LTE Outdoor CPE8000

System Manual

December 2016

Legal Rights

The material contained herein is proprietary, privileged, and confidential and owned by Telrad Networks or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Telrad Networks Ltd.

Telrad Networks Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

BreezeCOM®, BreezeMAX®, 4Motion® and/or other products and Telrad Networks/or services referenced herein are either registered trademarks, trademarks or service marks of Telrad Networks Ltd.

All other names are or may be the trademarks of their respective owners.

Statement of Conditions

The information contained in this manual is subject to change without notice. Telrad Networks Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All Telrad Networks Ltd. ("Telrad Networks") products purchased from Telrad Networks or through any of Telrad Networks' authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

(a) Telrad Networks warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Telrad Networks will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Telrad Networks' standard R&R procedure.

(b) With respect to the Firmware, Telrad Networks warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from invoice date (the "Warranty Period")". During the Warranty Period, Telrad Networks may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Telrad will be obligated to support solely the two (2) most recent Software major releases.

TELRAD NETWORKS SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

(a) The Software is sold on an "AS IS" basis. Telrad Networks, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. TELRAD NETWORKS SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH-RISK ACTIVITIES"). HIGH-RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. TELRAD NETWORKS SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH-RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT TELRAD NETWORKS'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED, ALL OF WHICH ARE EXPRESSLY DISCLAIMED. TELRAD NETWORKS' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. TELRAD NETWORKS NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

(a) TELRAD NETWORKS SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF TELRAD NETWORKS OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

PLEASE READ THESE SAFETY PRECAUTIONS!

RF Energy Health Hazard

The radio equipment described in this guide uses radio frequency transmitters. Although the power level is low, the concentrated energy from a directional antenna may pose a health hazard.

Do not allow people to come in close proximity to the front of the antenna while the transmitter is operating.

A distance of minimum 23 cm need to be maintain at all times

Protection from Lightning

Before connecting this instrument to the power line, make sure that the voltage of the power source matches the requirements of the instrument. The unit must be standards.

Disposal and Recycling Information

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Reduction of Hazardous Substances

This CPE is compliant with the EU Registration, Evaluation, Authorization and Restriction of Chemicals (REACH) Regulation (Regulation No 1907/2006/EC of the European Parliamentand of the Council) and the EU Restriction of Hazardous Substances (RoHS) Directive (Directive 2002/95/EC of the European Parliament and of the Council).

CE Conformance Declaration

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment can meet the following conformance standards:

- EN 60950/22 - Product Safety
- EN301489 EN301908 EN62311 - EMC requirements for radio equipment

This device is intended for use in all European Community countries.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with RSS-192 and 197 of the Industry Canada Rules. This equipment also complies with the limits for a class B digital device, pursuant to ETSI EN 301 489-1 and 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 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.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- this device must accept any interference received including interference that may cause undesired operation

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 23cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Industry Canada statement

This device complies with RSS-192 & RSS-197 of the Industry Canada Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-192 & CNR-197 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Users can obtain Canadian information on RF exposure and compliance from the Canadian Representative:

Nick Dewar Nick.Dewar@Telrad.com

Contents

1 Product Overview

CPE8000 is a high performance LTE CPE (Customer Premises Equipment) product designed to enable quick LTE service deployment to the remote customers. It provides high data throughput and networking features to end users who need both bandwidth and roaming capabilities in the certain area.

1.1 Product Highlights

Frequency Bands	Band 48 * - CBRS disclaimer : in case of CBRS the operating frequency is set by the Domain Proxy and not by manual configuration. The Domain proxy maintain the Frequency based on grant allocation at all times.
LTE Data Rate	Category 4 + UL-QAM64
LTE Tx Power	23 dBm
Antenna Gain	15dBi
User management	Web Gui / TR69
Dimensions	198 x 194 x 48 mm / 1.5Kg 7.8 x 7.6 x 1.9 in / 3.3 lb
Environmental	IP67 rating
Operational Temperature	Temperature range : -40 ~55℃
Package content	CPE, POE, Power cable (US or EU), Mount Kit, Ethernet cable

1.2 User Interface Specification

Model	Description & User Interface
CPE8000	- Panel antenna: B42_43 - 1 RJ45 10/100/1000M LAN Port - PWR, RUN, LAN, SIM, and LTE (1-6) LEDs - 48V/0.5A PoE supply, ODU Power <12 Watts - Dimensions: 203 mm (L) × 203 mm (W) × 76 mm (D) - Weight: 3 Kg

2 Getting Started

2.1 Packing list

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

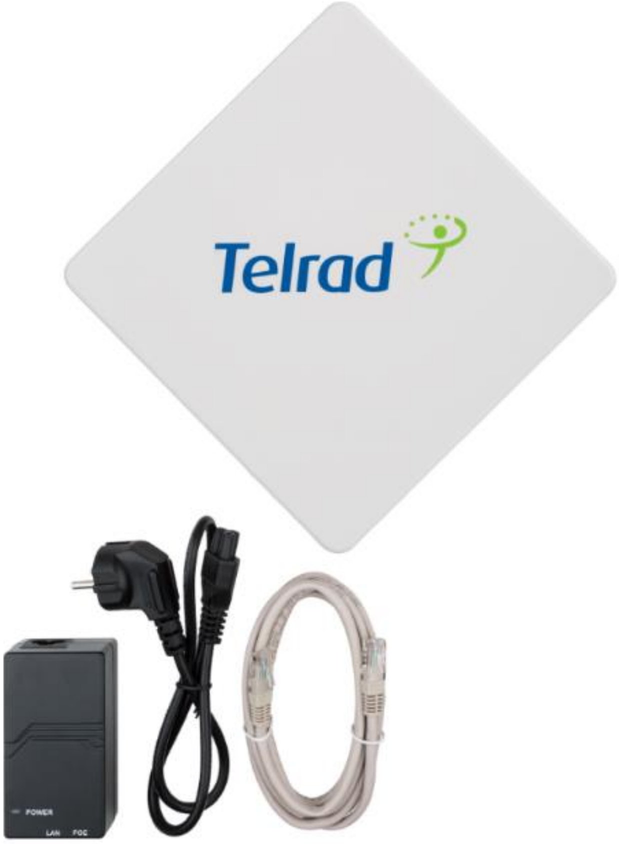
Table 2-1 Packing List

Outdoor CPE Products	Quantity
ODU unit	1
PoE adapter	1
Power cord	1
Mounting brackets	1
PC Ethernet Cable	1
Quick Installation Guide	1

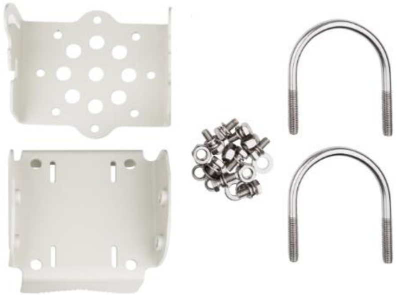
2.2 Unpacking the Equipment

Table 2-1 lists all the standard parts that are supplied in your LTE CPE Unit Installation Package.

Please take the time to unpack the package and check its contents against this list.



CPE8000, POE, Power Cable and LAN Ethernet cable



CPE8000 Mounting Kit

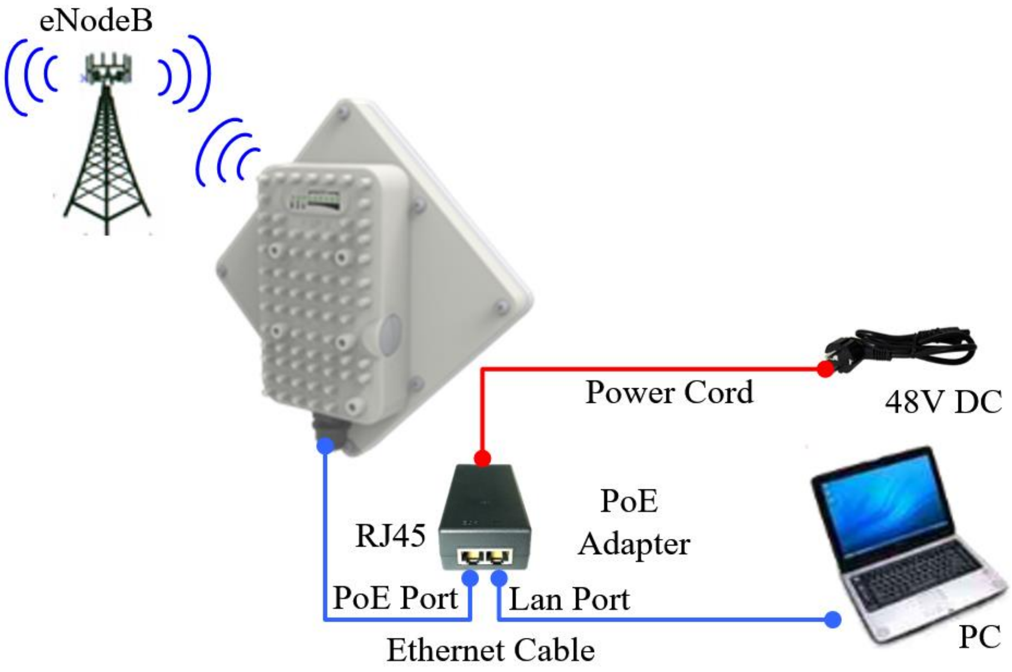
2.3 Installing the Equipment

2.3.1 Device connection

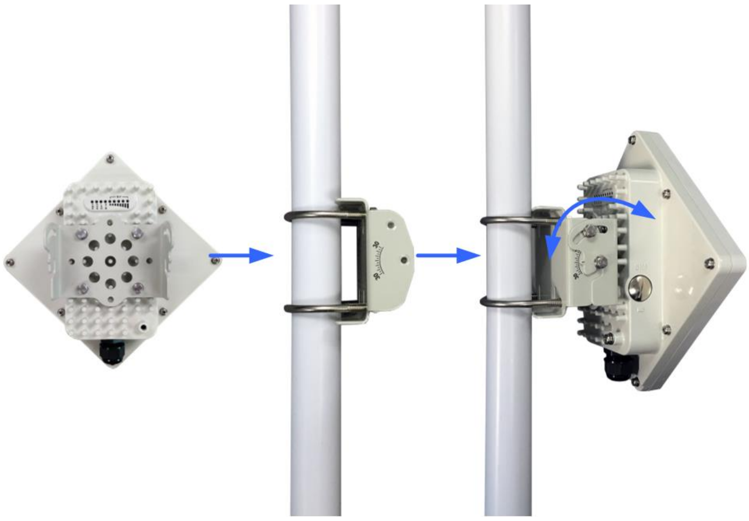
For outdoor CPE product, it is suggested that the CPE device be installed in a shaded area to avoid direct sun light exposure which may cause over heat in certain extreme weather condition. The CPE should be properly grounded for proper protection against lighting or power surge.

To power on the device, the outdoor CPE must use a 48V PoE integrated DC power supply adapter. The power adapters can operate in 100-240V AC range and therefore can be used in different country. Once the device is powered up, the user should wait for about 2 minutes before the device becomes operational. For CPE with the RUN LED indicator, a slowly flashing light indicates the system has completed the startup procedure.

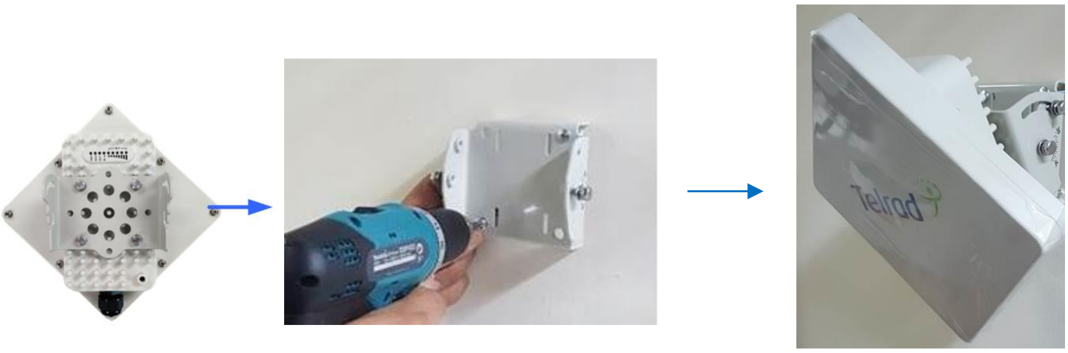
To connect PC, LAN switch or other type of IP device to the CPE product, the user should use standard CAT5 Ethernet cable and connect to the appropriate LAN port. Once connect the CPE LAN LED indicator should come on.



2.3.2 Installing Outdoor Unit (ODU) – Pole Mount

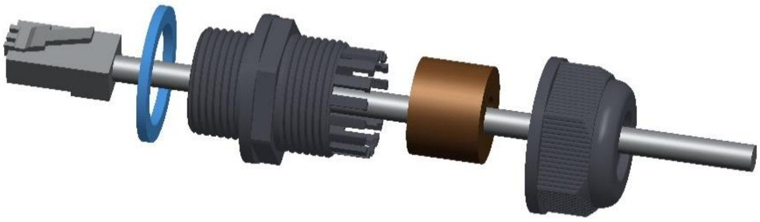


2.3.3 Installing Outdoor Unit (ODU) – Wall Mount



Note: The wall screws and screw anchors are not part of the package. Recommended screw size minimum 50mm length and 6-8mm diameter.

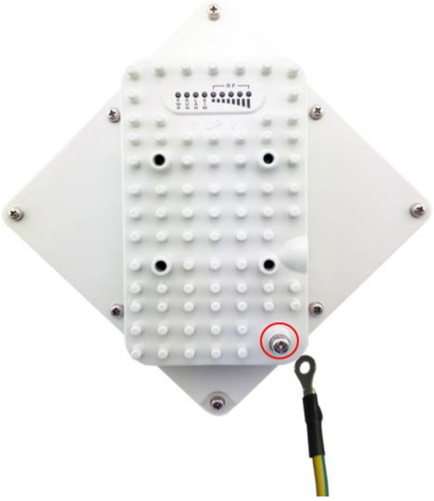
2.3.4 Header Connection:



2.4 Grounding

Make sure that the installation of the outdoor unit, antenna and cables is performed in accordance with all relevant national and local building and safety codes. Even where grounding is not mandatory according to applicable regulation and national codes, it is highly recommended to ensure that the outdoor unit and the antenna mast are grounded and suitable lightning protection devices are used so as to provide protection against voltage surges and static charges. In any event, Telrad is not liable for any injury, damage or regulation violations associated with or caused by installation, grounding or lightning protection.

The Grounding screw is located on the lower part at the back of the unit (see Figure below). Use 10 AWG cable for grounding.



Connect one of a grounding cable to the grounding screw and firmly tighten the grounding screw. Connect the opposite end of the grounding cable to a good ground (earth) connection.

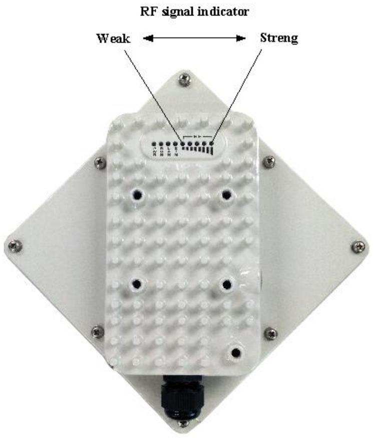
2.5 LED Display

LED Indicator	Function	Description
PWR	Power Indicator	Green Color – Device is powered on
RUN	System Run Indicator	Fast Blinking – Device is rebooting Slow Blinking – Device is in normal operation
LAN	LAN port status	Solid Green – LAN port is up Blinking Green – LAN data activity in progress
SIM	SIM Card Indicator	Light is on – SIM Card Error
RF (5 LEDs)	RF Signal Strength	5 level signal strengths indication by 5 green LEDs

2.6 RF Signal Adjustment

After the CPE outdoor unit has installed, the direction of antenna's azimuth and pitch angle needs to adjust for the best signal strength. In near line of sight condition, the CPE will have the best signal when the antenna is directly pointing the base station.

User can adjust the holder to change the direction and angle of the antenna while observing the RF LED on the outdoor unit which indicates the signal strength.



3 Managing CPE Device

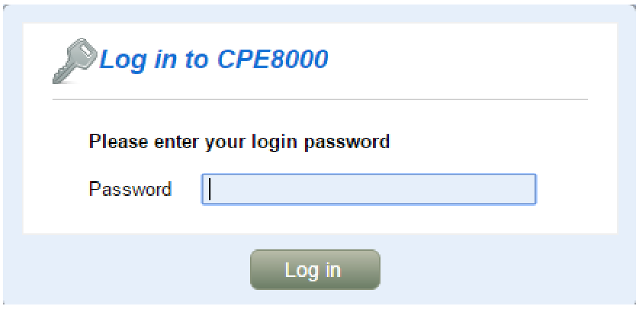
CPE8000 is a user-friendly LTE CPE, and very easy to configure and setup. Subscribers can just connect the device to their computer or home switch/router and the device is ready to provide Internet Services.

3.1 WEB Login

It is a preferred to setup the CPE using a Web browser from a local PC connected to device LAN port. The user should ensure that the connected PC have acquired IP address via DHCP from the device. After IP connectivity is established between the PC and CPE device, the user may launch a Web browser and specify http://192.168.254.251 in the address bar. A window will pop up requesting password. Input the user login password and then click the “Log in” button. After successful log on, the default home page of the WEB GUI interface will appear. Note that the default user passwords:

Operator user password: "Telrad4G"

End user password : "Admin"



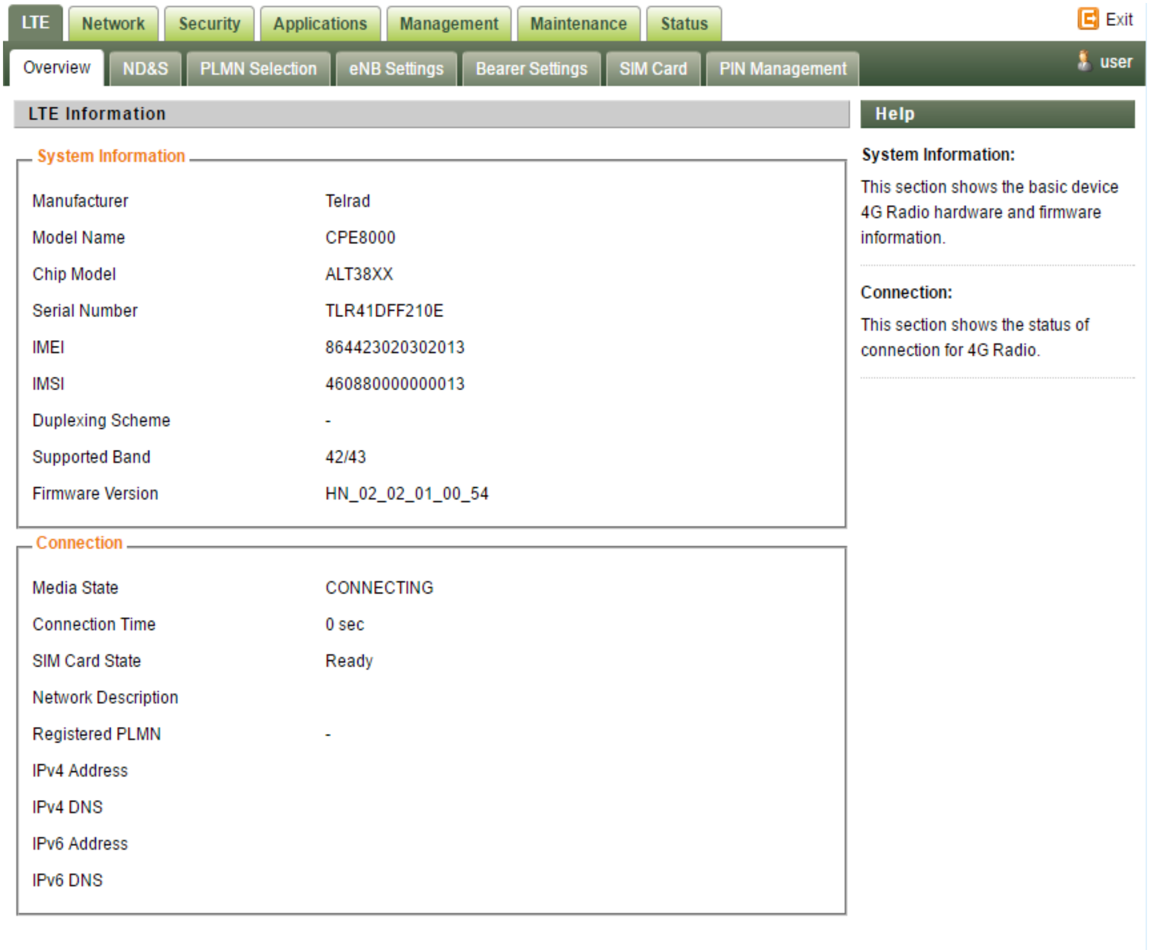
Log in to CPE8000

Please enter your login password

Password

3.2 Device Status

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	Telrad
Model Name	CPE8000
Chip Model	ALT38XX
Serial Number	TLR41DFF210E
IMEI	864423020302013
IMSI	460880000000013
Duplexing Scheme	-
Supported Band	42/43
Firmware Version	HN_02_02_01_00_54

Connection

Media State	CONNECTING
Connection Time	0 sec
SIM Card State	Ready
Network Description	
Registered PLMN	-
IPv4 Address	
IPv4 DNS	
IPv6 Address	
IPv6 DNS	

Help

System Information:

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

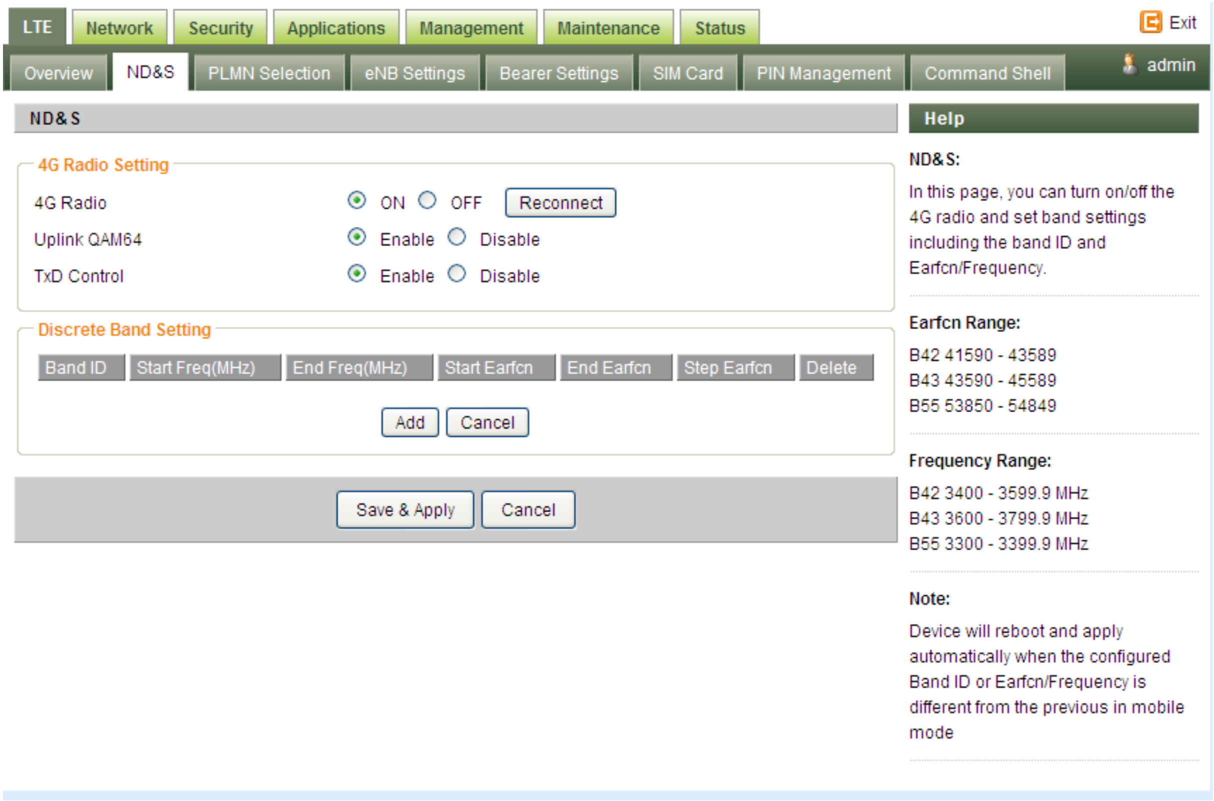
Connection:

This section shows the status of connection for 4G Radio.

3.3 ND&S (Network Discover and Selection)

In order to reduce frequency scanning time and fast connected, the user should configure fixed frequency and or range as follow picture: **LTE->ND&S.**

By default the CPE will scan the full band (3.3-3.8GHz), it is possible to define discrete band or frequency range.



ND&S

4G Radio Setting

4G Radio ● ON ○ OFF

Uplink QAM64 ● Enable ○ Disable

TxD Control ● Enable ○ Disable

Discrete Band Setting

Band ID	Start Freq(MHz)	End Freq(MHz)	Start Earfcn	End Earfcn	Step Earfcn	Delete

Help

ND&S:

In this page, you can turn on/off the 4G radio and set band settings including the band ID and Earfcn/Frequency.

Earfcn Range:

B42 41590 - 43589
B43 43590 - 45589
B55 53850 - 54849

Frequency Range:

B42 3400 - 3599.9 MHz
B43 3600 - 3799.9 MHz
B55 3300 - 3399.9 MHz

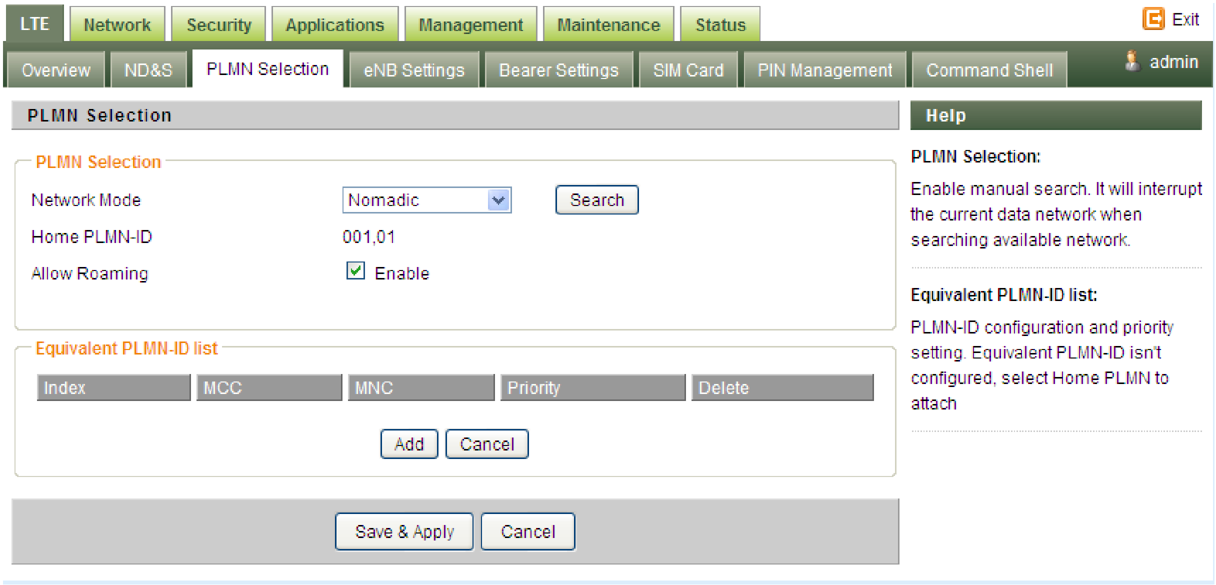
Note:

Device will reboot and apply automatically when the configured Band ID or Earfcn/Frequency is different from the previous in mobile mode

3.4 PLMN selection

Home PLMN-ID show the PLMN-ID according to SIM card, the format is MCC, MNC.

Operator can configure equivalent PLMN-ID list (up to 4) to allow UE to attach to specific non-home PLMN-IDs. The capability enables flexibility on the operator network, to define different PLMN-ID or multiple PLMN-IDs.



PLMN Selection

PLMN Selection

Network Mode: Nomadic

Home PLMN-ID: 001,01

Allow Roaming: ☑ Enable

Equivalent PLMN-ID list

Index	MCC	MNC	Priority	Delete

Help

PLMN Selection:

Enable manual search. It will interrupt the current data network when searching available network.

Equivalent PLMN-ID list:

PLMN-ID configuration and priority setting. Equivalent PLMN-ID isn't configured, select Home PLMN to attach

3.5 eNB Settings

3.5.1 Preferred eNB

When enable this option operator can “force” UE to attach to specific eNB (up to 8) with priority, in this way UE ignores its RF signal quality and is attached according to the configuration (MCC, MNC, ECI).

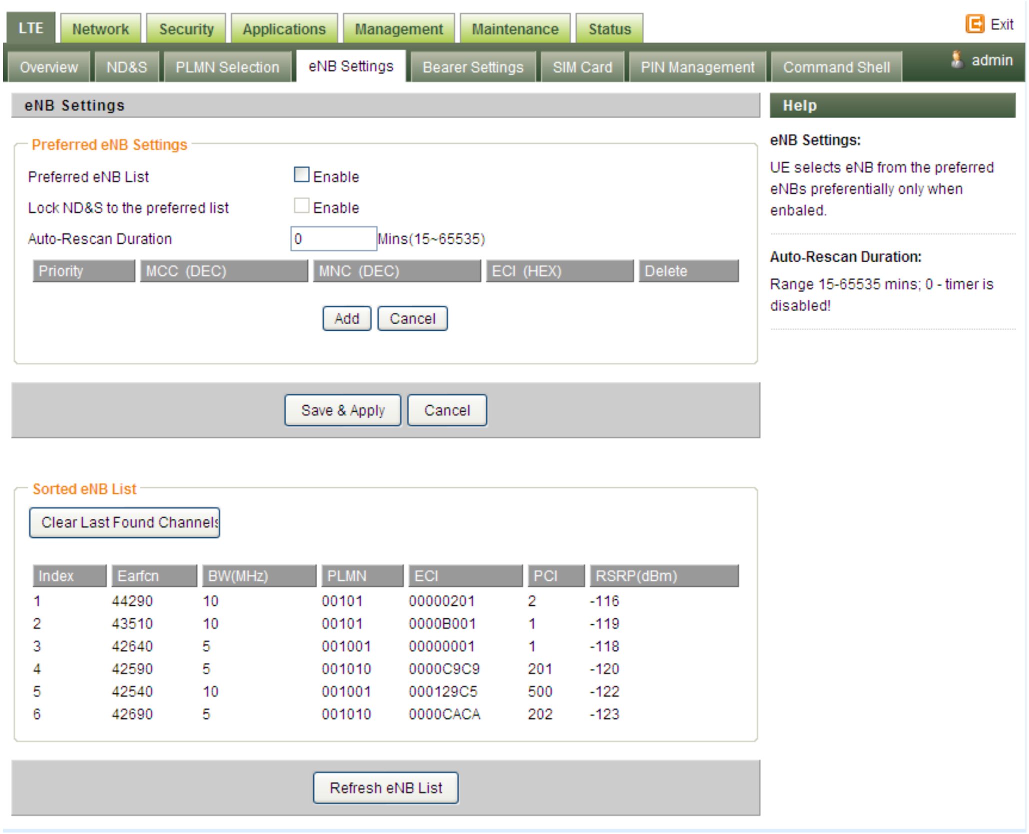
When UE is count not attached to any eNB in Preferred eNBs list, UE will attach to any other eNB with higher RF signal quality.

3.5.2 Lock ND&S

When selecting this option UE will attached only to eNB according to configuration (MCC, MNC, ECI).

3.5.3 Auto Rescan duration

When configuring this parameter, UE will drop RF signal after the configurable time interval and perform re-scanning of available eNBs according to Frequency Configuration and eNB settings.



eNB Settings

Preferred eNB Settings

Preferred eNB List	□ Enable
Lock ND&S to the preferred list	□ Enable
Auto-Rescan Duration	0 Mins(15~65535)

Priority	MCC (DEC)	MNC (DEC)	ECI (HEX)	Delete

Help

eNB Settings:

UE selects eNB from the preferred eNBs preferentially only when enbaled.

Auto-Rescan Duration:

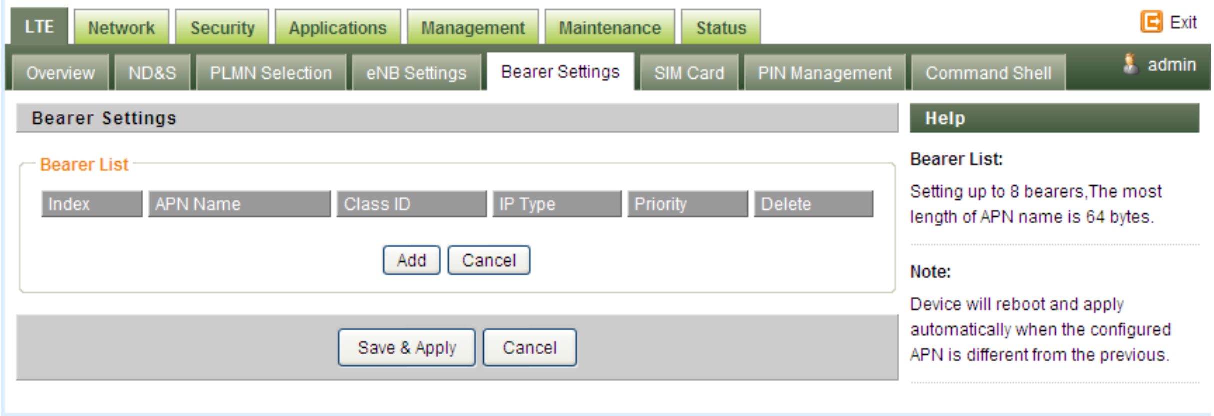
Range 15-65535 mins; 0 - timer is disabled!

Sorted eNB List

Index	Earfcn	BW(MHz)	PLMN	ECI	PCI	RSRP(dBm)
1	44290	10	00101	00000201	2	-116
2	43510	10	00101	0000B001	1	-119
3	42640	5	001001	00000001	1	-118
4	42590	5	001010	0000C9C9	201	-120
5	42540	10	001001	000129C5	500	-122
6	42690	5	001010	0000CACA	202	-123

3.6 Bearer Settings (Multiple PDNs)

The Bearer Settings List is designed for the user to configure the APN according to the operator network.



Index	APN Name	Class ID	IP Type	Priority	Delete

Bearer List:

Setting up to 8 bearers,The most length of APN name is 64 bytes.

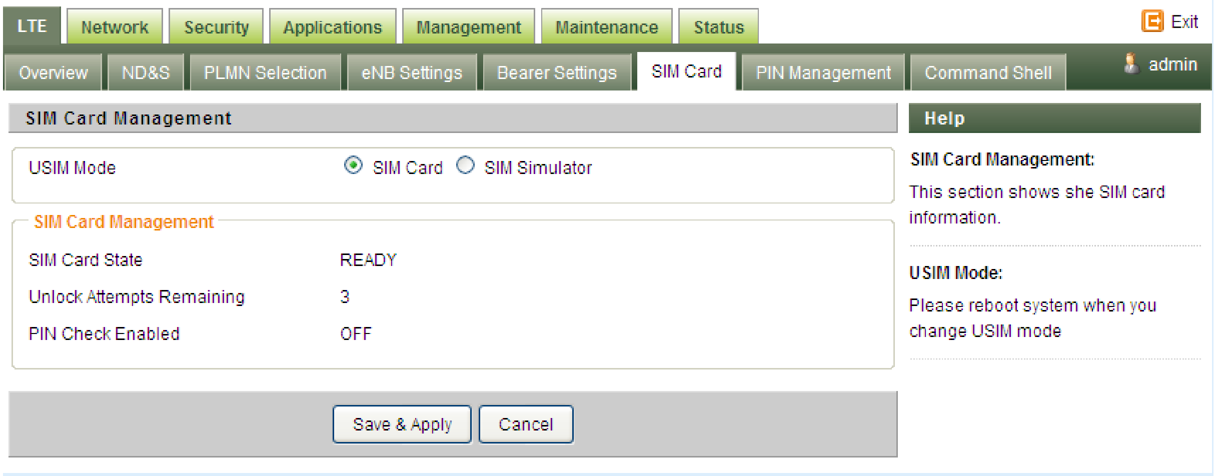
Note:

Device will reboot and apply automatically when the configured APN is different from the previous.

3.7 SIM Card

Operator can choose in which method he would like to work.

- SIM Card – based on SIM card hardware
- SIM simulator– in this method hardware SIM card is not needed, instead it is required to configure the Virtual SIM card credentials and synchronize with HSS/AAA user information



USIM Mode ● SIM Card ○ SIM Simulator

SIM Card State	READY
Unlock Attempts Remaining	3
PIN Check Enabled	OFF

SIM Card Management:

This section shows she SIM card information.

USIM Mode:

Please reboot system when you change USIM mode

3.8 Network

3.8.1 Internet

This tab is used to configure the CPE networking mode (e.g Router/NAT vs. L2 bridge mode).

3.8.1.1 Router/ NAT mode

The following parameters should be configured (please, refer to the settings shown in the below screenshot):

Connection Mode – defines the CPE networking mode. Should be set to "Router/ NAT"

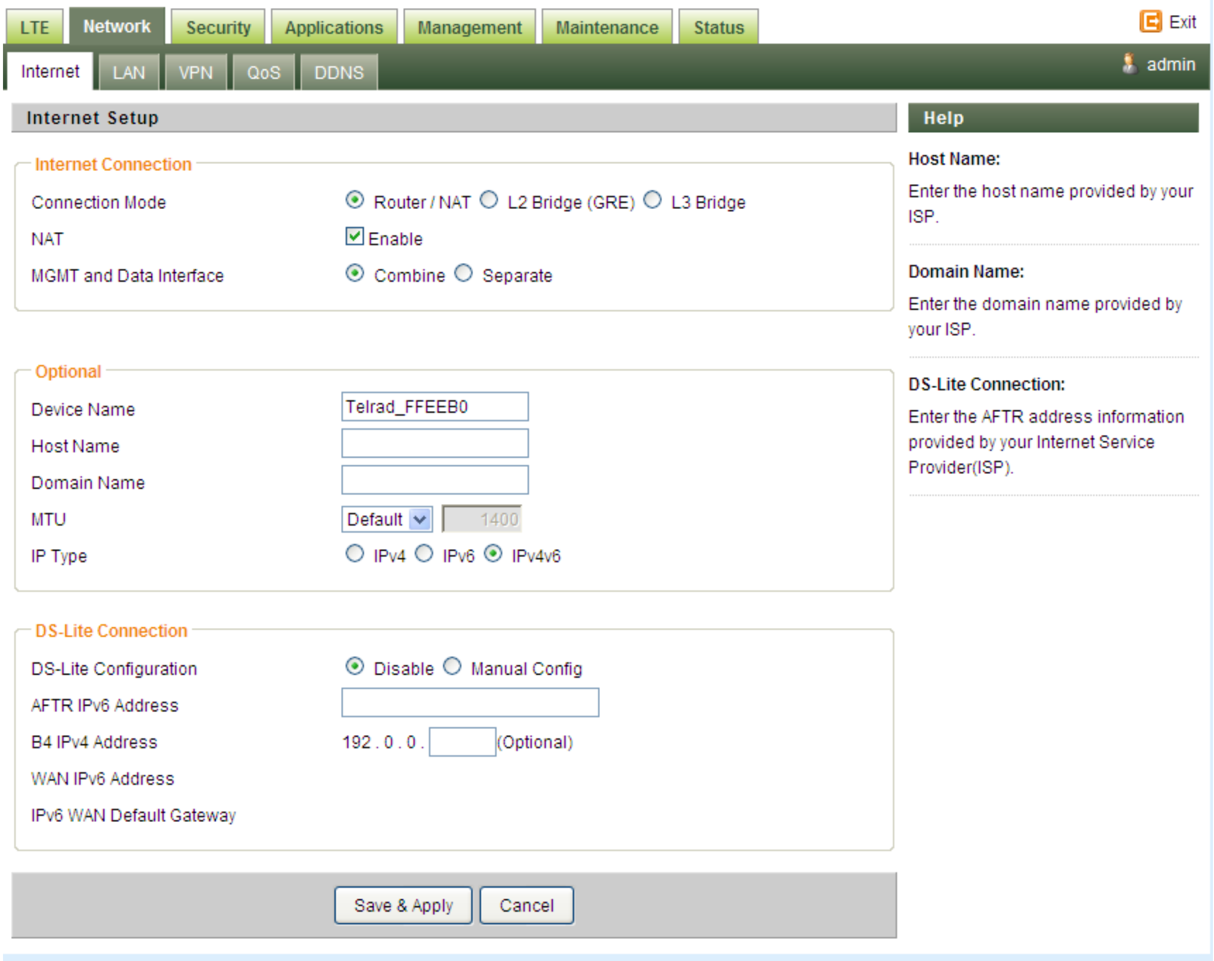
NAT Mode – enables/ disables NAT functionality. Should be checked.

***MGMT and Data* interface** – enables Management and Data (router) functions to use the same ("combined") or different ("separate") WAN-side interfaces. When configured in "separate" mode, multiple PDNs (one for Management and one for Data) must be configured. The default PDN is for Management and additional PDN is for data traffic. For "single PDN" mode, set this parameter to "combined".

Device Name, Host Name and Domain Name are optional parameters, used e.g. in DHCP. Recommended to leave the default values.

MTU – defines the Maximum Transmit Unit (maximum IP-level datagram size) before IP-layer fragmentation. 3GPP recommends use of 1400 bytes (default) to avoid packet drops and fragmentation on S1-U interface between eNB and EPC. Use the default value (1400).

IP Type – defines the IP stack of the CPE. The following values are available – IPv4, IPv6, IPv4v6 (dual stack). Set to IPv4.



Internet Setup

Internet Connection

Connection Mode ● Router / NAT ○ L2 Bridge (GRE) ○ L3 Bridge

NAT ☑ Enable

MGMT and Data Interface ● Combine ○ Separate

Optional

Device Name Telrad_FFEEB0

Host Name

Domain Name

MTU Default 1400

IP Type ○ IPv4 ○ IPv6 ● IPv4v6

DS-Lite Connection

DS-Lite Configuration ● Disable ○ Manual Config

AFTR IPv6 Address

B4 IPv4 Address 192 . 0 . 0 . (Optional)

WAN IPv6 Address

IPv6 WAN Default Gateway

Help

Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

DS-Lite Connection:
Enter the AFTR address information provided by your Internet Service Provider(ISP).

Figure [TBD]: Network/ Internet tab for Router/ NAT mode settings (modify screenshot IP Type to IPv4)

3.8.1.2 L2 bridge mode

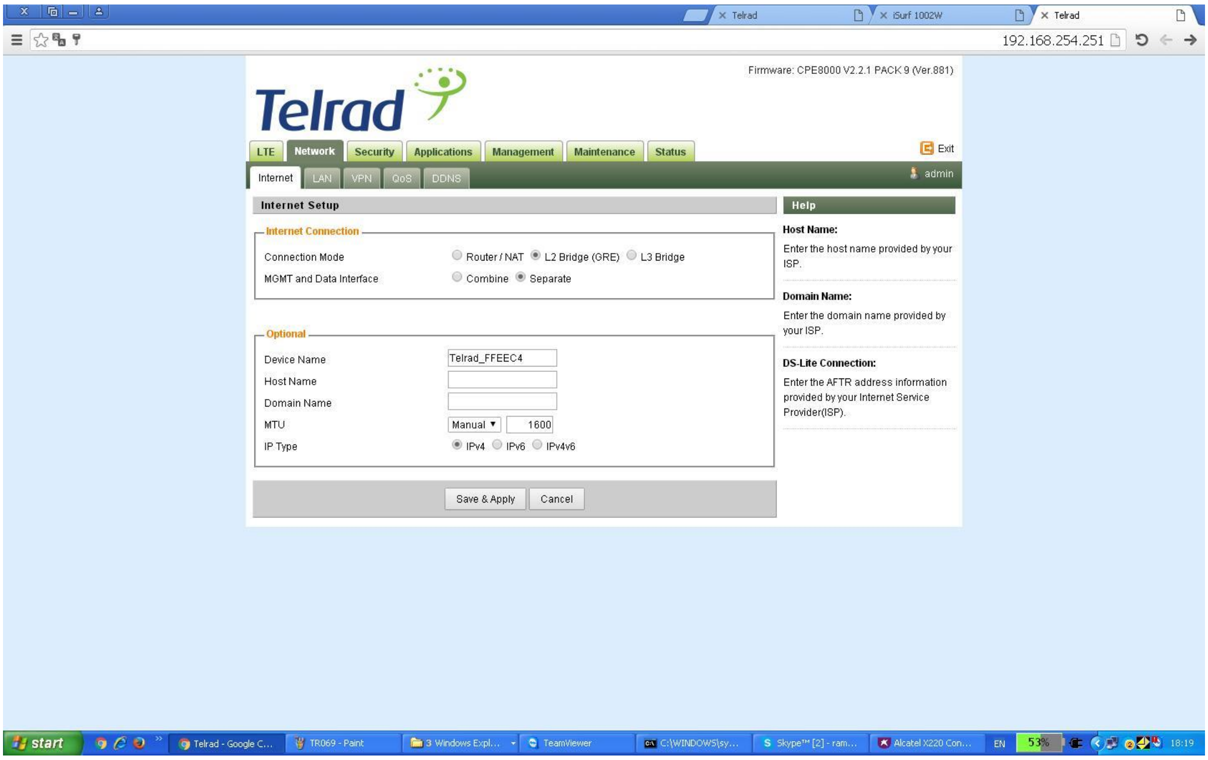
The following parameters should be configured (please, refer to the settings shown in the below screenshot):

Connection Mode – defines the CPE networking mode. Should be set to "L2 Bridge"

***MGMT and Data* interface** – not relevant for the L2 bridge mode. Leave default value "combined".

MTU – defines the Maximum Transmit Unit (maximum IP-level datagram size) before IP-layer fragmentation. For L2 traffic, it should be changed to "Manual" with value "1600" (bytes). The actual supported L2 datagram maximum packet size will be 1576 bytes.

IP Type – defines the IP stack of the CPE. The following values are available – IPv4, IPv6, IPv4v6 (dual stack). Set to IPv4.



Firmware: CPE8000 V2.2.1 PACK 9 (Ver.881)

Internet Setup

Internet Connection

Connection Mode ○ Router / NAT ● L2 Bridge (GRE) ○ L3 Bridge

MGMT and Data Interface ○ Combine ● Separate

Optional

Device Name: Telrad_FFEEC4

Host Name:

Domain Name:

MTU: Manual ▾ 1600

IP Type ● IPv4 ○ IPv6 ○ IPv4v6

Help

Host Name:
Enter the host name provided by your ISP.

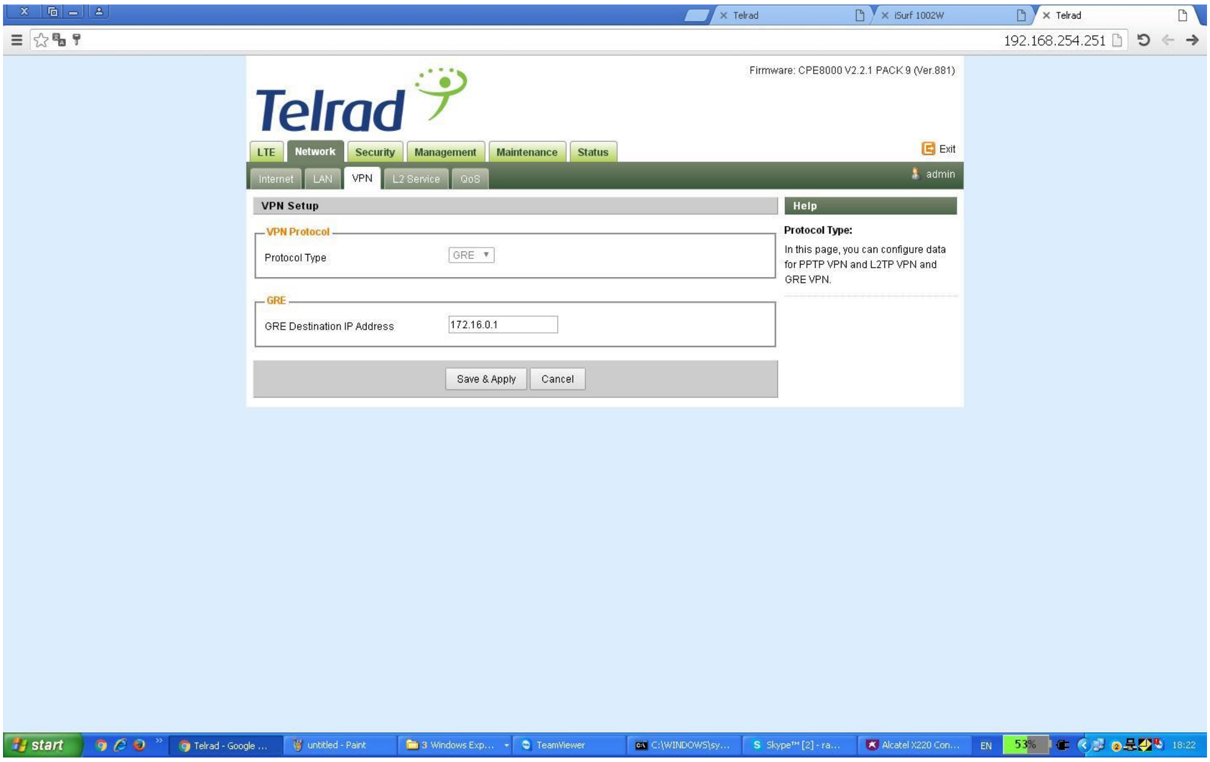
Domain Name:
Enter the domain name provided by your ISP.

DS-Lite Connection:
Enter the AFTR address information provided by your Internet Service Provider(ISP).

Figure [TBD] – Network/ Internet tab for L2 Bridge mode settings

When setting the CPE into the "L2 bridge" mode, verify that TSDF flow endpoint is configured correctly – i.e. matching the BreezeWAY EPC virtual IP ("TSDF L2 end point IP Address" value).

This should be configured in Network/ VPN tab. Verify that "GRE Destination IP address" is matching the BreezeWAY EPC parameter "TSDF L2 end point IP Address" in Networking/ Virtual Network EPC menu.



VPN Setup

VPN Protocol

Protocol Type: GRE

GRE

GRE Destination IP Address: 172.16.0.1

Help

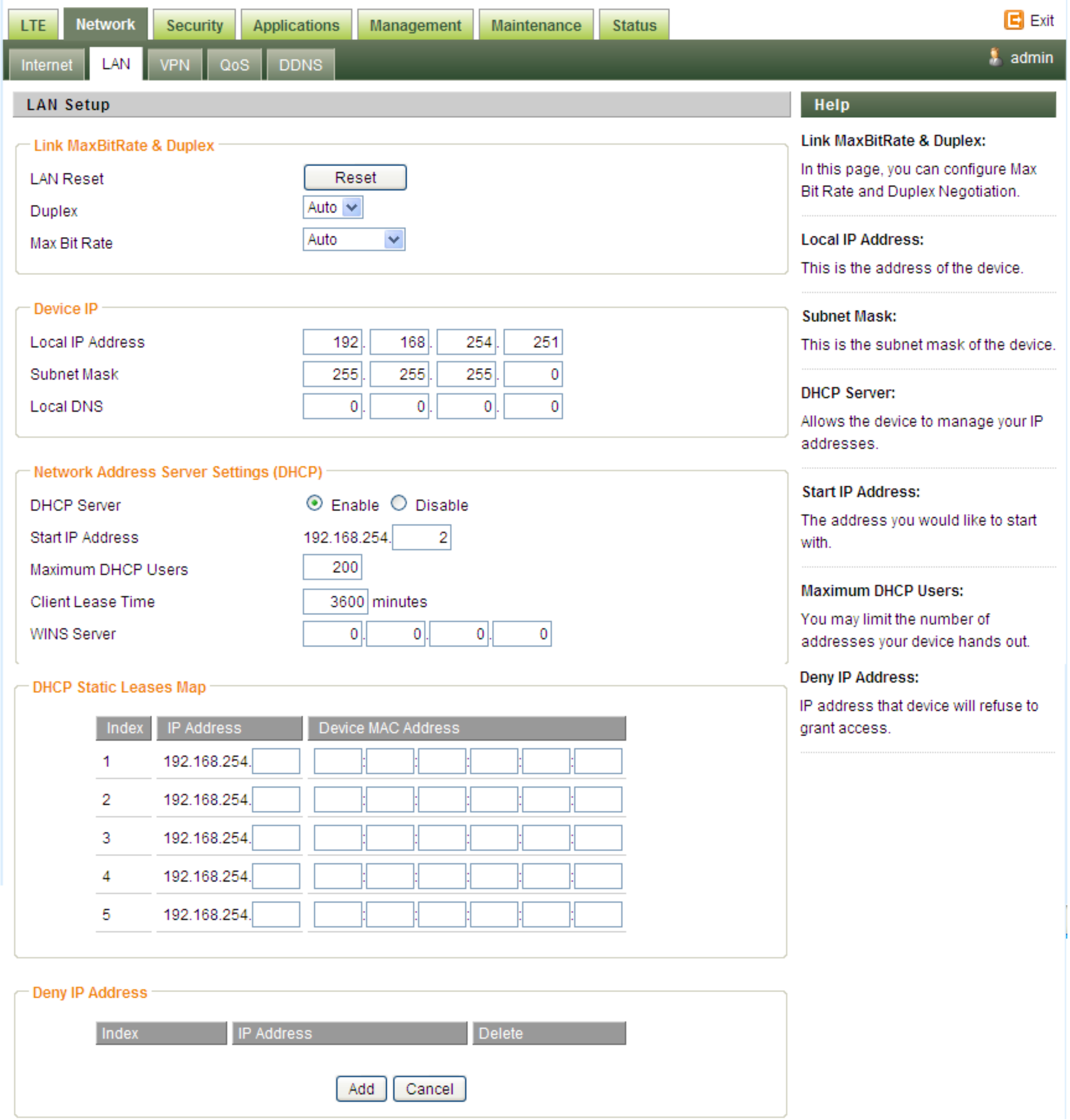
Protocol Type:

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

Figure [TBD] – Network/ VPN tab for L2 Bridge mode settings

3.8.2 LAN Configuration

A user can change LAN-side configuration, including the local management IP Address and DHCP server depending on the networking mode and network environment requirements.



LAN Setup

Link MaxBitRate & Duplex

LAN Reset	Reset
Duplex	Auto
Max Bit Rate	Auto

Device IP

Local IP Address	192 . 168 . 254 . 251
Subnet Mask	255 . 255 . 255 . 0
Local DNS	0 . 0 . 0 . 0

Network Address Server Settings (DHCP)

DHCP Server	● Enable ○ Disable
Start IP Address	192.168.254. 2
Maximum DHCP Users	200
Client Lease Time	3600 minutes
WINS Server	0 . 0 . 0 . 0

DHCP Static Leases Map

Index	IP Address	Device MAC Address
1	192.168.254.	: : : : :
2	192.168.254.	: : : : :
3	192.168.254.	: : : : :
4	192.168.254.	: : : : :
5	192.168.254.	: : : : :

Deny IP Address

Index	IP Address	Delete

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.

Maximum DHCP Users:

You may limit the number of addresses your device hands out.

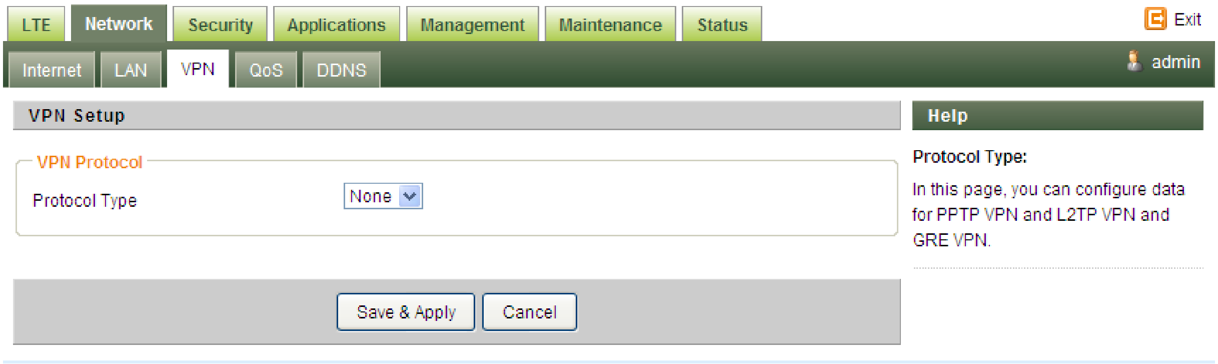
Deny IP Address:

IP address that device will refuse to grant access.

3.8.3 VPN

Enables to configure tunneling/ VPN modes.

The options are PPTP \ L2TP \ GRE. In L2 Bridge mode, GRE is selected automatically.



VPN Setup

VPN Protocol

Protocol Type: None

Help

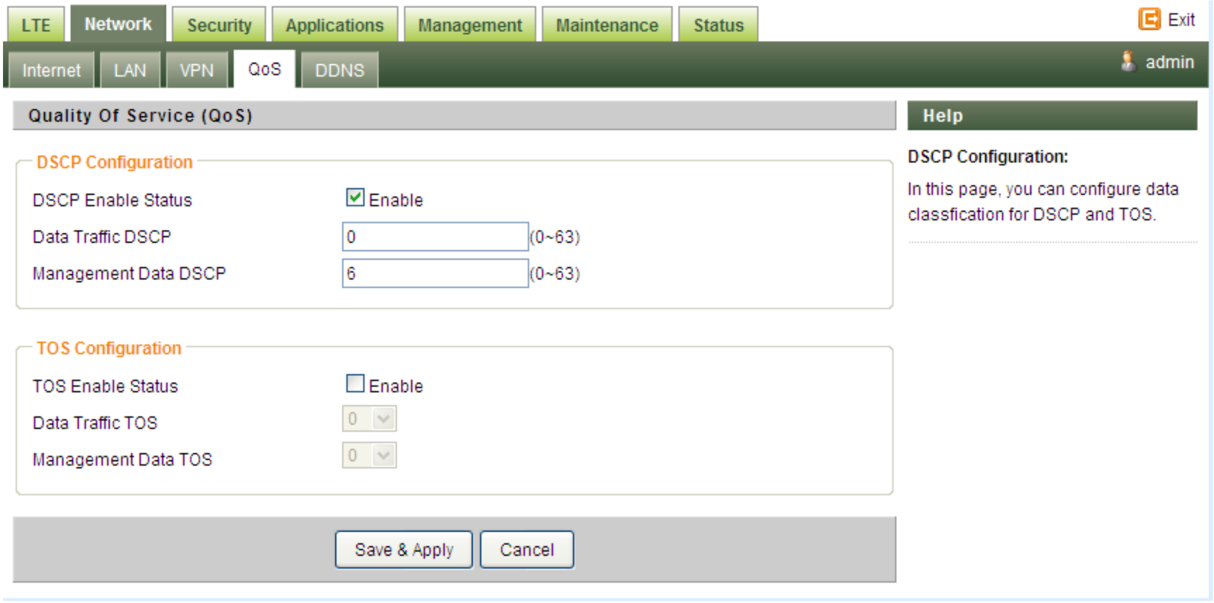
Protocol Type:

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

3.8.4 QoS

This Tab enables setting of DSCP values for CPE Management and user IP traffic in Router/ NAT mode.

The default DSCP value for CPE Management traffic is 6 (can be modified). The DSCP value for data traffic can be set to some specific value (non-zero) or left transparent (0 value).



Quality Of Service (QoS)

DSCP Configuration

DSCP Enable Status ☑ Enable

Data Traffic DSCP 0 (0~63)

Management Data DSCP 6 (0~63)

TOS Configuration

TOS Enable Status □ Enable

Data Traffic TOS 0

Management Data TOS 0

Help

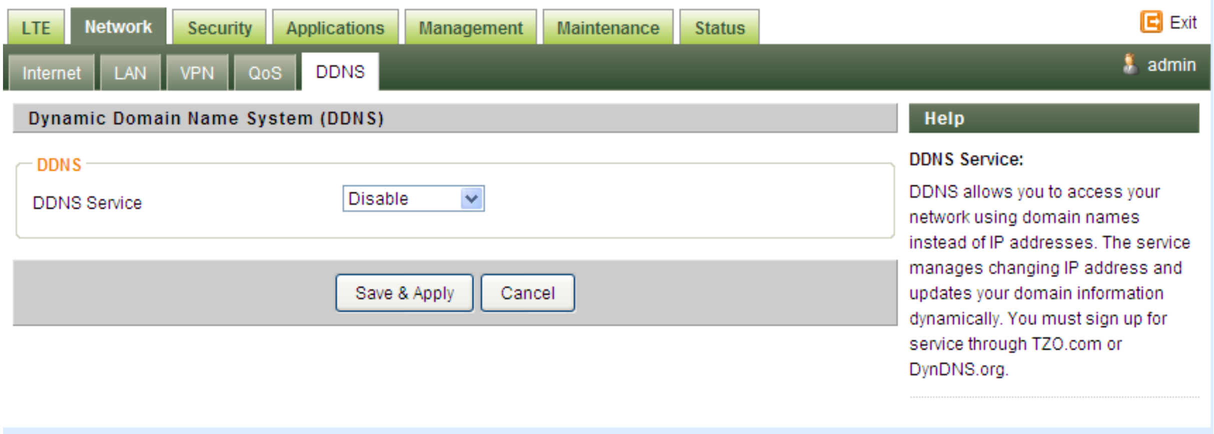
DSCP Configuration:

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

3.8.5 DDNS

Dynamic Domain Name System (DDNS) is a mechanism that can map a pre-defined domain name to a dynamic IP address (updating DNS server with the dynamically assigned IP address). This is useful when IP address for WAN interface is assigned dynamically.

If DDNS is enabled, clients can connect to CPE through “DDNS Host Name”.



Dynamic Domain Name System (DDNS)

DDNS

DDNS Service: Disable

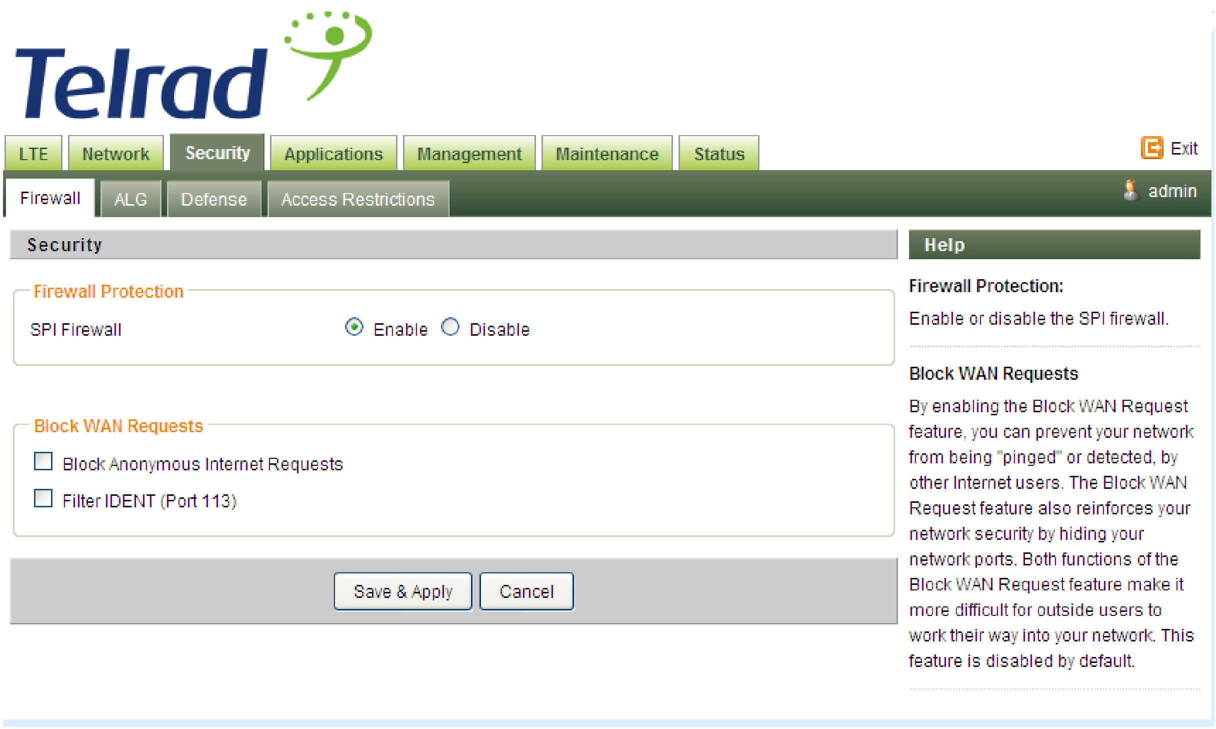
Help

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.

3.9 Security

3.9.1 Firewall



Security

Firewall Protection

SPI Firewall ● Enable ○ Disable

Block WAN Requests

□ Block Anonymous Internet Requests

□ Filter IDENT (Port 113)

Help

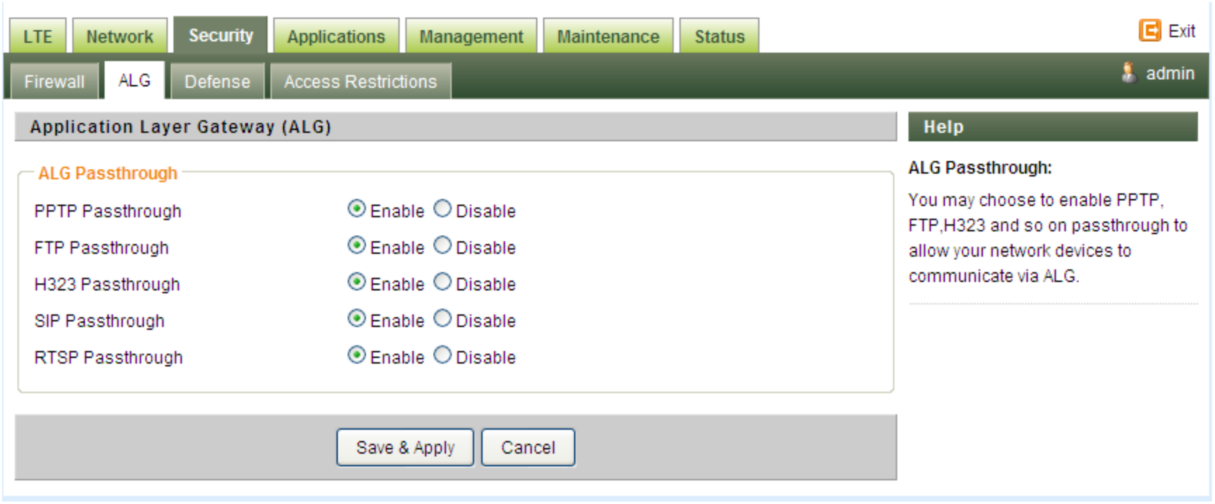
Firewall Protection:

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.

3.9.2 ALG (Application Layer Gateway)



Application Layer Gateway (ALG)

ALG Passthrough

PPTP Passthrough ● Enable ○ Disable

FTP Passthrough ● Enable ○ Disable

H323 Passthrough ● Enable ○ Disable

SIP Passthrough ● Enable ○ Disable

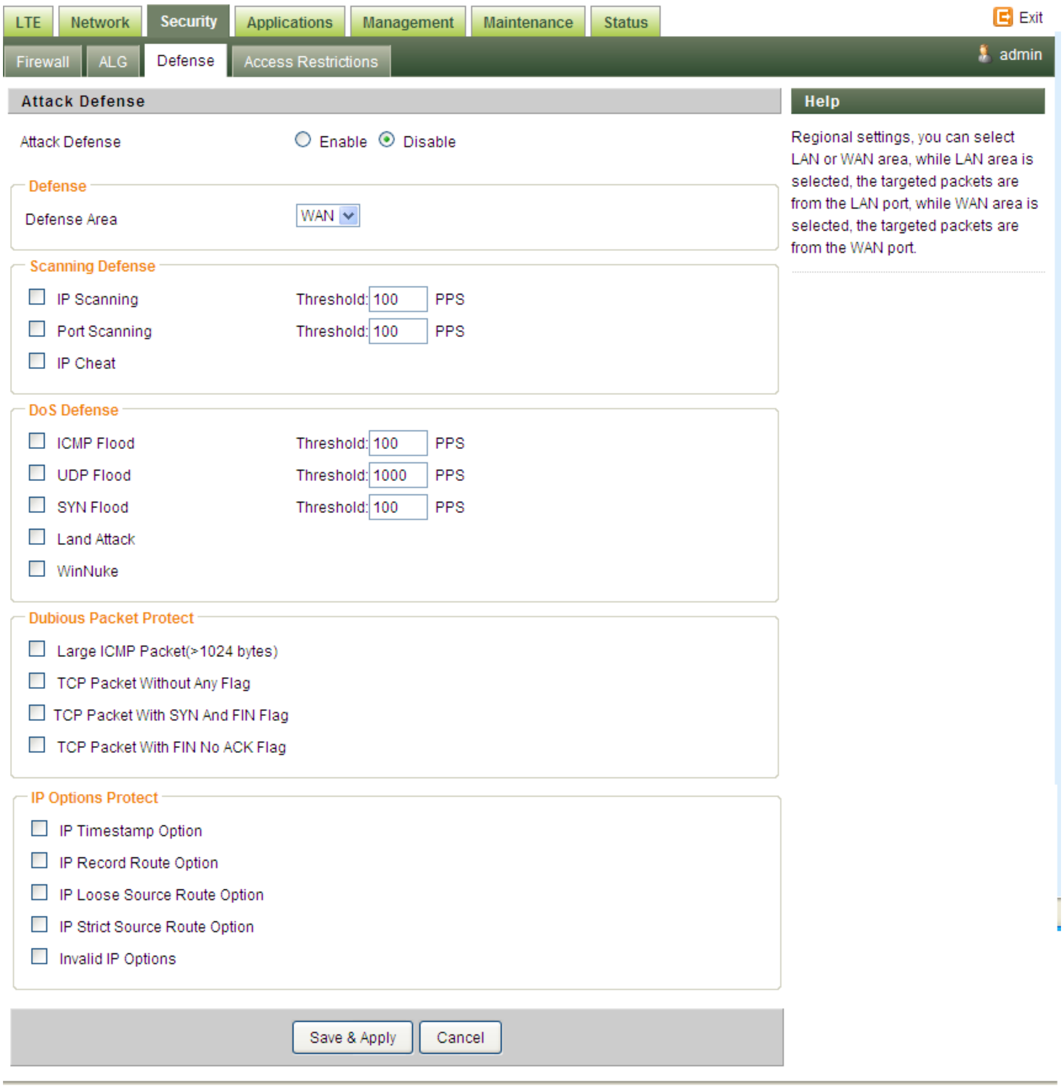
RTSP Passthrough ● Enable ○ Disable

Help

ALG Passthrough:

You may choose to enable PPTP, FTP,H323 and so on passthrough to allow your network devices to communicate via ALG.

3.9.3 Defense



Attack Defense

Attack Defense ○ Enable ● Disable

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

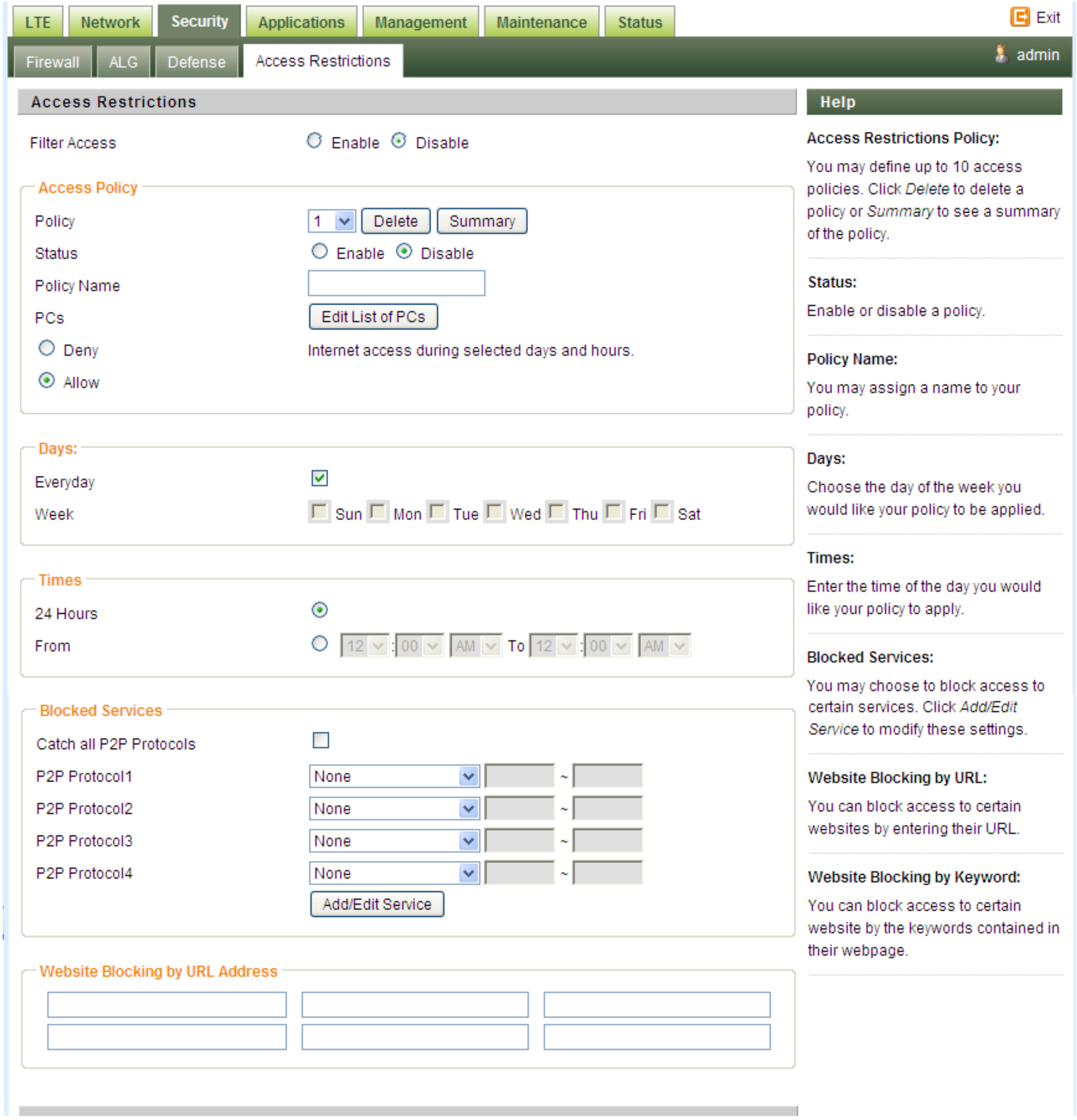
☐ IP Timestamp Option
☐ IP Record Route Option
☐ IP Loose Source Route Option
☐ IP Strict Source Route Option
☐ Invalid IP Options

Help

Regional settings, you can select LAN or WAN area, while LAN area is selected, the targeted packets are from the LAN port, while WAN area is selected, the targeted packets are from the WAN port.

3.9.4 Access restriction

Access Restriction provides a comprehensive way to control the network. First, users can block all the network traffic at certain time. For example, deny all the traffic from 10:00 to 12:00. Second, users can deny devices with certain MAC address accessing the network. Third, users can deny clients accessing certain URL.



Access Restrictions

Filter Access ○ Enable ● Disable

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

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.

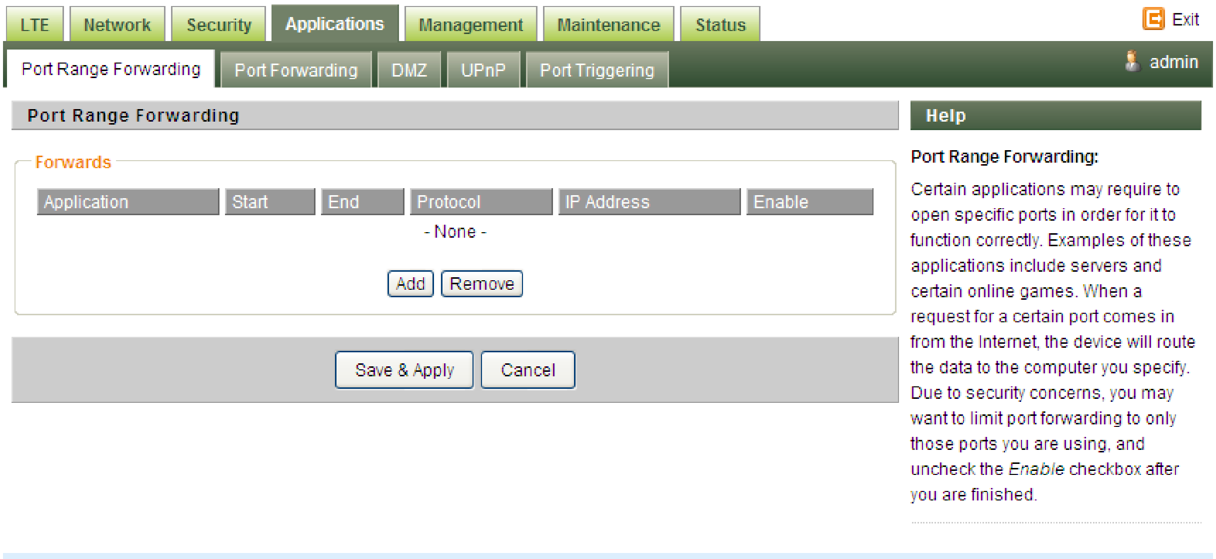
Website Blocking by Keyword:

You can block access to certain website by the keywords contained in their webpage.

3.10 Application

3.10.1 Port range forwarding

Port forwarding forwards the packet according to the port setting in this page. If packets with the port number in these ranges, packets will be forwarded to the designated LAN IP and LAN Port. This function is very useful when a server is set up in LAN side like FTP server.



Port Range Forwarding

Forwards

Application	Start	End	Protocol	IP Address	Enable

- None -

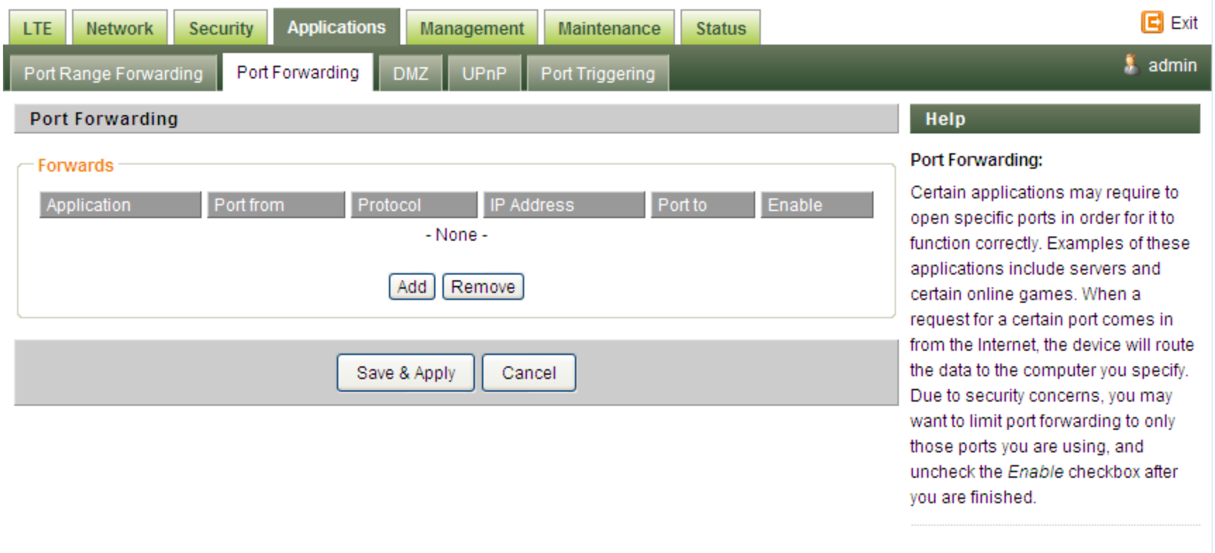
Help

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.

3.10.2 Port forwarding

Similar to Port range forwarding, but not in range.



Port Forwarding

Forwards

Application	Port from	Protocol	IP Address	Port to	Enable

- None -

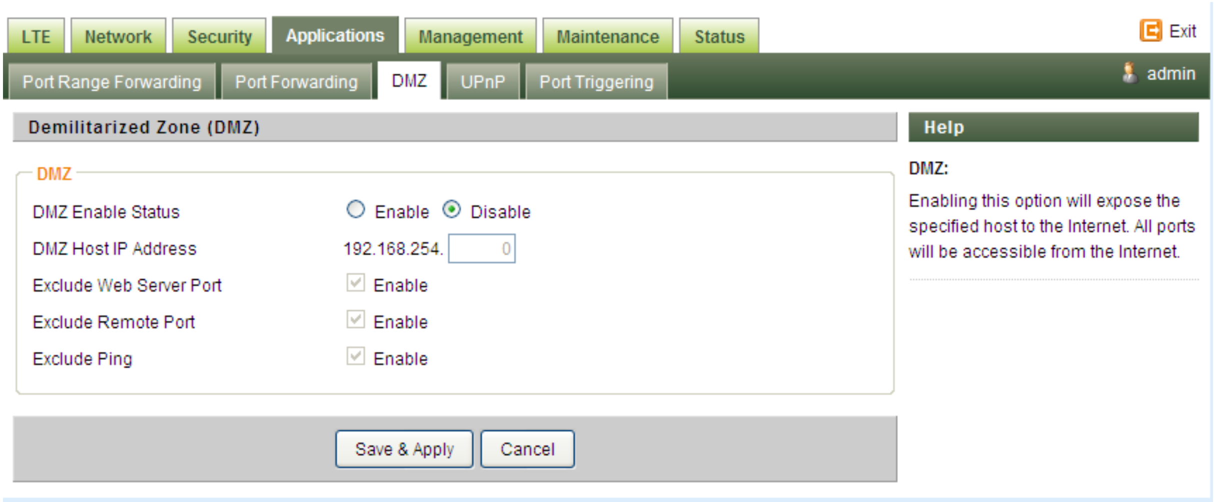
Help

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.

3.10.3 DMZ

All network traffic from WAN is forwarded to this IP address in LAN (default is disable).



Demilitarized Zone (DMZ)

DMZ

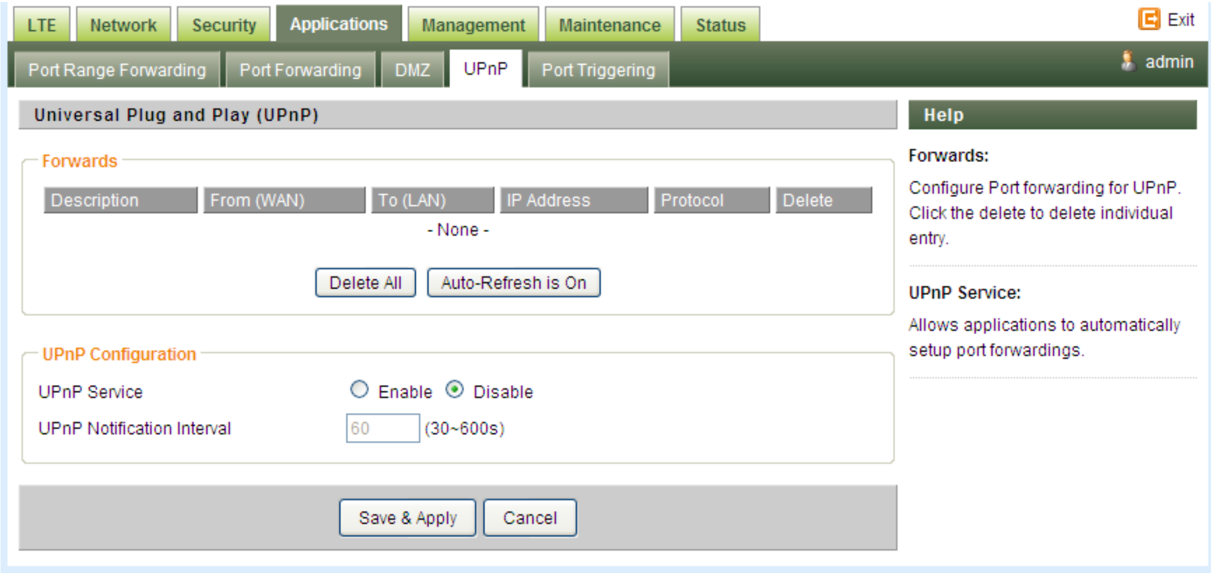
DMZ Enable Status	○ Enable ● Disable
DMZ Host IP Address	192.168.254. 0
Exclude Web Server Port	☑ Enable
Exclude Remote Port	☑ Enable
Exclude Ping	☑ Enable

Help

DMZ:

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

3.10.4 UPnP



Universal Plug and Play (UPnP)

Forwards

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

- None -

UPnP Configuration

UPnP Service	○ Enable ● Disable
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.

3.11.1 Port triggering

The table allows you to configure Port Trigger rules. Port Trigger is a way to automate port forwarding. Outbound traffic on predetermined ports ('trigger port') causes inbound traffic to specific ports (call it port P here) to be dynamically forwarded to the host which uses trigger port. Port P does not open if port triggering is not activated. Click “Add +” button to add a new rule, clicking “Remove” to delete the rule.

3.11.1.1 Application Name

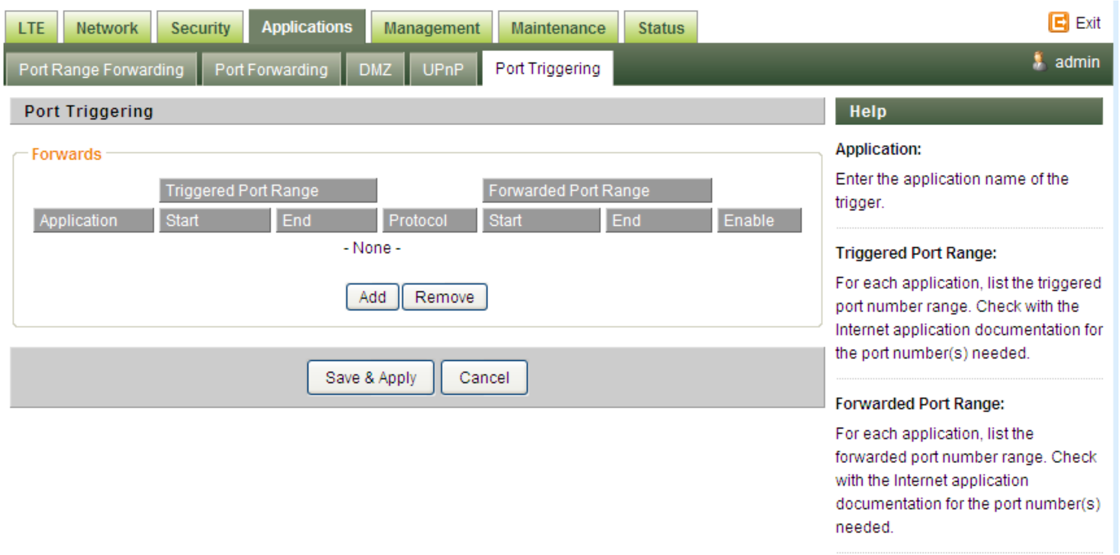
Name of the port trigger rule.

3.11.1.2 Triggered Range

Traffic passing through the port in the triggered range would automatically open the forwarded port in the forwarded range. The ports in the triggered range are LAN ones.

3.11.1.3 Forwarded Range

The ports that would be automatically opened when traffic pass through ports in the triggered range. The ports in the triggered range are WAN port.



Port Triggering

Forwards

	Triggered Port Range			Forwarded Port Range		
Application	Start	End	Protocol	Start	End	Enable
			- None -			

Help

Application:

Enter the application name of the trigger.

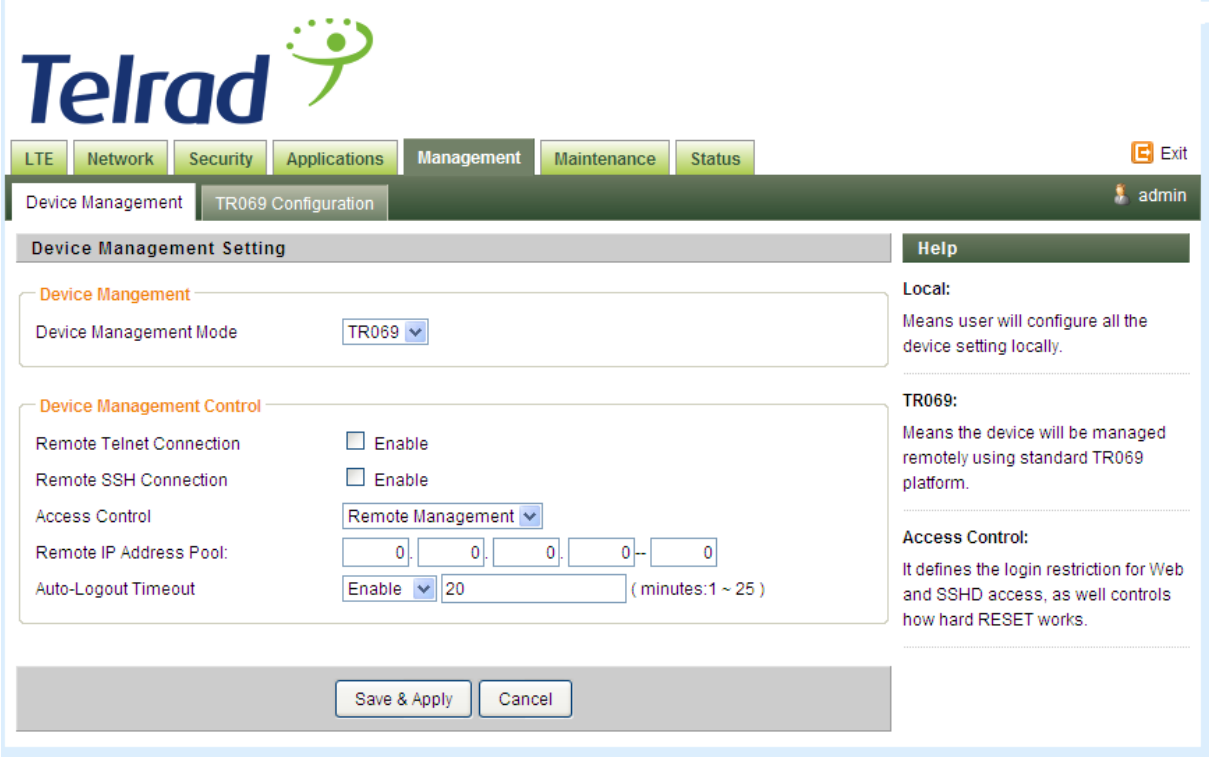
Triggered Port Range:

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.

3.12 Device Management



Device Management Setting

Device Mangement

Device Management Mode: TR069

Device Management Control

Remote Telnet Connection: □ Enable

Remote SSH Connection: □ Enable

Access Control: Remote Management

Remote IP Address Pool: 0 . 0 . 0 . 0 -- 0

Auto-Logout Timeout: Enable 20 (minutes:1 ~ 25)

Help

Local:

Means user will configure all the device setting locally.

TR069:

Means the device will be managed remotely using standard TR069 platform.

Access Control:

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

3.13 System reset and Factory defaults

3.13.1 System Reboot

To reboot the device, press Reboot.

3.13.2 Restore to factory default

To restore to factory default, press Restore.

3.14 Firmware/software upgrade in relation with CBRS

It is important to note that:

1. Firmware/software upgrade are apply in patches in order to not impact RF and other functionality

2. WInnForum compliance is guaranteed by the Domain proxy and therefore no impact in terms of protocol compliance

4 FCC Part 15 Compliance

15.19 (1) Receivers associated with the operation of a licensed radio service, *e.g.,* FM broadcast under part 73 of this chapter, land mobile operation under part 90 of this chapter, etc., shall bear the following statement in a conspicuous location on the device:

This device complies with part 15 of the FCC Rules. Operation is subject to the condition that this device does not cause harmful interference.

15.21 Telrad provided user manual inside the box

15.105 (b) – Pls refer to the safety compliance at the beginning of the document that describe the note that require as part of 15.105

5 FAQ and Troubleshooting

1) My PC cannot connect to the CPE.

- **Re-plug the PC Ethernet cable and check if the PC LAN connection is up or showing activity.**
- **Check if the PoE power adapter LED is on. If it is not, check the power cord and make sure it is connected properly. Also verify that the AC power supply is available.**
- **If the PC LAN shows no activity and PoE adapter LED is off but the power cord is connected properly and there is AC supply, then it is likely the PoE adapter is damaged. Please contact distributor to obtain replacement part.**

2) My PC cannot acquire IP from the CPE.

- **First check if the NIC is up and working properly. Then check the PC NIC configuration** and make sure the DHCP is enabled.

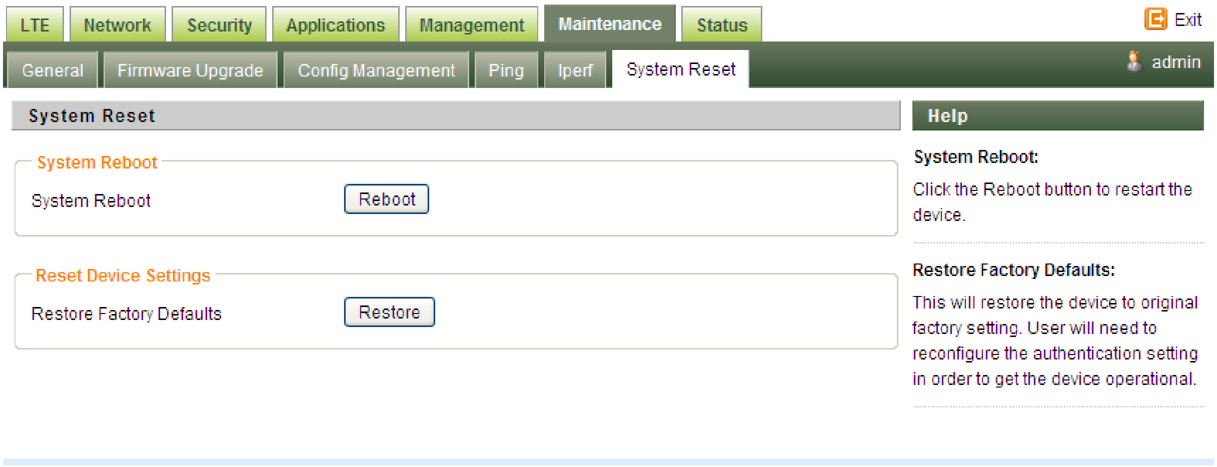
- Open the MS-DOS window, enter “ipconfig /release” and “ipconfig /renew” commands and see if PC can obtain IP correctly.
- If the problem persists, please contact the operator or distributor for further diagnose.

3) My CPE networking is not working properly.

- You may want to check if the LTE connection is up and running properly. You can do this by login the WEB GUI and check the Interface Info page.
- You may want to perform a factory reset and see if the problem is being corrected. You can do this by log into the WEB GUI using “admin” password and perform restore the unit to default factory setting.
- If the problem cannot be corrected by factory reset, please contact the operator or distributor for further diagnose.

4) I forgot the login password and like to reset the unit to factory default.

- Please contact the operator or distributor and give them the IMEI of the unit. The operator or distributor can issue you a RESET password for you to enter in the WEB login window.
- After the unit is reset to factory default, you can login using the default password.



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.