GLOBAL TELECOM

WE ENGINEER CONNECTIVITY

TITAN 4000

4G LTE-A CAT12 Outdoor CPE
Admin User Manual
V1.0

PLEASE READ THESE SAFETY PRECAUTIONS!

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

FCC Warning

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.

NOTE 1: 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.

NOTE 2: Any changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Contents

1. Overview

The TITAN4000 is highly innovative and patented LTE outdoor CPE product designed to enable quick and easy LTE fixed data service deployment for residential and SOHO customers. It provides high speed LAN services to end users who need both bandwidth and multi-media data service in enterprise or home. It can also be used to support wireless fall back service.

1.1. User Interface Specification

Model	Description & User Interface
TITAN4000	- 1 RJ45 10/100/1000M LAN port - SYS, MOD, SIM, ETH, Wi-Fi, RF (5 Signal intensity LEDs) - PoE DC 48V, Power < 18 Watts (Average) - Dimensions: 300 mm (L) × 290 mm (W) × 97 mm (D) - Weight: <5Kg - Operating Temperature: -40℃ to 65℃ - Storage Temperature: -40℃ to 85℃

2. Getting Started

2.1. Packing list and CPE Unit

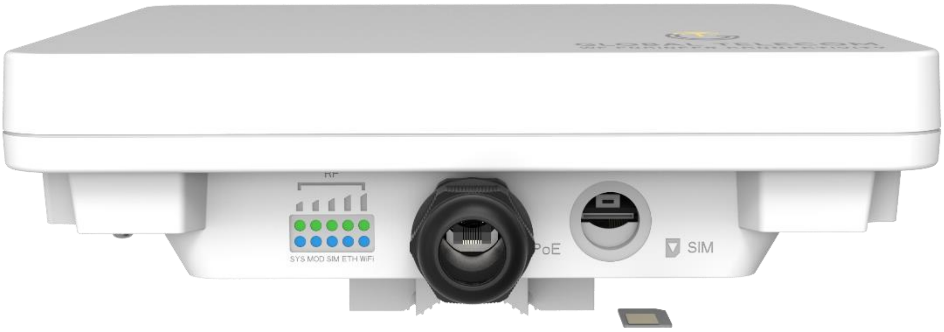
Upon receiving the product, please unpack the product package carefully. Each product is shipped with the following items:

Table 2-1 Packing List

Products	Quantity
CPE Unit	1
Clamp	2
Mounting Brackets	1
ETH Cable 2.0M	1
PoE Adapter	1
Power Cord 1.5M	1
Quick User Guide	1

If you find any of the items missed, please contact your local distributor immediately.

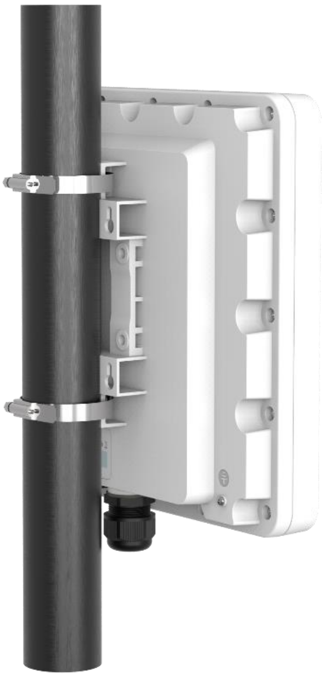
2.2. Installing the Equipment



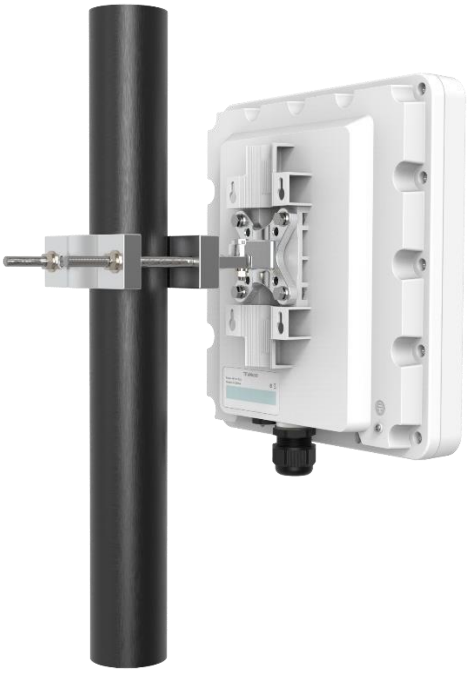
Open the SIM card cover, insert the SIM card and connected the ETH cable.

The user should use SFTP CAT5E Ethernet cable and connect to the appropriate LAN port

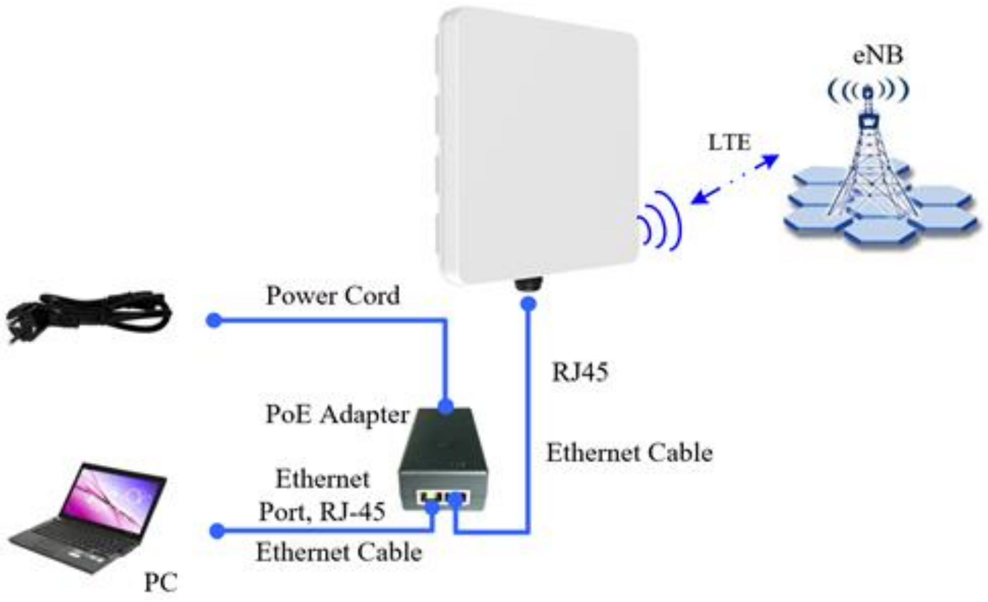
- **Clamp Mounting Option (Preferred Method)**



- **Bracket Mounting Option**



Connecting the Device



LED Display

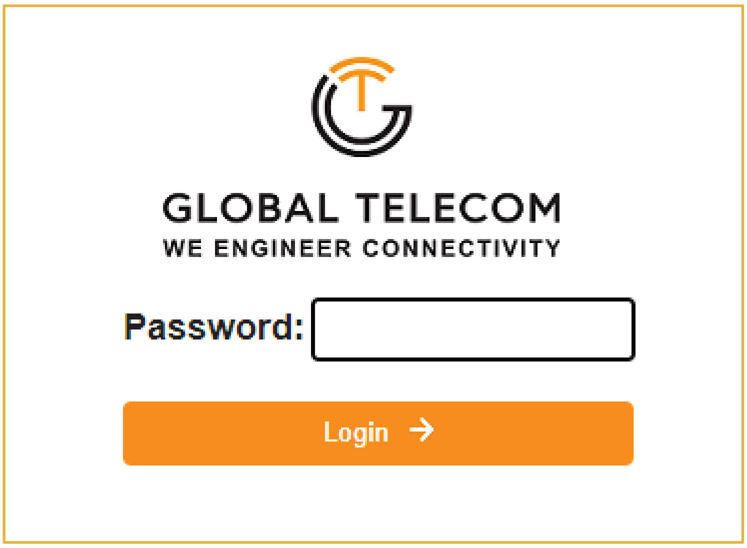
LED	Function	Description
SYS	System run indicator	Solid green – Device is in normal operation.
MOD	WAN port status	OFF – NO wireless network access. Solid Green – WAN data transmission in progress
SIM	SIM card indicator	Light is on – SIM card state is ready, Blinking Green – SIM card is error.
ETH	LAN port status	Solid Green – LAN port is up. Blinking Green –LAN port in working.
Wi-Fi	Wi-Fi indicator	Light is on –Wi-Fi is on.
RF (5LEDs)	RF Signal Strength	5 level signal strengths indication by 5 green LEDs. 1st Green LED: -115dBm < RSRP 2nd Green LED: -115dBm <= RSRP < -105dBm 3rd Green LED: -105dBm <= RSRP < -95dBm 4th Green LED: -95dBm <= RSRP < -85dBm 5th Green LED: -85 <= RSRP

3. Managing the CPE Device

3.1. WEB Login

It is recommended that you log in to the device by using a web browser from a PC that's connected to the device's LAN port. To log in, open a web browser and type http://192.168.0.1 in the address bar. A window will pop up requesting a password. Input the user login password and then click the "Login" button. After successfully logging in, the default home page will appear.

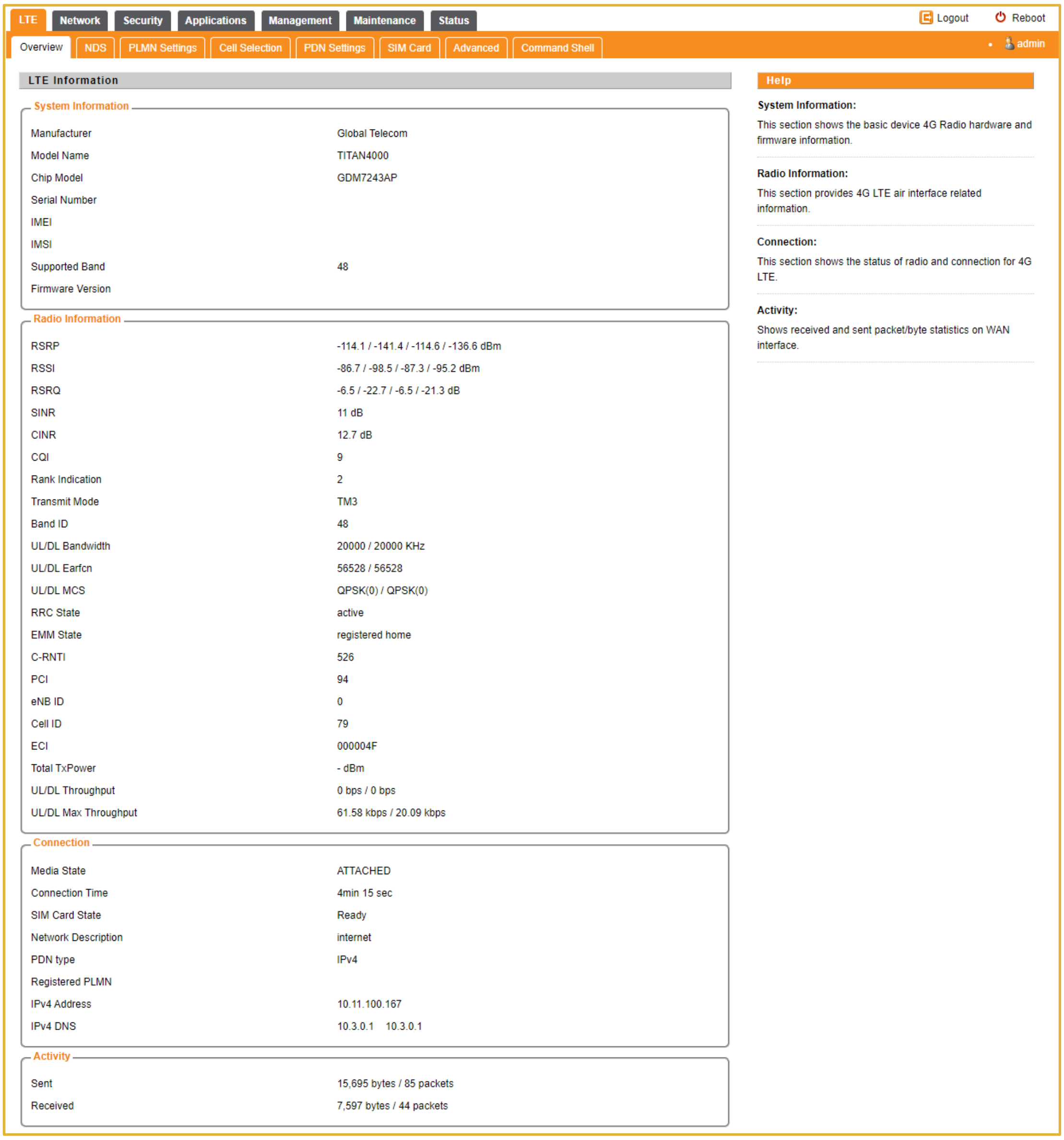
The default administrator password is "**Global + last 6 digits of MAC**".



4. LTE Configuration

4.1. Overview

Once the user is logged in, the following window device status window will be prompted for viewing. It contains both the system information, networking and device information configured for the device.



LTE Information

System Information

Manufacturer	Global Telecom
Model Name	TITAN4000
Chip Model	GDM7243AP
Serial Number	
IMEI	
IMSI	
Supported Band	48
Firmware Version	

Radio Information

RSRP	-114.1 / -141.4 / -114.6 / -136.6 dBm
RSSI	-86.7 / -98.5 / -87.3 / -95.2 dBm
RSRQ	-6.5 / -22.7 / -6.5 / -21.3 dB
SINR	11 dB
CINR	12.7 dB
CQI	9
Rank Indication	2
Transmit Mode	TM3
Band ID	48
UL/DL Bandwidth	20000 / 20000 KHz
UL/DL Earfcn	56528 / 56528
UL/DL MCS	QPSK(0) / QPSK(0)
RRC State	active
EMM State	registered home
C-RNTI	526
PCI	94
eNB ID	0
Cell ID	79
ECI	000004F
Total TxPower	- dBm
UL/DL Throughput	0 bps / 0 bps
UL/DL Max Throughput	61.58 kbps / 20.09 kbps

Connection

Media State	ATTACHED
Connection Time	4min 15 sec
SIM Card State	Ready
Network Description	internet
PDN type	IPv4
Registered PLMN	
IPv4 Address	10.11.100.167
IPv4 DNS	10.3.0.1 10.3.0.1

Activity

Sent	15,695 bytes / 85 packets
Received	7,597 bytes / 44 packets

Help

System Information:

This section shows the basic device 4G Radio hardware and firmware information.

Radio Information:

This section provides 4G LTE air interface related information.

Connection:

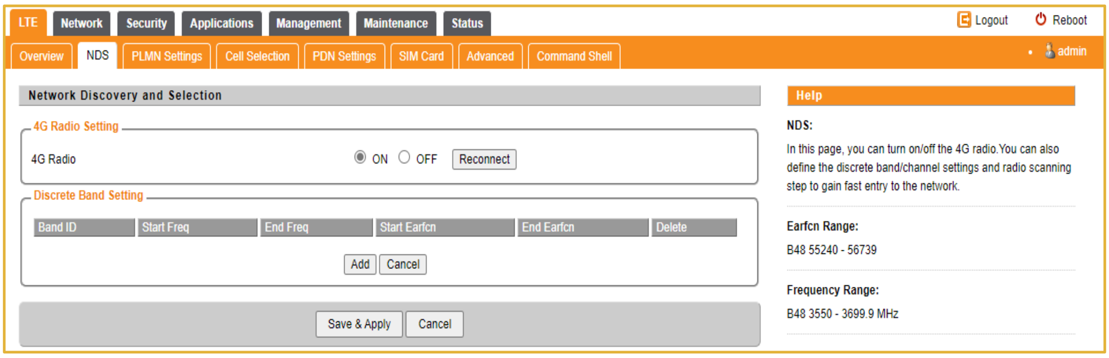
This section shows the status of radio and connection for 4G LTE.

Activity:

Shows received and sent packet/byte statistics on WAN interface.

4.2. ND&S Configuration

The LTE radio can be enabled or disabled via 4G Radio setting. The radio can also be reset via Reconnect.



Network Discovery and Selection

4G Radio Setting

4G Radio ● ON ○ OFF

Discrete Band Setting

Band ID	Start Freq	End Freq	Start Earfcn	End Earfcn	Delete

Help

NDS:

In this page, you can turn on/off the 4G radio.You can also define the discrete band/channel settings and radio scanning step to gain fast entry to the network.

Earfcn Range:

B48 55240 - 56739

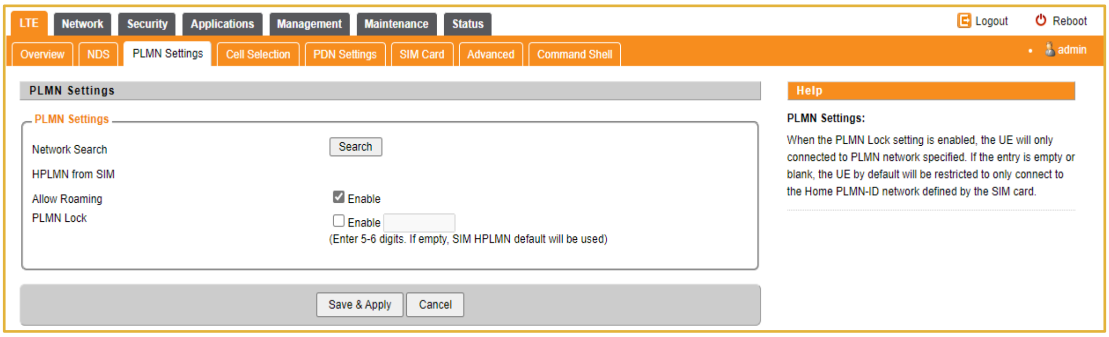
Frequency Range:

B48 3550 - 3699.9 MHz

Note: After configure any parameters of the device, you must click the “Save & Apply” button to save the configuration. Otherwise the configuration will not take effect.

4.3. PLMN Selection

The user can add and configure the PLMN list to restrict the CPE to attach. The CPE will attach to network according to the PLMN priority assigned.



PLMN Settings

PLMN Settings

Network Search

HPLMN from SIM

Allow Roaming ☑ Enable

PLMN Lock ☐ Enable

(Enter 5-6 digits. If empty, SIM HPLMN default will be used)

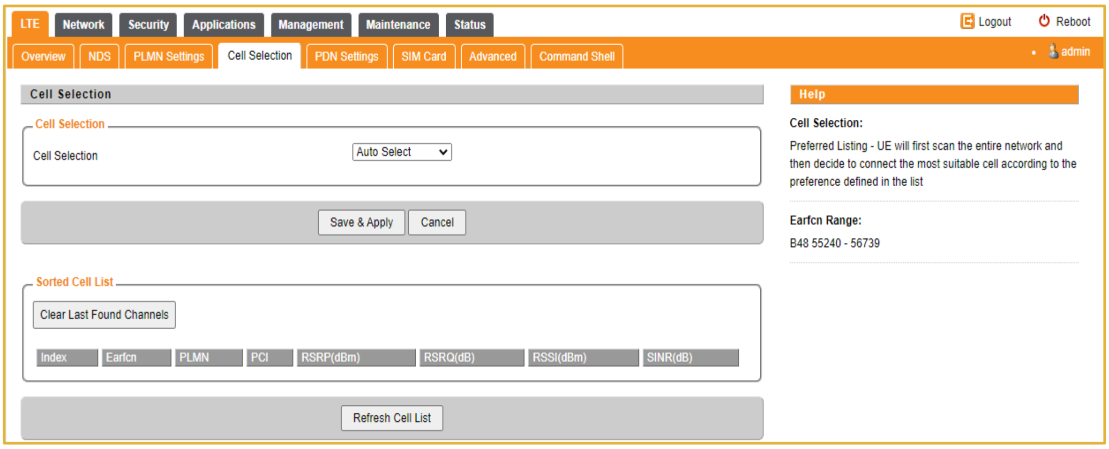
Help

PLMN Settings:

When the PLMN Lock setting is enabled, the UE will only connected to PLMN network specified. If the entry is empty or blank, the UE by default will be restricted to only connect to the Home PLMN-ID network defined by the SIM card.

4.4. Cell Selection

The cell selection menu is used to configure how CPE will select the best cell. User can configure the “Auto Select” mode to select cell based 3GPP standard. When configured with “preferred Listing”, user add the desired cell ID to the list and the CPE will attach to the appropriate cell after a full scan.



Cell Selection

Cell Selection

Cell Selection Auto Select

Sorted Cell List

Index	Earfcn	PLMN	PCI	RSRP(dBm)	RSRQ(dB)	RSSI(dBm)	SINR(dB)

Help

Cell Selection:

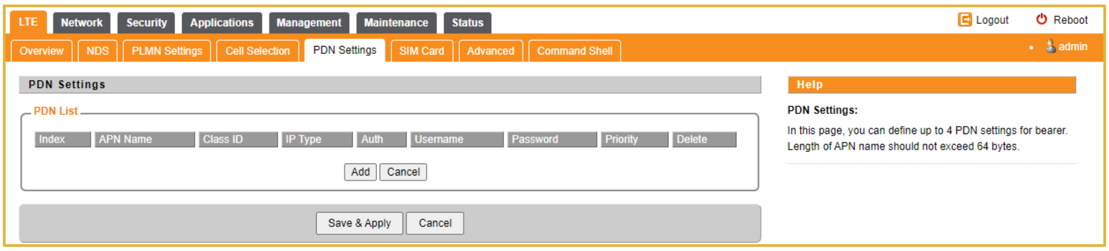
Preferred Listing - UE will first scan the entire network and then decide to connect the most suitable cell according to the preference defined in the list

Earfcn Range:

B48 55240 - 56739

4.5. PDN Setting

This menu is used to configure the operator APN profile. You can configure single or multiple APNs for the operator network.   The below shows an example of two APN configuration.



PDN Settings

PDN List

Index	APN Name	Class ID	IP Type	Auth	Username	Password	Priority	Delete

Help

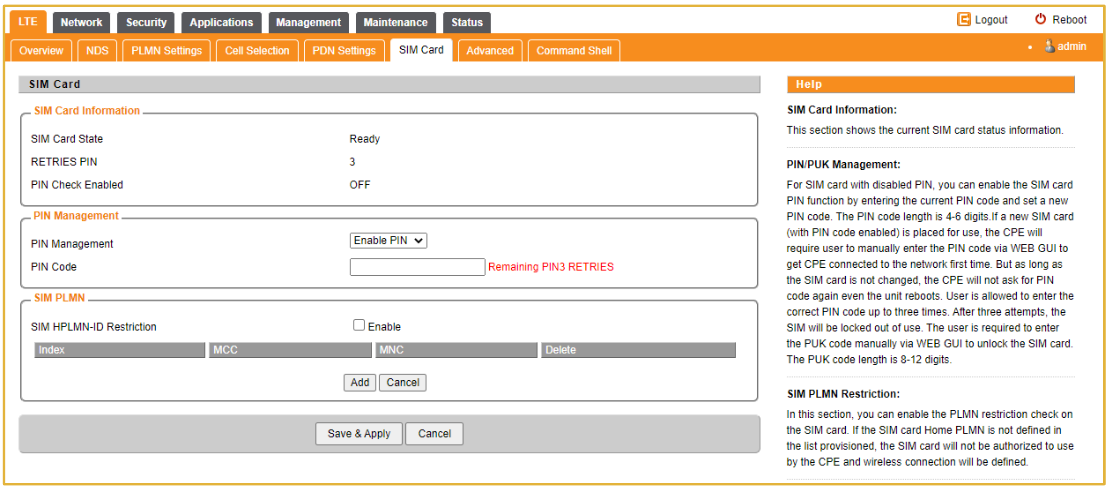
PDN Settings:

In this page, you can define up to 4 PDN settings for bearer. Length of APN name should not exceed 64 bytes.

You can view the APN status info in the Status menu.

4.6. SIM Card

The SIM card menu is used to view the SIM card status and perform PIN code management for SIM card. You disable or enable the SIM card PIN check on the CPE to bind the SIM card inserted.



SIM Card

SIM Card Information

SIM Card State	Ready
RETRIES PIN	3
PIN Check Enabled	OFF

PIN Management

PIN Management	Enable PIN
PIN Code	Remaining PIN3 RETRIES

SIM PLMN

SIM HPLMN-ID Restriction ☐ Enable

Index	MCC	MNC	Delete

Help

SIM Card Information:

This section shows the current SIM card status information.

PIN/PUK Management:

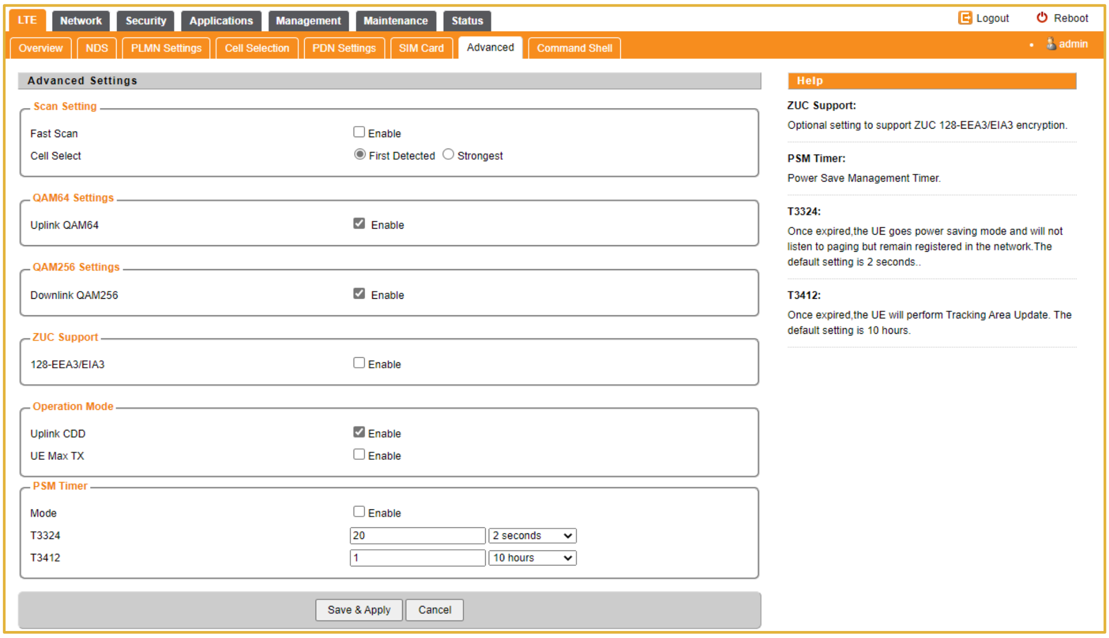
For SIM card with disabled PIN, you can enable the SIM card PIN function by entering the current PIN code and set a new PIN code. The PIN code length is 4-6 digits.If a new SIM card (with PIN code enabled) is placed for use, the CPE will require user to manually enter the PIN code via WEB GUI to get CPE connected to the network first time. But as long as the SIM card is not changed, the CPE will not ask for PIN code again even the unit reboots. User is allowed to enter the correct PIN code up to three times. After three attempts, the SIM will be locked out of use. The user is required to enter the PUK code manually via WEB GUI to unlock the SIM card. The PUK code length is 8-12 digits.

SIM PLMN Restriction:

In this section, you can enable the PLMN restriction check on the SIM card. If the SIM card Home PLMN is not defined in the list provisioned, the SIM card will not be authorized to use by the CPE and wireless connection will be defined.

4.7. Advanced

In this menu, you can configure advanced options for the CPE operation.



Advanced Settings

Scan Setting

Fast Scan □ Enable

Cell Select ● First Detected ○ Strongest

QAM64 Settings

Uplink QAM64 ☑ Enable

QAM256 Settings

Downlink QAM256 ☑ Enable

ZUC Support

128-EEA3/EIA3 □ Enable

Operation Mode

Uplink CDD ☑ Enable

UE Max TX □ Enable

PSM Timer

Mode □ Enable

T3324 20 2 seconds

T3412 1 10 hours

Help

ZUC Support:

Optional setting to support ZUC 128-EEA3/EIA3 encryption.

PSM Timer:

Power Save Management Timer.

T3324:

Once expired,the UE goes power saving mode and will not listen to paging but remain registered in the network.The default setting is 2 seconds..

T3412:

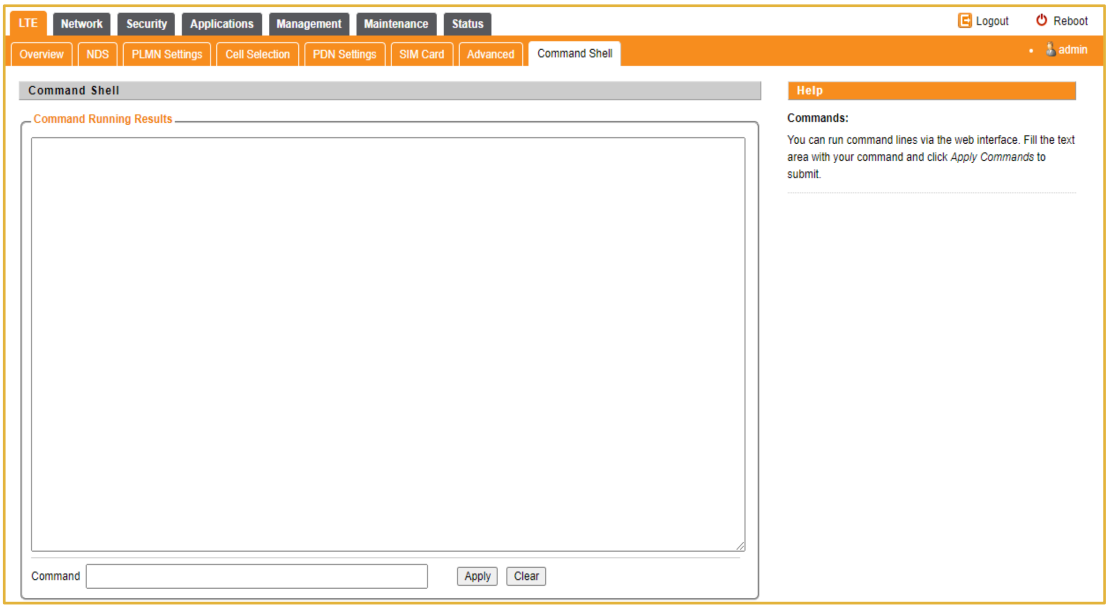
Once expired,the UE will perform Tracking Area Update. The default setting is 10 hours.

Fast scan will allow you to quickly connect to good cell when they are first found instead of search the best cell. The ZUC encryption support is only required when your core network (EPC) force to use the ZUC encryption for access authentication. The operation mode allows you to select the UE capability for receiving and transmitting.

In addition, the PSM timer and location service UE settings can also be configured for advanced users. Default settings should be used for normal operation.

4.8. Command Shell

The Command Shell is used to run LTE command via the WEB GUI interface. You can type the command and click the APPLY button to execute.



Command Shell

Command Running Results

Help

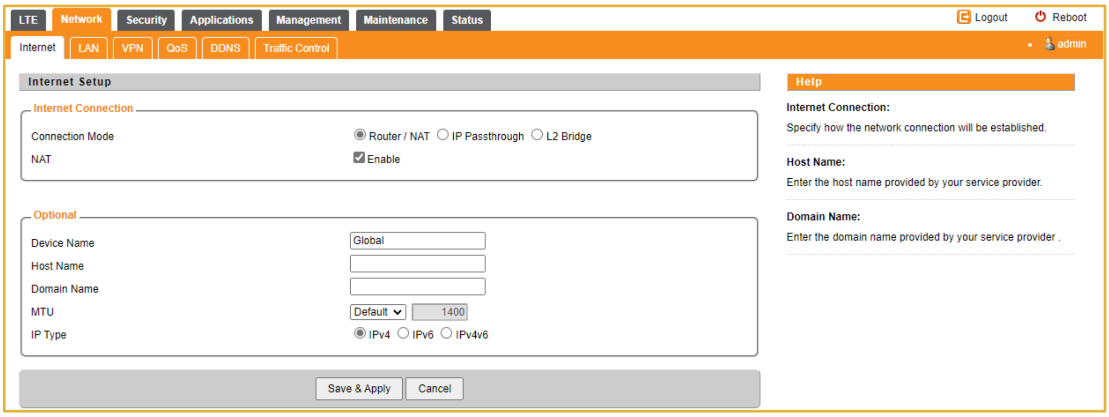
Commands:

You can run command lines via the web interface. Fill the text area with your command and click *Apply Commands* to submit.

5. Network Configuration

5.1. Internet

This section allows user to configure the CPE operation mode, device name, MTU and etc. The CPE default Operation Mode is Router, and the LAN PC connected to device LAN port will obtain IP address via DHCP server of the device. The default MTU Size is 1500, user can modify the MTU Size if necessary.



Internet Setup

Internet Connection

Connection Mode ● Router / NAT ○ IP Passthrough ○ L2 Bridge

NAT ☑ Enable

Optional

Device Name: Global

Host Name:

Domain Name:

MTU: Default 1400

IP Type: ● IPv4 ○ IPv6 ○ IPv4v6

Help

Internet Connection:
Specify how the network connection will be established.

Host Name:
Enter the host name provided by your service provider.

Domain Name:
Enter the domain name provided by your service provider .

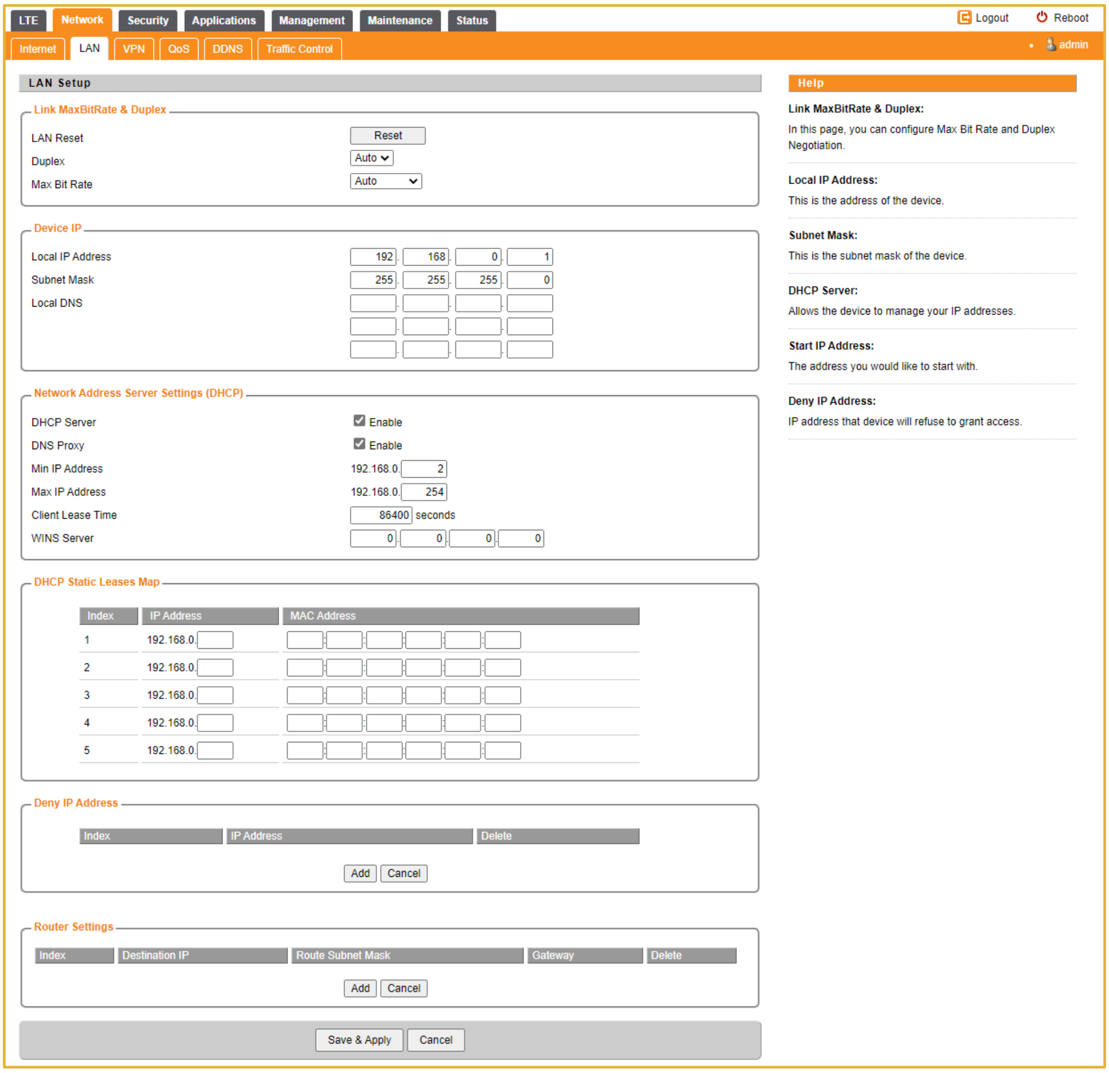
Note when setting the connection mode as L2 Bridge or L3 Bridge, there will be a warning window pops up. Remember the management IP address 192.168.0.1 and click the “ok” button.

When the user wants to manage the home page again, the PC should be configured a static IP address as 10.1.1.X manual in order to visit the CPE managing page http://10.1.1.1.

5.2. LAN Setting

The LAN setting allows user to specify the device LAN IP, DHCP server setting, Local DNS and etc. When Router mode is selected, the DHCP server should be enabled by default.

User is advised to leave the default setting unchanged for quick configuration and smooth device operation.



LAN Setup

Link MaxBitRate & Duplex

LAN Reset	Reset
Duplex	Auto
Max Bit Rate	Auto

Device IP

Local IP Address	192 . 168 . 0 . 1
Subnet Mask	255 . 255 . 255 . 0
Local DNS	

Network Address Server Settings (DHCP)

DHCP Server	☑ Enable
DNS Proxy	☑ Enable
Min IP Address	192.168.0. 2
Max IP Address	192.168.0. 254
Client Lease Time	86400 seconds
WINS Server	0 . 0 . 0 . 0

DHCP Static Leases Map

Index	IP Address	MAC Address
1	192.168.0.	
2	192.168.0.	
3	192.168.0.	
4	192.168.0.	
5	192.168.0.	

Deny IP Address

Index	IP Address	Delete

Add Cancel

Router Settings

Index	Destination IP	Route Subnet Mask	Gateway	Delete

Add Cancel

Save & Apply Cancel

Help

Link MaxBitRate & Duplex:
In this page, you can configure Max Bit Rate and Duplex Negotiation.

Local IP Address:
This is the address of the device.

Subnet Mask:
This is the subnet mask of the device.

DHCP Server:
Allows the device to manage your IP addresses.

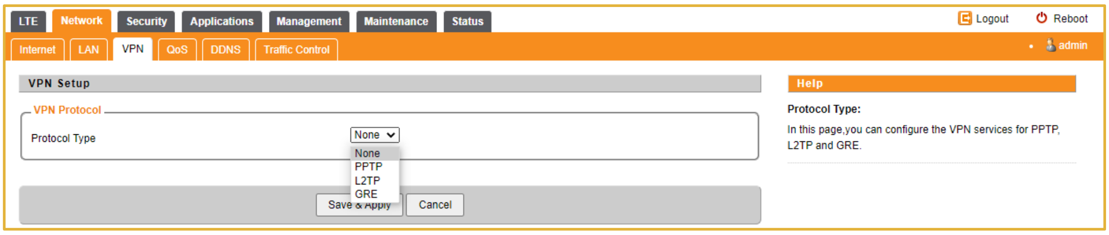
Start IP Address:
The address you would like to start with.

Deny IP Address:
IP address that device will refuse to grant access.

5.3. VPN Setting For Router Mode

This section allows user to configure VPN service for selected connection mode. In router mode, PPTP, L2TP and GRE can be selected. In L2 Bridge mode, only L2 GRE can be configured.

The router mode VPN configuration is shown below.



VPN Setup

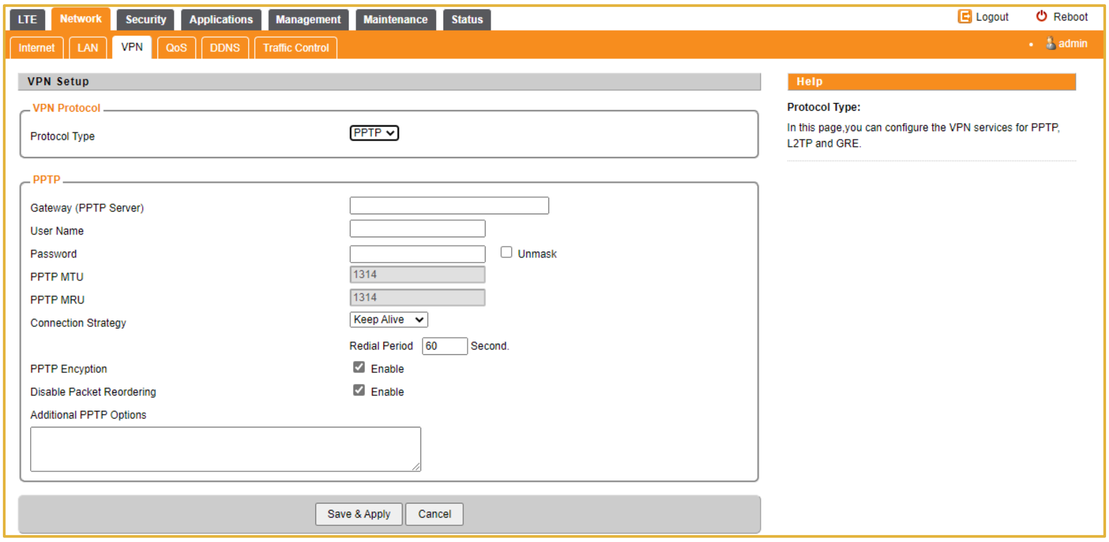
VPN Protocol

Protocol Type	None

Help

Protocol Type:
In this page,you can configure the VPN services for PPTP, L2TP and GRE.

The PPTP configuration under router mode is shown below.



VPN Setup

VPN Protocol

Protocol Type	PPTP

PPTP

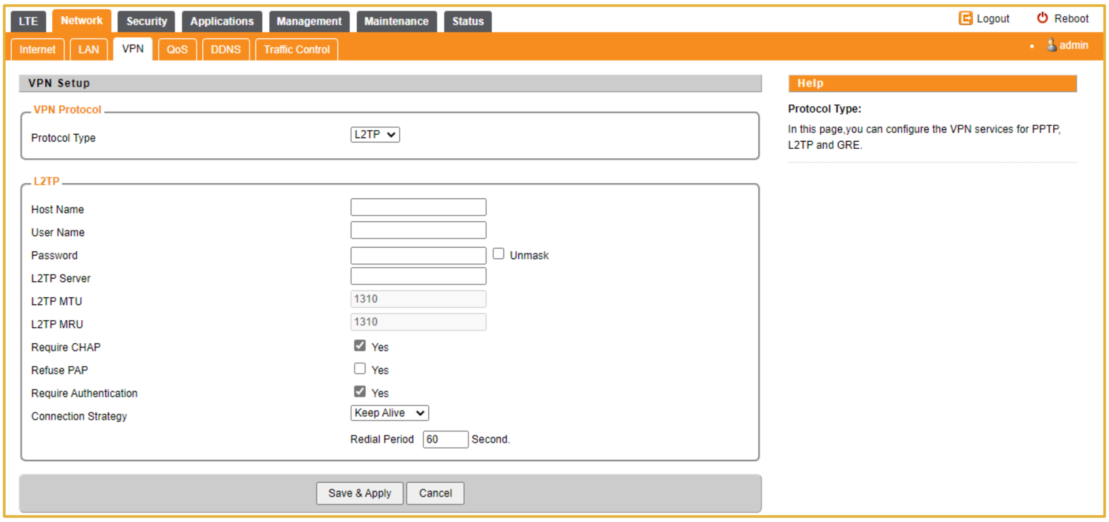
Gateway (PPTP Server)	
User Name	
Password	□ Unmask
PPTP MTU	1314
PPTP MRU	1314
Connection Strategy	Keep Alive
	Redial Period 60 Second.
PPTP Encyption	☑ Enable
Disable Packet Reordering	☑ Enable
Additional PPTP Options	

Help

Protocol Type:

In this page,you can configure the VPN services for PPTP, L2TP and GRE.

The L2TP configuration under router mode is shown as follows.



VPN Setup

VPN Protocol

Protocol Type	L2TP

L2TP

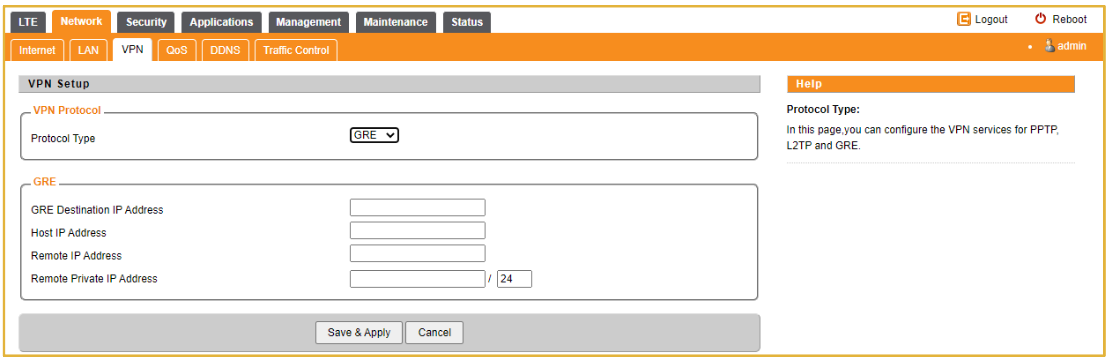
Host Name	
User Name	
Password	□ Unmask
L2TP Server	
L2TP MTU	1310
L2TP MRU	1310
Require CHAP	☑ Yes
Refuse PAP	□ Yes
Require Authentication	☑ Yes
Connection Strategy	Keep Alive
	Redial Period 60 Second.

Help

Protocol Type:

In this page,you can configure the VPN services for PPTP, L2TP and GRE.

The L2 GRE configuration under router mode is shown below.



VPN Setup

VPN Protocol

Protocol Type	GRE

GRE

GRE Destination IP Address	
Host IP Address	
Remote IP Address	
Remote Private IP Address	/ 24

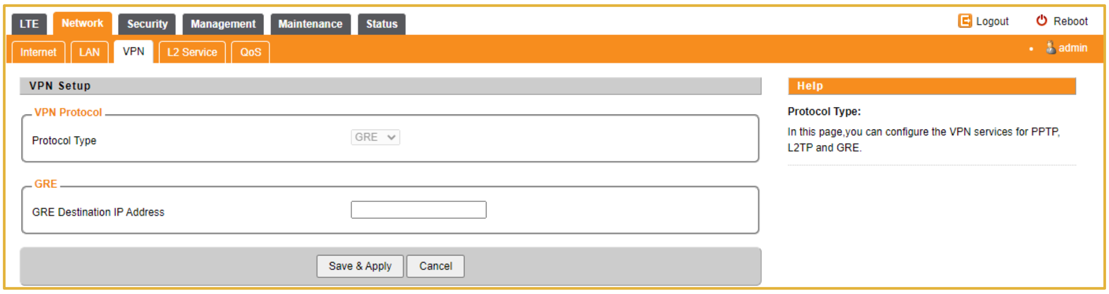
Help

Protocol Type:

In this page,you can configure the VPN services for PPTP, L2TP and GRE.

5.4. VPN Setting For L2 Bridge Mode

Under the L2 Bridge connection mode, only L2 GRE can be configured as follows.



VPN Setup

VPN Protocol

Protocol Type: GRE

GRE

GRE Destination IP Address:

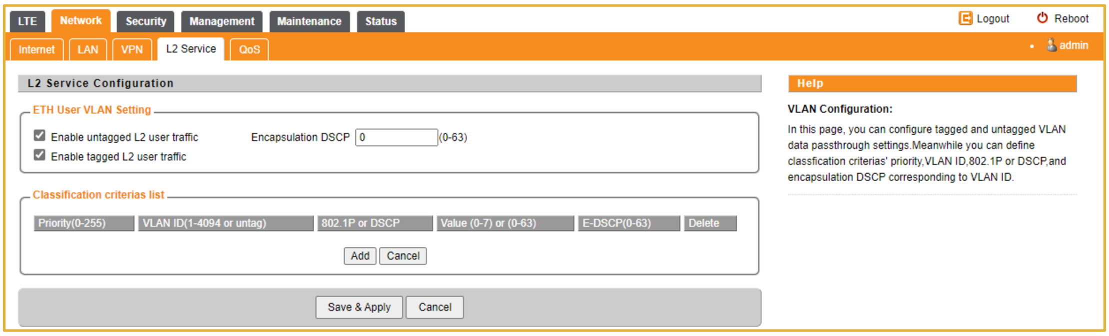
Help

Protocol Type:

In this page,you can configure the VPN services for PPTP, L2TP and GRE.

5.5. L2 Service For L2 Bridge Mode

Under the L2 Bridge connection mode, the user can use L2 Service configuration to manage and tag 802.1p or DSCP for different VLAN packets.



L2 Service Configuration

ETH User VLAN Setting

☑ Enable untagged L2 user traffic Encapsulation DSCP 0 (0-63)

☑ Enable tagged L2 user traffic

Classification criterias list

Priority(0-255)	VLAN ID(1-4094 or untag)	802.1P or DSCP	Value (0-7) or (0-63)	E-DSCP(0-63)	Delete

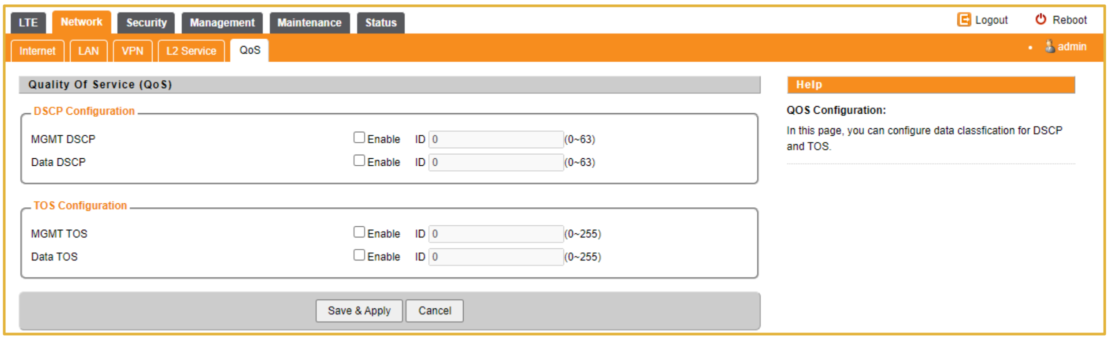
Help

VLAN Configuration:

In this page, you can configure tagged and untagged VLAN data passthrough settings.Meanwhile you can define classfication criterias' priority,VLAN ID,802.1P or DSCP,and encapsulation DSCP corresponding to VLAN ID.

5.6. QoS Setting

This configuration menu allows user to tag DSCP or TOS value for CPE local data (Management) and LAN port data (Data).



Quality Of Service (QoS)

DSCP Configuration

MGMT DSCP □Enable ID 0 (0~63)

Data DSCP □Enable ID 0 (0~63)

TOS Configuration

MGMT TOS □Enable ID 0 (0~255)

Data TOS □Enable ID 0 (0~255)

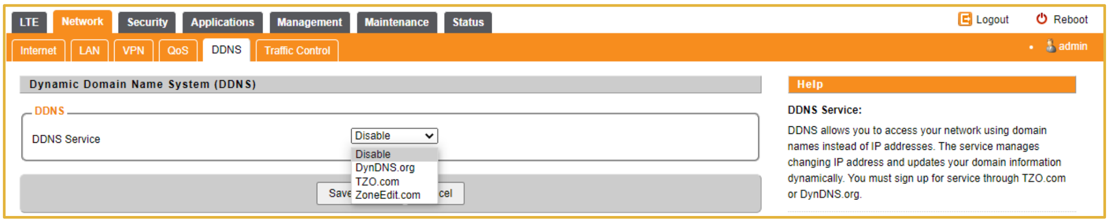
Help

QOS Configuration:

In this page, you can configure data classfication for DSCP and TOS.

5.7. DDNS Setting For Router Mode

This configuration menu allows user to configure use of different DDNS service for router mode operation.



Dynamic Domain Name System (DDNS)

DDNS

DDNS Service: Disable

Disable
DynDNS.org
TZO.com
ZoneEdit.com

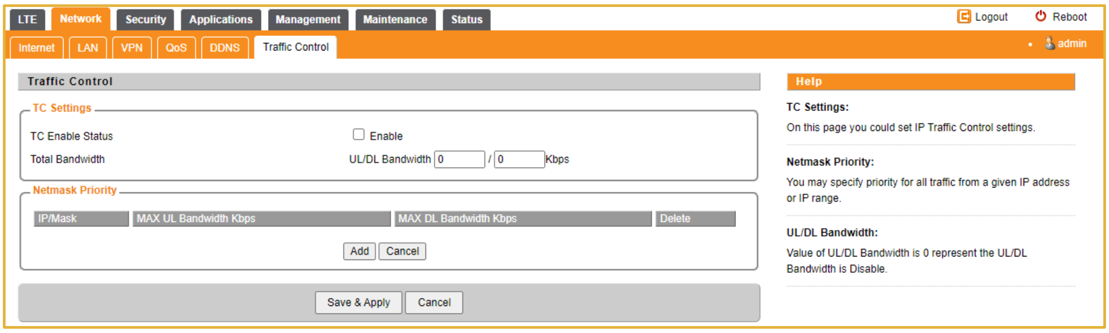
Help

DDNS Service:

DDNS allows you to access your network using domain names instead of IP addresses. The service manages changing IP address and updates your domain information dynamically. You must sign up for service through TZO.com or DynDNS.org.

5.8. Traffic Control Setting For Router Mode

This configuration menu allows user to configure the data priority and allowed bandwidth for LAN data traffic.



Traffic Control

TC Settings

TC Enable Status: □ Enable

Total Bandwidth: UL/DL Bandwidth 0 / 0 Kbps

Netmask Priority

IP/Mask	MAX UL Bandwidth Kbps	MAX DL Bandwidth Kbps	Delete

Help

TC Settings:

On this page you could set IP Traffic Control settings.

Netmask Priority:

You may specify priority for all traffic from a given IP address or IP range.

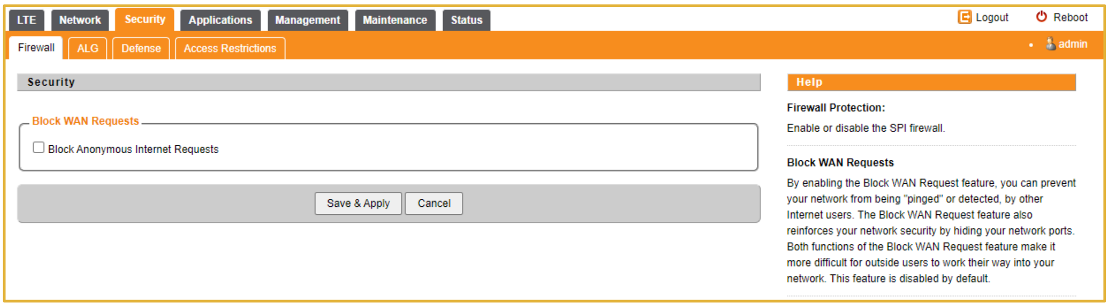
UL/DL Bandwidth:

Value of UL/DL Bandwidth is 0 represent the UL/DL Bandwidth is Disable.

6. Security Configuration

6.1. Firewall

This allows user to configure CPE firewall.



Security

Block WAN Requests

□ Block Anonymous Internet Requests

Help

Firewall Protection:

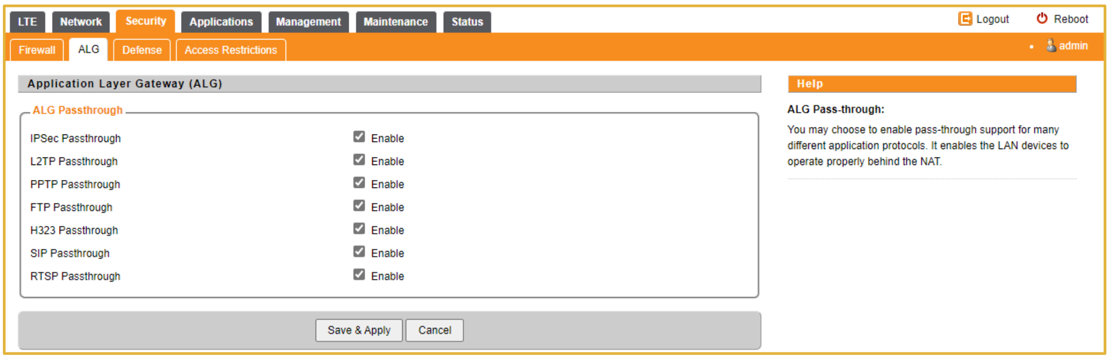
Enable or disable the SPI firewall.

Block WAN Requests

By enabling the Block WAN Request feature, you can prevent your network from being "pinged" or detected, by other Internet users. The Block WAN Request feature also reinforces your network security by hiding your network ports. Both functions of the Block WAN Request feature make it more difficult for outside users to work their way into your network. This feature is disabled by default.

6.2. ALG

This allows user to configure the application level gateways for many common applications.



Application Layer Gateway (ALG)

ALG Passthrough

IPSec Passthrough	☑ Enable
L2TP Passthrough	☑ Enable
PPTP Passthrough	☑ Enable
FTP Passthrough	☑ Enable
H323 Passthrough	☑ Enable
SIP Passthrough	☑ Enable
RTSP Passthrough	☑ Enable

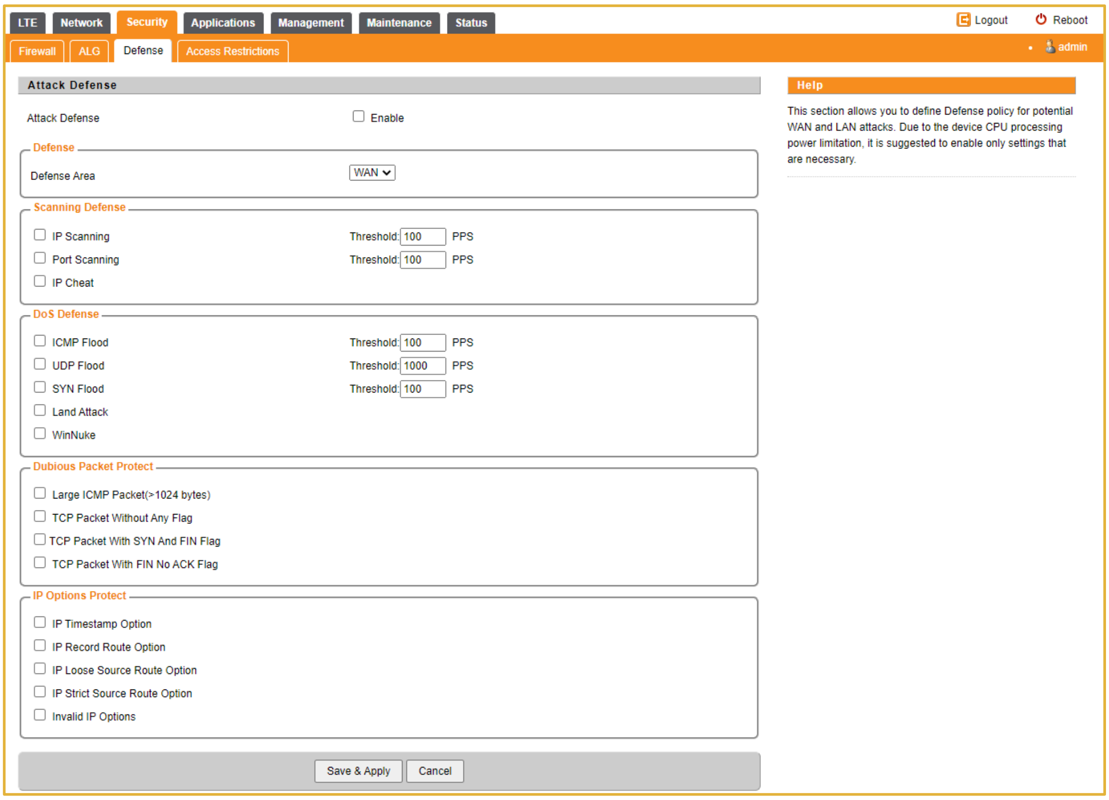
Help

ALG Pass-through:

You may choose to enable pass-through support for many different application protocols. It enables the LAN devices to operate properly behind the NAT.

6.3. Defense

This allows user to configure defense policy for the LTE and local LAN interface to prevent hostile attack.



Attack Defense

Attack Defense ☐ Enable

Defense

Defense Area: WAN

Scanning Defense

☐ IP Scanning	Threshold: 100 PPS
☐ Port Scanning	Threshold: 100 PPS
☐ IP Cheat	

DoS Defense

☐ ICMP Flood	Threshold: 100 PPS
☐ UDP Flood	Threshold: 1000 PPS
☐ SYN Flood	Threshold: 100 PPS
☐ Land Attack	
☐ WinNuke	

Dubious Packet Protect

- ☐ Large ICMP Packet(>1024 bytes)
- ☐ TCP Packet Without Any Flag
- ☐ TCP Packet With SYN And FIN Flag
- ☐ TCP Packet With FIN No ACK Flag

IP Options Protect

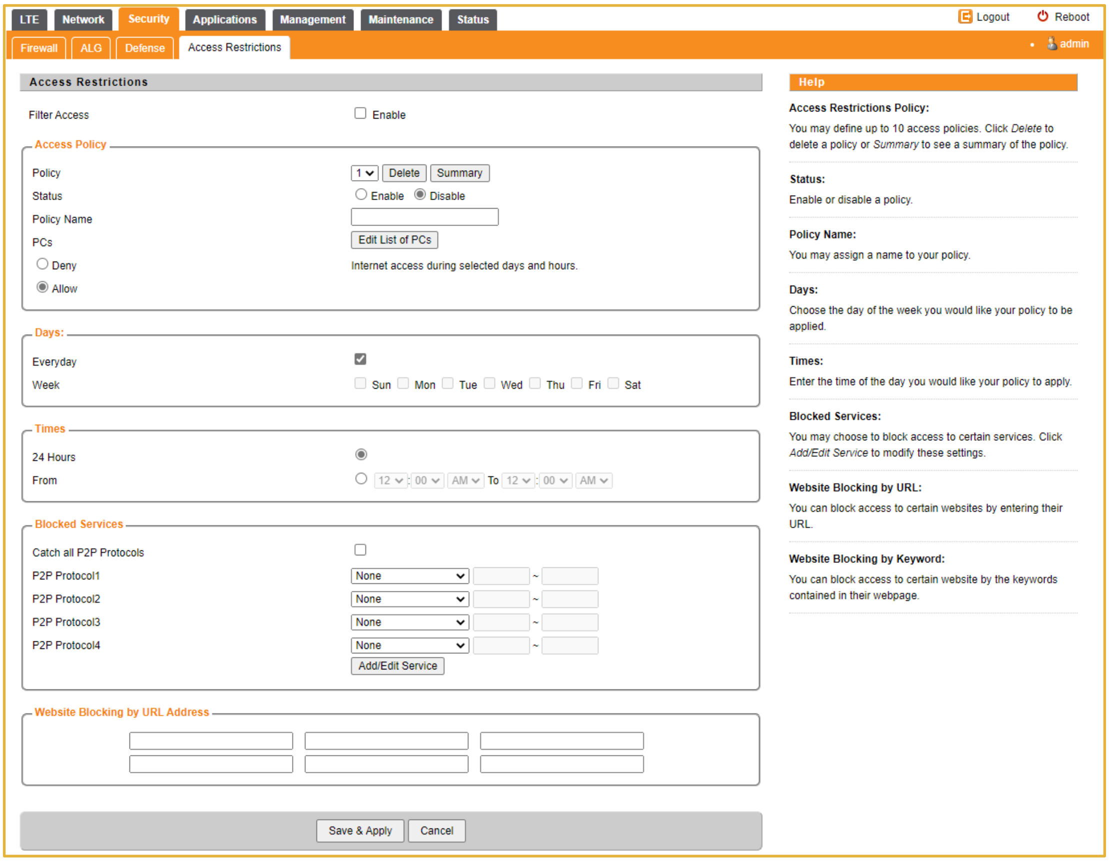
- ☐ IP Timestamp Option
- ☐ IP Record Route Option
- ☐ IP Loose Source Route Option
- ☐ IP Strict Source Route Option
- ☐ Invalid IP Options

Help

This section allows you to define Defense policy for potential WAN and LAN attacks. Due to the device CPU processing power limitation, it is suggested to enable only settings that are necessary.

6.4. Access Restrictions

This allows user to define access policy for LAN devices. It can support URL blocking as well.



Access Restrictions

Filter Access ☐ Enable

Access Policy

Policy 1 Delete Summary
Status ○ Enable ● Disable
Policy Name
PCs Edit List of PCs
○ Deny Internet access during selected days and hours.
● Allow

Days:

Everyday ☑
Week ☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

Times

24 Hours ●
From ○ 12 : 00 AM To 12 : 00 AM

Blocked Services

Catch all P2P Protocols ☐
P2P Protocol1 None ~
P2P Protocol2 None ~
P2P Protocol3 None ~
P2P Protocol4 None ~
Add/Edit Service

Website Blocking by URL Address

Save & Apply Cancel

Help

Access Restrictions Policy:
You may define up to 10 access policies. Click *Delete* to delete a policy or *Summary* to see a summary of the policy.

Status:
Enable or disable a policy.

Policy Name:
You may assign a name to your policy.

Days:
Choose the day of the week you would like your policy to be applied.

Times:
Enter the time of the day you would like your policy to apply.

Blocked Services:
You may choose to block access to certain services. Click *Add/Edit Service* to modify these settings.

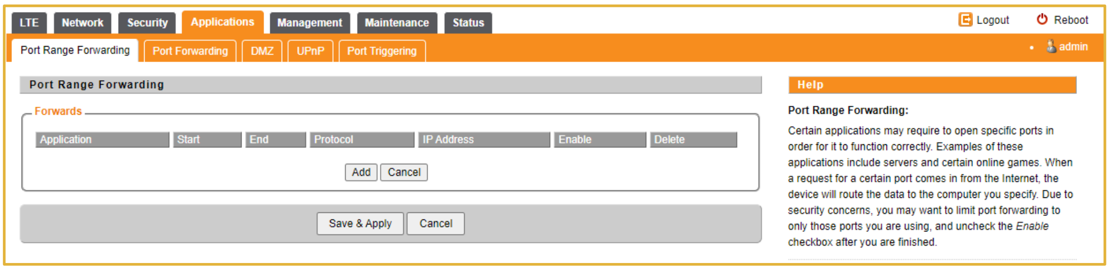
Website Blocking by URL:
You can block access to certain websites by entering their URL.

Website Blocking by Keyword:
You can block access to certain website by the keywords contained in their webpage.

7. Applications Configuration

7.1. Port Range Forwarding

This allows user to configure the port range forwarding rules for the CPE in router mode.



Port Range Forwarding

Forwards

Application	Start	End	Protocol	IP Address	Enable	Delete

Add Cancel

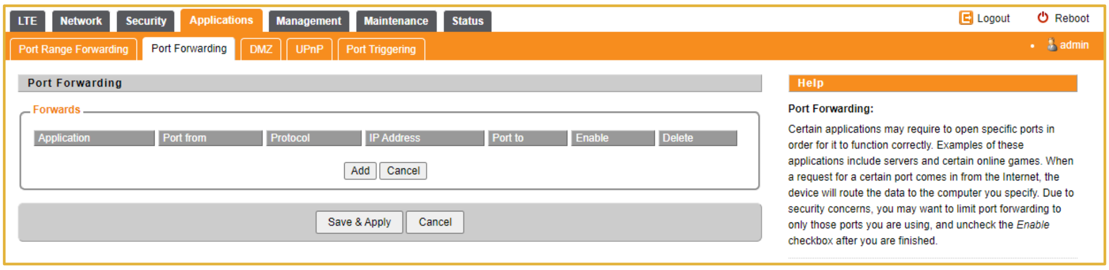
Save & Apply Cancel

Help

Port Range Forwarding:
Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the device will route the data to the computer you specify. Due to security concerns, you may want to limit port forwarding to only those ports you are using, and uncheck the *Enable* checkbox after you are finished.

7.2. Port Forwarding

This menu allows user to configure the port forwarding rules for the CPE in router mode.



Port Forwarding

Forwards

Application	Port from	Protocol	IP Address	Port to	Enable	Delete

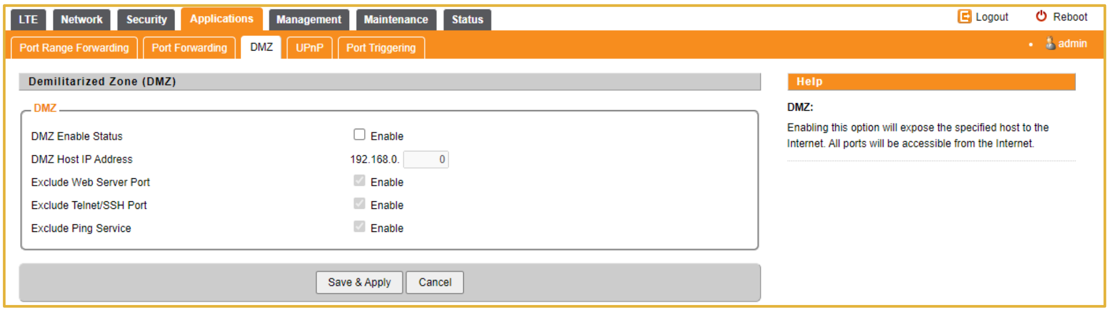
Help

Port Forwarding:

Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the device will route the data to the computer you specify. Due to security concerns, you may want to limit port forwarding to only those ports you are using, and uncheck the *Enable* checkbox after you are finished.

7.3. DMZ

This menu allows user to configure the DMZ setting for CPE in router mode. Web server, Telnet/SSH and Ping Service port can be exempted from DMZ mapping if required. By enabling DMZ option will make the specified local LAN host (DMZ IP) exposed to Internet.



Demilitarized Zone (DMZ)

DMZ

DMZ Enable Status	□ Enable
DMZ Host IP Address	192.168.0. 0
Exclude Web Server Port	☑ Enable
Exclude Telnet/SSH Port	☑ Enable
Exclude Ping Service	☑ Enable

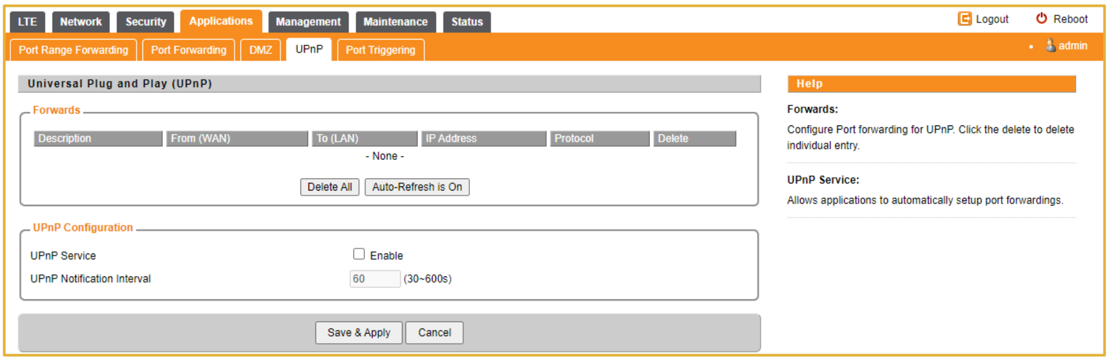
Help

DMZ:

Enabling this option will expose the specified host to the Internet. All ports will be accessible from the Internet.

7.4. UPnP

This menu allows user to configure the UPnP application for on-demand “DMZ” support. The current forwarding rules created can be viewed and cleared if required.



Universal Plug and Play (UPnP)

Forwards

Description	From (WAN)	To (LAN)	IP Address	Protocol	Delete

- None -

UPnP Configuration

UPnP Service	□ Enable
UPnP Notification Interval	60 (30~600s)

Help

Forwards:

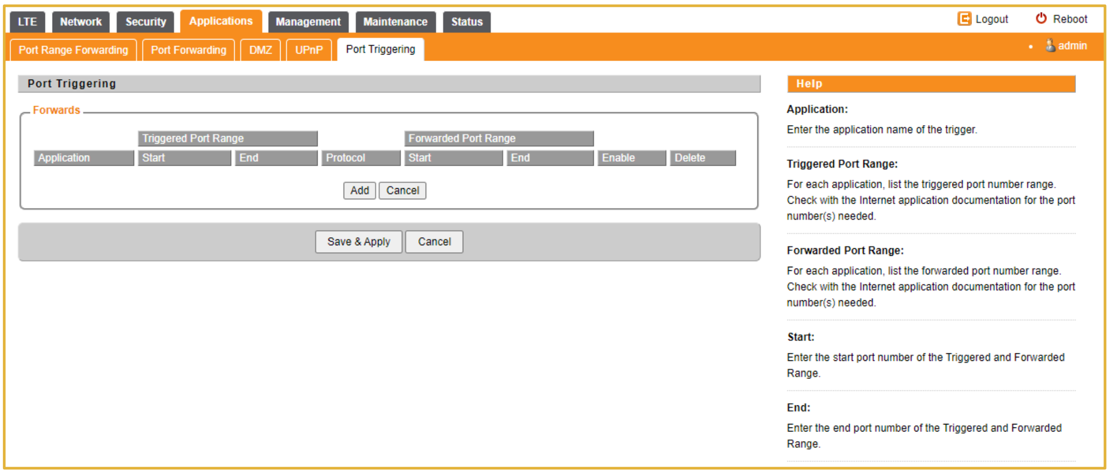
Configure Port forwarding for UPnP. Click the delete to delete individual entry.

UPnP Service:

Allows applications to automatically setup port forwardings.

7.5. Port Triggering

This menu allows user to configure forward certain port range to different port range for specific protocol.



Port Triggering

Forwards

	Triggered Port Range			Forwarded Port Range			
Application	Start	End	Protocol	Start	End	Enable	Delete

Help

Application:
Enter the application name of the trigger.

Triggered Port Range:
For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

Forwarded Port Range:
For each application, list the forwarded port number range. Check with the Internet application documentation for the port number(s) needed.

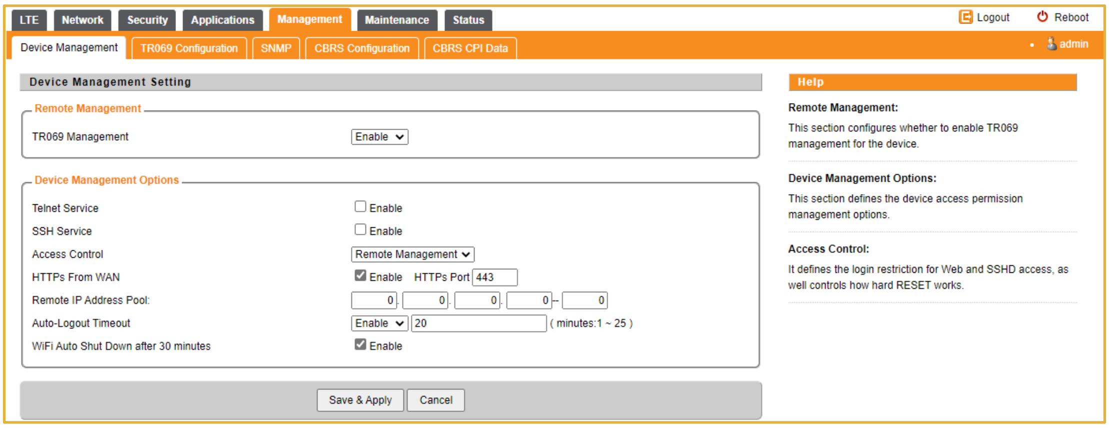
Start:
Enter the start port number of the Triggered and Forwarded Range.

End:
Enter the end port number of the Triggered and Forwarded Range.

8. Management

8.1. Device Management

The menu allows user to configure device management mode and various control. Telnet, SSH, and HTTPs can be enabled or disabled via configuration. Auto WEB GUI logout can also be configured.



Device Management Setting

Remote Management

TR069 Management: Enable

Device Management Options

Telnet Service: □ Enable
SSH Service: □ Enable
Access Control: Remote Management
HTTPs From WAN: ☑ Enable HTTPs Port 443
Remote IP Address Pool: 0 . 0 . 0 . 0 -- 0
Auto-Logout Timeout: Enable 20 (minutes:1 ~ 25)
WiFi Auto Shut Down after 30 minutes: ☑ Enable

Help

Remote Management:
This section configures whether to enable TR069 management for the device.

Device Management Options:
This section defines the device access permission management options.

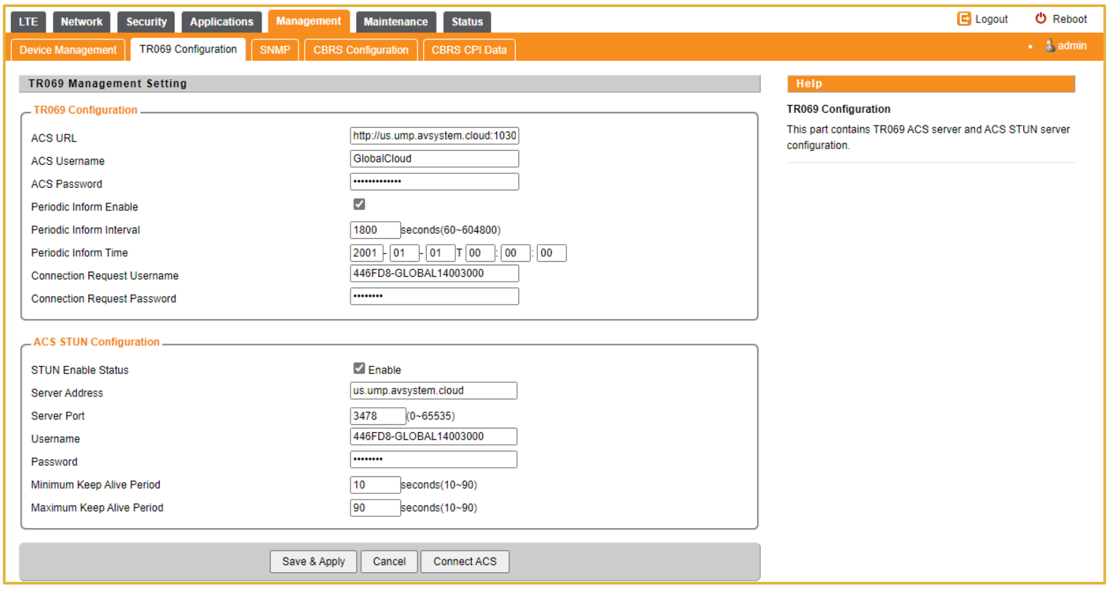
Access Control:
It defines the login restriction for Web and SSHD access, as well controls how hard RESET works.

When Telnet is enabled, user can telnet to CPE according to the below steps:

- CMD shell and run command:
- telnet 10.1.1.1
- Login: root
- Password: root123

8.2. TR069

The menu allows user to configure the necessary setting for TR069 management of the CPE device.



TR069 Management Setting

TR069 Configuration

ACS URL	http://us.ump.avsystem.cloud:1030
ACS Username	GlobalCloud
ACS Password	•••••••••••••
Periodic Inform Enable	☑
Periodic Inform Interval	1800 seconds(60~604800)
Periodic Inform Time	2001 - 01 - 01 T 00 : 00 : 00
Connection Request Username	446FD8-GLOBAL14003000
Connection Request Password	••••••••

ACS STUN Configuration

STUN Enable Status	☑ Enable
Server Address	us.ump.avsystem.cloud
Server Port	3478 (0~65535)
Username	446FD8-GLOBAL14003000
Password	••••••••
Minimum Keep Alive Period	10 seconds(10~90)
Maximum Keep Alive Period	90 seconds(10~90)

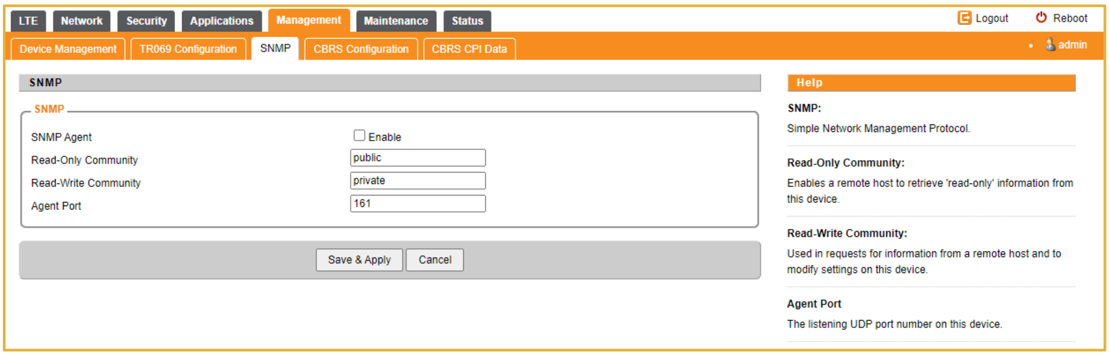
Help

TR069 Configuration

This part contains TR069 ACS server and ACS STUN server configuration.

8.3. SNMP

The menu allows user to configure the SNMP setting.



SNMP

SNMP

SNMP Agent	□ Enable
Read-Only Community	public
Read-Write Community	private
Agent Port	161

Help

SNMP:

Simple Network Management Protocol.

Read-Only Community:

Enables a remote host to retrieve 'read-only' information from this device.

Read-Write Community:

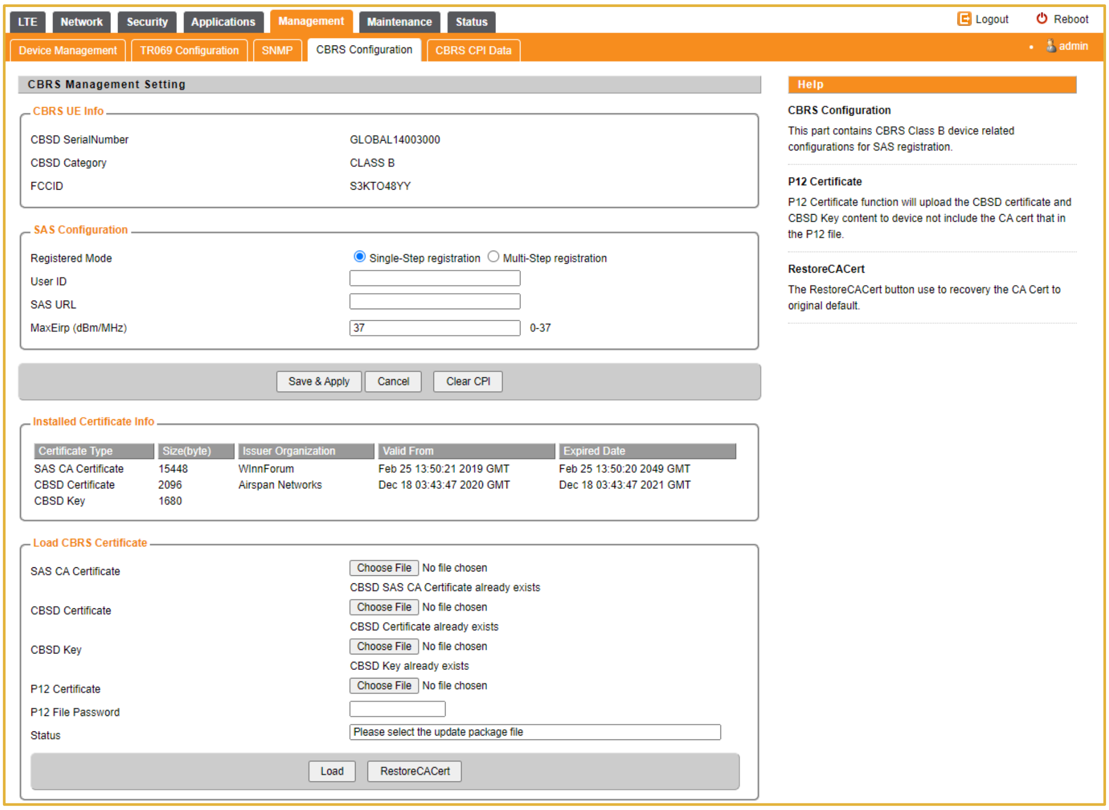
Used in requests for information from a remote host and to modify settings on this device.

Agent Port

The listening UDP port number on this device.

8.4. CBRS Configuration

The menu allows user to configure the necessary setting for CBRS SAS registration of the CPE device.



CBRS Management Setting

CBRS UE Info

CBSD SerialNumber	GLOBAL14003000
CBSD Category	CLASS B
FCCID	S3KTO48YY

SAS Configuration

Registered Mode	● Single-Step registration ○ Multi-Step registration
User ID	
SAS URL	
MaxEirp (dBm/MHz)	37 0-37

Save & Apply | Cancel | Clear CPI

Installed Certificate Info

Certificate Type	Size(byte)	Issuer Organization	Valid From	Expired Date
SAS CA Certificate	15448	WinnForum	Feb 25 13:50:21 2019 GMT	Feb 25 13:50:20 2049 GMT
CBSD Certificate	2096	Airspan Networks	Dec 18 03:43:47 2020 GMT	Dec 18 03:43:47 2021 GMT
CBSD Key	1680			

Load CBRS Certificate

SAS CA Certificate	Choose File No file chosen CBSD SAS CA Certificate already exists
CBSD Certificate	Choose File No file chosen CBSD Certificate already exists
CBSD Key	Choose File No file chosen CBSD Key already exists
P12 Certificate	Choose File No file chosen
P12 File Password	
Status	Please select the update package file

Load | RestoreCACert

Help

CBRS Configuration

This part contains CBRS Class B device related configurations for SAS registration.

P12 Certificate

P12 Certificate function will upload the CBSD certificate and CBSD Key content to device not include the CA cert that in the P12 file.

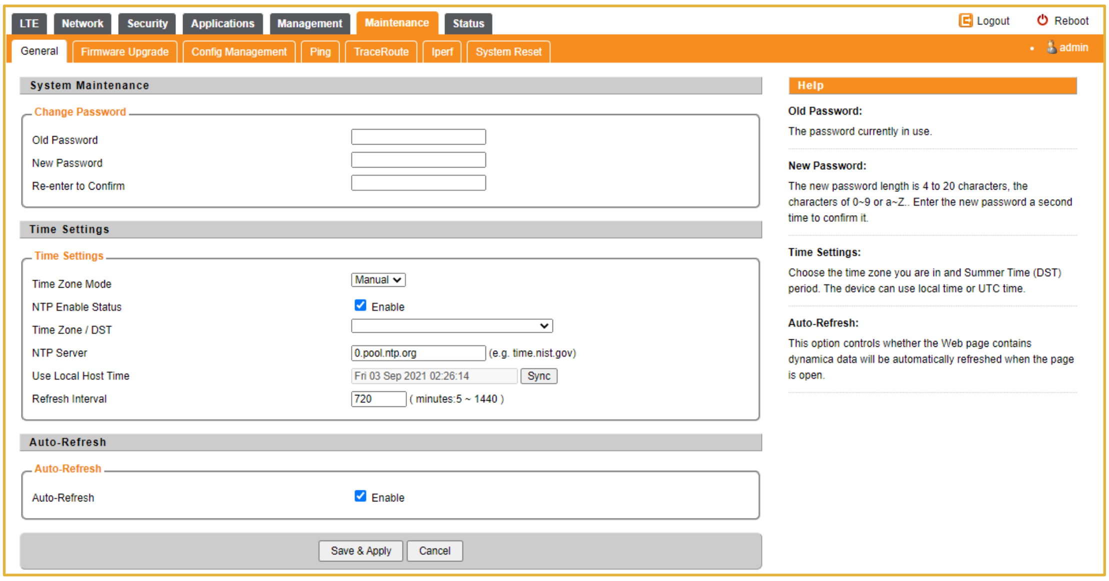
RestoreCACert

The RestoreCACert button use to recovery the CA Cert to original default.

9. Maintenance

9.1. General

The menu allows user to configure the WEB GUI login password, time and language setting.



System Maintenance

Change Password

Old Password	
New Password	
Re-enter to Confirm	

Time Settings

Time Settings

Time Zone Mode	Manual
NTP Enable Status	☑ Enable
Time Zone / DST	
NTP Server	0.pool.ntp.org (e.g. time.nist.gov)
Use Local Host Time	Fri 03 Sep 2021 02:26:14 Sync
Refresh Interval	720 (minutes:5 ~ 1440)

Auto-Refresh

Auto-Refresh

Auto-Refresh	☑ Enable

Save & Apply | Cancel

Help

Old Password:

The password currently in use.

New Password:

The new password length is 4 to 20 characters, the characters of 0~9 or a~Z.. Enter the new password a second time to confirm it.

Time Settings:

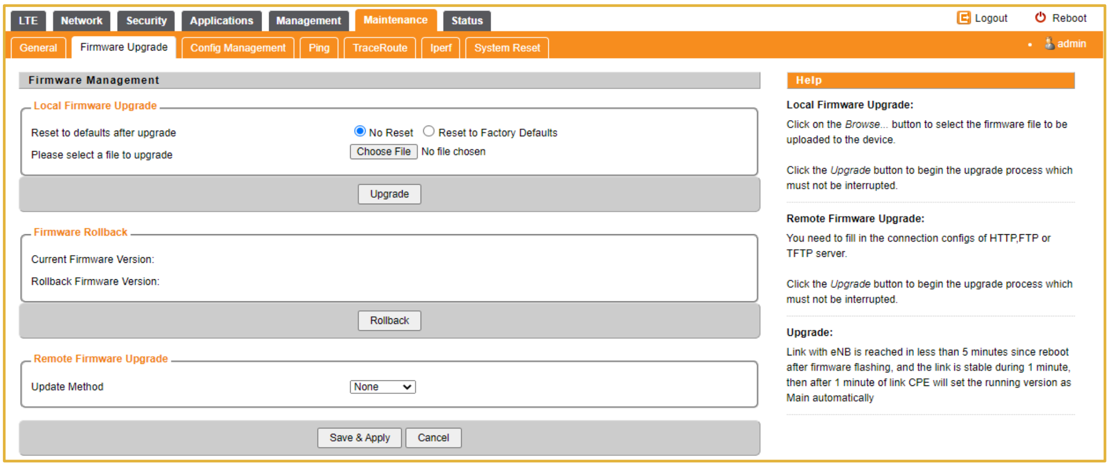
Choose the time zone you are in and Summer Time (DST) period. The device can use local time or UTC time.

Auto-Refresh:

This option controls whether the Web page contains dynamica data will be automatically refreshed when the page is open.

9.2. Firmware Upgrade

This menu allows user to perform firmware upgrade via WEG GUI with option to reset to factory setting. It can also configure the remote upgrade using FTP, TFTP or HTTP.



Firmware Management

Local Firmware Upgrade

Reset to defaults after upgrade ● No Reset ○ Reset to Factory Defaults

Please select a file to upgrade Choose File No file chosen

Upgrade

Firmware Rollback

Current Firmware Version:

Rollback Firmware Version:

Rollback

Remote Firmware Upgrade

Update Method None

Save & Apply Cancel

Help

Local Firmware Upgrade:

Click on the *Browse...* button to select the firmware file to be uploaded to the device.

Click the *Upgrade* button to begin the upgrade process which must not be interrupted.

Remote Firmware Upgrade:

You need to fill in the connection configs of HTTP,FTP or TFTP server.

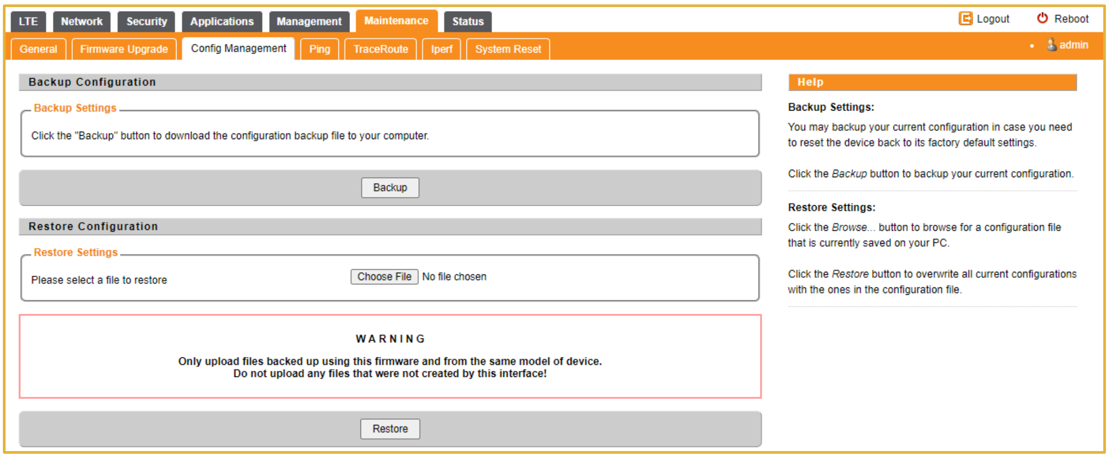
Click the *Upgrade* button to begin the upgrade process which must not be interrupted.

Upgrade:

Link with eNB is reached in less than 5 minutes since reboot after firmware flashing, and the link is stable during 1 minute, then after 1 minute of link CPE will set the running version as Main automatically

9.3. Config Management

This menu allows user to backup or restore device configuration file.



Backup Configuration

Backup Settings

Click the "Backup" button to download the configuration backup file to your computer.

Backup

Restore Configuration

Restore Settings

Please select a file to restore Choose File No file chosen

WARNING

Only upload files backed up using this firmware and from the same model of device.
Do not upload any files that were not created by this interface!

Restore

Help

Backup Settings:

You may backup your current configuration in case you need to reset the device back to its factory default settings.

Click the *Backup* button to backup your current configuration.

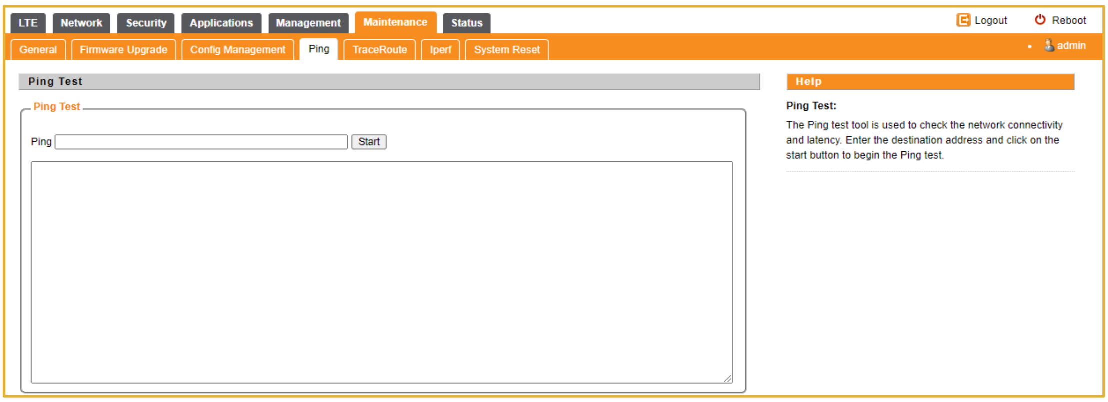
Restore Settings:

Click the *Browse...* button to browse for a configuration file that is currently saved on your PC.

Click the *Restore* button to overwrite all current configurations with the ones in the configuration file.

9.4. Ping

This menu allows user to perform PING tests using WEB GUI interface. Both IPv4 and IPv6 can be supported.



Ping Test

Ping Test

Ping Start

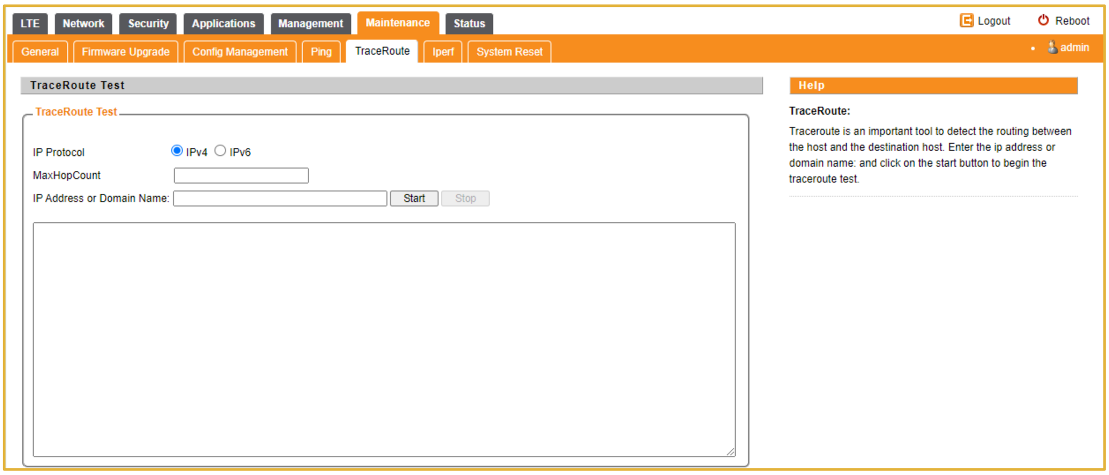
Help

Ping Test:

The Ping test tool is used to check the network connectivity and latency. Enter the destination address and click on the start button to begin the Ping test.

9.5. TraceRoute

This menu allows user to configure traceroute testing



TraceRoute Test

TraceRoute Test

IP Protocol ● IPv4 ○ IPv6

MaxHopCount

IP Address or Domain Name:

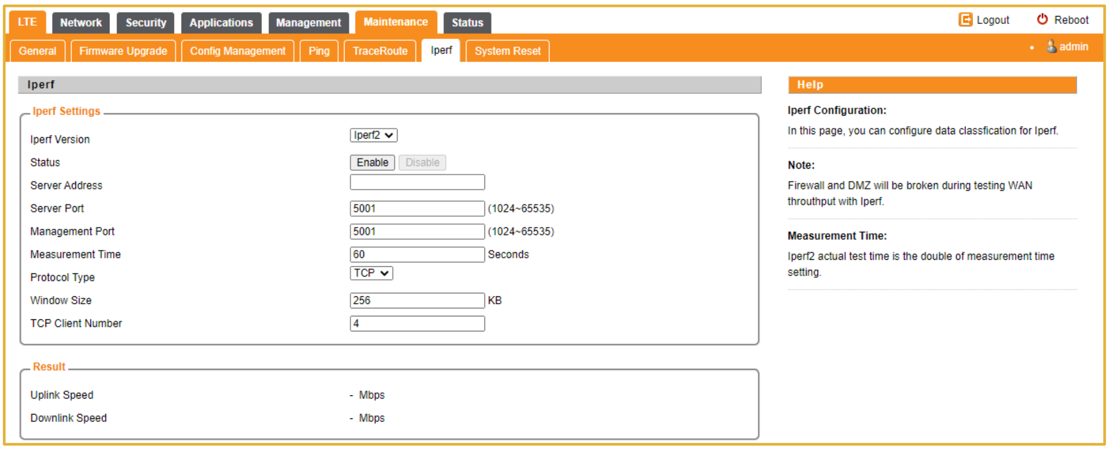
Help

TraceRoute:

Traceroute is an important tool to detect the routing between the host and the destination host. Enter the ip address or domain name: and click on the start button to begin the traceroute test.

9.6. Iperf

This menu allows user to configure iPerf testing using WEB GUI interface. Both TCP and UDP tests can be supported. Remote iPerf server is required to conduct the tests.



Iperf

Iperf Settings

Iperf Version	Iperf2
Status	Enable Disable
Server Address	
Server Port	5001 (1024~65535)
Management Port	5001 (1024~65535)
Measurement Time	60 Seconds
Protocol Type	TCP
Window Size	256 KB
TCP Client Number	4

Result

Uplink Speed	- Mbps
Downlink Speed	- Mbps

Help

Iperf Configuration:

In this page, you can configure data classfication for Iperf.

Note:

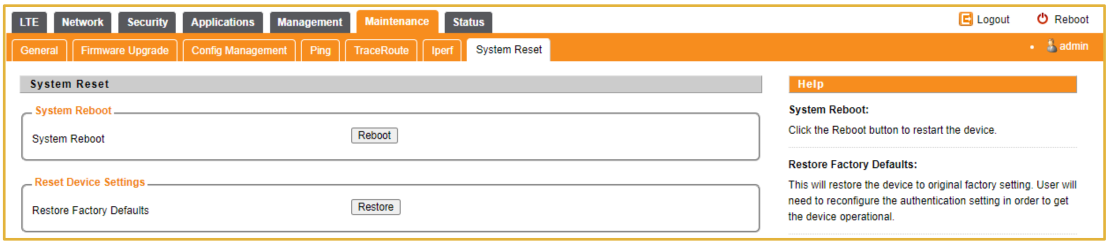
Firewall and DMZ will be broken during testing WAN throutput with Iperf.

Measurement Time:

Iperf2 actual test time is the double of measurement time setting.

9.7. System Reset

This menu allows user to reboot the device or restore the device to factory defaults. Special care needs to be taken when restoring factory defaults.



System Reset

System Reboot

System Reboot

Reset Device Settings

Restore Factory Defaults

Help

System Reboot:

Click the Reboot button to restart the device.

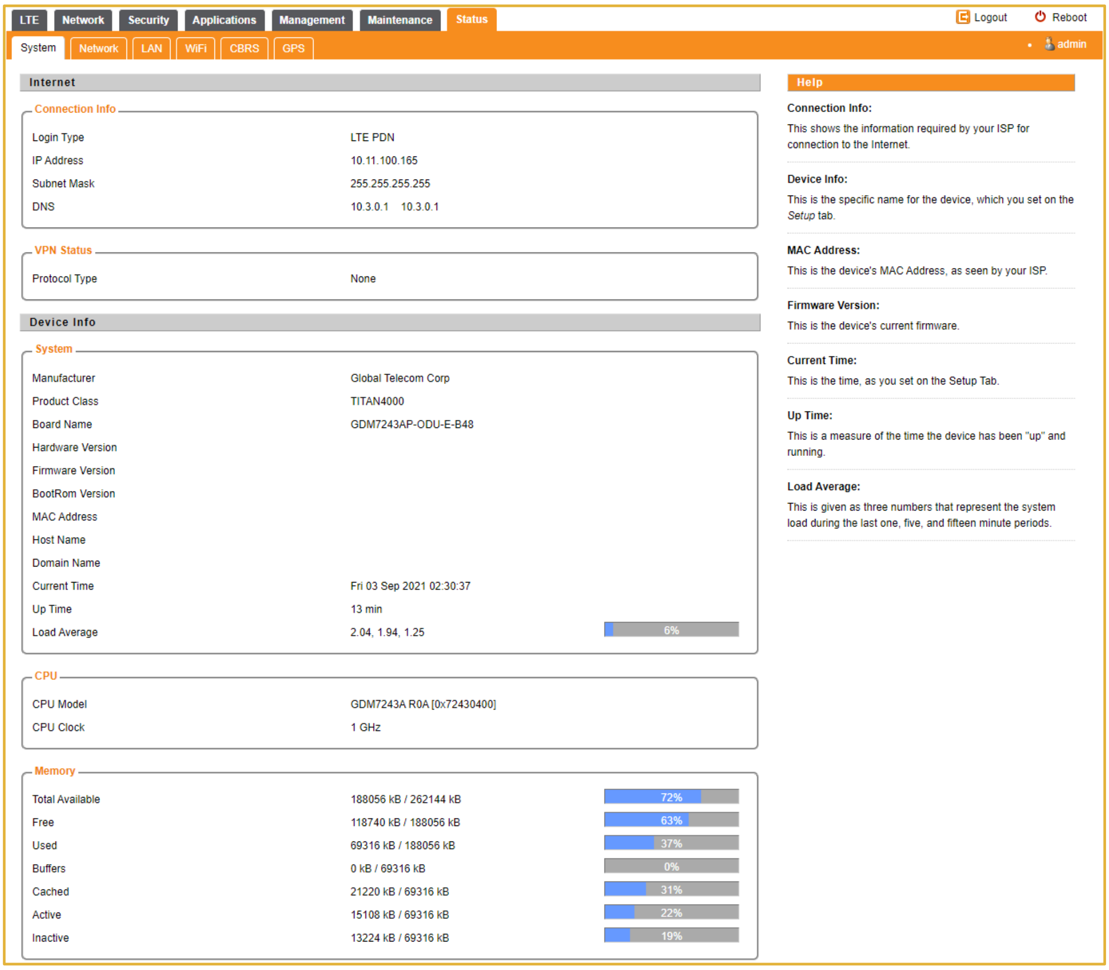
Restore Factory Defaults:

This will restore the device to original factory setting. User will need to reconfigure the authentication setting in order to get the device operational.

10.Status

10.1. System

The menu shows the general system info of the CPE device. It includes connection, system, CPE and memory usage information.



Internet

Connection Info

Login Type	LTE PDN
IP Address	10.11.100.165
Subnet Mask	255.255.255.255
DNS	10.3.0.1 10.3.0.1

VPN Status

Protocol Type	None

Device Info

System

Manufacturer	Global Telecom Corp	
Product Class	TITAN4000	
Board Name	GDM7243AP-ODU-E-B48	
Hardware Version		
Firmware Version		
BootRom Version		
MAC Address		
Host Name		
Domain Name		
Current Time	Fri 03 Sep 2021 02:30:37	
Up Time	13 min	
Load Average	2.04, 1.94, 1.25	6%

CPU

CPU Model	GDM7243A R0A [0x72430400]
CPU Clock	1 GHz

Memory

Total Available	188056 kB / 262144 kB	72%
Free	118740 kB / 188056 kB	63%
Used	69316 kB / 188056 kB	37%
Buffers	0 kB / 69316 kB	0%
Cached	21220 kB / 69316 kB	31%
Active	15108 kB / 69316 kB	22%
Inactive	13224 kB / 69316 kB	19%

Help

Connection Info:

This shows the information required by your ISP for connection to the Internet.

Device Info:

This is the specific name for the device, which you set on the *Setup* tab.

MAC Address:

This is the device's MAC Address, as seen by your ISP.

Firmware Version:

This is the device's current firmware.

Current Time:

This is the time, as you set on the Setup Tab.

Up Time:

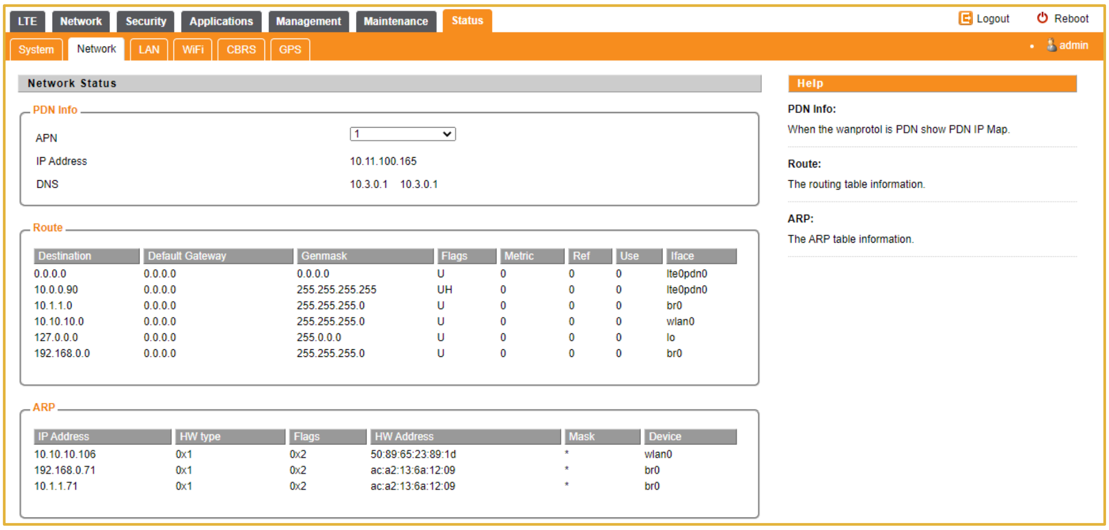
This is a measure of the time the device has been "up" and running.

Load Average:

This is given as three numbers that represent the system load during the last one, five, and fifteen minute periods.

10.2. Network

The menu shows the general network status that includes PDN interface info, device routing info, and ARP table.



Network Status

PDN Info

APN	1
IP Address	10.11.100.165
DNS	10.3.0.1 10.3.0.1

Route

Destination	Default Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	0.0.0.0	0.0.0.0	U	0	0	0	lte0pdn0
10.0.0.90	0.0.0.0	255.255.255.255	UH	0	0	0	lte0pdn0
10.1.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
10.10.10.0	0.0.0.0	255.255.255.0	U	0	0	0	wlan0
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	br0

ARP

IP Address	HW type	Flags	HW Address	Mask	Device
10.10.10.106	0x1	0x2	50:89:65:23:89:1d	*	wlan0
192.168.0.71	0x1	0x2	ac:a2:13:6a:12:09	*	br0
10.1.1.71	0x1	0x2	ac:a2:13:6a:12:09	*	br0

PDN Info:

When the wanprotol is PDN show PDN IP Map.

Route:

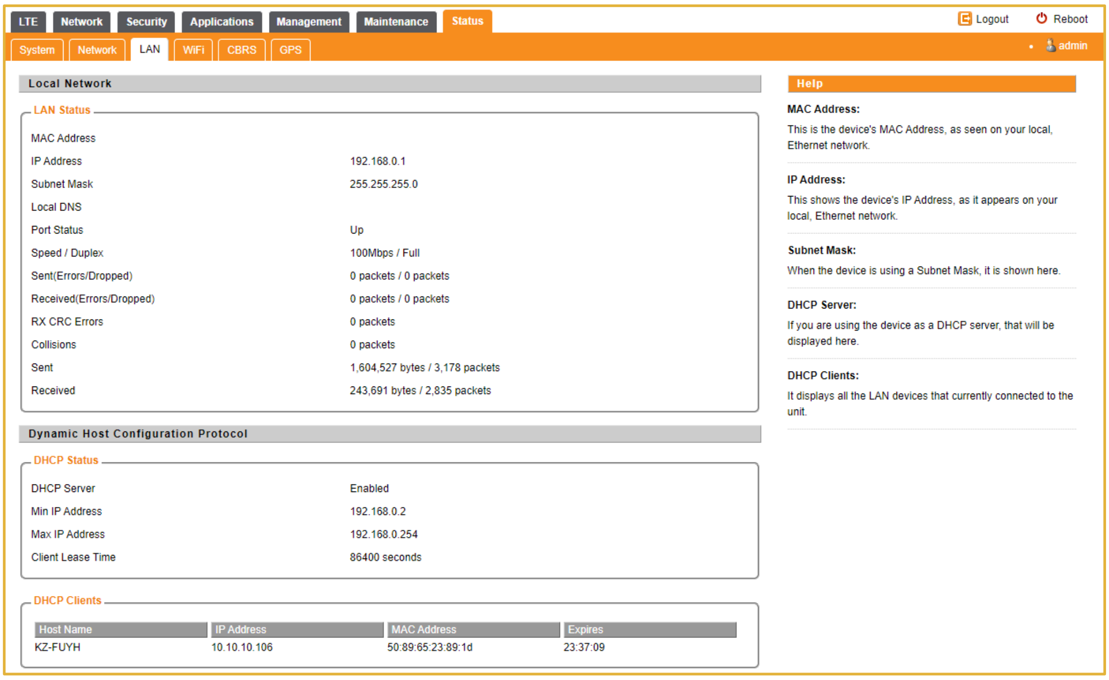
The routing table information.

ARP:

The ARP table information.

10.3. LAN

The menu shows the local LAN network status including the LAN interface and DHCP Server setting and current DHCP clients connected.



Local Network

LAN Status

MAC Address	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Local DNS	
Port Status	Up
Speed / Duplex	100Mbps / Full
Sent(Errors/Dropped)	0 packets / 0 packets
Received(Errors/Dropped)	0 packets / 0 packets
RX CRC Errors	0 packets
Collisions	0 packets
Sent	1,604,527 bytes / 3,178 packets
Received	243,691 bytes / 2,835 packets

Dynamic Host Configuration Protocol

DHCP Status

DHCP Server	Enabled
Min IP Address	192.168.0.2
Max IP Address	192.168.0.254
Client Lease Time	86400 seconds

DHCP Clients

Host Name	IP Address	MAC Address	Expires
KZ-FUYH	10.10.10.106	50:89:65:23:89:1d	23:37:09

MAC Address:

This is the device's MAC Address, as seen on your local, Ethernet network.

IP Address:

This shows the device's IP Address, as it appears on your local, Ethernet network.

Subnet Mask:

When the device is using a Subnet Mask, it is shown here.

DHCP Server:

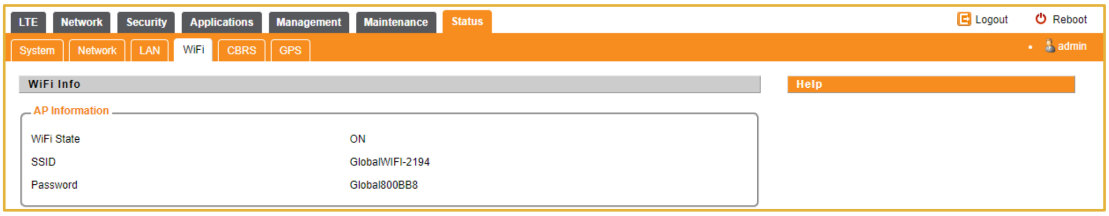
If you are using the device as a DHCP server, that will be displayed here.

DHCP Clients:

It displays all the LAN devices that currently connected to the unit.

10.4. Wi-Fi

The menu shows the Wi-Fi status, SSID & Password.



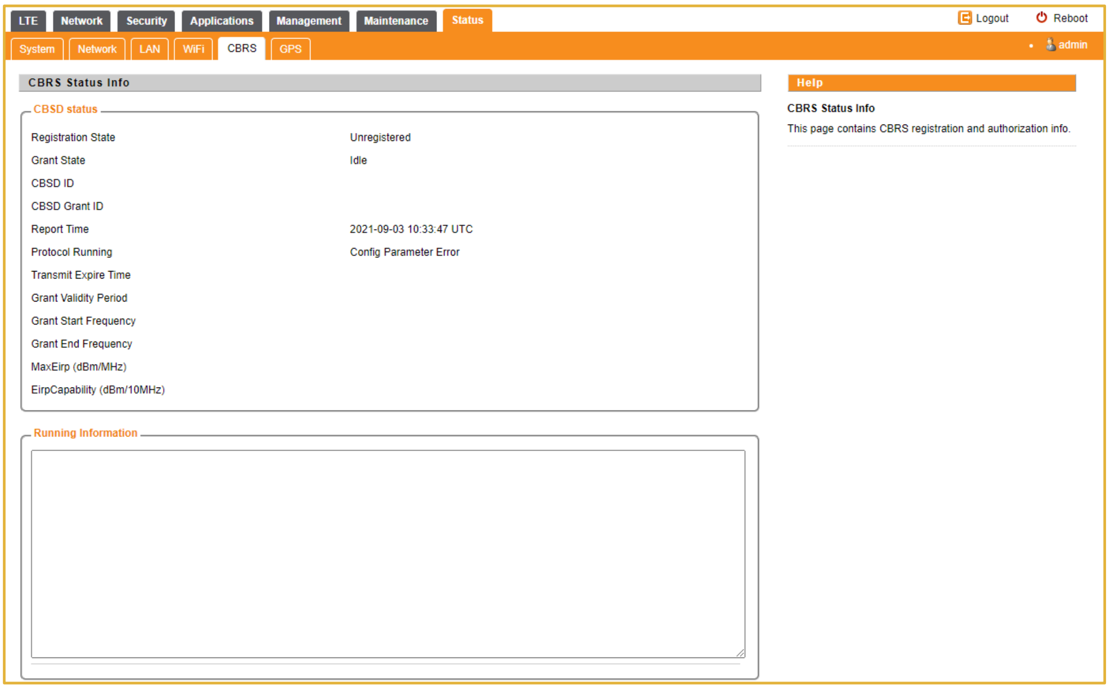
WiFi Info

AP Information

WiFi State	ON
SSID	GlobalWIFI-2194
Password	Global800BB8

10.5. CBRS

The menu shows CBRS registration and authorization info.



CBRS Status Info

CBSD status

Registration State	Unregistered
Grant State	Idle
CBSD ID	
CBSD Grant ID	
Report Time	2021-09-03 10:33:47 UTC
Protocol Running	Config Parameter Error
Transmit Expire Time	
Grant Validity Period	
Grant Start Frequency	
Grant End Frequency	
MaxEirp (dBm/MHz)	
EirpCapability (dBm/10MHz)	

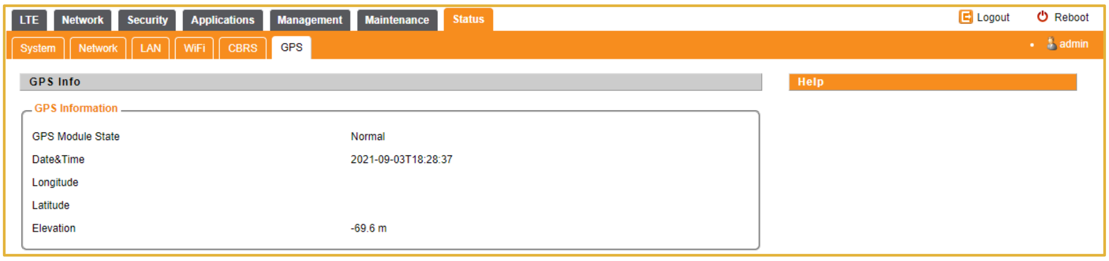
Running Information

CBRS Status Info

This page contains CBRS registration and authorization info.

10.6. GPS

The menu shows the GPS status info.



GPS Info

GPS Information

GPS Module State	Normal
Date&Time	2021-09-03T18:28:37
Longitude	
Latitude	
Elevation	-69.6 m

11.Troubleshooting

Q1: My PC cannot connect to the CPE.

- Check the PoE adapter LED is on and the CPE & PC ETH cables are securely connected. The CPE LED should work as described.
- Check the PC NIC driver is properly installed and configured.

Q2: My CPE networking is not working properly.

- Check and make sure you are within the LTE coverage area and the unit is attached to the network.
- Please also check the SIM card validity.

Q3: Unable to connect internet while the device is already connected to LTE.

- Check and verify your computer has proper NIC interface configured (DHCP or static IP). Unplug the PC ETH cable and reconnect again if required.
- If necessary, you may reboot the CPE by power off/on the CPE unit.