IP Filler				
	URL Fitter		Service Type	Protonal	
	Port Parwarding		eaten v	70F V	ł.
	Port Triagering		Tripper Part	Parmant Part	
	ALG			Contrast of the second]
	UPnP.		@Povimat: 1000.1500.ar 7000	9 Fermat: 1000/1909 er 1000	
	Attack Protection		Add Carcal		
12	VPN				
0	System	2		Same & Apply	

2.4.7 ALG

The Application Layer Gateway (ALG) function provides a security component that augments a firewall or the NAT used by the CPE (if WAN Network Mode = NAT). It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer control/data protocols such as FTP, H.323 ALG, SIP, and PPTP. You can enable the different types of application protocols by clicking on the check box next to the protocol name (Figure 2-26).

Figure 2-26 ALG

P Network			
	-	🕒 Settings	
Cellular		FTF ALG	H. 325 ALG
		C Enable	Enable E
Becurity	- 60		
		SIP ALG	PPTP ALD
Forewall Setting	P.	🖬 Enanle	C Enable
MAC Filter			
iP Filter			
1981, Filler			Serve & Apply
Part Ferwardin	6		
Part Triggering			

2.4.8 UPnP

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

Go to Security > UPnP to enable the CPE to be searched by other devices (Figure 2-27). Once enabled, any redirects of traffic will display in the *Active UPnP Redirects* section of the window.

Figure	2-27	UPnP
--------	------	------

Brucetts	1				-
II. Mator	1	E there was			
· metanick	14	() incorrect thing & they			
d. Getatar		Statistics (Second 1) and (Se	a second is a provide state of the	a be instant	
-		Active UPs# Red	rocts.		
Street later	-	Producer	Evenue Part	Chief Address	Cherr Part
44(114a)			There a	e or active restricts	
10.000					
100,100		UPnP Settings			
Torigonal		a second second second	Enter Mark 12		
For Traping					
8.0					
10.000		0	Sector Sector		

2.4.9 Attack Protection

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

In the Security > Attack Protection window (Figure 2-28), select the check box next to the flood protection options you want to enable. When you click the check box, the field on the right becomes editable. Accept the default timer value, in seconds, or enter a value for each type of attack protection.

Figure 2-28 Attack Protection

¥.	Arcella				
5	Status	۰.	B Security Chief Protection		
0	Network	÷.	E Settinge		
4	Cettuter	×.	A spaint multiple convertises TOP ETH FLOOD street.	101	
0	Becarrie	2	Separat multiple connections UDP PLOGO attact	800	
			C) epainel multiple connections ICHIP FLOOD attack	20	
	Freest Sallings		C against angle connections TCP SVN PLOOD afters	70	
	MAC Prime		C epanel single remembers UDP PLDOD attack	80	
	if Film-		C against single convectors 2007 91,000 stack	14.	
	1852.71844				
	Part Formatting		Const Sec.		
	Fict Triggaring				
	N.S.				
	18PtuP				
	Address Typescolory				



2.5 VPN Menu

The Virtual Private Network (*VPN*) menu (Figure 2-29) enables you to configure a connection between the CPE and a VPN, e.g., to access a corporate network when telecommuting for work. You can enable a Layer 2 Tunneling Protocol (L2TP) gateway or a Layer 2 network connection to the VPN.

Figure 2-29 VPN Menu

8	VPN	^
	IPSec	
	OpenVPN	

2.5.1 IPSec

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

The top of the IPSec window is where you can add one or more security policies (Figure 2-30). The status of each policy you create will display in the lower half of the window.

Figure 2-30 IPSec



To configure an IPSec policy for this CPE, select the *ADD POLICY* button (Figure 2-31). Enter the policy name, remote gateway, local and remote subnets, and pre-shared key for the VPN connection. The *Advance Settings* offer additional parameters such as key exchange version, IKE encryption method, etc. Refer to Table 2-5.

And Property

Figure 2-31 IPSec

IP Sec Palicy List

Settings				
Enable	Policy Name		Remote Galeway	
() Enable				
	O t to 32 characters		0 to address!	
Local Butnet	Ramite Subnet		Fra-Shared Key	
6 Status Frence (SCHATTON)	O'Consultance 112	WEIGHT	61 n. 122 marante	¥
Advance Settinge				
Kay Eschange Version	Negatiation Mone		WE Encryption	
ind 👻	initialize musile	~	5des -	~
WE DH Group	INE Authentication		ESP Entryption	
respitet 🗸 🗸	mit	*	- States	
ESP DH Group	ESP Authentication		Left Identifian	
	and the	*		
			0 1 12 12 characters	
Right Identifier	SayLife		UNEL National	
	10405		96.623	
Q L to JE characters	@ Second(125-858800)		Ø Sacarnitis (13-1641)	
ReineyMargin	Opdection		Dpttdelay	
-	majan	~	34	
(economic):			@ Seconds(1-355)	
Kayinghisa				
4				
O 3 maarts torrerer				

Table 2-5 IPSec

Field Name	Description
Enable	Click on the check box to enable IPSec
Policy Name	Enter a policy name using up to 32 characters
Remote Gateway	IP address of the remote gateway
Local Subnet	Optional: IP address of the local subnet
Remote Subnet	Optional: IP address of the remote subnet
Pre-Shared Key	Up to 128 characters
Key Exchange Version	Internet Key Exchange (IKE) encryption method version 2 or version 1. IKE is a protocol used to ensure security for virtual private
	network (VPN) negotiation and remote host or network access.
Negotiation Mode	Initiator mode or Responder mode
IKE Encryption	des, 3des, aes128, aes192, or aes256

<u>Bricells</u>

IKE DH Group	modp768, modp1024, modp1536, modp2048, or modp4096
IKE	md5, sha1, sha256, sha384, or sha512
Authentication	
ESP Encryption	des, 3des, aes128, aes192, or aes256
ESP DH Group	none, modp768, modp1024, modp1536, modp2048, or modp4096
ESP	md5, sha1, sha256, sha384, or sha512
Authentication	
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

2.5.2 OpenVPN

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

OpenVPN implements OSI Layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol. It supports flexible client authentication methods based on certificates, smart cards, and/or two-factor authentication, and allows user or group-specific access control policies using firewall rules applied to the VPN interface. Setting up OpenVPN involves configuring server and client settings. Refer to Figure 2-32, Figure 2-33 (server), and Figure 2-34 (client) configuration fields.

Figure 2-32 OpenVPN

Brucells							- Martineau address -
III Status	- 22	E					
S Meson	20	C OpenVPN					
S Celetr	- 52	Control Part Instan					
C biarty	+	Apport PS Instal	NCOS	a set be week?			
11. 111	125		Brailed	Branted	Part .	Protovol	
1944	_	aerver	ä		1984	-	field and
times.				144	1022210	(47)	44
C System	-	slient			1.04	175	
() kingest							
				Tree &	-		
				Text	-		

Figure 2-33 Server

Overview » Instance "server"

Allow clie	ent-to-client traffic	0			
	yerti	3		×	
		Q Security retra	92.)		
	port	21104			
		O TOPLOP set #1	at more linear an	E remain	
	sun_lav8	C Q Main for Daniel	Pet source		
	ARCYNT	10.00.0265.255.251	(0)		
		O Configure server	-129		
- Additional Field -	hidon		e staten set	ant.	
dev_type	hespative	10.100			
ifconfig server_bridge		O Halper directive to configurations	2.027/1144	duarajou ol -bud aus -bud-aus	61 - 944 AV 1923
comp_tzo secret	prote-			~	
pkcs12		O. Chie protected			
ca dh	client	D O Configure clam r	1004		
key					

Figure 2-34 Client

Overview » Instance "client"

Additional Field		1011010		
port O Set subsity vertically dev_type ifconfig server server_bridge comp_tzo keepalive secret pkcs12 cs dh cert key	- Additional Field -	verb	 Premise tost neme or plact 3 	~
server_bridge comp_tzo keepalive secret pkcs12 ca dh cert key	port dev_type ifconfig	tun_ipvð	 D Set substantiativ D Set substantiation (Set Sector) 	
keepalive secret proto utu v pkcs12 0 Gee princos ce dh sient 0 Curtipute sient mote key	server_bridge comp_lzo	mobind	Constant in item etimen	anji por
cB dh sient O Contpute silent mote key	keepailve secret pkcs12	proto	utp Ø Cha prittecol	~
key	ca dh cert	sient	O Contiguire silent mobel	
	key	1		
			The second s	
			Care & Apply	

2.6 System Menu

2.6.1 NTP

The operator's network may use up to 4 Network Time Protocol (NTP) servers to provide correct time-of-day to network devices. In the CPE GUI you can refresh the local time display using the *SYNC WITH BROWSER* button; select the time zone that the CPE is in; and enable NTP client to use the default or specified NTP servers for synchronization (Figure 2-35).

Figure 2-35 NTP

ï	Aicells	2			
6	Statue		E Scherr (MD)		
Ģ	Network		⊡ нт р		
ĥ	Cellular	-	Time Zone Coefficientian		
0	Security		Time Zone Configuration		
	VPN	÷	Local Time	Mon Aug 18 67 14 29 2022	Spin are briefly
0	System	~	Timezone	uto	÷
	9095				
	Account				
	Oynemic OK8		time Synchronization		
	was lating		Enable NTP stient	8	
	PTP Auto Uppr	-	NTP server candidates	A sported past replace	10
	Chevrone Contra			Commentation (see a second	40
	111-062			A speciel property of a	6
	8NMP			1. species transforming	- 13
	Nexion/Updata				
	Ping Hatchaug				
				_	

2.6.2 Account

This menu is used to change the login password for the CPE (Figure 2-36). The password must be 5 to 12 characters. Baicells recommends using a combination of upper- and lower-case letters and numbers.

Figure 2-36 Account

Bricells				(mittant line)
In Partice	1	E Contra Securit		
© Arbenti		EAmount		
di Catalat	\mathbf{E}	Even for one passarel (Permat of A, example of C		of apper and leaver some lefters and fumikers.
C Second	2	27 144441		
- vre	1		4 http://www.wa	
@ tautem.		Yee passons	e til stor mener	e.
105		Conferentian		
(Second			ALTERNIC CONTRACTOR	
Sprarm (ret				
WEB MRING			and internal literature	
0.02270.000.000	11.41			

2.6.3 Dynamic DNS

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

1	Incells							
-	Dates	-	E Spent Street (M					
0	Between	σ.	C Records State					
ŝ.	Salutar	\sim	Dearer, Diff. dises ros. de	seam on the method with a f	and instruments	No. No. of Concession, Name	1001007.00	
0	Data (1))		Hota Hista					
	Veni		Price the last	Alter	m.mack			
	Surrem.		You will find many kinds	to obtaining here, whereas or a	in DONE with	is with all optimity		
	-							
	Assessed		Oracritere					
U.	-		former or a sint of wordigen	a series and property in the last	-			
	mite fatting		To status polici setto	a put terr			and solution and	sheer to
	11200-041		Configuration	Registered (P	Dutter	Kent Update	Process (I) Nort? Nup	
	10.001		myddns_ipv4	promote an ample com We give	0	Serer Dooleg	- 3	
			11.20-11-12.5V-11.					
	Sector and sector and		myddris_ipvfi	Vis data		Distant		
	Prog Making							
	944							
	System Menergy	-			Tree & Destr.			

Figure 2-38 Dynamic DNS Global Settings

Global Settings

Allow non-public IP's	 C) O Remoubled and by patient stopping P's Pixel 0.8, 100, 100, 04/10, 127/8, 108,254/16, 172,16/12, 192 (18/16) (Pixel 122, 1000,14)
Date format	9.9
	Ø For supported codes look here Ø Current setting, 2022-05-15 87:19
Status directory	Transformillarmi
	Q. Directory contains PID and other status information for each tuning sector
Log directory	rearingendes
	O Divertity contains Log lives for each namery section
Log length	250
	Rember of last times stored in top Files

Back to Descrive Serve & Paper

Figure 2-39 IPv4 DDNS configuration

Details for myddns_ipv4

Enabled Of this service sector is disabled is could not be statued lackup Hostname Publication and the statued IP address version IP address IP address version IP address IP	isic Settings Advanced Bettings	Timer Settings Log File Viewer
B. If this service sector is disabled is could not be statist Necker from LLC1 methods and from obtable youthing reactions is disabled is could not be statist Necker from LLC1 methods and from obtable youthing reactions is disabled is could not be statist Necker from LLC1 methods and from obtable Peddress version Peddress version Peddress version Peddress version Peddress Peddress O DDNS Service provider (IPv4) Peddress O Defress which IP address O Defress which IP address O DDNS Service provider (IPv4) Peddress O DDNS Service provider (IPv4) Peddress O Defress which IP address O Defress which IP address O DDNS Provider Peddress O DDNS Service provider (IPv4) O Dotate UPL is the used for optioning your DDNS Provider Feloco instructions you will find on their WEE page. O DotAte UPL is the used for optioning your DDNS Provider Feloco instructions you will find on their WEE page. O DotAte UPL is the used for optioning your DDNS Provider Feloco instructions you will find on their WEE page. O DotAte UPL is be used for optioning your DDNS Provider Feloco instructions you will find on their WEE page. O DotAte UPL is the used for optioning your DDNS Provider Peddress (DOMAIN) in Update-UPL O Dotate UPL is used for optioning your DDNS Provider Peddress (DOMAIN) in Update-UPL O Peddress (DOMAIN) in Update-UPL O Peddress (USERPLANE) is Update-UPL O Peddress (PASS(WORD) is Update-	Enabl	les D
Leckup Hostmane Petrome/FODN is validate. ? Produces happen or necessary Paddress version IP address version IP address version IP vd-Address IP vd-Ad		Ø If this service sectors is disabled is could not be started. Nether hort LuCI interface har from contable.
Padress version Padress version Padress version Padress version PuP4-Address Pup4-A	Lookup Hostna	me yourbust startight over
IP address version IPv4-Address IPv6-Address IPv6-Address IDDNS Service provider (IPv4) Immunit Custom update-URL Immunit G Update URL to be used for updating your DDNS Provider Fullowing update-script Immunit G Update URL to be used for updating your DDNS Provider Fullowing update-script Immunit G Update URL to be used for updating your DDNS Provider Fullowing update-script Immunit G Update URL to be used for updating your DDNS Provider Fullowing update-script Immunit G Update URL to be used for updating your DDNS Provider Fullowing Update-script Immunit G Update URL to be used for updating your DDNS Provider Hostname/Domain Immunit Immunit Immuni		Hearrame/FQ2H to validate. If IP update happen or necessary
DDNS Service provider (IPv4) • animum • animu	IP address vers	ian Py4-Address
DDNS Service provider (IFV4) Custom update-URL Custom update-URL O Update URL to be used for optiding your ODNS Provider Solor instructione you will find on their WES page. Custom update-script Hostname/Domain Paseword Paseword Paseword O Papinoes (PASS(VORD) in Update-URL)		DiPv6-Address
DDNS Service provider (IPV4) Custom update-URL Custom update-URL Custom update-script Custom update-script Hostname:Domain Paseword Pasewor		Ordinax which IP address "IPV4/IPvd" is send to the DDNB provider
Custom update-URL O Update URL to be used for opdating your ODNS Provider Foldoe instructions you will find on their WES page. O Custom update script In the used for updating your DDNS Provide O Custom update script to be used for updating your DDNS Provide Pastername O Replaces (DDNAIN) in Update-URL Username O Replaces (DDNAIN) in Update-URL O Replaces (FASD/VORD) in Update-URL	DDNS Service provider (IP)	v4)
O Update UPL its be used for updating your DDNS Provider Follow instructions your will find on their WES page. Custom update-script O Custom update script Hostname/Domain your_complications Username Paseword Paseword O Replaces (PASEWORD) in Update-UPL	Custom update-U	RL
Custom update-script Hostname/Domain Hostname/Domain Paper.comment Username Paper.comment		O Update UPL to be used for optiating your ODNS Provider. Follow instructions you will find on their WES page.
Custom update scrut to be used for updating your DDNS Provid Hostname/Domain produces (DOMAIN) in Update-UPL Username Paseword	Custom update-scr	ript
Hostname/Domain profile com O Replaces (DOMAIN) in Update-URL Username O Replaces (USERNAME) in Opdate-URL Paseword O Replaces (PASS/NORD) in Update-URL		 Oustom update scrut to be used for updating your DONS Provider
Paperson (USERNAME) in Update-URL Paperson P	Hostname/Dom	ain partnal accepts can
Vsername Papeword Paseword Q Replaces (PASS/VORD) in Update-URL		 Repares (DOV(AV)) in Update-URL
Papeword Paseword	Userna	me)na_annana
Paseword (Replaces (RASS/WORD) in Update-DRL		Ø Papiates (USERNAME) in Optimi-URL
Q: Replaces (RASS/VORD) in Update-DRL.	Pasowo	ard
		Q Replaces (RASS/VORD) in Update-URL
Use HTTP Secure	Use HTTP Seco	ure 🗆





Figure 2-40 IPv6 DDNS configuration

Details for: myddns_lpv6

Enabled C Prim's service section is disabled it could not be stamed. Native: from LuCI Interface for from consete Lookup Hostmame peatroame/PODN to salidate. If IP update happen or necessary IP address version IPv4-Address IP address version IPv4-Address IP address version IPv4-Address IP of Address IPv4-Address IP of DDNS Service provider (IPv6) reader Custom update-URL insurg/UEEENVANE() (PASSWORD(D)) (PV O Update URL to be used for update for good DDNS Provider Polos unstructions you will find on their WEEB page. Custom update-seript Imputition update societ to be used for update-URL IP address (DOMAIN) in Update-URL Insurget societ to be used for update-URL IP assword Replaces (IPASSWORD) in Update-URL IP assword Imputition update-URL IP assword IPASSWORD) in Update-URL IP assword IPAstores (IPASSWORD) in Update-URL	Enabled If this service sectors is disabled it could not be stamed. Nether than LuCl interface nor tion couple. Lookup Hostmane Journal PODN to salidate. If IP update happen or necessary IP address version IPv4-Address IPv6-Address IPv6-Address IPv6-Address DDNS Service provider (IPv6) Custom update-URL Intuit/DEENNANE(IPASSWORD) Quation update-URL Intuit/DEENNANE(IPASSWORD) Quation update-Script Quation update-script Quation codes societ to be used for updating your DDNS Provider. Follow instructions you will find on their VEB page. Custom update-script Quation codes societ to be used for updating your DDNS Provider. Follow instructions you will find on their VEB page. Quation codes societ to be used for update-URL. Quation codes (IDSENAME) in Opdate-URL. Quation codes (IDSENAME) in Opdate-URL. Quational (MASEWORD) in Update-URL. Quational (MASEWORD) in Update-URL. Quational (MASEWORD) in Update-URL. Quational (MASEWORD) in Update-URL. Quational societ to communication with DDNS previder.		Maximoed periods	100	senuita	roß une niemei		
O Prime service sectors is disabled from that be started. Nether from LuCl interface for from contails I put heat beamyle cam Protections PCON to salicate. If IP update happen or necessary Prot-Address Prot-Address IP address version IP address version IP update switch P address 'Pr4:Pr4' is send to the DDNS provide O Defines which P address 'Pr4:Pr4' is send to the DDNS provide O Defines which P address 'Pr4:Pr4' is send to the DDNS provide O Defines which P address 'Pr4:Pr4' is send to the DDNS provide O Defines which P address 'Pr4:Pr4' is send to the DDNS provide O Defines which P address 'Pr4:Pr4' is send to the DDNS provide O Defines which P address 'Pr4:Pr4' is send to the DDNS provide O Define which P address 'Pr4:Pr4' is send to the DDNS provide O Define which P address 'Pr4:Pr4' is send to the DDNS provide O Define which P address 'Pr4:Pr4' is send to the DDNS provide O Define which P address 'Pr4:Pr4' is send to the DDNS Provide O Define update-URL Hostname/Domain Ver_uxamame Practaces (DDNAN(in Update-URL Password Practaces (PASSWORD) in Update-URL Password Practaces (PASSWORD) in Update-URL Use HTTP Secure O Paratace accuration with DDNS provider	Print service sector is disabled it could not be stamed. Nether from LuCi interface nor from consele purified basing PGDN to validate, if IP update happen or necessary P address version P address version P doress version P doress version O Defines which P econess (Pv4:Pvd) is send to the ODNS provide Custom update-URL intuit[USERNAME][PV656WORD][gyue Outlos Service provider [IPv6] Custom update-URL MultipleEnNAME][PV656WORD][gyue Outlos to used for updating your CONS Provider Follow instructions you will find on their WEB page. Custom update-script O Custom update-script O Custom update-script O Custom update-script O Custom update-script O Replaces (IDDMAN)[in Update-URL Voe_ummans O Replaces (IDDMAN)[in Update-URL Password Pastures (IPASSWORD) in Update-URL Use hTTP Secure O Entotic secure communication with DDNS provider O Entotic secure commun		En	abied	0			
Lookup Hostname Puthod inample.com Paddress version Pv4-Address Pv	Lookup Hostname Pushtet sample.com Paddress version Paddress version Prv4.Address Prv6-Address ODNS Service provider (IPv6] Custom update-URL Custom update-URL Paddress URL to be used for updating your DDNS Provider Fadou instructions you will find on their WEB page. Custom update-script OUNS Provider (IPv6] Pushtet asserpts com Paddress (IPASSWORD) in Update-URL Username Password Pasiess (IPASSWORD) in Update-URL Use HTTP Secure Paties secure communication with DDNS provider				O It mix Naither fr	service section is d on LuCI interface r	sabled it could not be star or from conacle	tel.
Hostmane P201/to skildate, if IP liptote happen or necessary IP address version IP address version IPv4-Address IPv6-Address IPv6-Address O Defrees which IP ecoress IPv4:IPv6 is send to the ODN3 provide DDNS Service provider (IPv6) Custom update-URL Intu-II[U0ETNAAME] (PASEWOND)()(vu) OUdate URL In the used for updating your CONIS Provider Follow instructions you will find an their VEB page. Custom update-seript O Custo	Postmane/PODNIc validate, if IP update happen or necessary Padress version Padress version Padress which P address O Defines O Define O De		Lookup Host	name	joine	anisripte core		
IP address version IPv4.Address IPv0-Address IPv0-Address DDNS Service provider (IPv0) Implifutchwakt) (PASSWORD)(gyun) Custom update-URL Implifutchwakt) (PASSWORD)(gyun) Custom update-URL Implifutchwakt) (PASSWORD)(gyun) Custom update-URL Implifutchwakt) (PASSWORD)(gyun) Custom update-seript Implifutchwakt) (PASSWORD)(gyun) Custom update-seript Implifutchwakt) (PASSWORD)(gyun) Pastmane/Domain Implifutchwakt) (PASSWORD)(gyun) Visername Replaces (DOMAIN) in Update-URL) Visername Replaces (DOMAIN) in Update-URL) Password Implifutchese (PASSWORD) in Update-URL) Use HTTP Seture Implifutchese communication with DDNS provider	IP address version IPv4-Address IPv6-Address IPv6-Address DDNS Service provider (IPv6) Imment P address (IPv4)Pvf1 is sent is the DDNS provid Custom update-URL Imment IPv6ERNANEL (IPADSINORD)(Ipvoin) Custom update-URL Imment IPv6ERNANEL (IPADSINORD)(Ipvoin) Custom update-URL Imment IPv6ERNANEL (IPADSINORD)(IPV0in) Custom update-seript Imment security for be used for lipotiting your DDNS Provider Follow instructions you will find on their VEE page. Custom update-seript Imment security for Update-URL IPV0int Excernine Hossname/Domain yournust security for Update-URL IPV0int IPD0int IPV0int IPV0iPV0iPV0int I				Q Heatri	ema/FCOH) to salida	te. If IP update happen of	nacessary)
IPv0-Address O Defines which P econess 1Pv4:Pvd is send to the DDNS provide DDNS Service provider (IPv0] Custom update-URL Intuit(UDEDNAME) (PASSINOND)@yww O Update-URL Intuit(UDEDNAME) (PASSINOND)@yww O Update-URL Custom update-script			IP address ve	noista	OIPv4.A	ddress		
O Defress which IP address (IPv41Pvd) is send to the DDNS previous DDNS Service provider (IPv6) Custom update-URL IntuinjudDDNANA() (PASSWORD)(Qyour) O Update-URL O Update-URL Usetom update-script O Custom update-script O Replaces (IDOMAIN) in Update-URL Username O Replaces (IDOMAIN) in Update-URL O Replaces (ISSERNAME) in Update-URL O Replaces (ISSERNAME) in Update-URL O Replaces (IFASSWORD) in Update-URL Use HTTP Secure O O Enable secure communication with DDNS provider	Ordenes which Precoress (PektPed) is send to the CONS provider ODNS Service provider (IPv6) Custom update-URL Usedom update-URL Usedom update-seript O Update URL to be used for updating your CONS Provider Follow instructions you will find on their WES page. Outrom update script to be used for lupdating your CONS Provider Postname/Domain vermust exempte cam Prepieces (ICOMAN) in Update-URL Username Password Password Password Username Q Repieces (USERNAME) in Update-URL Username Password Password Date HTTP Secure O Enable secure communication with CDNS provider Password Pastore secure communication with CDNS provider Password Pastore secure communication with CDNS provider Password Pastore secure communication with CDNS provider				* IPv8-A	ddress		
DDNS Service provider (IPv6) Custom update-URL Intuil(USEXNAME) (PASSINORD)(Qyour) OUDDATE-URL Ustom update-script Custom update-script O Custom update-script O Custom update script to be used for updating your DDNS Provide Hostname/Domain Verunted exempte com O Replaces (DDMAIN) in Update-URL Username O Replaces (USERNAME) in Update-URL Password Pasinces (PASSWORD) in Update-URL Use HTTP Secure C O Enable secure communication with DDNS provider	DDNS Service provider (IPv6) Custom update-URL Public URL to be used for updating your CDNS Provider Follow instructions you will find on their WEB page. Custom update-script O Custom update-script O Custom update-script O Custom update-script O Custom update script to be used for updeting your ODNS Provid Hostname/Domain Provider script to be used for updeting your ODNS Provid Hostname/Domain Provider script to be used for updeting your ODNS Provid O Custom update script to be used for updeting your ODNS Provid O Repteces (IDDMAN(I in Update-URL) Username O Repteces (USDSNAME) in Update-URL Password O Repteces (IPASSWORD) in Update-URL Use HTTP Secure O Enable secure communication with DDNS provider				O Define	s which IP pooress	Policy is send to the	00%5 previde
Custom update-URL InterritUSETRIAANED (PASSINOND)@your O Update URL to be used for updating your DDNS Provider Follow instructions you will find on their WEB page. O Custom update-script O Custom update script to be used for updating your DDNS Provider Hostname/Domain your_usemane O Replaces (DOMAIN) in Update-URL Username Password Image (PASSINOND) in Update-URL Use HTTP Secure Image because communication with DDNS provider	Custom update-URL interrpdbERNAWE)(PASSWORD)(gyver @ Update URL to be used for updating your DDNS Provider Follow instructions you will find on their WEB page. Custom update-script @ Custom update script to be used for updating your DDNS Provid # O Custom update script to be used for updating your DDNS Provid # O Custom update script to be used for updating your DDNS Provid # O Custom update script to be used for updating your DDNS Provid # O Custom update script to be used for update-URL Username @ Replaces (DDMAIN) in Update-URL # Password @ Replaces (USERNAME) in Opdate-URL Use HTTP Secure @ Facilie secure communication with DDNS provider	D	DNS Service provider ([Pv6]	- Country	H	~	
Custom update-script Custom update-script Custom update-script Custom opdate script to be used for updating your DDNS Provide Hostname/Domain Ver_usemane Replaces (DDMAIN) in Update-URL Ver_usemane Replaces (USERNAME) in Opdate-URL Ressword Replaces (PASSWORD) in Update-URL Use HTTP Secure Provide COMPARIANE Provide URL COMPARIANE P	O Update URL to be used for updating your CDNS Provider. Follow instructions you will find on their WEB page. O Custom update-script O Custom update script to be used for updating your DDNS Provid Hostname/Domain Visername O Repleces (DDMAIN) in Update-URL Username O Repleces (DDMAIN) in Update-URL Username O Repleces (VSERNAME) in Opdate-URL Use HTTP Secure O Enable secure communication with DDNS provider		Custom update	URL	inip://pr	EERMANE) (PASSING	HD30you	
Custom update-script O Custom opdate script to be used for lopdeting your DDNS Provide Hostname/Domain Province (DOMAIN) in Update-URL Username Password Pas	Custom update-script © Custom update script to be used for lipdeting your DDNS Previd Hostname/Domain © Replaces (DOMAIN) in Update-URL Username © Replaces (USERNAME) in Opdate-URL Password © Replaces (IMSEWORD) in Update-URL Use HTTP Secure © Enable secure communication with DDNS provider				O Update Follow ins	e URL to be used to itructions you will fi	r vodeling your CONS Pro of on their WEB page.	Nder.
Custom update script to be used for lipdeting your DDNS Provide Hostname/Domain yourtionLaxangle.com @ Replaces (DOMAIN) in Update-URL Username @ Replaces (USERNAME) in Update-URL Password @ Replaces (PASSWORD) in Update-URL Use HTTP Secure @ Enable secure communication with DDNS provider	Custom update script to be used for updating your DDNS Provid Indexname/Domain Veruname Veruname Veruname Veruname Password Pass		Custom update-	script				
Hostname/Domain yourtool axangle.com © Replaces (DOMAIN) in Update-URL Username © Replaces (USERNAME) in Opdate-URL Password © Replaces (PASSWORD) in Opdate-URL Use HTTP Secure © Enable secure communication with DDNS provider	Hostname/Domain yournoot, example, com © Replaces (DOMAIN) in Update-URL Username © Replaces (USERNAME) in Opdate-URL Password © Replaces (PASSWORD) in Update-URL Use HTTP Secure © Enable secure communication with ODNS provider				O Custo	e agidate sorigi to b	e used for lipdeting your C	DNS Provide
O Replaces (DOMAIN) in Update-URL Vour_usemane O Replaces (USERNAME) in Opdate-URL Password O Replaces (PASSWORD) in Update-URL Use HTTP Secure O O Enable secure communication with DDNS provider	O Replaces (DOMAN) in Update-URL Ver_ummane O Replaces (USERNAME) in Update-URL Password Password Password Password O Replaces (PASSWORD) in Update-URL O O Enable secure communication with DDNS provider		Hostname/Oc	main	youthind	avangle con		
Username	Username ver_ummane © Replaces (USERNAME) in Optimi-URL Password @ © Replaces (PASSWORD) in Optimi-URL Use HTTP Secure () © Enable secure communication with DDNS provider				O Repla	tes (DOMAIN) in Up	date-URL	
Password	Password		User	name	9907_00	mana		
Password	Password				0 Replat	ees (USERNAME) /	Opdata-URL	
O Replaces (PASSWORD) in Update-URL Use HTTP Secure O Enable secure communication with DDNS provider	PRotectes (PASSWORD) in Update-URL Use HTTP Secure O Enable secure communication with DDNS provider		Past	word		0 0		
Use HTTP Secure () © Enable secure communication with DDNS provider	Use HTTP Secure () © Enable secure communication with DDNS provider				9 Papla	ies (FASSWORD) I	Update-URL	
O Enable secure continuitication with DDNG provider	Enable secure communication with DDHS provider		Use HTTP S	ecure	9			
					0.51353	E BECUIE CONTRUNCI	oon with DDNS provider	

2.6.4 WEB Setting

WEB Setting provides the ability to configure and manage the CPE remotely (Figure 2-41). This is especially helpful when a user calls in for technical assistance. In "1.4 Log In", you used this Web application with the default URL of <u>http://192.168.150.1.</u> Refer to Table 2-6 for a description of each field.

Figure 2-41 WEB Setting

Ĩ.	Aicells			
69	Status	-	E Stree (MC3 Setting	
0	Network	÷	🖂 Settings	
4	Cellular	-	HETP	HTTFFor
			0	84
8	lecurity	$\sim 10^{-1}$		
			HTTPS	HTTPSPort
.9	VPN	1.00	a	40
a	System	100		
			Allow HTTPS Loge From WAN	Redress HTTPS
	NUE		0	D.
	Account			
	Dynamic Dws			Service and the service of the servi
	WED Aviling			Seve & Austr

Table 2-6 WEB Setting

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

2.6.5 FTP Auto Upgrade

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



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

If you are using a dedicated FTP server for this purpose, select the *Enable* check boxes next to *FTP Auto Upgrade* and *Check New FW after setup* (Figure 2-42). Enter the FTP server IP address and the *Path And File* text suffix. If login permissions are required to access the server, enter the username and password. To configure a set interval for the CPE to check the server for new firmware, select the check box next to *Use custom Interval* and enter the interval time, in hours. The range is 1-2400 hours.

1	Aucells						-
10	listen	1	······································				
0	Network	×	🗇 Settings				
ŝ	Celsiar	-	FTF Ayas Uppade				
9	lectrity						
-1	171	÷.	Chalte Have PW phar callup Chalter		Pag Sarver 102.108-1.1		Path And Pha
	System.	9					Andrew Calculation for the
	14779		Usernene	-	Passent	24	Use susces inscript
	Addapted		Charte Name FW Parents				
	Oyname.dwit		1				
	vies seting		# trul (200)				
	and Ander Spage						
	TRACK		10		Service Appendix		

Figure 2-42 FTP Auto Upgrade

2.6.6 TR-069

If your network operates using a TR-069 auto-configuration server (ACS), the ACS will automatically provide the CPE configuration settings. Once you set up both the ACS and the CPE, you do not need to enter any other parameters through the CPE GUI. Use the *TR069* sub-menu to enable the TR-069 function for the CPE (Figure 2-43). Refer to Table 2-7 for a description of each field.

Figure 2-43 TR-069

Bruce	lis -			The later set of
III Status	- 21	B Acces-19(0)		
© Retexts	- 52	🗇 Settings		
il centre		THEMS B Evolution		
10 Security		ACT Top	ATS Astrony	
= vrn	50	10. ¥		
d System	1.0		8 HE2H	
- ARTE		User Name	Passant	
Associat		Herr		
Tynemy	00	CPE paloits suppling		
103.00	14	S Every		
111.645	13.87494	Telses	Studies	Suttane
		A Designation of the local division of the l	A description in Facility . Start with	Witnessed Address of Contractor
şinis-			a university of the	a temperatific to de
Bastynery	u dale:	17.01		
Freq Halo	****	B Acotta		
64.0		this barear	Dan Savai Part	Value Allow (married
8431540	habe		(44%)	
Eystate N	eesagee			 Generalizz-Sill
Displace	Ç			
Report			See Street	

Table 2-7 TR-069

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



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

2.6.7 SNMP

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

To enable SNMP, select the *Enable* check box (Figure 2-44). Complete the settings per the field descriptions in Table 2-8.

Figure 2-44 SNMP **AICells** 1 System | 274/P E Status 4 C Network 🖻 Settings SNMP il Cellular 🗇 Enable O Security NMS Address NMS Port C VPN 162 C Lystam Listening Fort Trap Community NTP 10.1 public Assessed Version Dynamic DNE VAV5-WEE Satting FTP Auto Upgrade Read Community RW Community paintie) private TR-048 STATES? Restore/Update Since & App Etter Weinheiter 46

Table 2-8 SNMP	Table 2-8 SNMP				
Field Name	Description				
SNMP	Enable the Simple Network Management Protocol by clicking the check box.				
NMS Address	NMS server IP address				
NMS Port	NMS server port number				
Listening Port	CPE port number				
Trap Community	Public or private - identifier to distinguish read/write permissions for data				
Version	Select the SNMP version you are implementing - V1&V2c (for SNMPv1+SNMPv2c) or V3 (for SNMPv3)				
Read Community	Public or private read-only community name				
RW Community	Public or private read/write community name				

2.6.8 Restore/Update

Use the System > Restore/Update menu to reset the CPE to its factory default settings, to manually update the firmware, or to manually update a module within the firmware - meaning to apply a patch to the current firmware (Figure 2-45).

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

Figure 2-45 Restore/Update

ĩ	Bricells		
ET	Status	*	······································
G	Network	-	Click "Generate archive" to download a tar analyse of the surgest configuration like. To result the first according tragest.
÷	Cellular	-	Download backup
e	Security		Converses and the
8	VPN		🖂 Reset to defaults
0	System		Perform reserve
	ATP Account		To resoure configuration thes, you set upload a previously generated sector anthree here.
	Dynamic DNS		Phone select a lin
	WEB betting		Carried extrant.
	PTP Auto Opgrad	18	Uplead a systepyrate-compatible image have to replace the raying formate. Check 'Keep settings'
	TR-063		E Flash new firmware image
	BNME		Pares setut a lin E Setut für 2 Kasp settings
	Restorational		Times integer

2.6.8.1 Restore

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

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

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

2.6.8.2 Update Firmware

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

To update (upgrade) the CPE to a different firmware version (Figure 2-45):

1. Download the image file from the Baicells support website (Baicells > Support > Downloads), and save it to your computer.

- 2. Under *Flash new firmware image*, determine if you want to keep the current configuration settings on the CPE. If you do, select the check box next to **Keep settings**.
- 3. Click on **Choose File** to navigate to the new image file on your computer, and then click on **FLASH IMAGE** to initiate the upgrade.

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

2.6.9 Ping Watchdog

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

To enable the watchdog function (Figure 2-46):

- 1. Select the check box next to Enable and enter an IP address accessible by Internet for the CPE to try to ping.
- 2. Set the period of time, in seconds, for the ping to timeout. The range is 1-65535 seconds.
- 3. Enter the number of times to try to ping the address, in the range of 1-65535 times.
- 4. Enter the maximum number of times the CPE can try the ping but fail before the CPE initiates a reboot. The range is 1-65535 times.

Figure 2-46 Ping Watchdog

Brucelis				Marian and
= vPN	E. Specify Denning			
Pysion Attp Acto Acto	 C Settings Fing Webbing Discuss P Advance to Ping R Competitioners, by R Settings R Competitioners, by R Settings R Setting R	Prog Teresco (Taxondo) 20 40	Ping Dave 16 W 101-14145	
Kastataipptata		-		
This matching		Serve & Apple		

2.6.10 SAS

CPE realizes equipment registration, authentication and spectrum access license acquisition through SAS.



SAS menu provides SAS info and SAS settings, as shown in Figure 2-47.

Figure 2-47 SAS Menu

1	Bricelis					Warman
2	Descript.	1	B. Sec. 201			
	174		🗄 \$43 lefe			
0	Apress	222	30	82123+82+09120	manufacture (Same	1.05
	1479		A06.6	conver, but	Call right meaning	2285.5.50vg
			Arrany	1	faither burning .	2010 il Miris
	Summer State		Sens Services	8,2784	Far-resolution (20.3994
	1		Avenue Made	(marta)	Statistic Statistics	104
	NEX WORK		Annual and Annual Contract	42.	Dell-Harris	Easter
	CLA YOUR AND AND A	199	Dana Tan	and a state of the second seco	Radio Source.	Destant
	10.000					
	And P		E SA3 Settinge			
	formation in		Ammetal248	Sel. 11 Febr		
	Prog Television					
	10.0			The second second		

Table 2-9 SAS Info field description

Field Name	Description
SN	Serial number of the product
FCC ID	FCCID of the product
Category	Product category (A or B)
Radio	Antenna technology
Technology	
Antenna Height	Antenna type
Туре	
Group Type	SAS CPE Device Group Category
Antenna Gain	Antenna gain
Cell High	The highest frequency of the current LTE access band
Frequency	
Cell Low	The lowest frequency of the current LTE access band
Frequency	
Bandwidth	LTE current bandwidth
Granted	SAS server authorized power
EIRP(10MHz)	
SAS Status	SAS current status
Radio Status	Current RF status of LTE

2.6.10.1 SAS Settings

- 1. Select the enabling mode of SAS function.
 - Automatic (B48) select On, automatically turn on SAS (when the device is connected to band48, SAS will be turned on automatically; when the device is connected to non band48, SAS will be turned off automatically).

Figure 2-48 Automatic SAS	
🖃 SAS Settings	
Automatic(B48)	SAS
🔿 Off 🔘 On	🗇 Enable
	Save & Apply

• Automatic (B48) select Off, turn on SAS manually (If enable is selected for SAS, it means the SAS function is turned on; if not selected, it means the SAS function is turned off).

Figure 2-49 SAS Settings

843	
C Enable	
Registration Method	ACS Server URL
🐵 Mutt-Brep 🕐 Single-Step	
Cell Sign	
	8A3 Bratie Registration Method Mutti-Step Cell Sign

- 2. Select SAS access mode.
 - Select Domain Proxy: SAS proxy. Implement SAS access through OMC.
 - Select Direct SAS: SAS direct connection. CPE is directly connected to SAS server.
- 3. In Direct SAS mode, you need to select SAS registration mode.
 - Select Multi-Step: multi step registration. This registration mode is used when the installation information of the device already exists on the SAS server.
 - Select Single-Step: single step registration. This registration mode is used when there is no installation information of the device on the SAS server.



4. Configure SAS parameters.

Field Name	Description
ACS Server URL	Web address of the auto-configuration server (ACS). When the access method is Domain Proxy , the default DP server is the ACS URL configured on the TR069 page and cannot be edited manually.
SAS Server URL	The address of the SAS server in direct mode. When the access method is Direct SAS , you can manually change the URL.
User ID	Enter the user name to access the ACS server
Call Sign	Device identifier

5. When Single-Step registration mode is selected, antenna parameters need to be configured.

Figure 2-50 Antenna Parameters

		D Enalis			
Actess Natural		Negational Vetros		DAS Derver URL : Topo I mercelo dal arroro DIDECT 2	
unar 10		Call Right			
Lattuite.		Linghole		Indian Dephyment	
	1.43.2* - 30.04		1.402.36 - 302.342	- Biles'	*
Altenna Hagto		Ansenia Azimute		Antanta Doentili	New Jac

Table 2-11 Antenna Parameters

Description
Latitude of the CPE antenna location in degrees
Longitude of the CPE antenna location in degrees
Whether the CPE antenna is indoor or not
The CPE antenna height
Boresight direction of the horizontal plane of the antenna in degrees



Field Name	Description
Antenna	Antenna down tilt in degrees and is an integer
Downtitle	
Antenna	The CPE antenna beamwidth
Beamwidth	

2.6.10.2 CPI Settings

When Single-Step is selected for the registration method in SAS settings, the CPI settings area appears, as shown in Figure 2-51.

Figure 2-51 CPI Settings

CP11D	CP1 Name	install Time	
		- Autor	
Ipload Centificate		200	

CPI (Certified Professional Installer) Settings is used to verify the information of the installer.

- 1. Enter CPI ID or CPI name.
- 2. Enter the Install Time or click the Auto button.
- 3. Click Choose file to select CPI certificate file from this computer.
- 4. Click **SAVE & APPLY** to make the configuration effective.

2.6.11 SAS Certificates

Upload the certificate required for CPE to connect with SAS server.

Three types of certificates can be uploaded: SAS Client Cert, SAS Client Key and SAS Server CA.

After the certificate is uploaded successfully, the certificate file name can be displayed in the Certificate List. If you need to replace the certificate, you can click the **Remove** button on the right side of the certificate to delete the certificate, and then upload the new certificate again.

Figure 2-52 SAS Certificates

Bricelis				Access Advert
WER Saiting	E Apress (3) (1) (- Million			
TTP AND Uppose				
79.000	E SAL Certificates	timed facilities		
Autor.		Para site) per patiente	10 Xamiri bas	
Restrictions	SAS Client Cert			
mag meaning	SAS Clieft Key SAS Barvar CA			
11.1	III Confirmenting			
Statements	Bold Glass Date	Bell Diant Yay	645 Date Carl	
Xysten: Maveegeri	1000000	1		

2.6.12 System Messages

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

Figure 2-53 System Messages

1	Bhicells		Belinkaler - Egi
8	Buttan	-	E form from from the
0	Network	-	I System Manager
4	Cathlan	3	Hon Aug 18 00:50:20 2022 Gaeman notice metids: Interface 'Man4' has link conceptiming in Mag 18 00:00:20 2022 deeman notice metids: Interface 'Wan4' is setting up now
10	Intering	÷	Hen Avg 18 00 81 26 2022 deamon state metals ward (2004) satapet fracted, 42.00.0 Hen Avg 28 00.8126 2022 deamon satable matific ward (2007); singer fracted, 42.00.0 Hen Avg 28 00.8126 2022 deamon colors matific ward (20078); solders fracted, 42.00.0
1	-	8	Hen Aug 18 00/00/06 2022 daemon monice metids werd (20082): unitary an Faind Hen Aug 18 00/00/06 2022 daemon monice metids werd (20082): unit Entry an Faind Hen Aug 18 00/00/06 2022 daemon monice metids werd (20082): unit Entry and Found
	hysness	~	Hon Avg 18 00.95.26 2022 Geamon moning menids: Mane (20068): uni: Long not frund Hon Avg 18 00.95.26 2022 Geamon moning menids: Ward (20088): uni: Entry not Frund Hon Avg 18 00.00.26 2022 Geamon moning matific ward (20088): uni: Entry not frund
	WIP .		Hun Aug 16 00 00 16 2022 Basener notice metific went (20071): out. Entry not froms Hen Aug 16 00:51:24 2022 Basener notice metific want (20071): out. Entry not from Hon Aug 18 00:51:24 2022 Basener notice metific want (20071): out. Entry not from
	4101007		Hav Avg 18 53/81126 2022 deamont.notice hetids/ web3 10078// udhups/ eerding diamoner Han Avg 18 00/85126 2022 deamont.notice hetids/ web3 102711/ udhups/ eerding diamoner Han Avg 18 00/85126 2022 deamont.notice hetids/ web4 (20048// udhups/ eerding diamoner
	General Dec		Hen Avg 18 00/80/24 2022 deaman.optics helids weed 200021: adhesi: sending discover Hen Avg 18 00/80/24 2022 new horize shell 1980 1272 is not in consection. Hen Avg 18 00/80/27 2022 deaman.infb 20/2021 fe80 :4867/9475/662/4020 appeared on 4054
	TTP LATE Specific	2	Ham Aug 15 00-50:27 2022 daemon.err dramarg114071; roy intreasing /pon//sys/max/mone/pine. Non Aug 15 00:50:27 2022 daemon.err dramasg114071; interface ette 1124 failet na join INUP Hon Aug 15 00:50:17 2022 daemon.err dramasg114071; try interface (join/sys/mar/mone/pine)
	10.000		Hot Ray 18 00.00117 2012 deeman art stategiild07): interface eth4.1121 failes to juit DMCB Hot Ray 15 00:01.27 2022 deeman ert deemangiild07): interface eth4.1121 failes to juit DMCB Hot Ray 16 00:00:07 2022 deeman ert deemangiild07): interface eth4.1121 failed to tot TMCD
	1000		Han Kay 18 00.00127 2022 deemon eva dhamaaq(22407) tiy Lorskasing /pool/sys/mat/dode-uptom Han Kay 18 00.0127 2022 daemon eva dhamaaq(22407) tiyahandase ette 1122 failed to yukn 2007 Han Kay 18 00.0127 2022 daemon eva dhamaaq(22407)
	freitrie (peter		Man Aug 18 00:80:27 2022 deamon motion weithouspa:5211: Terminating on signal Non Aug 18 00:85:27 2022 deamon units : 36/2012, fe00: 4607.7427.7427.7427.7428.000 Non Aug 10 00:00:27 2022 deamon units : 36/2022, fe00: 4007.7427.7427.4417.7427.4417.7427.
	mag methods		Non Aug 18 00:00.27 2022 Resmon info 11(NUL) fail: 4abd 74d2 fail 4207 appeared in eth. 1 Non Aug 18 00:00:27 2022 Geamon notice netlds want (2072): othrps: lawse of 10.00.10.20 a Non Aug 18 00:00:27 2022 Geamon notice netlds want (2072): othrps: lawse of 10.00.10.20 a
	ALL DOUT ALL DA		Han Aug 18 00.00 27 2022 Basers morine metific ward (20071): uni Energy non Found Han Aug 18 00.00 27 2022 Gasers, notice metific ward (20071): uni: Energy non Found +
			*
	Depier		Daras Daras

2.6.13 Diagnosis

The System > Diagnosis menu provides 3 types of diagnostic tests that may be used for

troubleshooting connection issues: Ping and Traceroute (Figure 2-54).

Figure 2-54 Diagnosis

Aicelis			- Millane
10.0	E Greet Display		
Abbient Opramie OAB WER Anlang FTP Anto Upprote	E Method Haltot 210 egeneties • Peg © Transform © text	Ę	
78.00) 8007 8009-0122849	E Ping Tarpe P	metere Simur	 Parroge Stee
Fog Hannang En F Sn E Gerffftaller	Treasur 19 10 - Section (1955)	Corr (4 Without 10	- ALTER LITERAL
There generates	The local division of		
Courses in the local division of the local d			

2.6.13.1 Ping

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

Figure 2-55 Ping Diagnosis Settings

Method of Diagnostics			
Fing C TraceRoute C Ipe	rf .		
Ping			
Target IP	Interface		Package Size
	GETAULT	~	54
			 Bytest1+20001
Timeout	Count		
10.			
40 (ALLOWER) 1-120	• times:11-10:		

Table 2-12 Ping Diagnosis parameters

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

2.6.13.2 Trace Route

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



Figure 2-56 Trace Diagnosis Settings

Table 2-13 Trace Diagnosis parameters

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

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

2.6.13.3 Iperf

Iperf diagnostic debugging is used to test throughput.

Figure 2-57 Iperf Diagnosis Settings

O Ping O TraceRoute 🔹 (perf			
perf			
Scatomiza CMD			
	10010-0000-0000		
Veralan	Pintpoel		Targat IP
v 2 mg	240	~	192.198.21.198
Port	Time		Oeta length
8004	ADAID		Sam
	O time of seconds to traver	er Tertit	
Bandwidth	Command		
1000			
6 bandwittin to serve at in additional	0 eg. losif /s /c 182,148,13 5001 -1 10000udp -8 1000	(60 ⁻¹ -9) 9-1	

Table 2-14 Iperf Diagnosis parameters

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

2.6.14 Reboot

Use the Reboot menu to perform a reboot of the CPE, as shown in Figure 2-58. It can take several minutes for the reboot to complete. After it reboots, the CPE GUI will display the login screen.



Caution: The reboot action will disrupt service.

Figure 2-58 Reboot

Bricells	
545 Certificates	E Specie Palant
Kyslam Hennagen	- Reboot
Diagnosis	and a second sec
(Balance)	

2.7 Logout

When you click on the Logout menu, you are automatically logged out of the CPE and returned to the login screen (Figure 2-59).

Figure 2-59 Logout

Bricells	1	
🗄 Status	-	Bacollo
G Natwork	. 1 .	DAICEIIS
🖞 Cellular	÷	Diar Logis
Security		Usenane
E VPN	~	Patient
© System	×	
G Logout)—	

Appendix: Regulatory Compliance

FCC Compliance

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Warning:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 30cm between the radiator & your body.

- FCC regulations restrict the operation of this device to indoor use only.
- The operation of this device is prohibited on oil platforms, cars, trains,

boats, and aircraft, except that operation of this device is permitted in large aircraft while flying above 10,000 feet in the 5.925-6.425 GHz band.

• Operation of transmitters in the 5.925-7.125 GHz band is prohibited for control of or communications with unmanned aircraft systems.