LTE Outdoor CPE9000

System Manual

October 2017

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 OROTHERWISE, 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).

Content

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

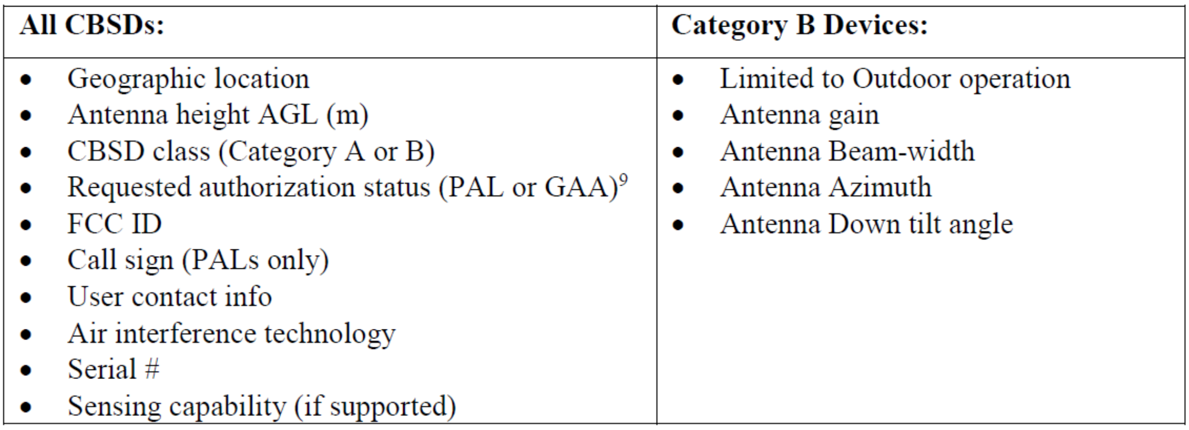
(a) TELRAD NETWORKS SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), 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).

USA CBRS Band Category B device

The CPE9000 requires installation by a CPI (Certified Professional Installer) as defined in Section 96.39 and 96.45

of FCC part 96 requirements. The Compact is Classified as a Category B CBSD which requires the following info be recorded and uploaded as part of the CPI process per section 96.45



All CBSDs:	Category B Devices:
• Geographic location • Antenna height AGL (m) • CBSD class (Category A or B) • Requested authorization status (PAL or GAA)[9] • FCC ID • Call sign (PALs only) • User contact info • Air interference technology • Serial # • Sensing capability (if supported)	• Limited to Outdoor operation • Antenna gain • Antenna Beam-width • Antenna Azimuth • Antenna Down tilt angle

The CPE9000 (Category B CBSD)) must report to a SAS to register and obtain spectrum grants per FCC part 96. Local administration should be executed through the domain proxy and all freq, bandwidth and power adjustments must be handled in coordination with the SAS and grant process. The device is not authorized to transmit without a grant and ships with TX disabled. It is the responsibility of the CPI to populate the CPI database and obtain a grant before the Device is permitted to Transmit. Location will be recorded by the professional installer and reported to the CPI database along with the other parameters listed in the above table

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 50cm between the radiator and your body.

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

About this Guide

This document provides information and procedures on the installation and configuration of Telrad Outdoor CPE9000. You could utilize the information in this guide to set up your device.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures. In addition, you should be familiar with the following:

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating system and troubleshooting knowledge. LTE CPE has a web GUI which supports http/https protocol; it could be used to configure the CPE settings through the web browser by user’s PC. Please refer to the following pages for more detail.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

!!!	Very important information. Failure to observe this may result in damage.
!	Important information that should be observed.
i	Additional information that may be helpful but not required.
bold	Menu commands, buttons and input fields are displayed in bold

Introduction

CPE9000 Product Highlights

- TD-LTE – 3GPP Release 10, UE Category 6
- Supports wired (LAN port)
- High gain 15dBi embedded Antenna
- Device Management – Web, TR69 & SNMP
- IP67 environmental rating – fully ruggedized, suitable for the harshest outdoor deployment scenarios

CPE9000 Outdoor specification

Radio specification

Standard Compliance	3GPP Rev. 9/10, UE Cat 6
Duplex Mode	TDD
Frequency Bands	B48
Channel bandwidth (MHz)	10, 20
Modulation	DL: MCS1 - MCS28 (QPSK, 16QAM, 64QAM) UL: MCS1 – MCS28 (QPSK, 16QAM, 64QAM) Uplink 64QAM with Telrad eNodeB
L1	MIMO TM1, TM2, TM3, TM4, TM8
L2 & L3	Multiple APN PLMN and Cell Selection
Authentication	USIM and SIM function
QoS	Non-GBR, GBR
MTU Size	Layer 2 - 1,600 bytes Layer 3 – 1,500 bytes

Outdoor CPE 9000 –Electrical / Physical Specifications

Dimensions (HxWxD)	260 x 250 x 80 mm
Weight	1.2 Kg | 2.6 lbs
Physical Interface	LAN - 1x100M/1Gb Base-T

Maximum Transmit Power	23 dBm
Antenna	1TX/2RX, 15dBi
Power Source	PoE
Environmental	IP67 - withstands harsh weather and outdoor environments
Operating Temperature	-40° to 55° C | -40° to 131° F
Humidity	5% to 95% non-condensing
ESD Rating	+/-15KV
Power Consumption	6.7W
Regulatory Compliance	2.X GHz: • CE: 2.3-2.4 GHz and 2.5-2.7 GHz • FCC: 2.5-2.7 GHz 3.X GHz: • CE: 3.4-3.8 GHz • FCC: 3.55-3.7 GHz* requires domain proxy , only B48 supported • IC: 3.475-3.7 GHz

PoE Adapter Specification

Power Source	100~240VAC
Output Power (PoE)	56V / 0.45A
User Interfaces	Data only : 1xLAN RJ45
Maximum cable length	100m

Product Package

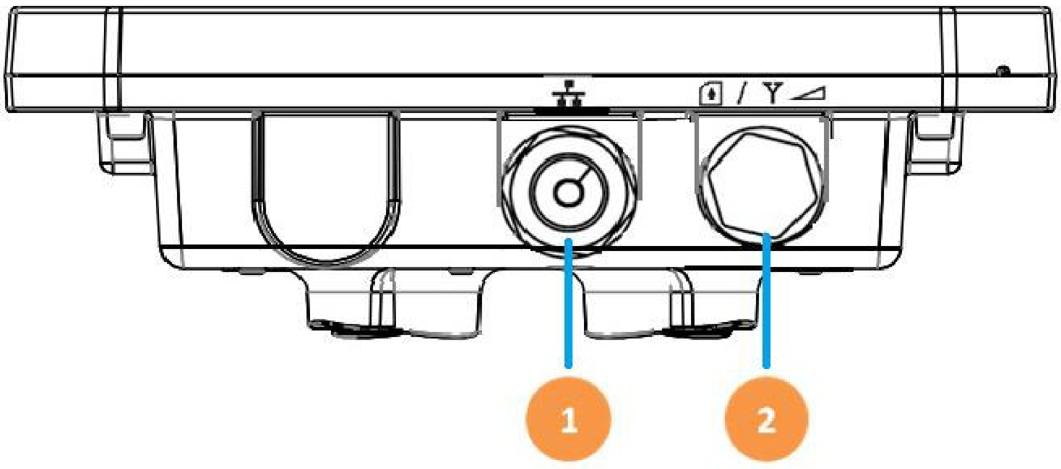
	Item	Qty
1	LTE Outdoor CPE	1
2	Quick Installation Guide	1
3	PoE Adapter	1
4	Power Plug	1
5	Mounting Kit	1

!	If any item of mentioned above is missing or damaged, please contact our customer support immediately.

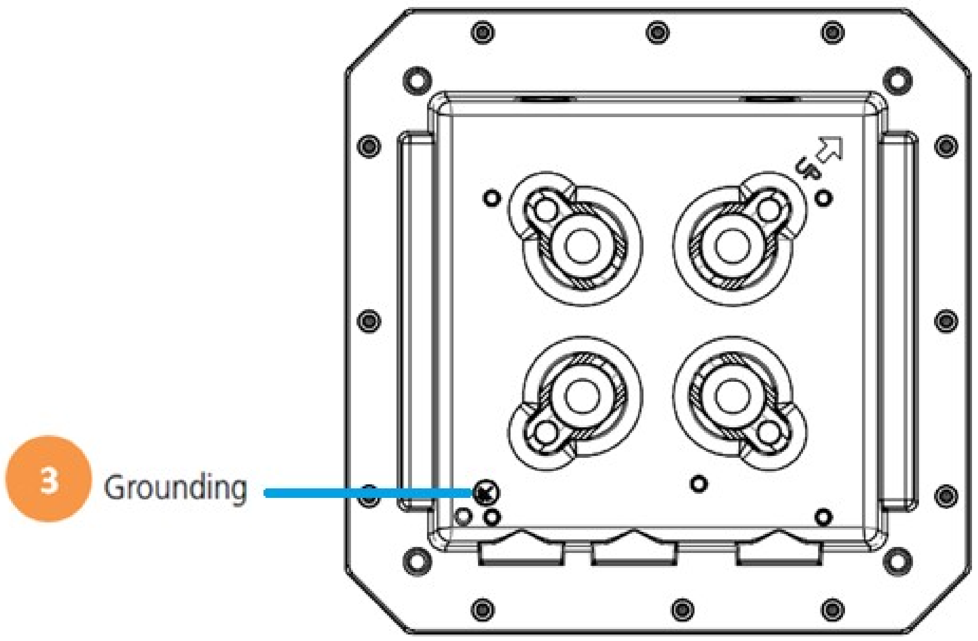
Connectors

The Outdoor LTE CPE CPE9000 has following connectors (from left to right):

1. One RJ-45 connector for connecting to the PoE adaptor.
2. LED indicator inside and SIM card slot for inserting SIM card.
3. A grounding screw on the rear panel.



The Grounding screw (marked ₸) is located on the rear panel of the ODU.



LED Indicators

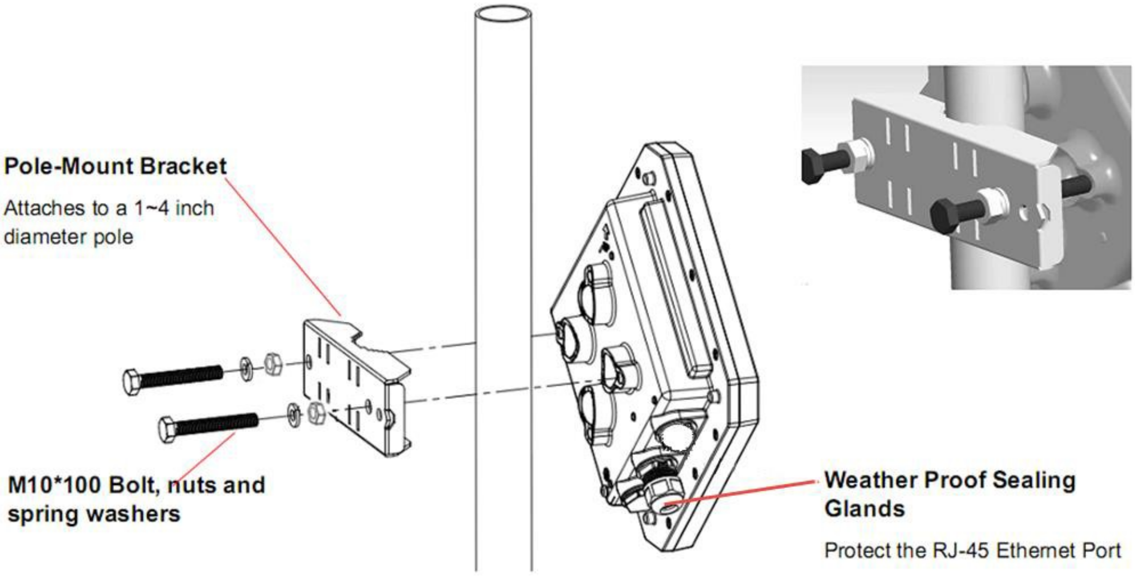
LED name	Location	Color	LED Behavior	Status Indication
LED List	🔵🟡🟢 🔴🟡🟢			
MAIN power	🔵○○ ○○○	**Blue**	**ON**	Power On
			OFF	Power Off
Ethernet status	○🟡○ ○○○	**Yellow**	**Steady ON**	Detect Ethernet Device Connected
			Blinking	Detect IAD
			OFF	No Ethernet action

SIM status	○○🟢 ○○○	**Green**	**Steady ON**	SIM Detected
			Blinking when On-hook	PUK / PIN Code
			OFF	No SIM Detected
LTE Status LED :			When CPE is power on, each LED indicates each link status	
Link Status 1	○○○ 🔴○○	**Red**	**Steady ON**	SINR < 9dB
Link Status 2	○○○ 🔴🟡○	**Red/ Yellow**	**Steady ON**	9dB $\leq$ SINR < 16dB
Link Status 3	○○○ 🔴🟡🟢	**Red/ Yellow/ Green**	**Steady ON**	16dB < SINR

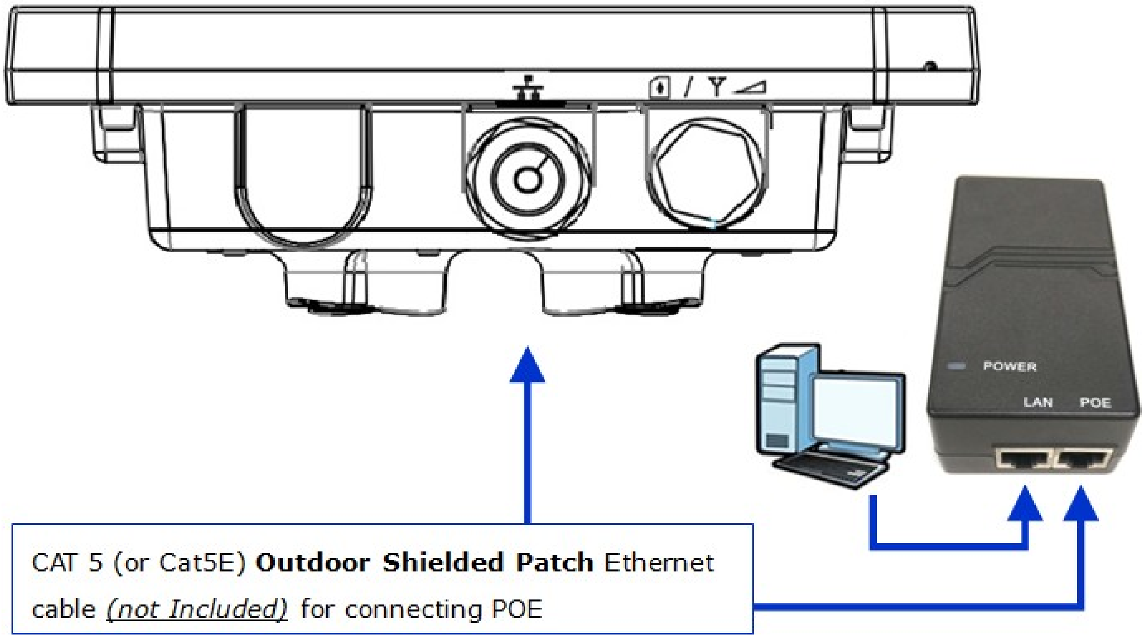
Installation

- **Selecting a Location:** LTE Outdoor CPE should be pole-mounted outdoors and aligned so its antenna faces the nearest LTE eNodeB. When selecting a suitable location for the unit, consider these guidelines:
  - Place LTE Outdoor CPE as high as possible to achieve the best possible link quality.
  - Place the LTE Outdoor CPE away from power and telephone lines.
  - Avoid placing LTE Outdoor CPE too close to any metallic reflective surfaces.
  - Be sure to ground LTE Outdoor CPE with an appropriate grounding wire (not included) by attaching it to the grounding screw on the unit and to a goodground connection.

- **Mounting the ODU:** Mount LTE Outdoor CPE on a 1”-4” pole using the supplied kit, or the optional tilt accessory.
    - **Using the clamp**
        1. Thread the M10*100mm bolt through a spring washer, flat washer and the bracket holes.
        2. With the connector facing downward, attaché LTE Outdoor CPE to a 1”-4” pole.
        3. Attach the bracket to the other side of the pole.
        4. Thread the M10*100mm bolts through both holes on either side, and tighten the nuts.


Pole-Mount Bracket
Attaches to a 1~4 inch diameter pole
M10*100 Bolt, nuts and spring washers
Weather Proof Sealing Glands
Protect the RJ-45 Ethernet Port

Connecting the Cables

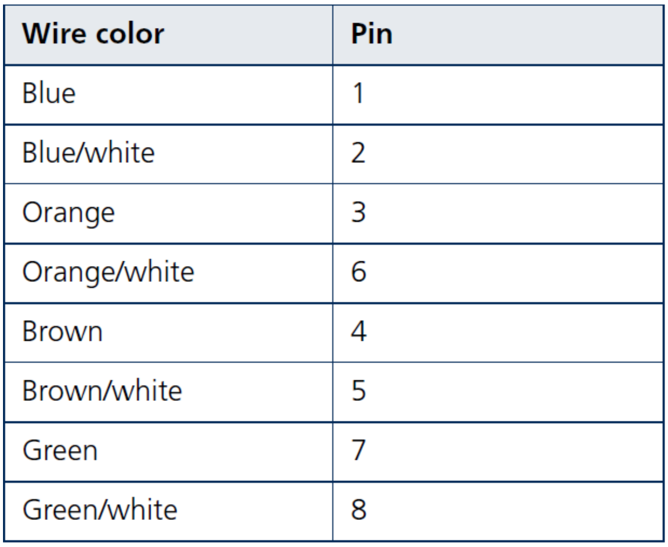


CAT 5 (or Cat5E) **Outdoor Shielded Patch** Ethernet cable *(not Included)* for connecting POE

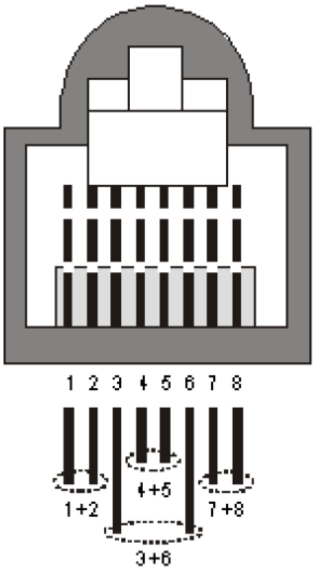
- **Outdoor Connection:** Connect a grounding cable between the Ground terminal of the LTE outdoor CPE and a good ground connection.
- **Preparing and connecting the cable:** Use only UTP-FTP 4x2x24AWG CAT. 5E outdoor cable from an approved manufacturer. The cable provides pin-to-pin connection on both ends.

  1. **Prepare the cable:** Use a crimp too for RJ-45 connectors to prepare the wires. Insert them into the appropriate pins and use the tool to crimp the connector. Make sure to do the following:
     - Remove as small a length as possible of the external jacket. Verify that the external jacket is well inside the sealing cover when connected to the unit, to ensure good sealing.
     - Pull back the shield drain wire before inserting the cable into the RJ-45 connector, to ensure a good connection with the connector's shield after crimping.

The following figure shows the required wire pair connections. The color codes used in standard cables supplied by the manufacturer are as listed in the table.

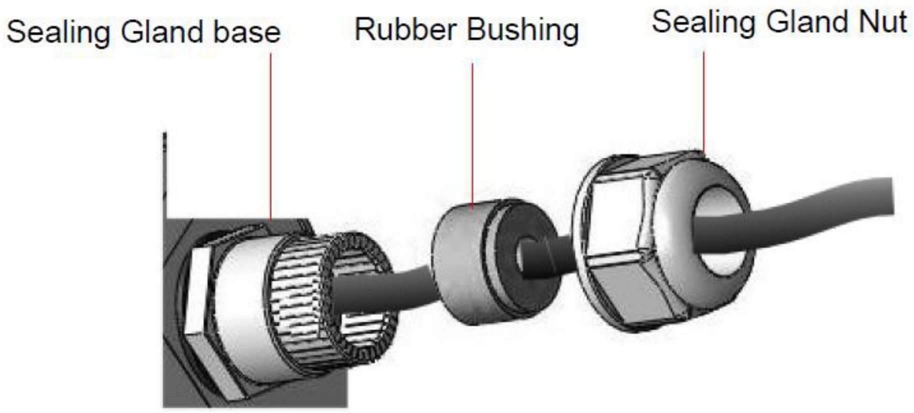


Wire color	Pin
Blue	1
Blue/white	2
Orange	3
Orange/white	6
Brown	4
Brown/white	5
Green	7
Green/white	8



2. **Connect the cable**

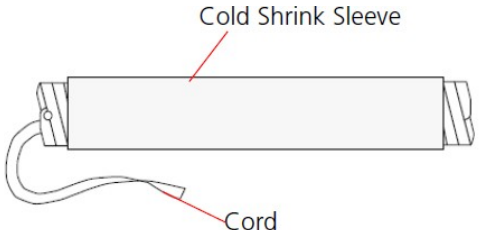
- Remove the sealing cable gland plug from the gland nut.
- Open the sealing gland nut and remove it. Don not disassembles the gland base from the bracket.
- Insert the cable into the sealing gland base and connect it to the RJ-45 connector at the bottom of the CPE. Make sure the connector is completely inserted and tightened.
- Insert the rubber bushing on the cable into the gland base.

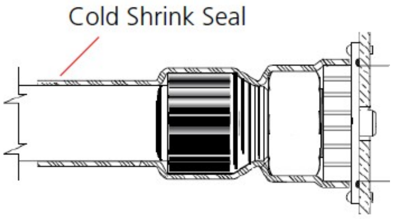


- Tighten the gland nut. Use the dedicated tool for fastening the sealing glands.

3. **Seal the connector**

   - Attach the mastic tape (Scotchfil™ Electrical Insulation Putty) and wrap it around the connector butting up against the connector. Do not over stretch.
   - Squeeze to tighten the mastic sealer. Make sure there are no air bubbles.
   - Slide the cold shrink sleeve on top of the connector. Make sure that the sleeve covers both cable connector and unit connector.

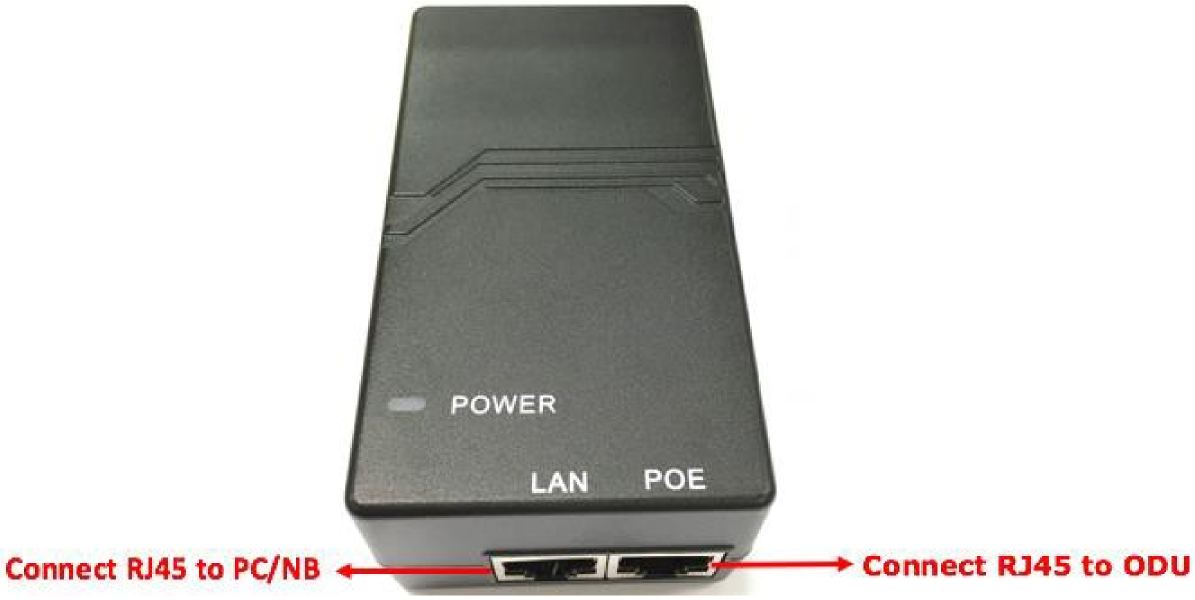




   - Pull the cord slowly to shrink the sleeve.

- **Indoor Connection**

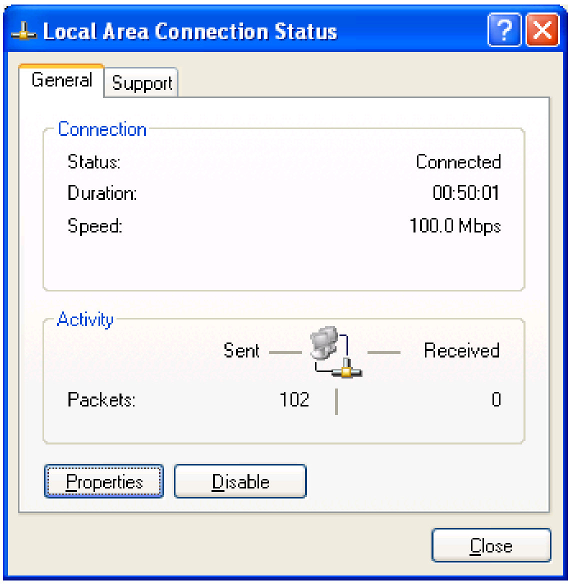
  1. It is assumed that the RJ-45 cables are already connected to the LTE outdoor CPE. Assemble an RJ-45 connector with a protective cover on the other end of the LTE outdoor CPE cable.
  2. Connect the other end of the cable from ODU to the PoE adaptor which labeled **“POE”**
  3. Connect RJ45 cable from PoE adaptor which label **“LAN”** to a PC/NB/Hub/Switch.



!	Use **ONLY** the PoE adaptor which supplied with the ODU. Otherwise, LTE Outdoor CPE may be damaged.

4. Plug in PoE into power line. The device will start the booting process. Please wait for a minute to let the booting process complete.

5. Select **Local Area Connection Status** from Windows task bar and click **Properties**.



Connection

Status: Connected

Duration: 00:50:01

Speed: 100.0 Mbps

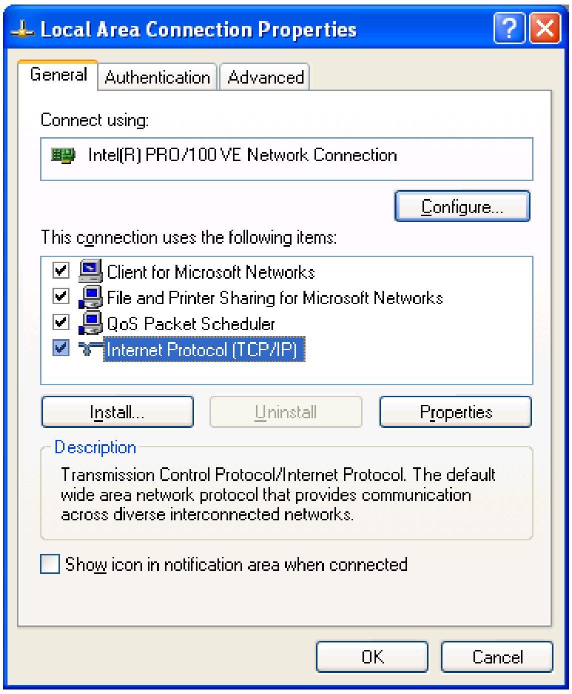
Activity

Sent — Received

Packets: 102 | 0

Local Area Connection Status

6. Double click on the **Internet Protocol (TCP/IP).**



Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks

☑ File and Printer Sharing for Microsoft Networks

☑ QoS Packet Scheduler

☑ Internet Protocol (TCP/IP)

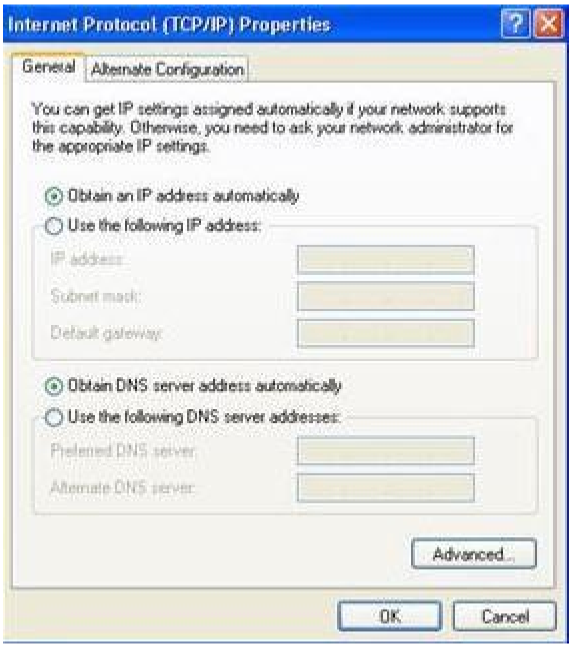
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

Local Area Connection Properties

7. Select **Obtain an IP address automatically / Obtain DNS server address automatically** and click **OK.**


Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

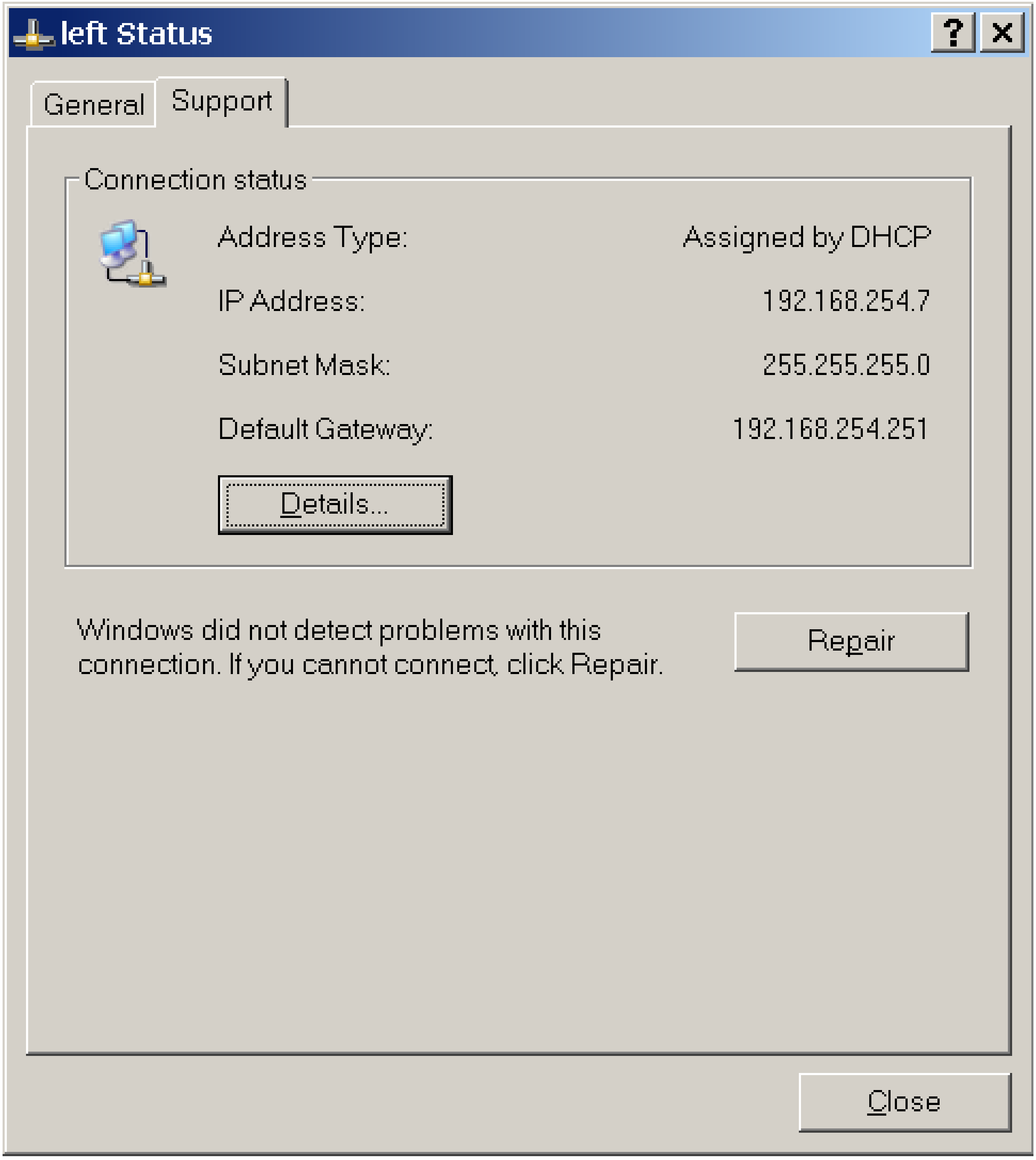
○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

Internet Protocol (TCP/IP) Properties

8. By now, the device should have got IP address from your DHCP server.



Connection status

Address Type: Assigned by DHCP

IP Address: 192.168.254.7

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.254.251

Windows did not detect problems with this connection. If you cannot connect, click Repair.

9. How to verify CPE has a successful connection to the LTE eNodeB. This can be verified by observing the signal strength LEDs (Please refer **LED Indications** section in **Introduction** chapter of this manual to find the location of these LEDs on the

device). At least one of these LEDs glowing continuously is an indication of successful connection to the Base Station. Now you can start browsing the Internet.

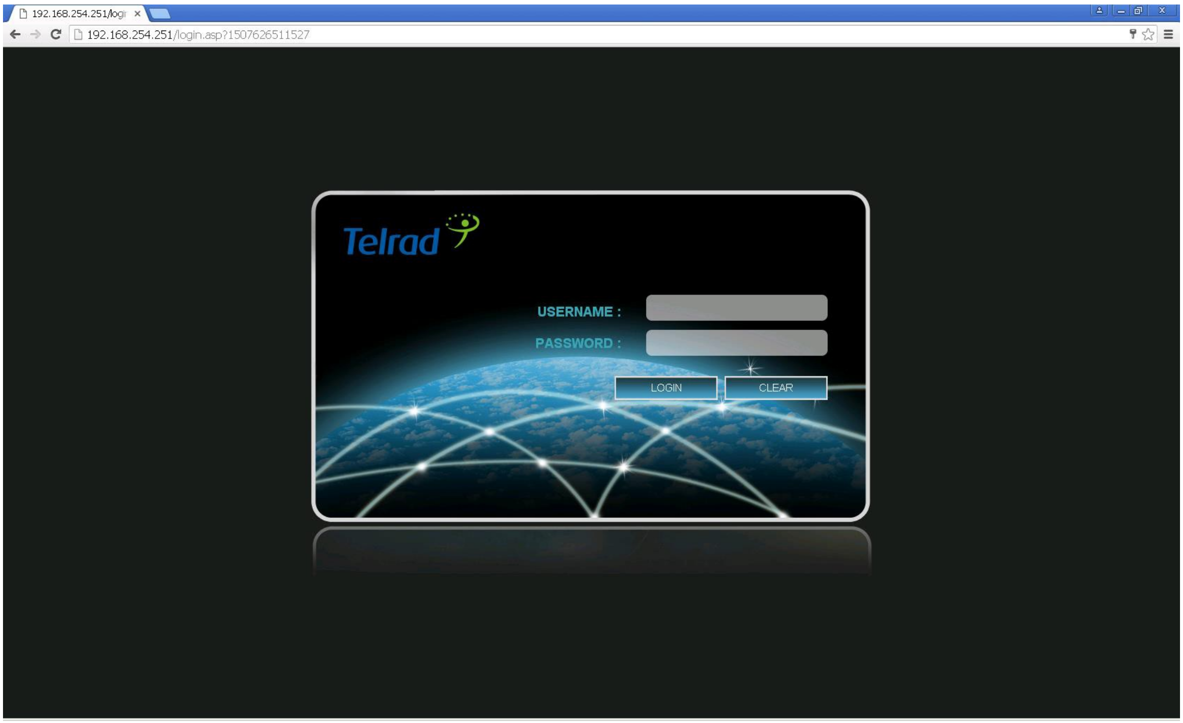
Web Interface

Login to Web-GUI

Users' devices are assumed in CPE LAN side. Please follow the steps below to configure your device through the web interface:

Step1: Open the Web browser (Ex: Internet Explorer, Firefox or Chrome) and enter the default IP address of CPE, which is : **http://192.168.254.251**

Web browser

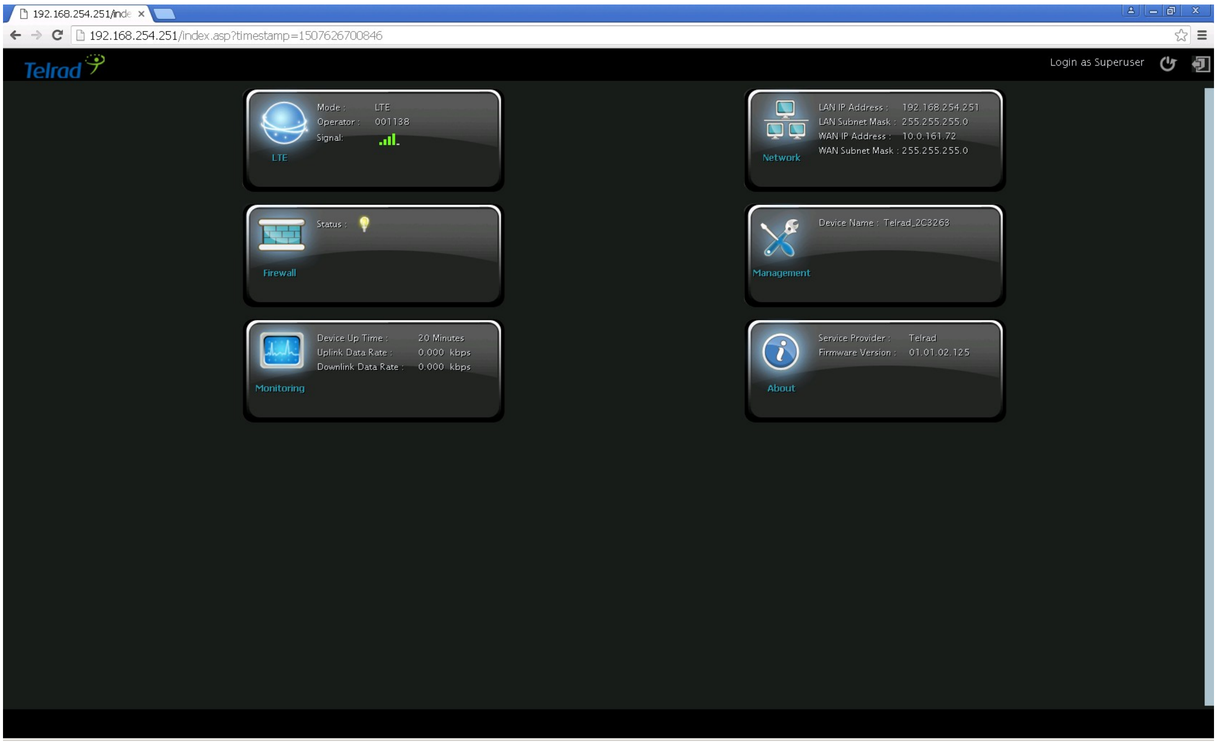


Step2: Enter USERNAME/PASSWORD to access the web management interface. The default is **operator / Telrad4G** for operator and admin / admin for end-user.

Web management interface

Step3: After successful login, you can see “Brief Summary Page”. Brief Summary Page is composed of many blocks and each block contains its own feature. A concise description is presented in the block. Users can click on it to enter “Detailed Configuration Page” to see the complete settings or tweak the configuration.

Detailed information about this page will be stated below.



192.168.254.251/index.asp?timestamp=1507626700846

Login as Superuser

Mode : LTE
Operator : 001138
Signal:

LAN IP Address : 192.168.254.251
LAN Subnet Mask : 255.255.255.0
WAN IP Address : 10.0.161.72
WAN Subnet Mask : 255.255.255.0

Status :

Device Name : Telrad_2C3263

Device Up Time : 20 Minutes
Uplink Data Rate : 0.000 kbps
Downlink Data Rate : 0.000 kbps

Service Provider : Telrad
Firmware Version : 01.01.02.125

Brief Summary Page

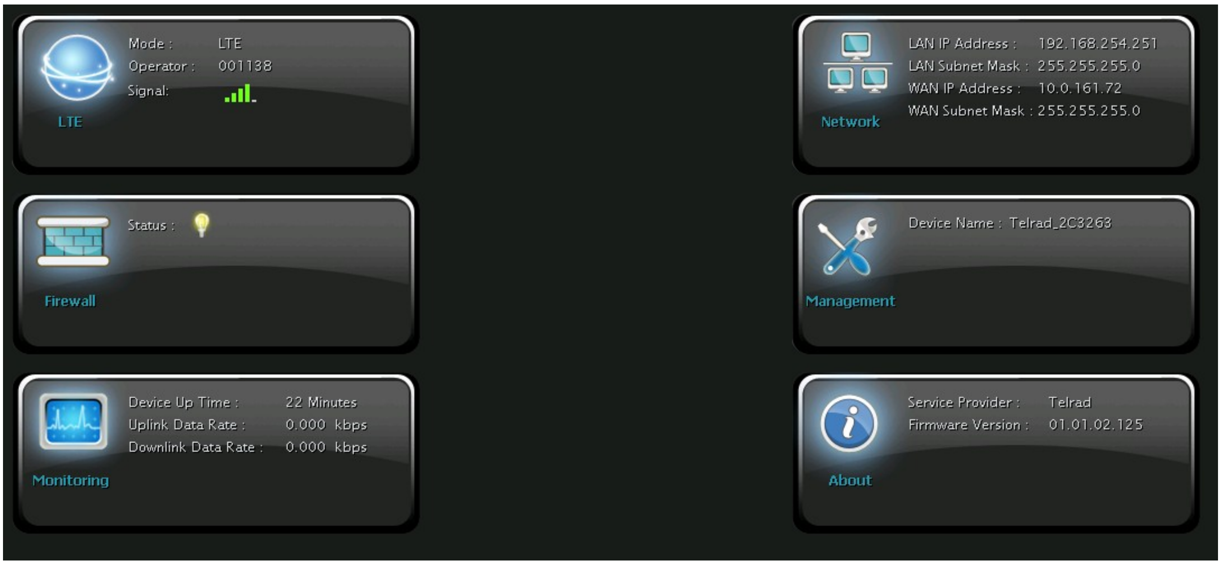
Brief Summary Page

After you’ve opened up GUI page, the first page you see is “Brief Summary Page”. This window shows all the current settings and system information. It gives you an overview of the current status of your device.

After login, users can see a “**Brief Summary Page**” about all functions of LTE CPE, each block is a link to “**Detailed Configuration Page**”.

(Ex: Click “**Network**”, you can go to “**Network**” main menu with sub-menu like DHCP or Port Forwarding and other settings about Network)

Detailed information for each block is in the below table.



Mode : LTE
Operator : 001138
Signal:

LAN IP Address : 192.168.254.251
LAN Subnet Mask : 255.255.255.0
WAN IP Address : 10.0.161.72
WAN Subnet Mask : 255.255.255.0

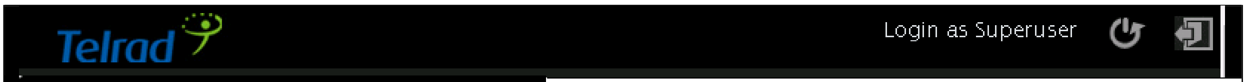
Status :

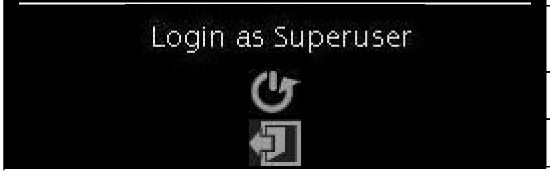
Device Name : Telrad_2C3263

Device Up Time : 22 Minutes
Uplink Data Rate : 0.000 kbps
Downlink Data Rate : 0.000 kbps

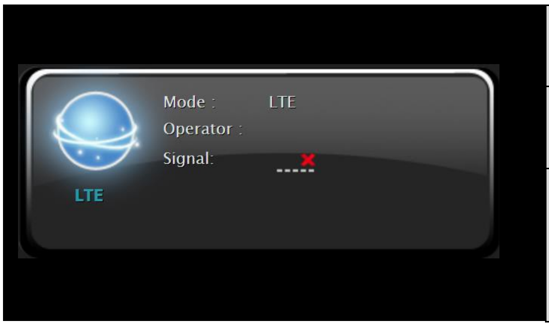
Service Provider : Telrad
Firmware Version : 01.01.02.125

GUI Interface

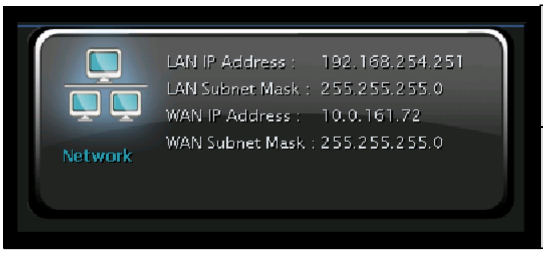


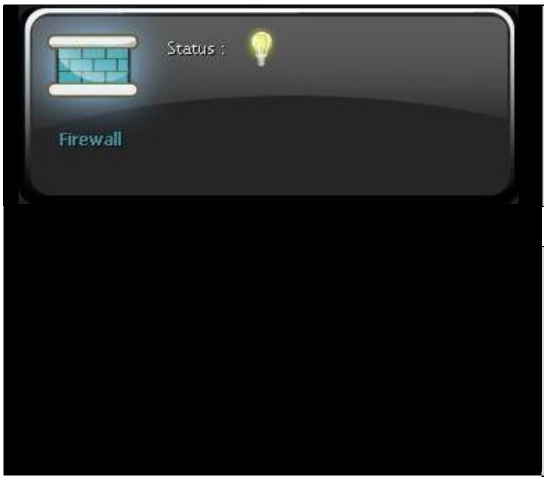
	Logo of Service Provider.
 Login as Superuser	Login Identity, could be **Superuser** or **Enduser**
	Button of **REBOOT**
	Button of **LOGOUT**

❗	, this logo is an example. It can be customized if needed.

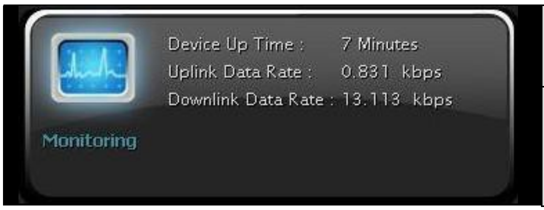
 Mode : LTE Operator : Signal: ----✗ LTE	Mode:	**LTE**
	Operator:	Either **APN Name** (LTE mode)
	Signal:	▂▄▆█ ▂▄▆_ ▂▄__ ▂___ ____ (More bar means better signal) ----✗ (Disconnect, no signal)

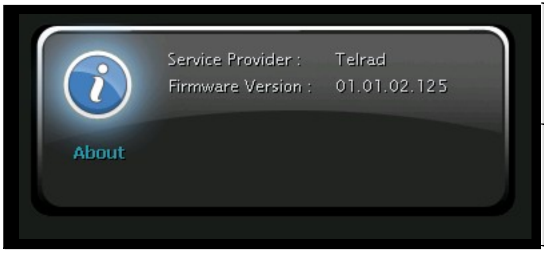
❗	Signal: ▂▄▆█ Only an example, the real signal depends on local connection environment.

 Network LAN IP Address : 192.168.254.251 LAN Subnet Mask : 255.255.255.0 WAN IP Address : 10.0.161.72 WAN Subnet Mask : 255.255.255.0	LAN IP:	LAN IP of CPE
	WAN IP:	WAN IP of CPE

 Firewall Status :	Status:	● means Firewall is enabled ○ means Firewall is disabled.
	Device Name:	Name of LTE CPE in LAN side

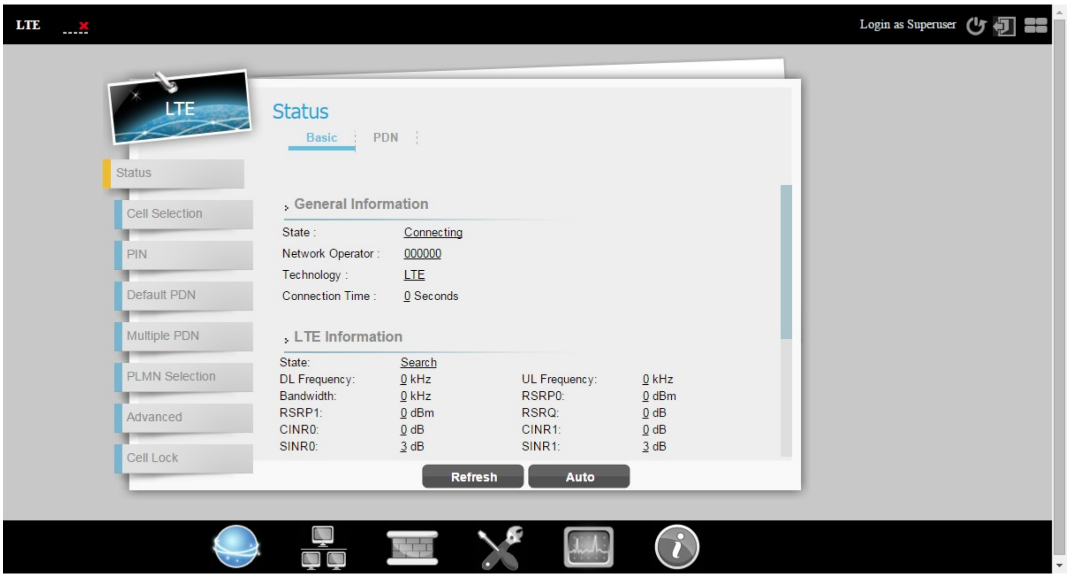
!	Device Name **Telrad_2C3263** is just an example. In general, it looks like XXXXX_YYYYYY (XXXXX = Service Provider) (YYYYYY = Last six words of WAN MAC.)

 Monitoring Device Up Time : 7 Minutes Uplink Data Rate : 0.831 kbps Downlink Data Rate : 13.113 kbps	Device Up Time:	The uptime from the bootup of LTE CPE
	Uplink / Downlink Data Rate:	Uplink / Downlink Rate of the LTE CPE

 About Service Provider : Telrad Firmware Version : 01.01.02.125	Service Provider:	The service provider of this LTE CPE. (Generic is just an example)
	Firmware Version:	Firmware Version of this LTE CPE.

Detailed Configuration Page

After clicking any block in "Brief Summary Page", the webpage would be switched to the "Detailed Configuration Page". (Take "Mobile Network" block for example)



General Information

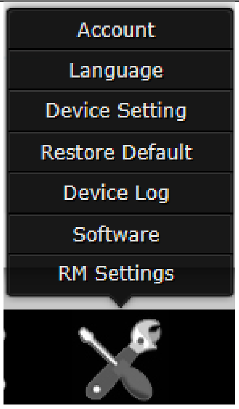
State : Connecting
Network Operator : 000000
Technology : LTE
Connection Time : 0 Seconds

LTE Information

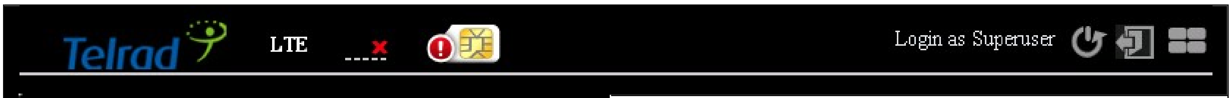
State:	Search		
DL Frequency:	0 kHz	UL Frequency:	0 kHz
Bandwidth:	0 kHz	RSRP0:	0 dBm
RSRP1:	0 dBm	RSRQ:	0 dB
CINR0:	0 dB	CINR1:	0 dB
SINR0:	3 dB	SINR1:	3 dB

Detailed Configuration Page

Main Menu	Show the current main menu
Sub Menu	Clickable, can jump to another Sub Menu under the same Main Menu
Quick Panel	Each icon in **Quick Panel** represents a "Main Menu", when users click it, a list of "Sub Menu" will be popped up. By using **Quick Panel**, users can quickly jump to the desired Sub Menu under other Main Menu. (For example, if the user wants to do "Restore Default", Click "**Managemen**t" Icon then click "**Restore Default**")



Pop up Sub Menu in Quick Panel



Telrad	Logo of service provider.
LTE	Current service, could be **LTE**
📶	Signal bar, more bar means better signal ----✕ means no signal or disconnection.
❗	When CPE cannot Detect SIM card, the ICON will appear.
Login as Superuser	Login identity, could be **Superuser** or **Enduser**
↻	Button of **REBOOT**
⎆	Button of **LOGOUT**
▦	Button to go Back to **brief information Page**

Menu Structure

After entering “Detailed Configuration Page”, the user can quickly jump to the specified Sub Menu. (By clicking “**Quick Panel**” at the bottom of the page.)

Users can refer to the menu structure given below:

LTE	Status
	Cell Selection
	PIN
	Default PDN
	Multiple PDN
	PLMN Selection
	Advanced
	Cell Lock
Network	Status
	WAN Setting
	LAN Setting
	QoS
	Port Management
	DSCP
	MGMT Service
Firewall	Basic
	L3 MGMT Filter
	L3 DATA filter
	L2 Filter
	Access Restriction
Management	Account
	Language
	Device Setting
	Restore Default
	Device Log
	Software
	RM Settings
Monitoring	Status
	Iperf
	Diagnostic Tools
About	Status

Reference Manual

LTE

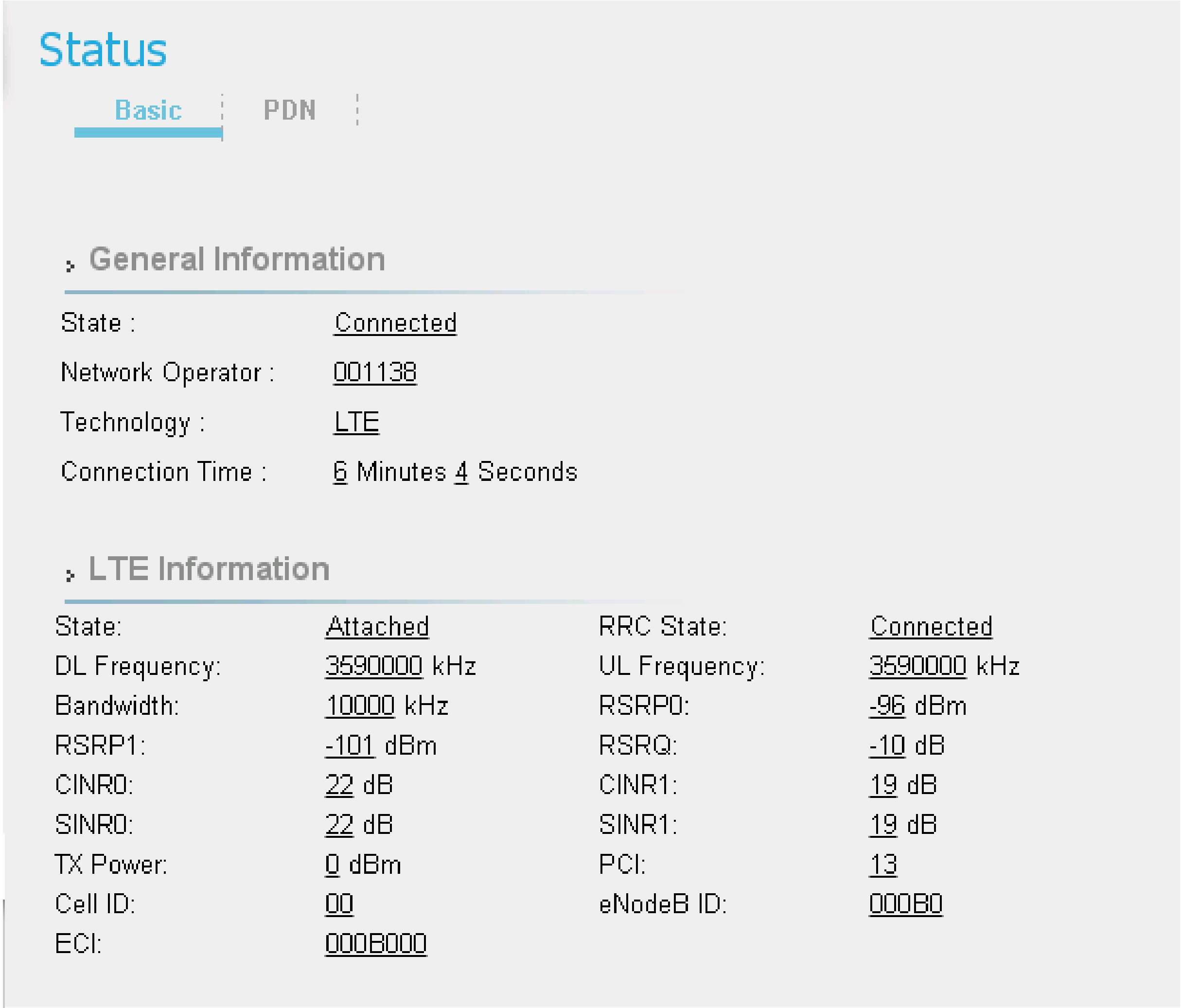
In “**LTE**” main menu, user can see the LTE basic information and uplink/downlink status. All the setting about LTE placed here such as LTE Earfcn and PIN code, PDN, multiple PDN, PLMN search and Cell Lock.

	Display in **Brief Summary Page**
	Display in “**Quick Panel**” of **Detailed Configuration Page**

- Menu Structure:

LTE	Status
	Cell Selection
	PIN
	Default PDN
	Multiple PDN
	PLMN Selection
	Advanced
	Cell Lock

LTE | Status | Basic



Status

Basic | PDN

General Information

State :	Connected
Network Operator :	001138
Technology :	LTE
Connection Time :	6 Minutes 4 Seconds

LTE Information

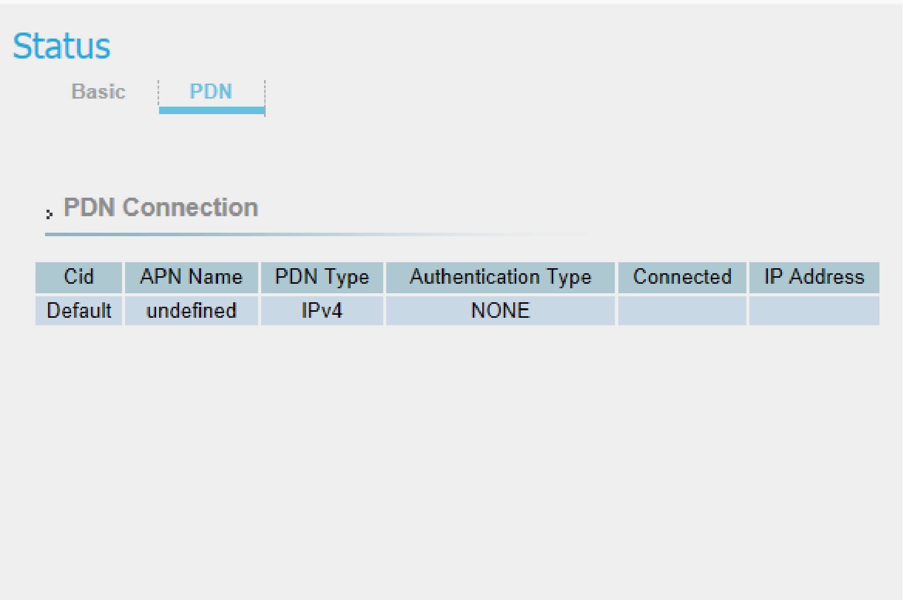
State:	Attached	RRC State:	Connected
DL Frequency:	3590000 kHz	UL Frequency:	3590000 kHz
Bandwidth:	10000 kHz	RSRP0:	-96 dBm
RSRP1:	-101 dBm	RSRQ:	-10 dB
CINR0:	22 dB	CINR1:	19 dB
SINR0:	22 dB	SINR1:	19 dB
TX Power:	0 dBm	PCI:	13
Cell ID:	00	eNodeB ID:	000B0
ECI:	000B000		

LTE > Status

- **General Information**
  - **State:** Possible states are connecting and connected.
  - **Network Operator:** It shows APN name.
  - **Technology:** LTE.
  - **Connection Time:** the accumulated time after the state is “connected”.
- **LTE Information**
  - **RRC State:**
    - **Device Init:** Detect LTE module.
    - **SIM Detecting:** As titled.

        - **Device Ready:** Unlock pin code.
        - **Search:** Scan the available eNodeB.
        - **Network Entry:** Cell detection.
        - **Attached:** As titled.
        - **Idle:** As titled.
        - **No Signal:** NAS attached RRC detached.
    - **DL Frequency:** Downlink frequency.
    - **UL Frequency:** Uplink frequency.
    - **Bandwidth:** As titled.
    - **RSRP0:** Reference signal receiving power of path 0.
    - **RSRP1:** Reference signal receiving power of path 1.
    - **RSRQ:** Reference signal receive quality.
    - **CINR0:** The quality of the signal of path 0.
    - **CINR1:** The quality of the signal of path 1.
    - **SINR0:** Signal to interference plus noise ratio of path 0.
    - **SINR1:** Signal to interference plus noise ratio of path 1.
    - **TX Power:** Transmission power.
    - **PCI:** Physical cell identity.
    - **Cell ID:** Cell Identity, a part of cell global identification.
    - **eNodeB ID:** Identity of connected eNodeB.
- **UpLink Status**
    - **Data Rate:** The upload speed.
    - **TX Bytes:** Number of sending bytes.
    - **Packets:** Number of sending packets.
- **DownLink Status**
    - **Data Rate:** The download speed.
    - **RX Bytes:** Number of received bytes.
    - **Packets:** Number of received packets.

LTE | Status | PDN



Cid	APN Name	PDN Type	Authentication Type	Connected	IP Address
Default	undefined	IPv4	NONE		

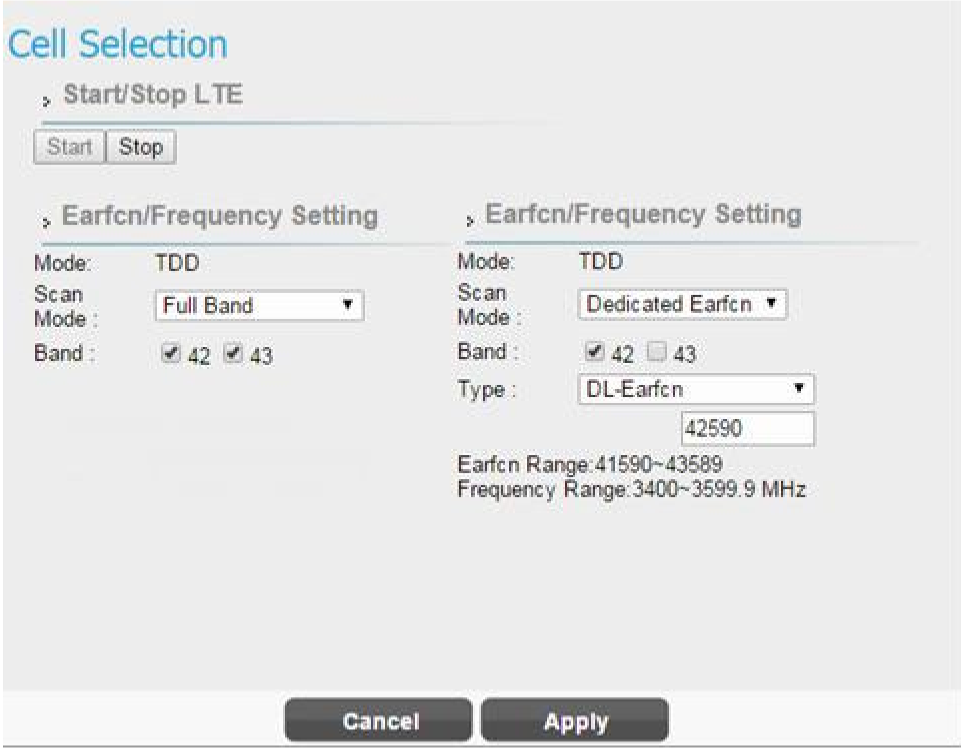
LTE > Status > PDN

- **Cid:** Identity number of PDN connection.
- **APN Name:** Access point name identifies specific packet data network.
- **PDN Type:** The connection type of each packet data network.
- **Authentication Type:** The Authentication type of each packet data network.
- **Connected:** The Connection status of each packet data network.
- **IP Address:** The IP address of each packet data network.

!	The first Cid of PDN should be considered as default. The Cid sequence would be started from 2.

LTE | Cell Selection

note only B48 supported in US*



Mode: TDD
Scan Mode : Full Band
Band : ☑ 42 ☑ 43

Mode: TDD
Scan Mode : Dedicated Earfcn
Band : ☑ 42 □ 43
Type : DL-Earfcn
42590
Earfcn Range:41590~43589
Frequency Range:3400~3599.9 MHz

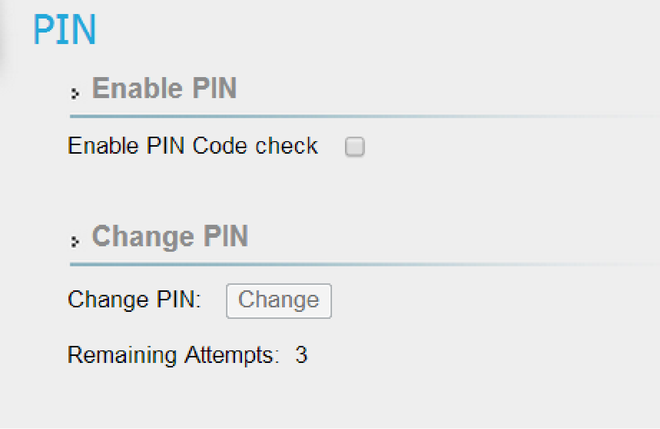
LTE > Cell Selection

- **Mode:** TDD
- **Scan Mode:** Full Band or Dedicated Earfcn. Searching full band would take much longer time than Dedicated Earfcn.
- **Band:** 48
- **Type:** DL-Earfcn or Dl-Frequency.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

!	**LTE Band** 48 **and Earfcn/Frequency Range** are just an example. Real number is determined by the user's requirement.

LTE | PIN



PIN

Enable PIN

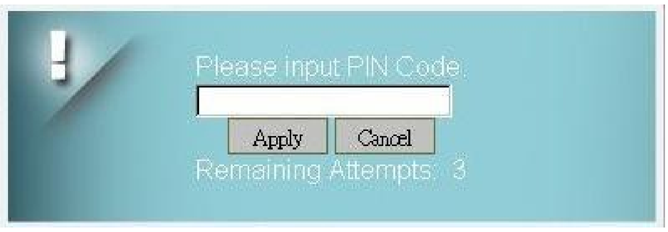
Enable PIN Code check □

Change PIN

Change PIN:

Remaining Attempts: 3

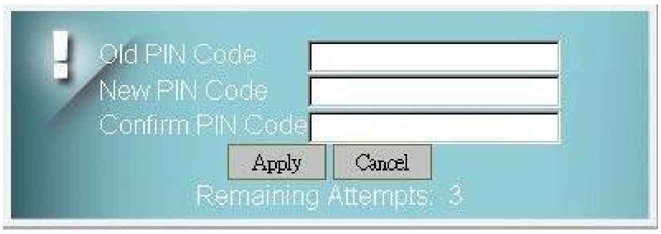
LTE > PIN



Please input PIN Code

Remaining Attempts: 3

LTE > PIN > Enable PIN



Old PIN Code

New PIN Code

Confirm PIN Code

Remaining Attempts: 3

LTE > PIN > Change PIN

- **Enable PIN:** Enable/Disable PIN code protection.
- **Change PIN:** Change the PIN code.
- **Remaining Attempts:** remaining times to try PIN code.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

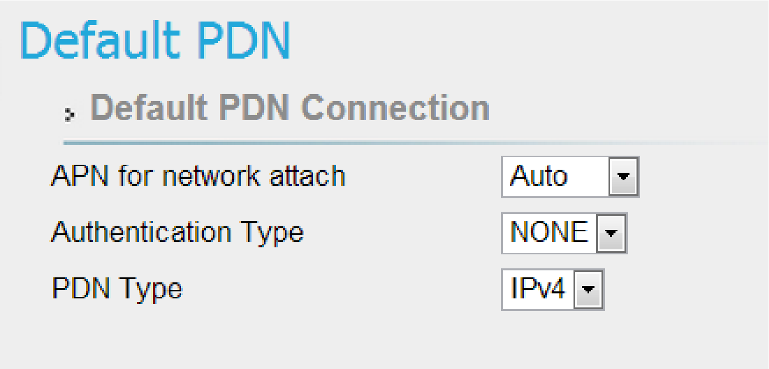
!	Please make sure the current technology is **LTE**. It can be checked from upper left corner of Web-GUI.

!	If you enter wrong PIN more than three times (maximum numbers of attempts allowed), your SIM card will become “PUK-locked” status. Please contact your service provider for further unlock instruction.

!	**Remaining Attempts** is just an example. Real number is determined by user's SIM card.

!	If users want to change the PIN code of SIM card, they need to enable “**Enable PIN code check**” function in advance.

LTE | Default PDN



Default PDN

Default PDN Connection

APN for network attach: Auto

Authentication Type: NONE

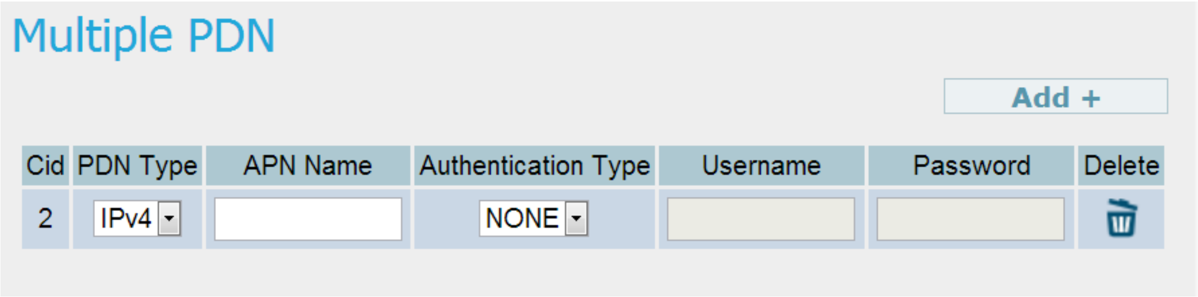
PDN Type: IPv4

LTE > Default PDN

- **APN for network attach:** Users can choose **Auto** or **Manual**. If choosing **Manual**, users need to specify an APN Name.
- **Authentication Type:** There are **None**, **PAP** and **CHAP** to choose from**.** If choosing PAP or CHAP, users need to specify the username and password.
- **PDN Type:** Only support IPv4 right now.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

LTE | Multiple PDN



Cid	PDN Type	APN Name	Authentication Type	Username	Password	Delete
2	IPv4 ▾		NONE ▾			🗑

LTE > Multiple PDN

Multiple PDN is a wonderful way to separate different network service. For example, users can have **Default PDN** for management and **multiple PDN** for data transfer.

- **PDN Type:** Only support IPv4 right now.
- **APN Name:** As titled.
- **Authentication Type:** There are **"None"**, ***"PAP (Password authentication protocol)"***, or ***"CHAP (Challenge Handshake Authentication Protocol)"*** to choose from. If choosing PAP or CHAP, users need to specify the username and password.

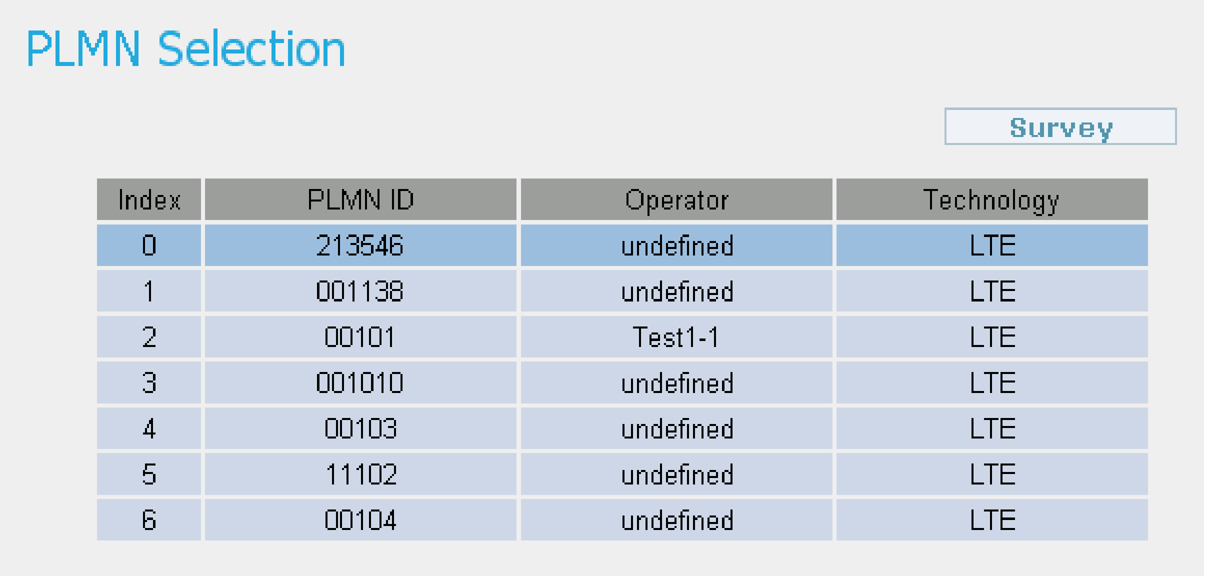
Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

!	APN name can't be empty. The type of the authentication is determined by the user's service provider.

!	The CPE supports at most 7 PDN connections (Cid 2 to 8)

LTE | PLMN Selection

PLMN selection is a technique to keep connecting to ISP for CPE.
If CPE search PLMNs, it will be recorded in the table below.



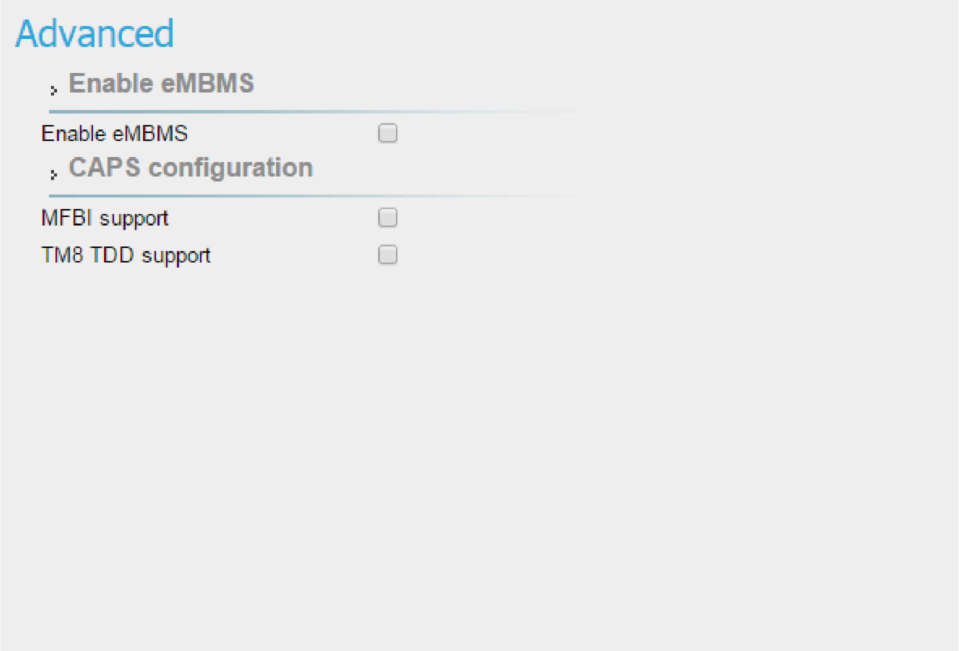
PLMN Selection

Index	PLMN ID	Operator	Technology
0	213546	undefined	LTE
1	001138	undefined	LTE
2	00101	Test1-1	LTE
3	001010	undefined	LTE
4	00103	undefined	LTE
5	11102	undefined	LTE
6	00104	undefined	LTE

- **"Survey" button:** to scan all the PLMN around the CPE
- **Index:** Number of PLMN.
- **PLMN ID:** Identification of PLMN and depends on eNodeB. (e.g. 00101)
- **Operator:** Name of ISP
- **Technology:** e.g. LTE

LTE | Advanced (Not part of current release)

The below capabilities depending on eNodeB features supported and IOT, therefore these features currently not available. For further details, please contact Telrad team.



Advanced

› Enable eMBMS

Enable eMBMS □

› CAPS configuration

MFBI support □

TM8 TDD support □

LTE > Advanced

eMBMS is a way to deliver popular multimedia content to a mass audience. It provided an efficient broadcasting of content only to interested receivers.

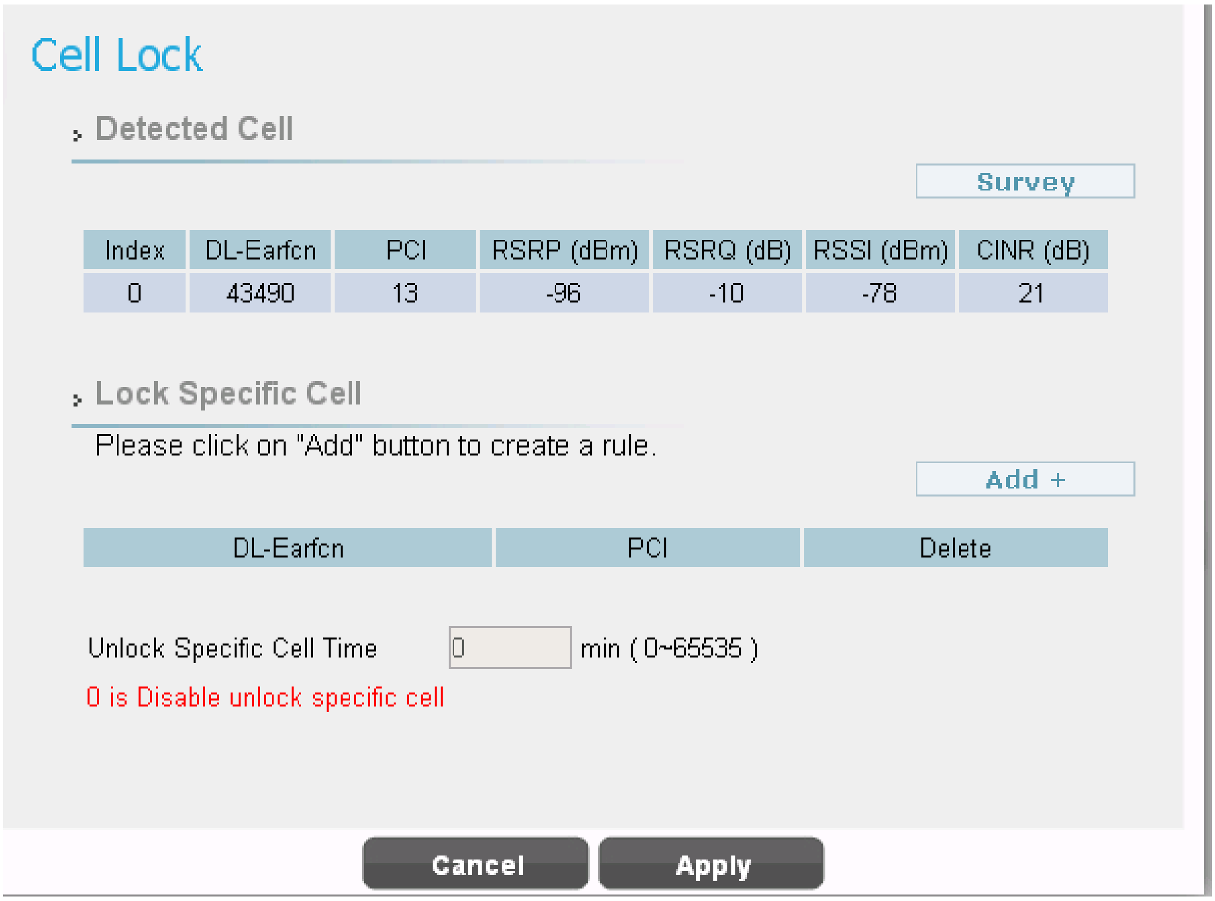
MFBI is Multi-Frequency Band Indicator. Allow CPE connect to another Band with overlap frequency. For Example (CPE set Band 38 can connect to eNodeB with Band 41)

TM8 TDD is support dual layer beamforming

- **Enable eMBMS:** User can enable this service via check this box.
- **MFBI Support:** User can enable this service via check this box.
- **TM8 TDD support:** User can enable this service via check this box.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

LTE | Cell Lock



Cell Lock

Detected Cell

Index	DL-Earfcn	PCI	RSRP (dBm)	RSRQ (dB)	RSSI (dBm)	CINR (dB)
0	43490	13	-96	-10	-78	21

Lock Specific Cell

Please click on "Add" button to create a rule.

DL-Earfcn	PCI	Delete

Unlock Specific Cell Time 0 min (0~65535)

0 is Disable unlock specific cell

LTE > Cell Lock

Cell Lock is use to lock CPE into specific Cell. CPE will only connect to specific cell that define in the list. The list contains up to 10 in priority to others cells.

- **Detected Cell**
  - **"Survey" button:** to scan all surrounding coverage cell
  - **Index:** Number of Cell.
  - **DL-Earfcn:** Downlink EUTRA Absolute radio-frequency channel number
  - **PCI:** Physical cell identity.
  - **RSRP (dBm):** Reference signal receiving power.
  - **RSRQ (dB):** Reference signal receive quality.
- **Lock Specific Cell**

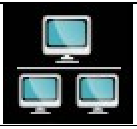
- Click **“Add +”** button to add a new rule, clicking **“Delete”** icon 🗑) to delete the rule.
- **Add:** User can lock specific cell by click add. Maximum CPE can input 10 Cell in the list.
- **DL-Earfcn:** Downlink EUTRA Absolute radio-frequency channel number.
- **PCI:** Physical cell identity.
- **Delete:** Remove specific cell lock**.**

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

⚠	While use Cell Lock, please do survey for scanning surrounding eNodeB coverage cell by click “survey” button

Network

The “Network” page allows user to configure network function such as WAN setting, LAN Setting, QOS, Port Management, DSCP, and MGMT Service.

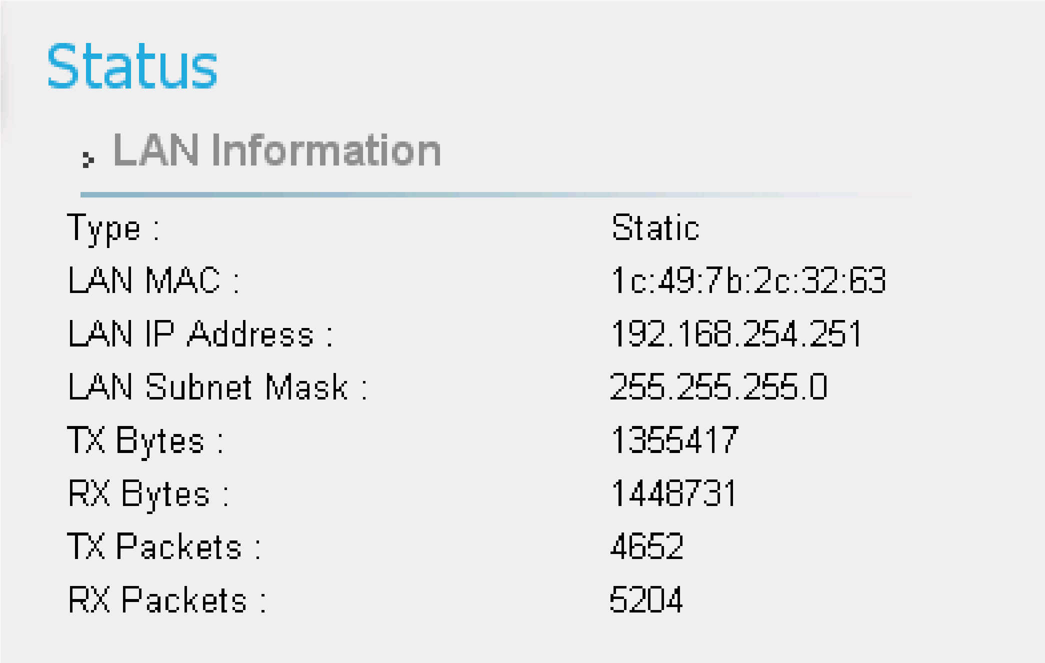
	Display in **Brief Summary Page**
	Display in “**Quick Panel**” of **Detailed Configuration Page**

- **Menu Structure:**

Network	Status
	WAN Setting
	LAN Setting
	QoS
	Port Management
	DSCP
	MGMT Service

Network | Status

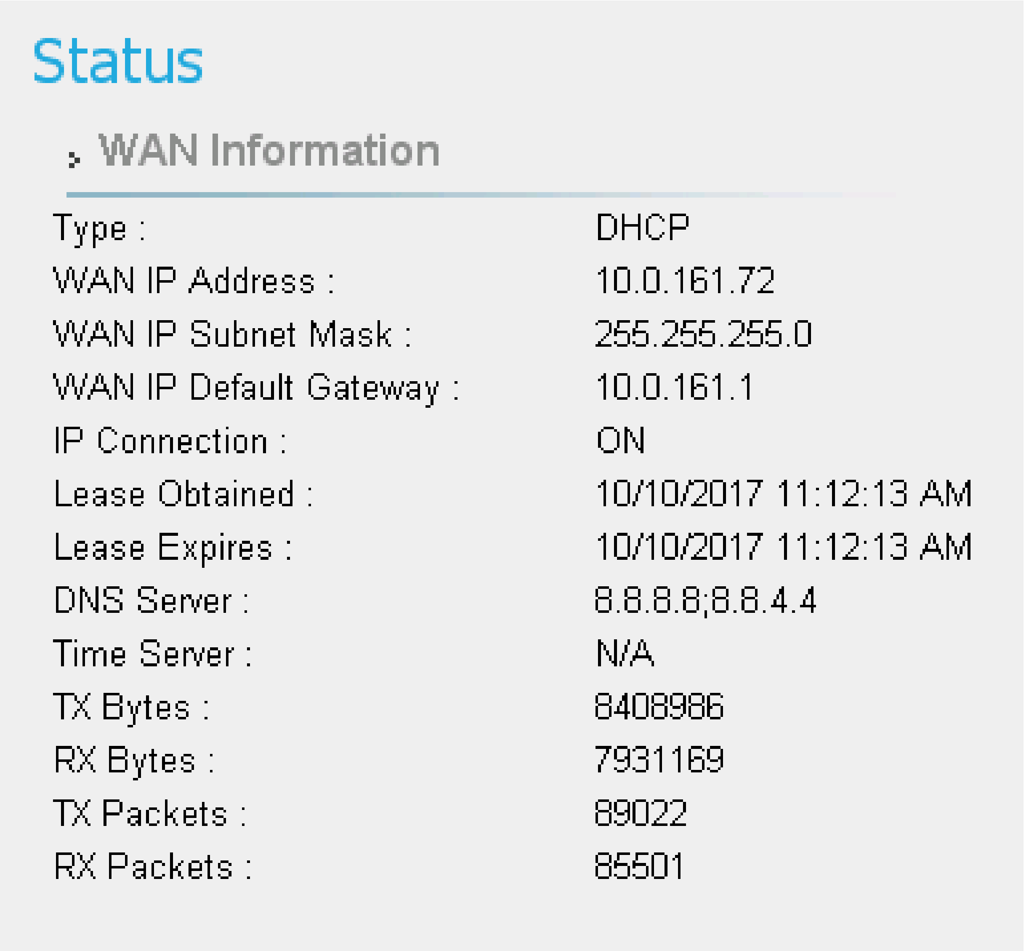
- **LAN Information**



Type :	Static
LAN MAC :	1c:49:7b:2c:32:63
LAN IP Address :	192.168.254.251
LAN Subnet Mask :	255.255.255.0
TX Bytes :	1355417
RX Bytes :	1448731
TX Packets :	4652
RX Packets :	5204

Network > Status > LAN Information

- **WAN Information:** This section shows WAN IP, MAC, Gateway, DNS Server, Time Server of LTE CPE and statistics of TX and RX Bytes and Packets of WAN interface. These values may differ from "Single PDN" to "Multiple PDN", in NAT Mode with "Multiple PDN enable" and "Separate" WAN MGMT and Data Interface, will get two WAN IP, one for MGMT(Management packets, to CPE), one for Data(Date, transfer to LAN side).



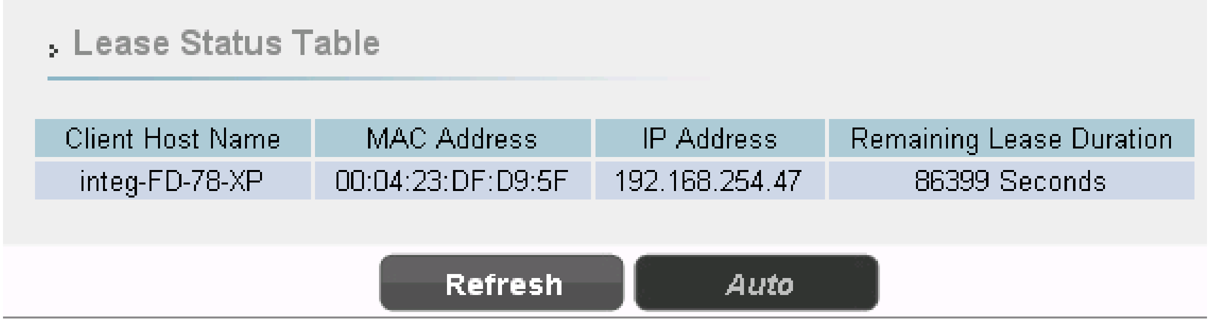
Status

WAN Information

Type :	DHCP
WAN IP Address :	10.0.161.72
WAN IP Subnet Mask :	255.255.255.0
WAN IP Default Gateway :	10.0.161.1
IP Connection :	ON
Lease Obtained :	10/10/2017 11:12:13 AM
Lease Expires :	10/10/2017 11:12:13 AM
DNS Server :	8.8.8.8;8.8.4.4
Time Server :	N/A
TX Bytes :	8408986
RX Bytes :	7931169
TX Packets :	89022
RX Packets :	85501

Network > Status > WAN Information

- **Lease Status Table:** This section shows all clients who get IP from DHCP server in LTE CPE.



Lease Status Table

Client Host Name	MAC Address	IP Address	Remaining Lease Duration
integ-FD-78-XP	00:04:23:DF:D9:5F	192.168.254.47	86399 Seconds

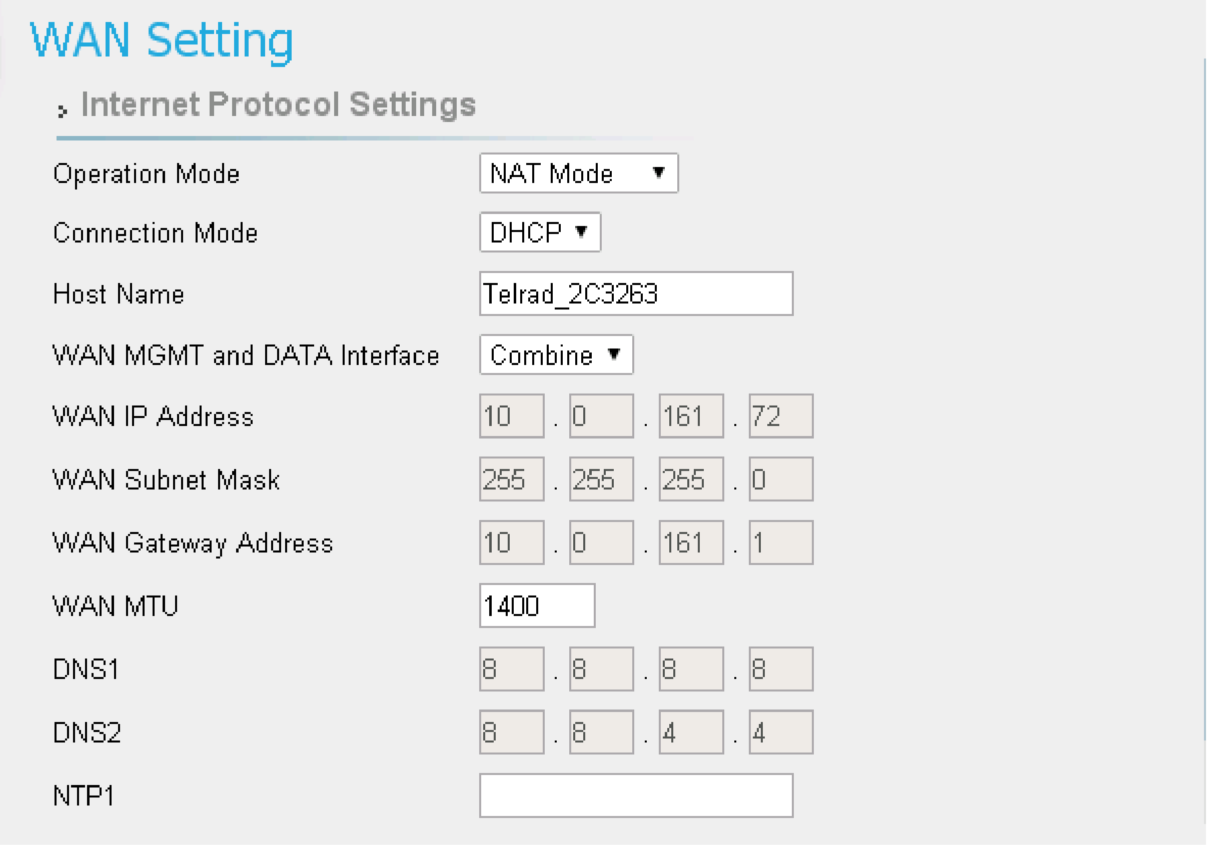
Network > Status > Lease Status Table

Refresh button	Click the "Refresh" button to trigger refresh manually.
Auto button	This button will update the status information periodically.

	The period can be set from “GUI Refresh Time” in page **Management / Device Setting**)

❗	The address and TX/RX bytes are all examples here. Real values depend on the local ISP provider..

Network | WAN Setting (NAT Mode)



WAN Setting

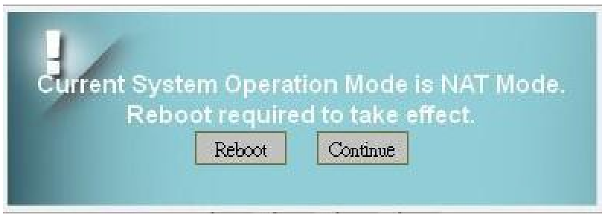
› Internet Protocol Settings

Operation Mode	NAT Mode ▼
Connection Mode	DHCP ▼
Host Name	Telrad_2C3263
WAN MGMT and DATA Interface	Combine ▼
WAN IP Address	10 . 0 . 161 . 72
WAN Subnet Mask	255 . 255 . 255 . 0
WAN Gateway Address	10 . 0 . 161 . 1
WAN MTU	1400
DNS1	8 . 8 . 8 . 8
DNS2	8 . 8 . 4 . 4
NTP1	

Network > WAN Setting

- **Operation Mode:** The mode includes NAT, Tunnel, Bridge and Router Mode. The following pages will show how to configure "NAT mode".

!	Changing the "**Operation Mode**" needs reboot to take effect. A pop-up window will ask users to "**Reboot**" or "**Continue**". If you select "**Reboot**", CPE would reboot right away. If you select "**Continue**", CPE would not reboot automatically, you need to reboot it manually.



Current System Operation Mode is NAT Mode.
Reboot required to take effect.

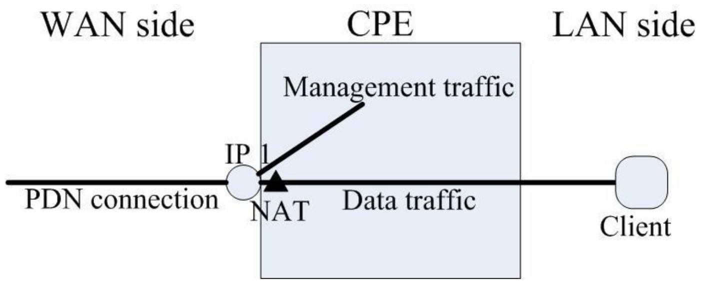
Pop-up windows to confirm reboot

- **Connection Mode:** “**DHCP**” or “**Static**”.
  - ➢ If “DHCP” mode is selected, CPE would automatically acquire configuration information from a DHCP server.
  - ➢ If “Static” mode is selected, users have to manually enter the required information in below fields.
- **Host Name:** currently no function.

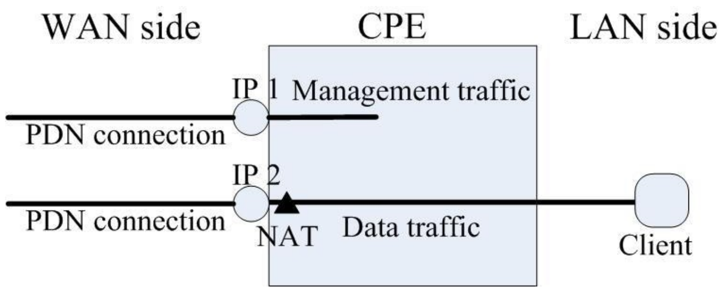
!	Host Name“**Telrad_2C3263”** Just an example here, in general, it will be like XXXXX_YYYYYY (XXXXX = Service Provider) (YYYYYY = Last six words of WAN MAC)

- **WAN MGMT and DATA Interface:** Users can choose “**Separate**” to use different Interface for MGMT and Data traffic, or just use “**Combine**” which means using same interface for MGMT and Data. “**Separate**” only works in LTE mode.

  Below are two simple pictures that describe this function.



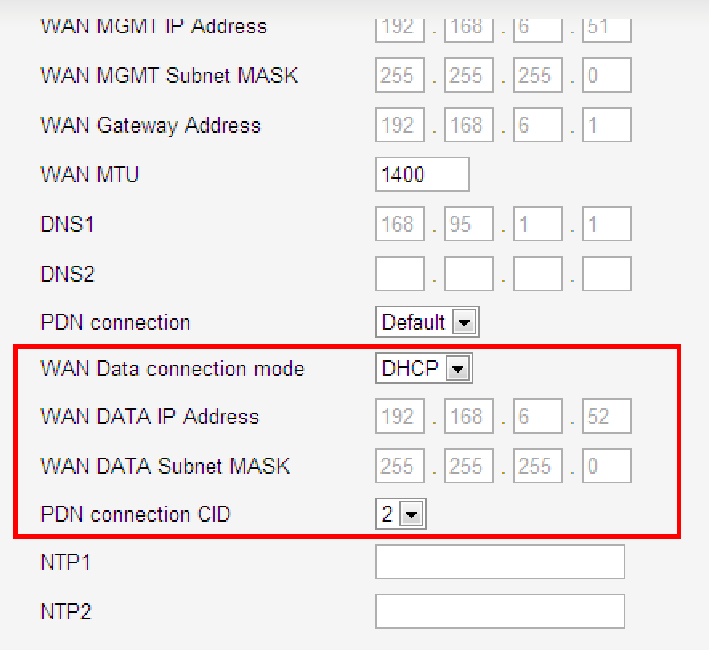
*NAT mode, choosing “**Combine**” in WAN MGMT and Data Interface*



*NAT mode, choosing “**Separate**” in WAN MGMT and Data Interface*

!	If users choose “**Separate**” in WAN MGMT and Data Interface, make sure other PDN is well configured in page ***LTE > Multiple PDN***.

- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when the connection mode is “**DHCP**” and editable when the mode is “**Static**”. If “**Combine**” is selected in “**WAN MGMT and Data Interface**”, data and management traffic share the same interface. If “**Separate**” is selected, another WAN IP address, subnet mask and gateway address to configure data traffic will be shown.



WAN MGMT IP Address	192 . 168 . 6 . 51
WAN MGMT Subnet MASK	255 . 255 . 255 . 0
WAN Gateway Address	192 . 168 . 6 . 1
WAN MTU	1400
DNS1	168 . 95 . 1 . 1
DNS2	. . .
PDN connection	Default
WAN Data connection mode	DHCP
WAN DATA IP Address	192 . 168 . 6 . 52
WAN DATA Subnet MASK	255 . 255 . 255 . 0
PDN connection CID	2
NTP1	
NTP2	

Two WAN IP, one for MGMT, other for DATA

- **WAN MTU:** This value is “Maximum Transmission Unit”. The size of a single packet can only be as large as MTU. If the size of the packet exceeds MTU, the packet would be fragmented.

- **DNS1/2:** Domain Name Server, editable when users select “Static” in “Connection Mode”. Otherwise, DNS information will be given by DHCP server.

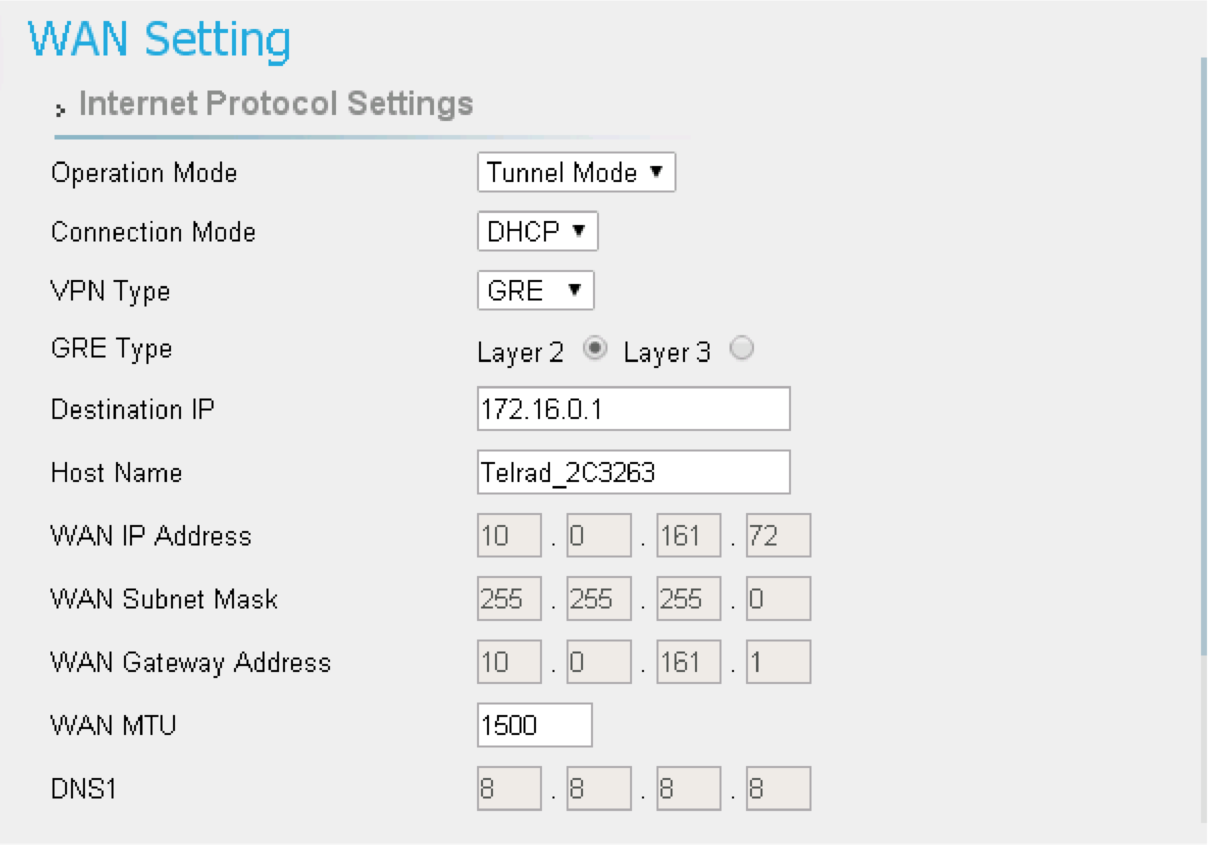
- **PDN connection CID for MGMT:** If selecting "**Separate**" in "**WAN MGMT and DATA Interface**", users need to assign the PDN used as MGMT. By now, the only option is "Default".
- **PDN connection CID for DATA:** If selecting "**Separate**" in "**WAN MGMT and DATA Interface**", users need to choose from 2-8 for WAN DATA connection. Please make sure this PDN is configured beforehand in page ***Mobile Network > Technology > LTE > Multiple PDN***.

- **NTP1/2:** Users can specify two NTP servers in "IP" or "Domain name" format.

```
For example 45.79.167.181 or 0.us.pool.ntp.org
```

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | WAN Setting (Tunnel Mode – Layer 2 GRE Only)



WAN Setting

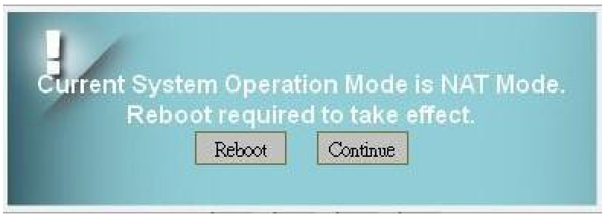
Internet Protocol Settings

Operation Mode	Tunnel Mode ▼
Connection Mode	DHCP ▼
VPN Type	GRE ▼
GRE Type	Layer 2 ● Layer 3 ○
Destination IP	172.16.0.1
Host Name	Telrad_2C3263
WAN IP Address	10 . 0 . 161 . 72
WAN Subnet Mask	255 . 255 . 255 . 0
WAN Gateway Address	10 . 0 . 161 . 1
WAN MTU	1500
DNS1	8 . 8 . 8 . 8

Network > WAN Setting > PPTP, L2TP, GRE

- **Operation Mode:** The mode includes **NAT**, **Tunnel**, **Bridge** and **Router** Mode. The following pages will show how to configure “Tunnel mode”.

!	Changing the “**Operation Mode**” needs reboot to take effect. A pop-up window will ask users to “**Reboot**” or “**Continue**”. If you select “**Reboot**”, CPE would reboot right away. If you select “**Continue**”, CPE would not reboot automatically, you need to reboot it manually.



Current System Operation Mode is NAT Mode.
Reboot required to take effect.

Pop-up windows for reboot confirm

- **VPN Type:** PPTP (with IPsec) – Not supported
  L2TP (with IPsec & BCP Disable/Enable) – Not supported
  GRE (Layer2/ Layer3) Tunnel Mode - Only Layer 2 supported
- **GRE Type (Layer 2)/ Destination IP Address:** The IP address of the peer to build GRE tunnel with CPE.

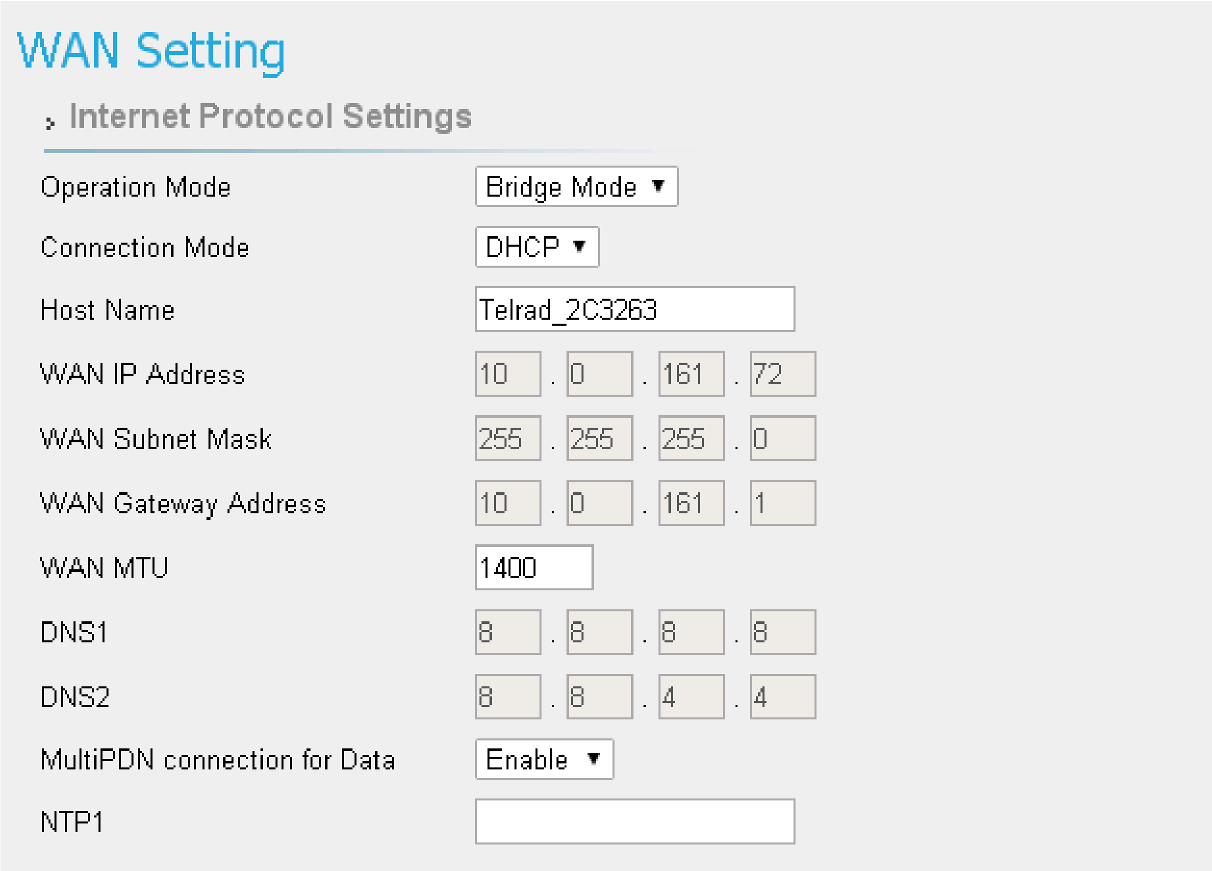
❗	All information need in this page are assigned by "Tunnel Server". Like Server IP, Username and Password.

- **Connection Mode:** "DHCP" or "Static".
  - ➢ If "DHCP" mode is selected, CPE would automatically acquire configuration information from a DHCP server.
  - ➢ If "Static" mode is selected, users have to manually enter the required information in below fields.
- **Host Name:** Currently no function.

- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when users select "**DHCP**" in "**Connection Mode**".
- **WAN MTU:** This value is "Maximum Transmission Unit". It is the largest size of a single packet.
- **DNS1/2:** Domain Name Server. It is editable when users select "**Static**" in "**Connection Mode**". Otherwise, these values will be given by DHCP server.
- **NTP1/2:** It is used to calibrate the time in CPE. Users can specify two NTP servers in "IP" or "Domain name" format.
  For example **45.79.167.181** or **0.us.pool.ntp.org**

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | WAN Setting (Bridge Mode) - NOT SUPPORTED BY TELRAD



WAN Setting

› Internet Protocol Settings

Operation Mode: Bridge Mode ▾

Connection Mode: DHCP ▾

Host Name: Telrad_2C3263

WAN IP Address: 10 . 0 . 161 . 72

WAN Subnet Mask: 255 . 255 . 255 . 0

WAN Gateway Address: 10 . 0 . 161 . 1

WAN MTU: 1400

DNS1: 8 . 8 . 8 . 8

DNS2: 8 . 8 . 4 . 4

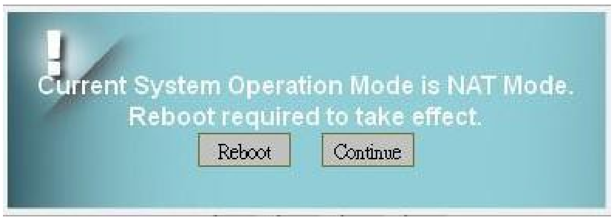
MultiPDN connection for Data: Enable ▾

NTP1:

Network > WAN Setting

- **Operation Mode: users have NAT**, **Tunnel**, **Bridge** and **Router** Mode to choose from. The following pages show how to configure “**Bridge mode**”.

!	Changing the “**Operation Mode**” needs reboot to take effect. A pop-up window will ask users to “**Reboot**” or “**Continue**”. If you select “**Reboot**”, CPE would reboot right away. If you select “**Continue**”, CPE would not reboot automatically, you need to reboot it manually.



Current System Operation Mode is NAT Mode.
Reboot required to take effect.

Pop-up windows for reboot confirm

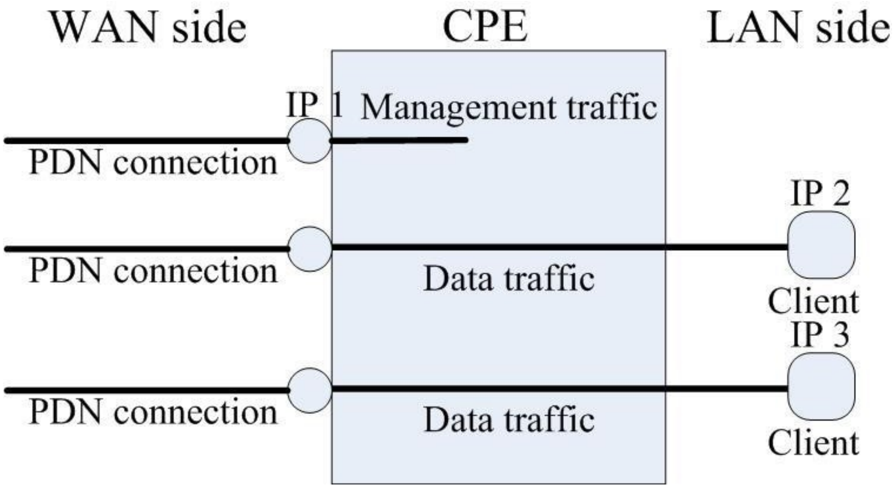
- **Connection Mode:** “DHCP” or “Static”.
  - ➢ If “DHCP” mode is selected, CPE would automatically acquire configuration information from a DHCP server.
  - ➢ If “Static” mode is selected, users have to manually enter the required information in below fields.
- **Host Name:** Currently no function.

!	Host Name“**Telrad_2C3263”** Just an example here, in general, it will be like XXXXX_YYYYYY (XXXXX = Service Provider) (YYYYYY = Last six words of WAN MAC)

- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when “**Connection Mode**” is “**DHCP**” and editable when “**Connection Mode**” is “**Static**”.
- **WAN MTU:** This value is “Maximum Transmission Unit”. It is the largest size of a single packet.
- **DNS1/2:** Domain Name Server. It is editable when users select “**Static**” in “**Connection Mode**”. Otherwise, these values will be given by DHCP server.
- **MultiPDN connection for Data (Only in Bridge Mode):** If it is enabled, CPE will pre-create PDN connections for local clients. Thus, a client requests an IP address from CPE, CPE will reply an IP gotten from one of APN.

  If it is disabled, only one default PDN will be established, clients need another way to get IP address.

  Below is an example for “**enabled**” case.



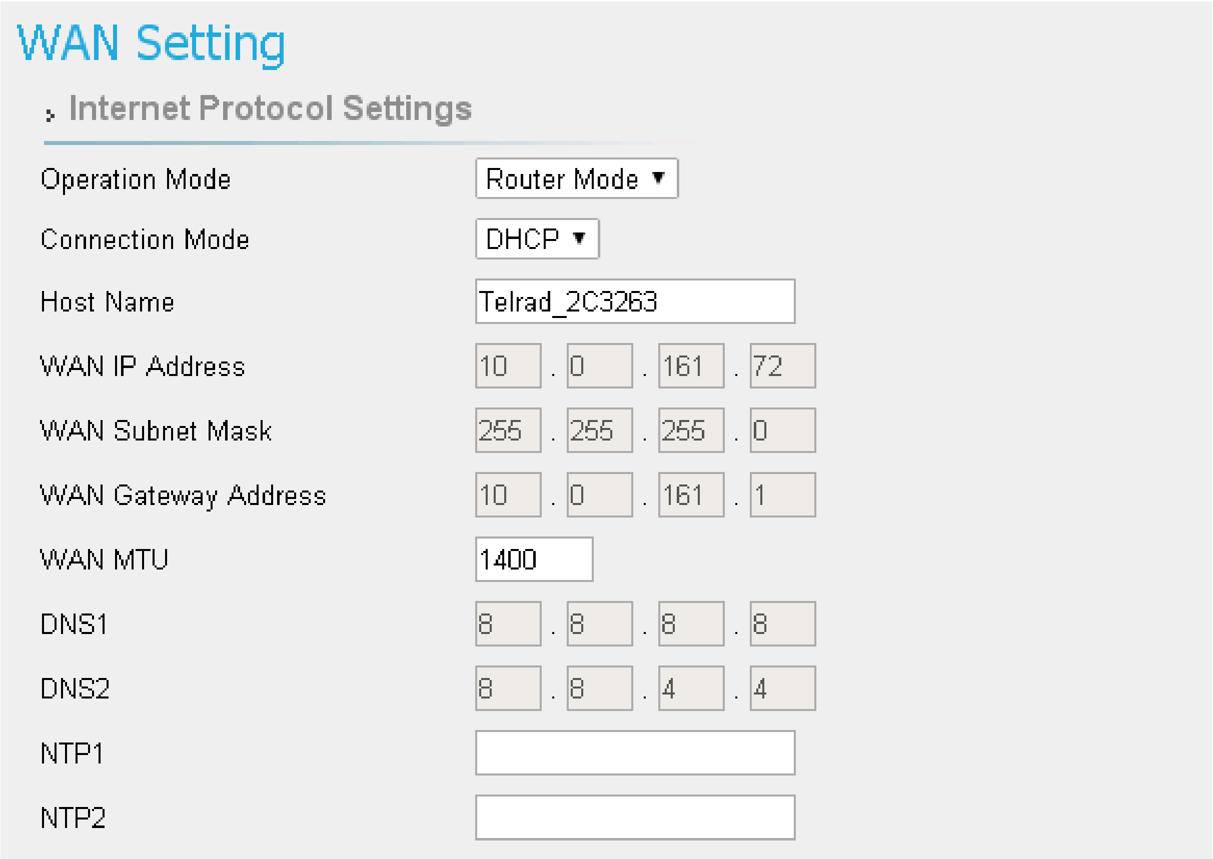
Multi-PDN in Bridge Mode

- **NTP1/2:** It is used to calibrate the time in CPE. Users can specify two NTP servers in “IP” or “Domain name” format. For example **45.79.167.181**or **0.us.pool.ntp**

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | WAN Setting (Router Mode)

- **Operation Mode:** users have **NAT**, **Tunnel**, **Bridge** and **Router** mode to choose from. The following pages will show how to configure “**Router mode**”.



WAN Setting

Internet Protocol Settings

Operation Mode	Router Mode ▼
Connection Mode	DHCP ▼
Host Name	Telrad_2C3263
WAN IP Address	10 . 0 . 161 . 72
WAN Subnet Mask	255 . 255 . 255 . 0
WAN Gateway Address	10 . 0 . 161 . 1
WAN MTU	1400
DNS1	8 . 8 . 8 . 8
DNS2	8 . 8 . 4 . 4
NTP1	
NTP2	

Network > WAN Setting

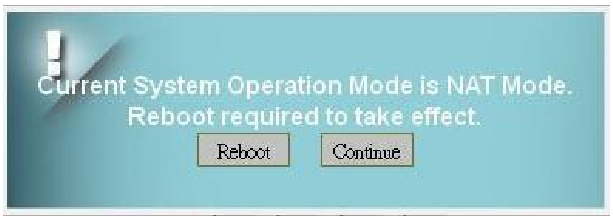
- **Connection Mode:** “DHCP” or “Static”.
  - ➢ If “DHCP” mode is selected, CPE would automatically acquire configuration information from a DHCP server.
  - ➢ if “Static” mode is selected, users have to manually enter the required information in below fields.
- **Host Name:** Currently no function.

!	Host Name“**Telrad_2C3263”** Just an example here, in general, it will be like XXXXX_YYYYYY (XXXXX = Service Provider) (YYYYYY = Last six words of WAN MAC.)

- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when “**Connection mode**” is “**DHCP**” and editable when “**Connection mode**” is “**Static**”.

- **WAN MTU:** This value is "Maximum Transmission Unit". It is the largest size of a single packet.
- **DNS1/2:** Domain Name Server. It is editable when users select "**Static**" in "**Connection Mode**". Otherwise, these values will be given by DHCP server.
- **NTP1/2:** It is used to calibrate the time in CPE. Users can specify two NTP servers in "IP" or "Domain name" format. For example **45.79.167.181** or **0.us.pool.ntp.org**

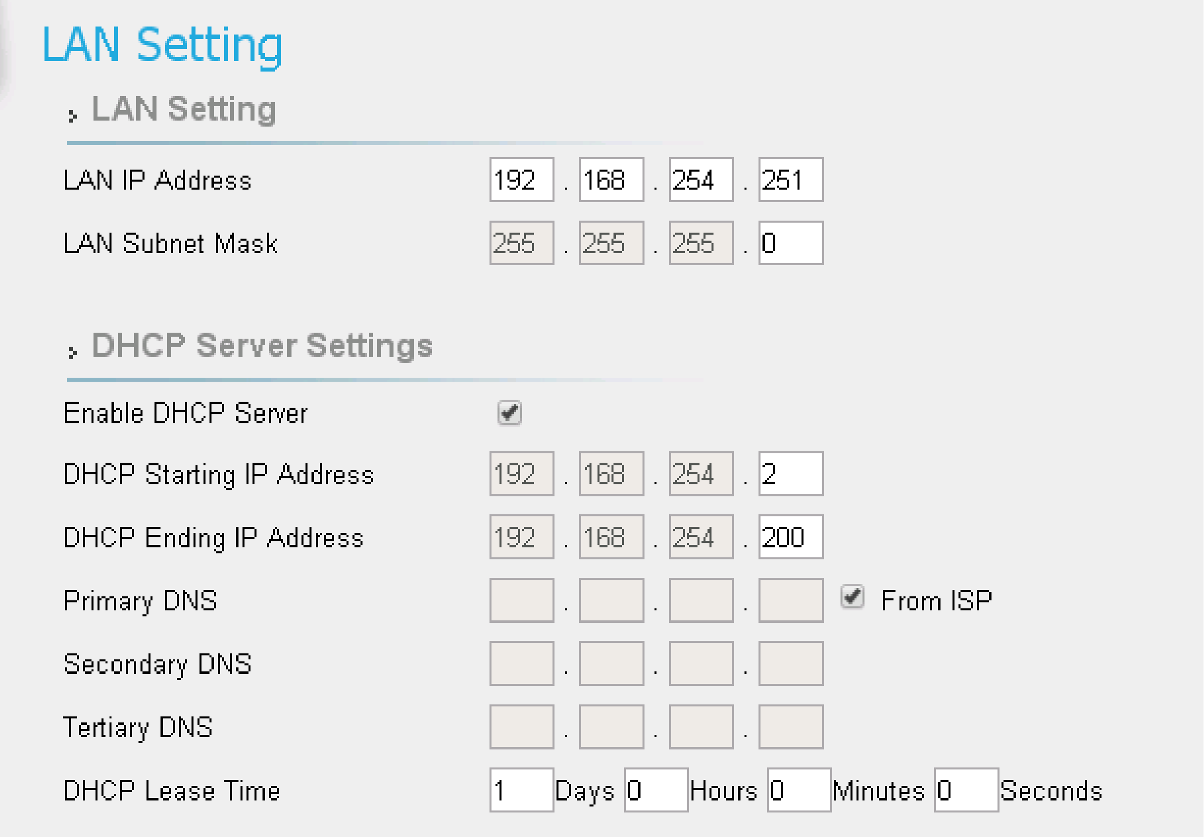
!	Changing the "**Operation Mode**" needs reboot to take effect. A pop-up window will ask users to "**Reboot**" or "**Continue**". If you select "**Reboot**", CPE would reboot right away. If you select "**Continue**", CPE would not reboot automatically, you need to reboot it manually.


Current System Operation Mode is NAT Mode.
Reboot required to take effect.

Pop-up windows for reboot confirm

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | LAN Setting



LAN Setting

LAN Setting

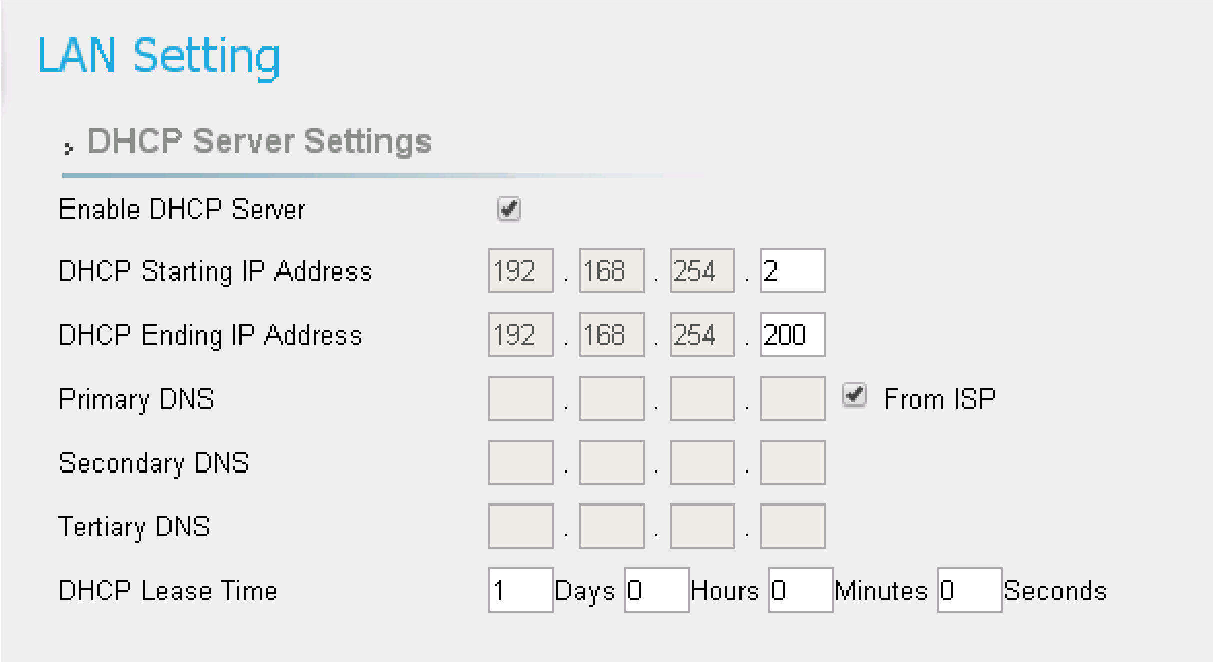
LAN IP Address	192 . 168 . 254 . 251
LAN Subnet Mask	255 . 255 . 255 . 0

DHCP Server Settings

Enable DHCP Server	☑
DHCP Starting IP Address	192 . 168 . 254 . 2
DHCP Ending IP Address	192 . 168 . 254 . 200
Primary DNS	. . . ☑ From ISP
Secondary DNS	. . .
Tertiary DNS	. . .
DHCP Lease Time	1 Days 0 Hours 0 Minutes 0 Seconds

Network > LAN Setting

- **LAN Setting:**
  - ➢ **LAN IP Address / Subnet Mask:** The IP address and subnet mask used by CPE in LAN
    - ◆ If users choose "**L2TP with BCP Enabled**" in "**Operation Mode**", this IP only means a back-up IP address. When users cannot link to CPE web GUI due to the dynamic IP address, users can use the back-up IP address to link to CPE web GUI instead.
    - ◆ If users choose other tunnel mode, this IP means LAN side domain and Web GUI IP address.(This IP will change IP prefix in "**DHCP Server**" , "**Port Forwarding**" and "**Port Trigger**")
- **DHCP Server:** (Available in NAT, Tunnel, Router Mode)



LAN Setting

DHCP Server Settings

Enable DHCP Server	☑
DHCP Starting IP Address	192 . 168 . 254 . 2
DHCP Ending IP Address	192 . 168 . 254 . 200
Primary DNS	. . . ☑ From ISP
Secondary DNS	. . .
Tertiary DNS	. . .
DHCP Lease Time	1 Days 0 Hours 0 Minutes 0 Seconds

Network > LAN Setting

CPE has a built-in DHCP server to manage the distribution of IP addresses. A device connected to CPE through the Ethernet port would obtain a dynamic IP address from CPE.

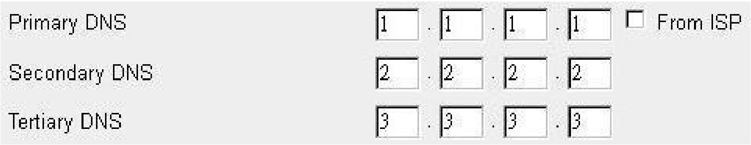
- **Enable DHCP Server:** enable/disable DHCP server
- **DHCP Starting IP Address:** The starting IP address assigned by DHCP server.
- **DHCP Ending IP Address:** The ending IP address assigned by DHCP server.

!	Notice that Ethernet share the same DHCP server, the range of IP addresses should not be narrow. Otherwise, clients cannot get LAN IP addresses.

- **From ISP:** When the checkbox is ticked, clients set CPE as DNS server, but CPE will only act as a "**DNS relay**". The following picture is captured from a PC in LAN, DNS Server field is 192.168.254.251 (LAN IP of CPE). DNS request will be sent to 192.168.254.251 then forwarded to ISP DNS Server.

If users want to know DNS Servers obtained from ISP, It can be found in “**Network > Status > WAN Information > DNS Server**”

- **Primary/Secondary/Tertiary DNS:** If the checkbox “**From ISP**” is not ticked, users can designate the DNS server for DHCP clients. Two pictures below are captured from CPE and a PC in LAN, DNS fields are “1.1.1.1”, “2.2.2.2” and “3.3.3.3”. Clients’ DNS request will be directly sent to the first operative server in the order of primary, secondary and tertiary DNS.



Primary DNS	1 . 1 . 1 . 1	□ From ISP
Secondary DNS	2 . 2 . 2 . 2	
Tertiary DNS	3 . 3 . 3 . 3	

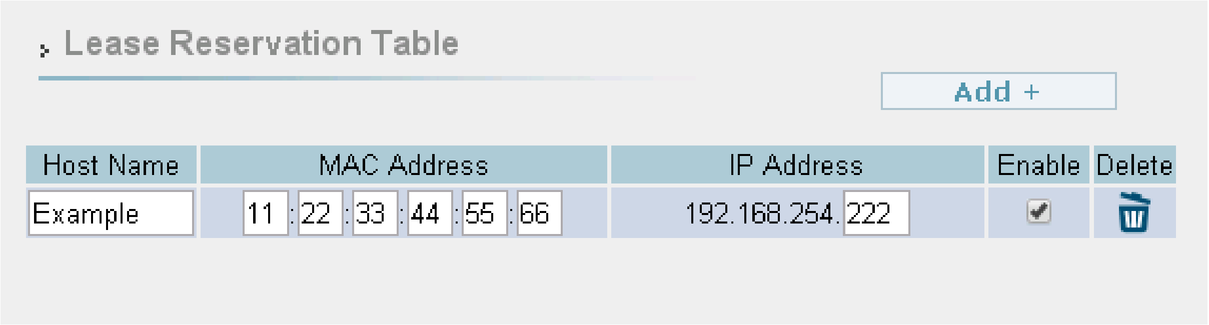
Network > DHCP Server > not From ISP

“1.1.1.1”, “2.2.2.2” and “3.3.3.3” are examples.

- **DHCP Lease Time:** The life time of the IP assigned by DHCP server(range: 2 minutes-365days)

- **Lease Reservation Table:** This table records the mapping of MAC and IP addresses. Clients with the specific MAC address in the table would get the corresponding IP address. Click “**Add +**” button to add a new mapping, clicking **“Delete”** icon 🗑) to delete it. To enable the mapping, users have to tick the “**Enable**” checkbox.

  An example is illustrated below. If a client with MAC Address “**11:22:33:44:55:66**” requests IP, DHCP server will assign IP “**192.168.254.222**” and the host name “**Example**” to it.



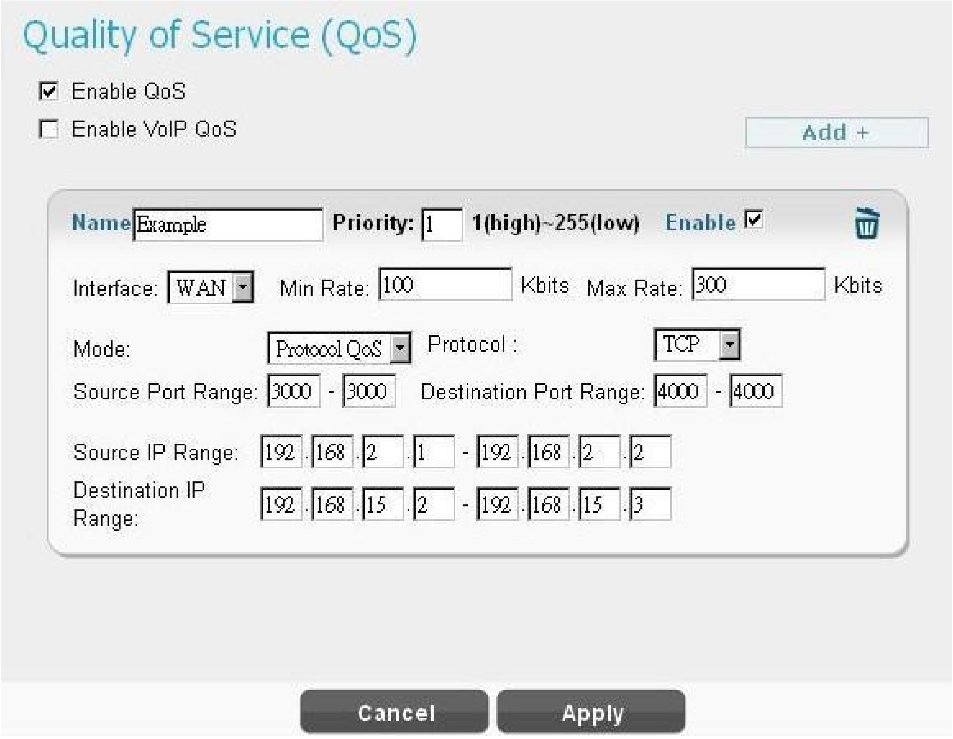
Lease Reservation Table

Host Name	MAC Address	IP Address	Enable	Delete
Example	11 : 22 : 33 : 44 : 55 : 66	192.168.254.222	☑	🗑

!	“Example”, “11:22:33:44:55:66”, “192.168.254.222” are examples here.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | QoS (Available in NAT, Tunnel, Router Mode)



Quality of Service (QoS)

☑ Enable QoS

☐ Enable VoIP QoS

Name: Example Priority: 1 1(high)~255(low) Enable ☑

Interface: WAN Min Rate: 100 Kbits Max Rate: 300 Kbits

Mode: Protocol QoS Protocol : TCP

Source Port Range: 3000 - 3000 Destination Port Range: 4000 - 4000

Source IP Range: 192 .168 .2 .1 - 192 .168 .2 .2

Destination IP Range: 192 .168 .15 .2 - 192 .168 .15 .3

Network > QoS

QoS stands for "Quality of Service", different network services can be prioritized. Users have to add rules which designate that network flow through certain port ranges or IP address range would have a guaranteed sending rate. Click **"Add +"** button to add a new rule, clicking **"Delete"** icon 🗑) to delete the rule.

- **Enable QoS:** Enable/disable QoS.
- **Enable VoIP QoS: S**et generic rules for VoIP service, like UDP and TCP port 5060, 11720….
- **Name:** Name of the rule.
- **Priority:** Priority of each rule, "**1**" is the highest priority, "**255**" is the lowest priority.
- **Enable:** Enable/Disable the rule.
- **Interface:** The interface that the rule is applied to.
- **Min Rate:** The guaranteed sending rate if the traffic needs at least min rate and the bandwidth is abundant.
- **Max Rate:** The maximum sending rate" if the bandwidth is abundant**.**

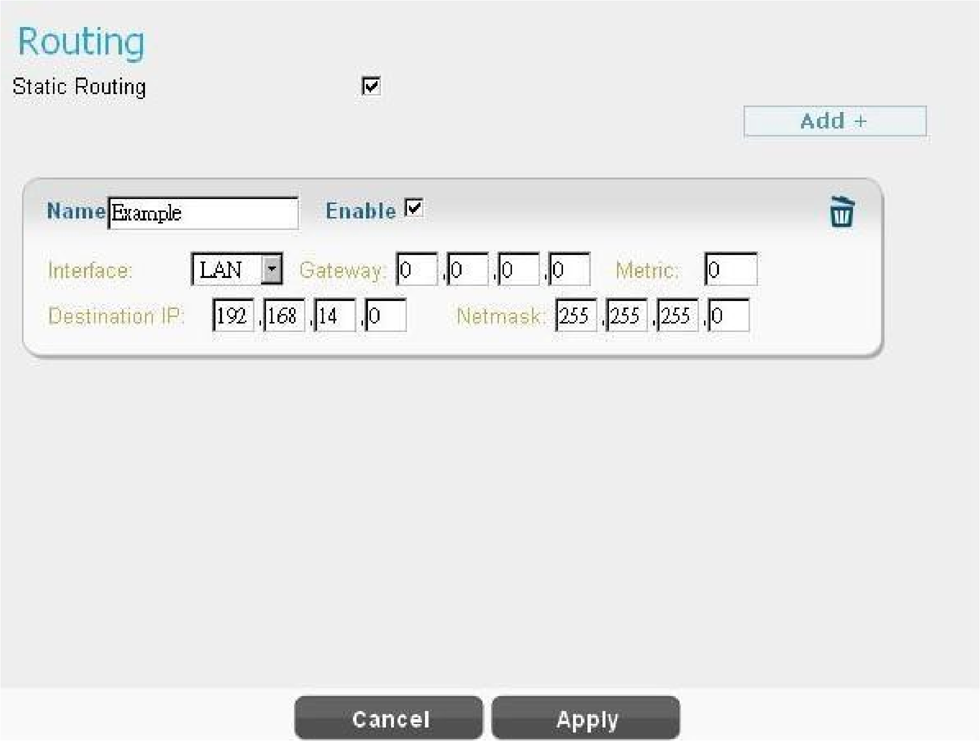
!	About **Min Rate** and **Max Rate**, we can discuss this in 3 cases. For example, Min Rate=**50** kbps Max Rate=**100** kbps 1. If **20** kbps is needed, the traffic will only get **20** kbps, CPE will not give it **50** kbps (50 kbps=Min Rate, this can prevent wasting bandwidth) 2. If **60** kbps is needed, the traffic at least gets **50** kbps and CPE tries to satisfy **60** kbps requirement. 3. If **200** kbps is needed, the traffic will only get **100** kbps due to max rate constraint.

- **Mode:** Only protocol QoS
- **Protocol:** "TCP", "UDP", "ICMP" and "ANY". ANY includes TCP, UDP and ICMP.
- **Source/ Destination Port Range and Source/ Destination IP Range:** The port and IP range of the traffic that needs QoS.

!	Source/Destination Port and Source/Destination IP can be an **empty value**, which means "**DON'T CARE**".

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | Routing (Available in Tunnel, Router Mode)



Routing

Static Routing ☑

Name Example Enable ☑

Interface: LAN Gateway: 0 .0 .0 .0 Metric: 0

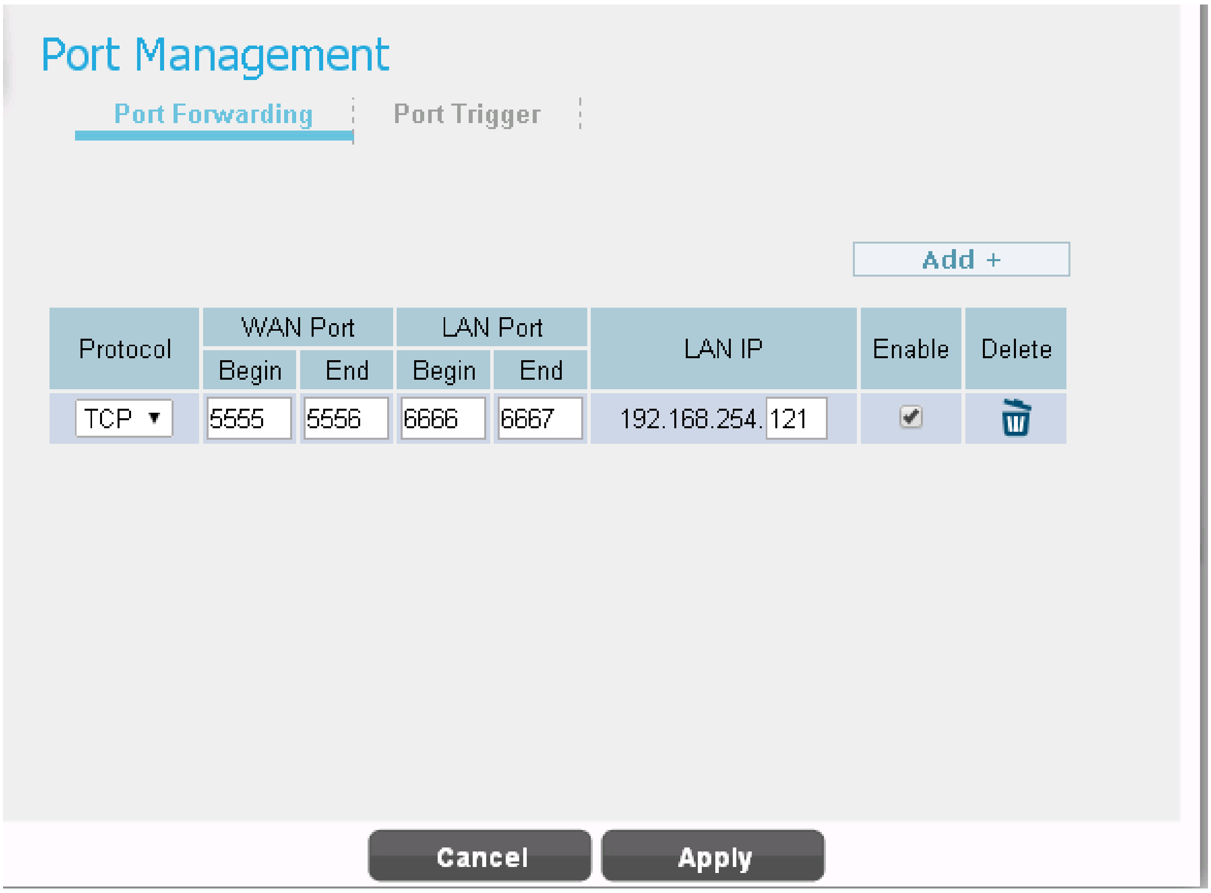
Destination IP: 192 .168 .14 .0 Netmask: 255 .255 .255 .0

Network > Routing

Users can designate routing rules of CPE

- Static Routing: Enable/Disable static routing.
- Click **“Add +”** button to add a new rule, clicking **“Delete”** icon 🗑) to delete the rule.
- **Name:** Name of the rule.
- **Enable:** Enable/Disable the rule.
- **Interface:** The interface that the rule is applied to.
- **Gateway:** The gateway of the routing rule
- **Metric:** The metric of the routing rule. It’s the distance related to the route.
- **Destination IP:** The destination IP or a subnet.
- **Netmask:** The subnet mask of the rule.

Network | Port Management | Port Forwarding (Available in NAT, Tunnel Mode)



Protocol	WAN Port		LAN Port		LAN IP	Enable	Delete
	Begin	End	Begin	End			
TCP ▾	5555	5556	6666	6667	192.168.254. 121	☑	🗑

Network > Port Management > Port 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.

- Click **"Add +"** button to add a new rule, clicking **"Delete"** icon 🗑) to delete the rule.
- **Protocol:** TCP or UDP.
- **WAN Port:** The range of WAN port.
- **LAN Port:** The range of LAN port.
- **LAN IP:** Enter the IP which desires to receive forwarded packets.
- **Enable:** Enable/Disable the rule

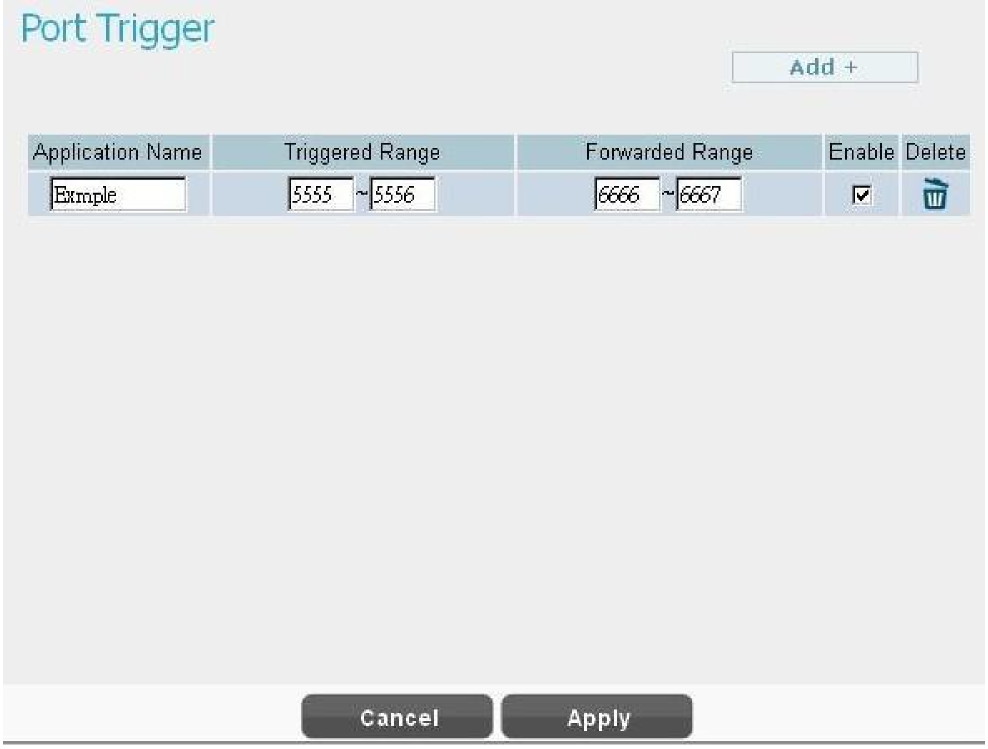
- **Delete:** Delete the rule.

❗	WAN Port 53, 68, 113, 123, 161, 2948, 7547, 58603 are reserved for management use.

❗	The priority of port forwarding rules is higher than DMZ. Users can set DMZ and it will not influence port forwarding.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | Port Management | Port Trigger (Available in NAT, Tunnel Mode)



Application Name	Triggered Range	Forwarded Range	Enable	Delete
Exmple	5555 ~ 5556	6666 ~ 6667	☑	🗑

Network > Port Management > Port Trigger

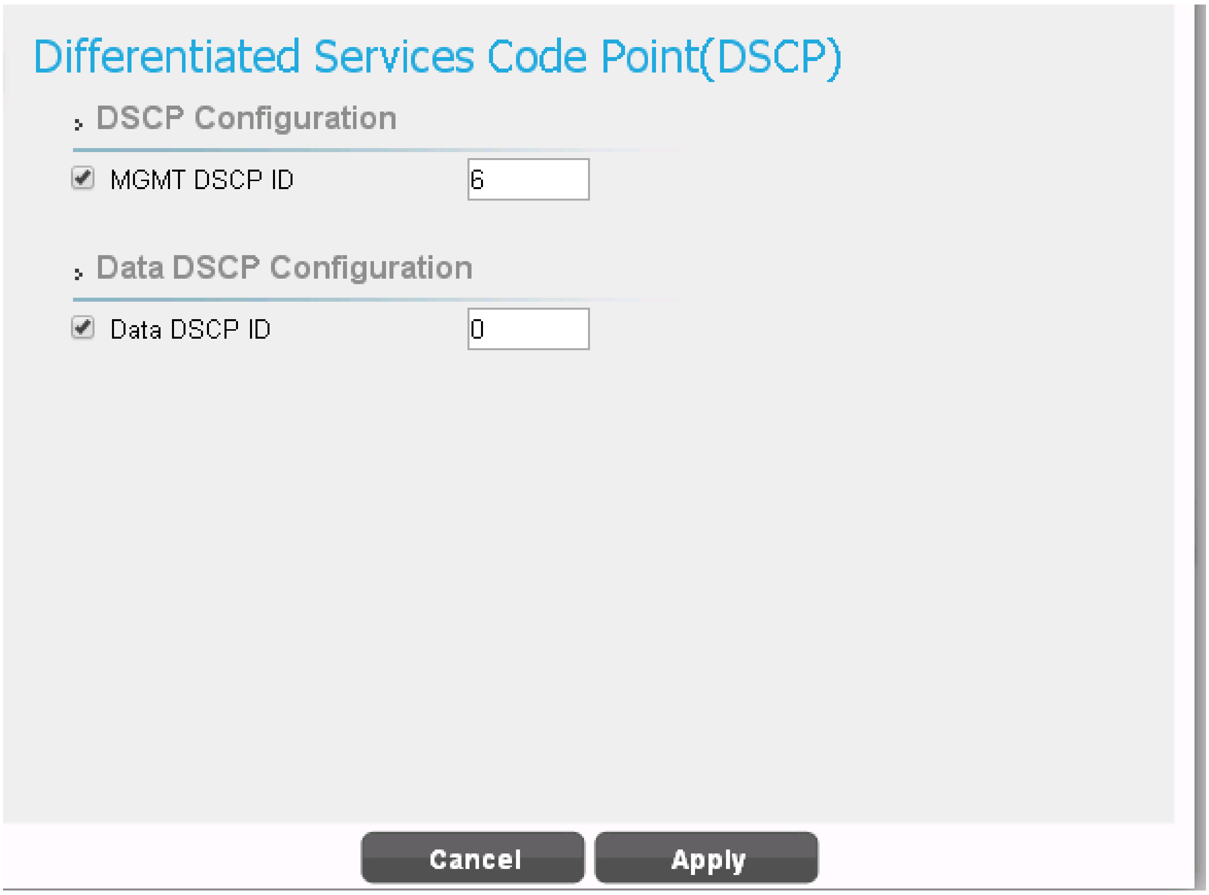
The table allows you to configure Port Trigger rules. Port Trigger is a way to automate port forwarding. Outbound traffic on predetermined ports ('trigger port') causes inbound traffic to specific ports (call it port **P** here) to be dynamically forwarded to the host which uses trigger port. Port **P**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

- **Application Name:** Name of the port trigger rule.
- **Triggered Range:** Traffic passing through **t**he port in the triggered range would automatically open the forwarded port in the forwarded range. The ports in the triggered range are LAN ones.
- **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.

- **Enable:** Enable/Disable the rule.
- **Delete:** Delete the rule.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | DSCP



Differentiated Services Code Point(DSCP)

☑ MGMT DSCP ID 6

☑ Data DSCP ID 0

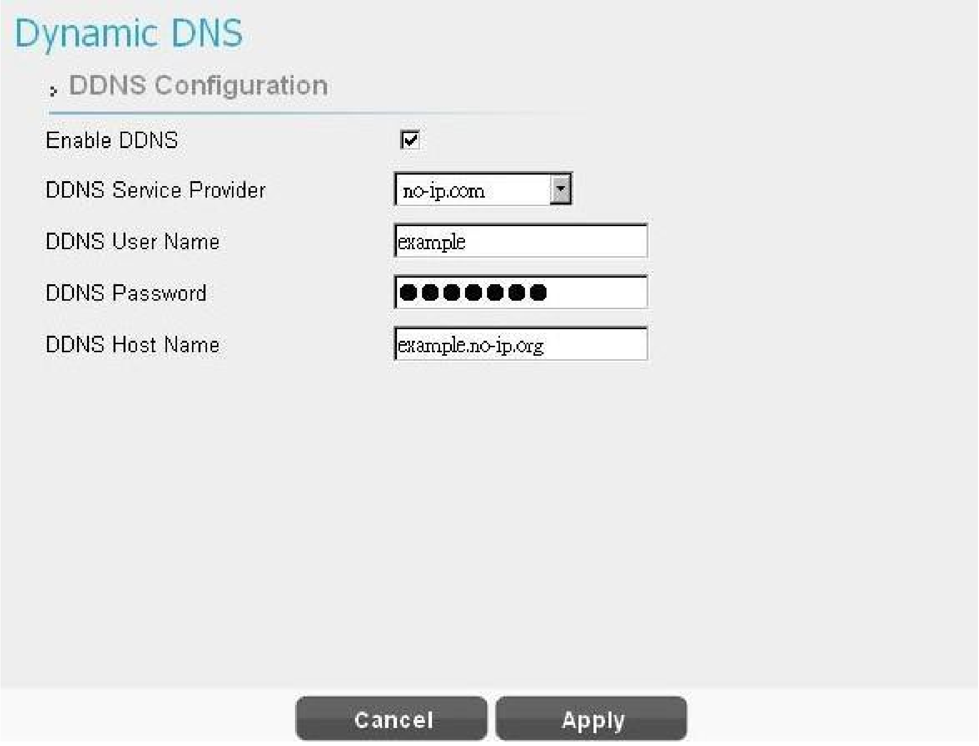
Network > DSCP

Differentiated Services Code Point (DSCP) is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing quality of service (QoS) on modern IP networks.

- **DSCP value range is between 0~63**

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | MGMT Service | Dynamic DNS



Dynamic DNS

DDNS Configuration

Enable DDNS	☑
DDNS Service Provider	no-ip.com
DDNS User Name	example
DDNS Password	●●●●●●●
DDNS Host Name	example.no-ip.org

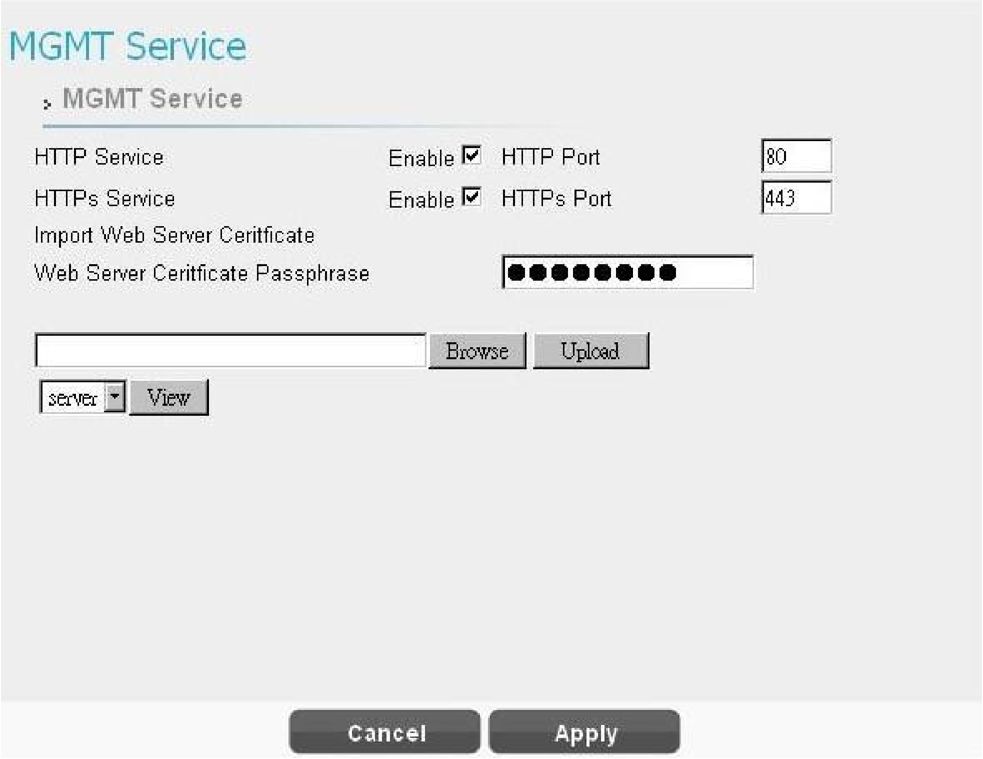
Network > MGMT Service > Dynamic DNS

Dynamic Domain Name System (DDNS) is a mechanism that can map a fixed domain name to a dynamic IP address. This is very useful when you can only get a dynamic IP in WAN. If DDNS is enabled, clients can connect to CPE through "DDNS Host Name".

- **Enable DDNS:** Enable/Disable DDNS.
- **When DDNS is enabled,** select the DDNS service provider you registered from the drop-down list, and configure the following parameters: **DDNS Service Provider**, **DDNS User Name**, **DDNS Password**, and **DDNS Host Name**.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Network | MGMT Service | Web Service



MGMT Service

MGMT Service

HTTP Service Enable ☑ HTTP Port 80

HTTPs Service Enable ☑ HTTPs Port 443

Import Web Server Ceritficate

Web Server Ceritficate Passphrase ●●●●●●●●●

Network > MGMT Service

MGMT service is about HTTP and HTTPs configuration.

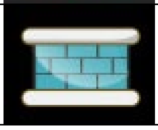
- **HTTP Service:** When it is enabled, clients in the LAN side can link to CPE HTTP service. Users can set the port used by HTTP service.
- **HTTPs Service:** When it is enabled, clients in the LAN can link to CPE HTTPs service. Users can set the port used by HTTPs service. Clients in the WAN side are able to link to CPE HTTPs service when "**HTTPs service**" is on and "**allow HTTPs login from WAN"** in firewall section is on. Please note that the clients in LAN and WAN may use different ports to link to CPE HTTPs service.
- **Import WEB Certificate:** The certificate is used by HTTPs service, users can upload the certificate and prepare the passphrase for CPE and view the current certificate through view button.

❗	The port number setting in this page is only for LAN; if users want to login to GUI from WAN, it needs to enable ***"Allow Https login from WAN"*** in **"**Firewall | Basic".

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Firewall

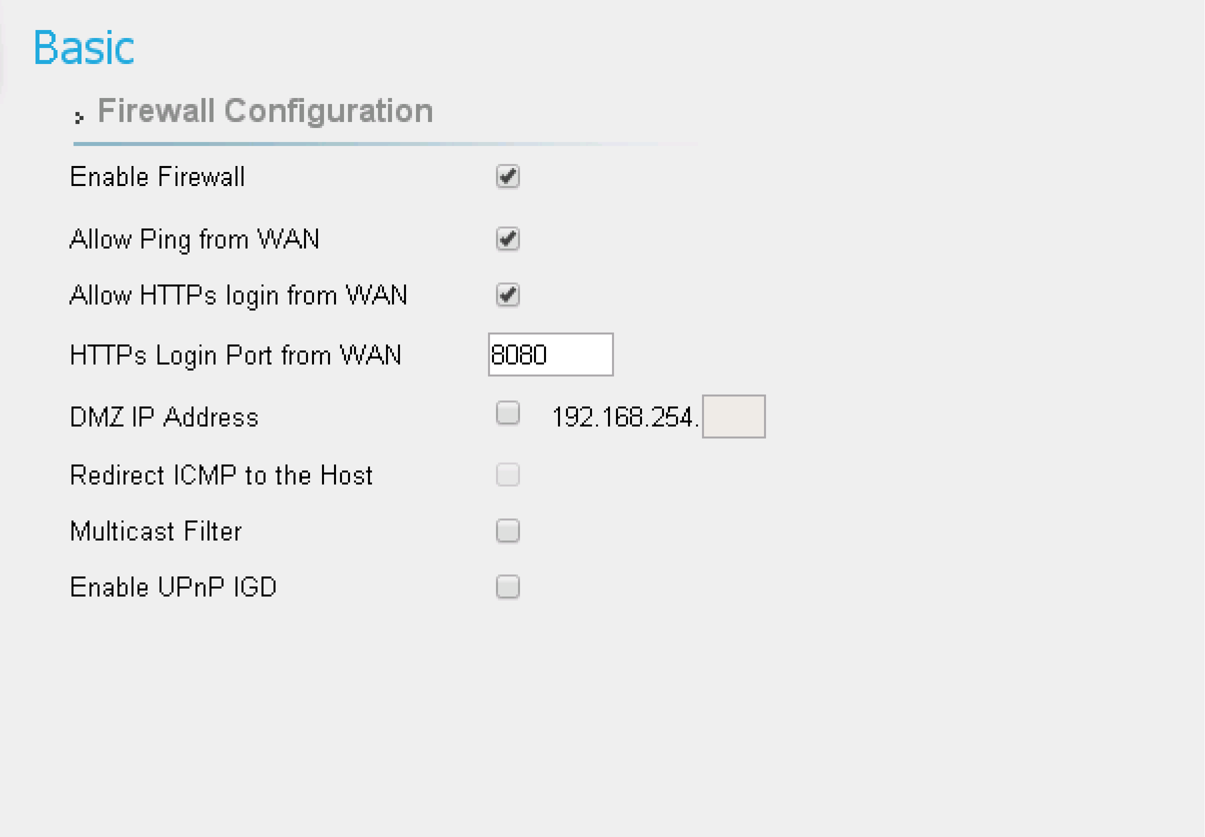
The “Firewall” page allows user to configure firewall to block and grant some network access.

	Display in **Brief Summary Page**
	Display in “**Quick Panel**” of **Detailed Configuration Page**

- **Menu structure:**

Firewall	Basic
	L3 MGMT Filter
	L3 DATA filter
	L2 Filter
	Access Restriction

Firewall | Basic



Basic

Firewall Configuration

Enable Firewall	☑
Allow Ping from WAN	☑
Allow HTTPs login from WAN	☑
HTTPs Login Port from WAN	8080
DMZ IP Address	□ 192.168.254.
Redirect ICMP to the Host	□
Multicast Filter	□
Enable UPnP IGD	□

Firewall > Basic

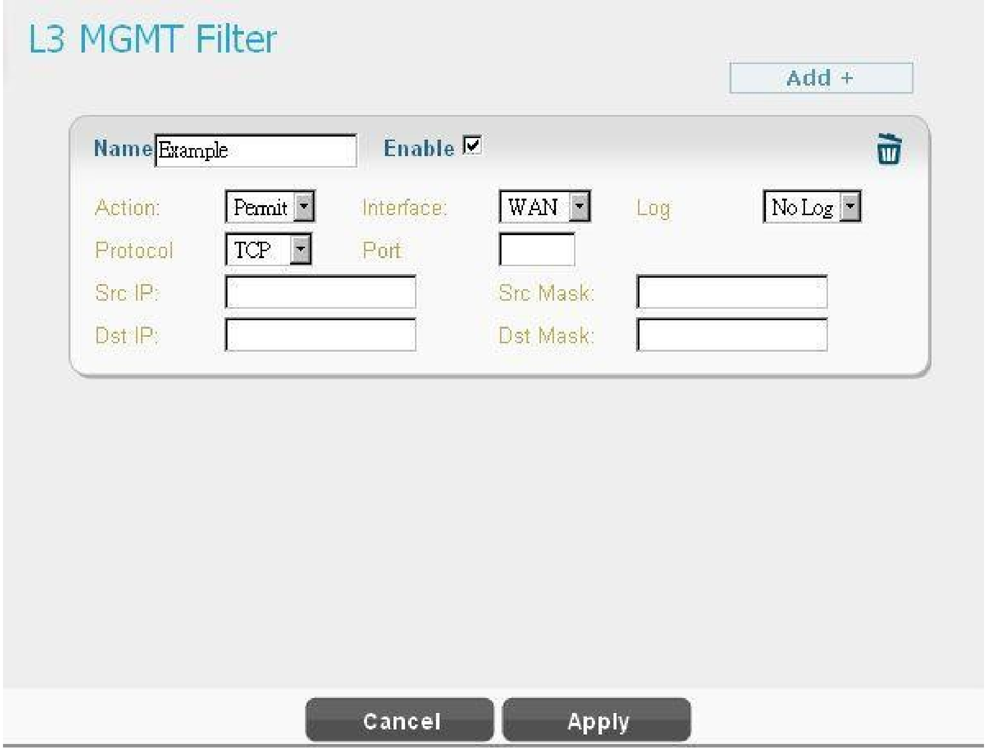
- **Enable Firewall:** Enable/Disable firewall.
- **Allow ping from WAN**: As titled.
- **Allow HTTPs login from WAN:** It is available only when HTTPs Service is enabled in Network | MGMT Service.
- **HTTPs Login Port from WAN:** As titled.
- **DMZ IP Address:** All network traffic from WAN is forwarded to this IP address in LAN.
- **Redirect ICMP to the host:** The function will be activated if DMZ is enabled. Tick the checkbox to have CPE pass ICMP messages to hosts, or un-tick the checkbox to let the CPE reply ICMP messages.
- **Multicast Filter**: If the checkbox is ticked, multicast packets would be dropped; otherwise,

they pass through.

- **Enable UPnP IGD:** Active UPnP function on CPE.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Firewall | L3 MGMT Filter



L3 MGMT Filter

Name	Example	Enable ☑			
Action:	Permit	Interface:	WAN	Log	No Log
Protocol	TCP	Port			
Src IP:		Src Mask:			
Dst IP:		Dst Mask:			

Firewall > L3 MGMT Filter

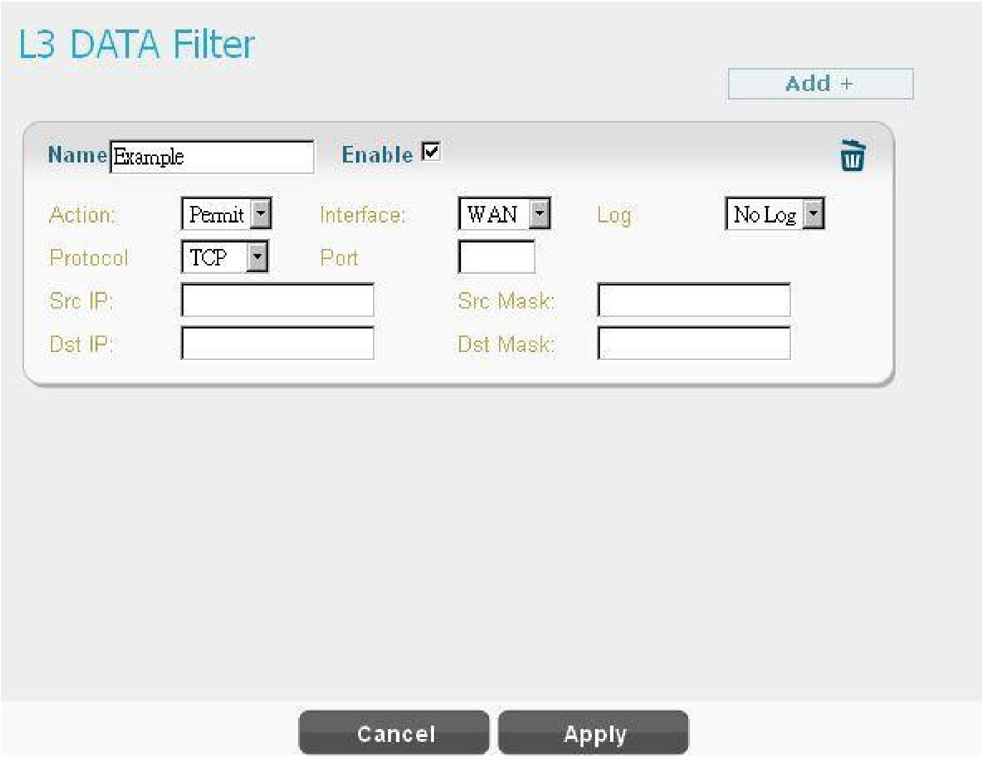
L3 MGMT filter disallow/allows packets with certain ports and IP address which is sent to CPE.

- Click **"Add +"** button to add a new rule, clicking **"Delete"** icon 🗑) to delete the rule.
- **Name:** The name of the rule.
- **Action:** Select "Permit" or "Deny" to allow the access or reject the traffic.
- **Interface:** Select which interface users want to block/allow the traffic from. Available options are "WAN", "LAN", or "BOTH".
- **Log:** Select "Log" to have log records, or "No Log" to disable it. (users would not see it, log is printed in the console.)
- **Protocol:** Protocol to filter. Available options are TCP, UDP, ICMP, or ANY.
- **Port:** The port number to filter.
- **Src IP:** The source IP to filter.
- **Dst IP:** The destination IP to filter.
- **Src Mask:** It would be used with Src IP to form a subnet.

- **Dst Mask:** It would be used with Dst IP to form a subnet.
- **Enable:** Enable/Disable the rule.
- **Delete:** Delete the rule. You need to press the apply button to take effect.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Firewall | L3 DATA Filter



L3 DATA Filter

Name: Example   Enable ☑

Action:	Permit	Interface:	WAN	Log	No Log
Protocol	TCP	Port			
Src IP:		Src Mask:			
Dst IP:		Dst Mask:			

Firewall > L3 DATA Filter

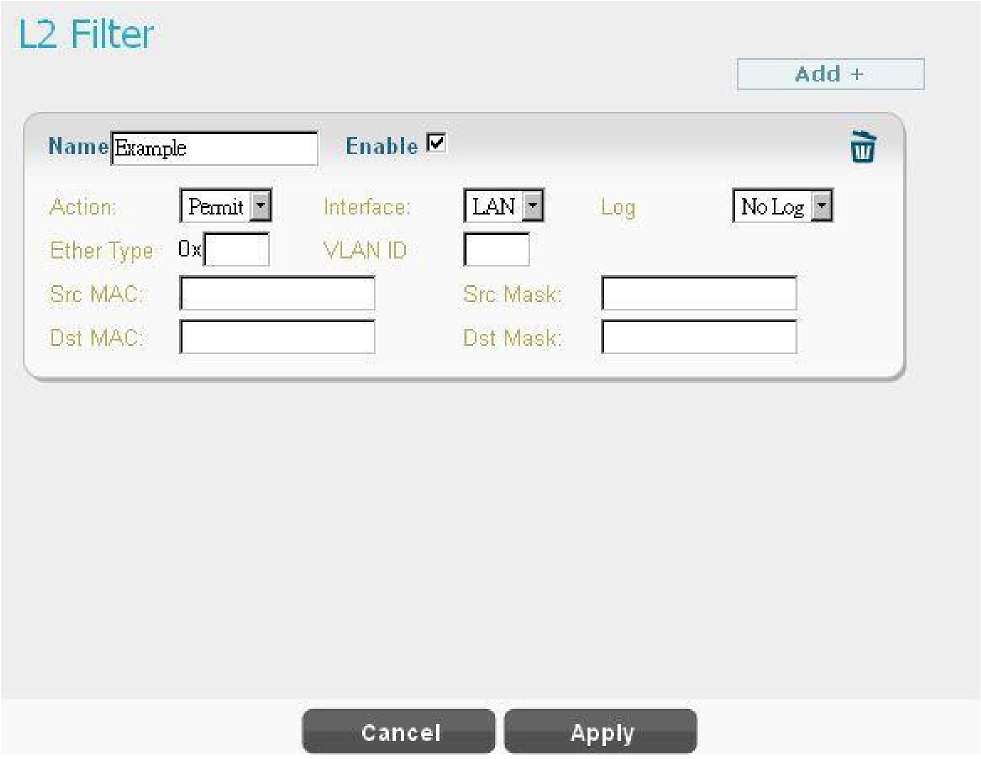
L3 DATA filter disallow/allows packets with designated ports and IP address to the device which is not CPE.

- Click **"Add +"** button to add a new rule, clicking **"Delete"** icon 🗑) to delete the rule.
- **Name:** The name of the rule.
- **Action:** "Permit" or "Deny" to allow or to reject the traffic.
- **Interface:** Select which interface users want to block/allow the traffic from. Available options are "WAN", "LAN", or "BOTH".
- **Log:** Select "Log" to have log records, or "No Log" to disable it. (users will not see it , the log is printed in the console.)
- **Protocol:** Protocol to filter. Available options are TCP, UDP, ICMP, or ANY.
- **Port:** The port number to filter.
- **Src IP:** The source IP to filter.

- **Dst IP:** The destination IP to filter.
- **Src Mask:** It would be used with Src IP to form a subnet.
- **Dst Mask:** It would be used with Dst IP to form a subnet.
- **Enable:** Enable/Disable the rule.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Firewall | L2 Filter



L2 Filter

Name: Example
Enable ☑

Action:	Permit	Interface:	LAN	Log	No Log
Ether Type	0x	VLAN ID			
Src MAC:			Src Mask:		
Dst MAC:			Dst Mask:		

Firewall > L2 Filter

L2 filter can filter packets in layer 2 of the 7-layer OSI model of computer network.

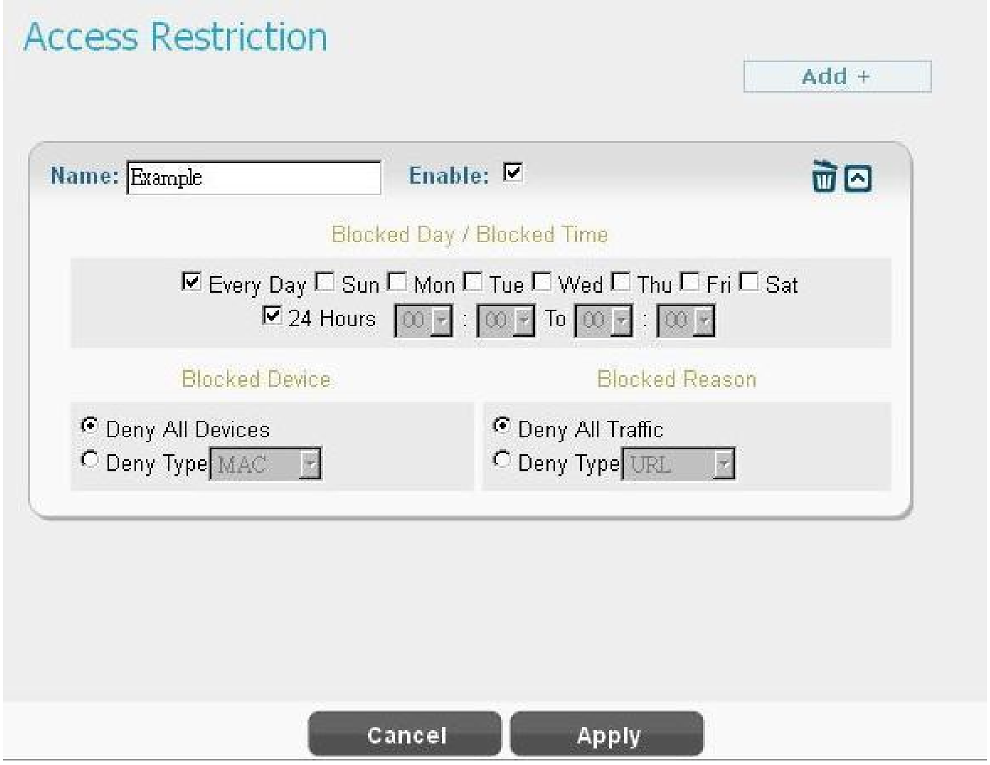
- Click **"Add +"** button to add a new rule, clicking **"Delete"** icon 🗑) to delete the rule.
- **Name:** Enter the name of the rule.
- **Action:** Select "Permit" or "Deny" to allow or reject the traffic.
- **Interface:** only LAN.
- **Log:** Select "Log" to have log records, or "No Log" to disable it. (Users will not see it, the log is printed in the console.)
- **Ether Type:** EtherType is a two-octet field in an Ethernet frame, which is used to indicate which protocol is encapsulated in the payload of an Ethernet frame. Enter the Ether Type code (Range: 0600~FFFF) according to the protocol you use.
- **VLAN ID:** IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) in Ethernet network; and VLAN ID is the identification of the VLAN. VLAN ID is a unique VLAN identifier, the number range is from 0 to 4095.

- **Src MAC:** The source MAC to filter.
- **Dst MAC:** The destination MAC to filter.
- **Src Mask:** The source Mask to filter.
- **Dst Mask:** The destination Mask to filter.
- **Enable:** Enable/Disable the rule.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

!	The format of MAC address should be XX:XX:XX:XX:XX:XX

Firewall | Access Restriction



Access Restriction

Name: Example Enable: ☑

Blocked Day / Blocked Time

☑ Every Day □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

☑ 24 Hours 00 : 00 To 00 : 00

Blocked Device

● Deny All Devices

○ Deny Type MAC

Blocked Reason

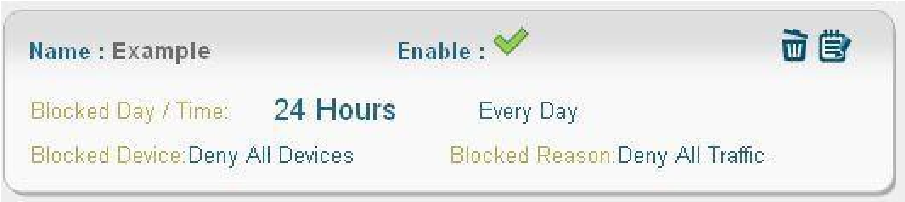
● Deny All Traffic

○ Deny Type URL

Firewall > 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.

- Click **"Add +"** button to add a new rule, clicking **"Delete"** icon 🗑) to delete the rule.
- After pressing "**Apply**" button, the access restriction rule is graphically presented in the following manner. Click 📝 to edit, and click ⏶ to fix it.



Name : Example Enable : ✓

Blocked Day / Time: 24 Hours Every Day

Blocked Device: Deny All Devices Blocked Reason: Deny All Traffic

Firewall > Access Restriction (Digest)

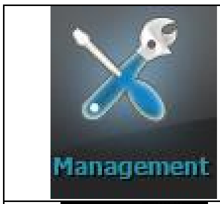
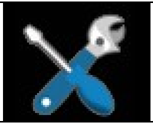
- **Name:** The name of the rule.

- **Enable: E**nable/Disable the rule.
- **Blocked Day / Blocked Time:** The day and time to block the network.
- **Blocked Device:** Block the device with specified MAC address or block packets with specified IP range.
- **Blocked Reason:** (1) block all traffic (2) block packets with specified keyword.

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

Management

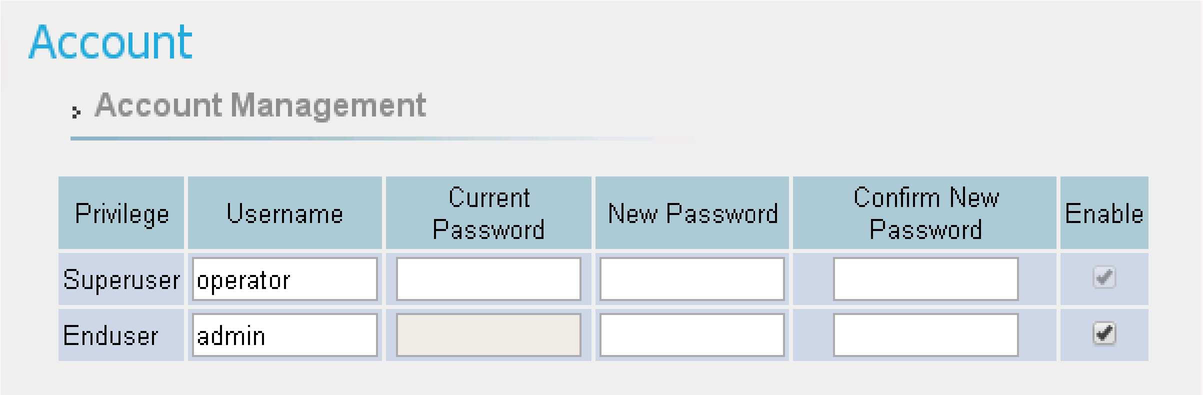
The “Management” page allows user to configure the main system parameters such as password, language, device time/name …etc.

	Display in **Brief Summary Page**
	Display in “**Quick Panel**” of **Detailed Configuration Page**

- **Menu structure:**

Management	Account
	Language
	Device Setting
	Restore Default
	Device Log
	Software
	RM Settings

Management | Account



Account

› Account Management

Privilege	Username	Current Password	New Password	Confirm New Password	Enable
Superuser	operator				☑
Enduser	admin				☑

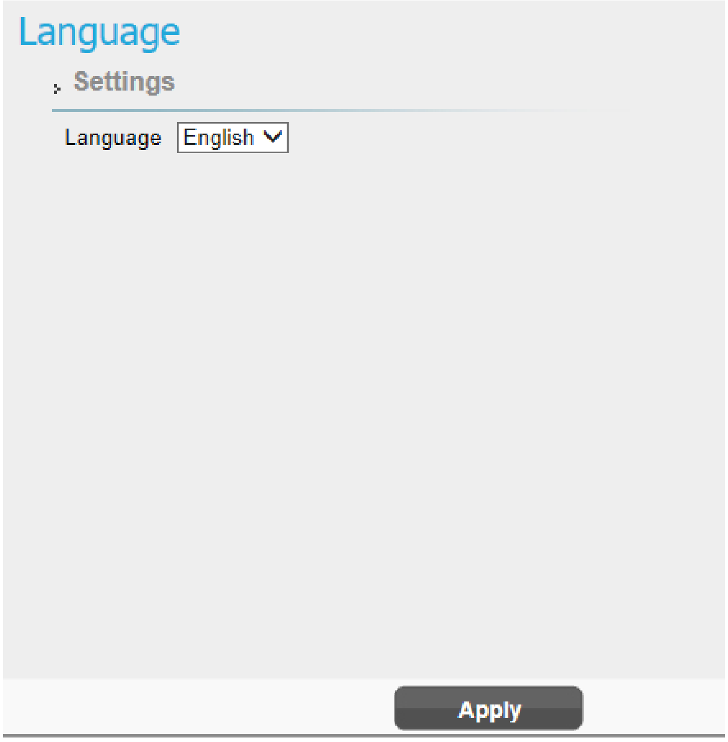
Management > Account Management

The Account Management page lets you change the default username and password for Superuser and Enduser.

- There should be at least 9 characters for the password. Click ***"Apply"*** to save this change. Tick the checkbox ***"Enable"*** to enable the account.

Apply button	Commit the changes made and save them to the CPE device.
Cancel button	Reset fields to the last saved values

Management | Language



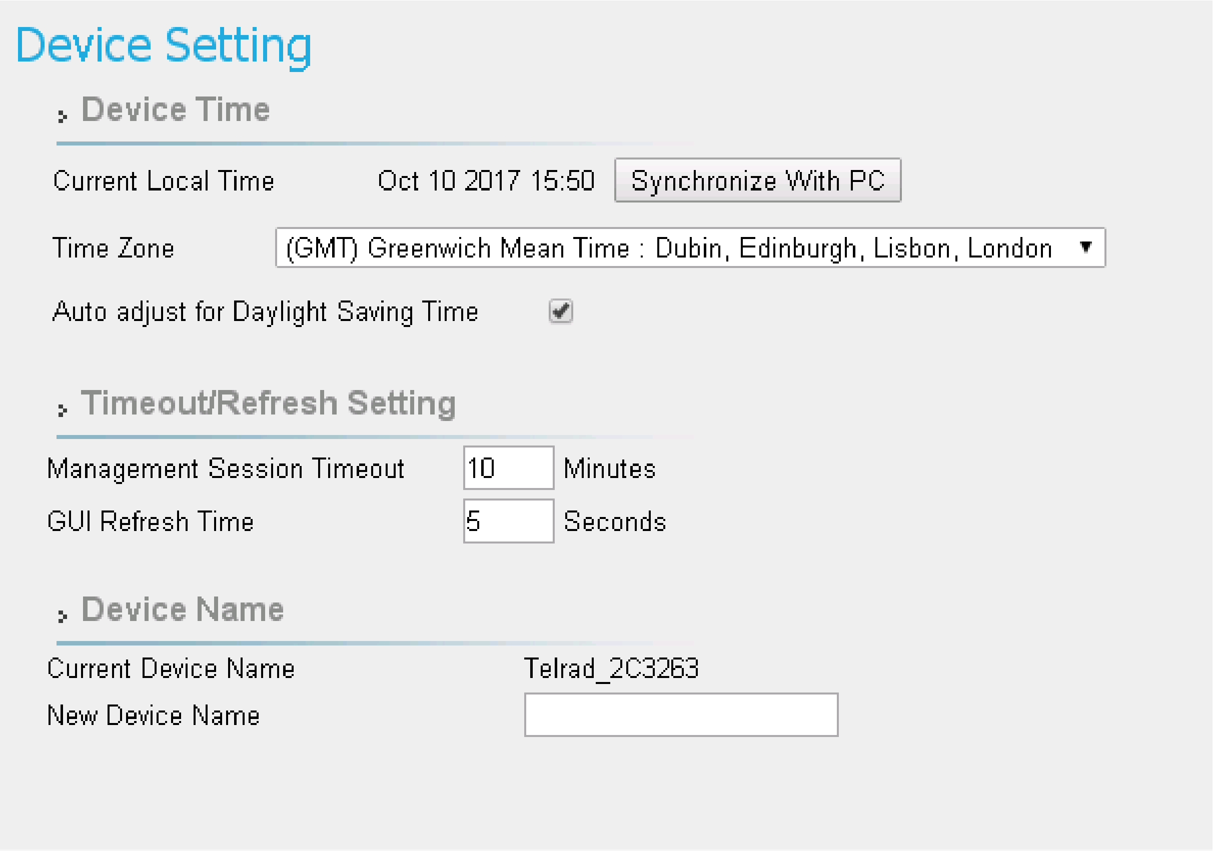
Language: English

Management > Language

The language page allows user to switch the language used in the web. Select the language you want from the drop down list and then click ***"Apply"*** button to apply the changes.

Apply button	Commit the changes made and save them to the CPE device.

Management | Device Setting



Device Setting

Device Time

Current Local Time Oct 10 2017 15:50 Synchronize With PC

Time Zone (GMT) Greenwich Mean Time : Dubin, Edinburgh, Lisbon, London ▼

Auto adjust for Daylight Saving Time ☑

Timeout/Refresh Setting

Management Session Timeout 10 Minutes

GUI Refresh Time 5 Seconds

Device Name

Current Device Name Telrad_2C3263

New Device Name

Management > Device Setting

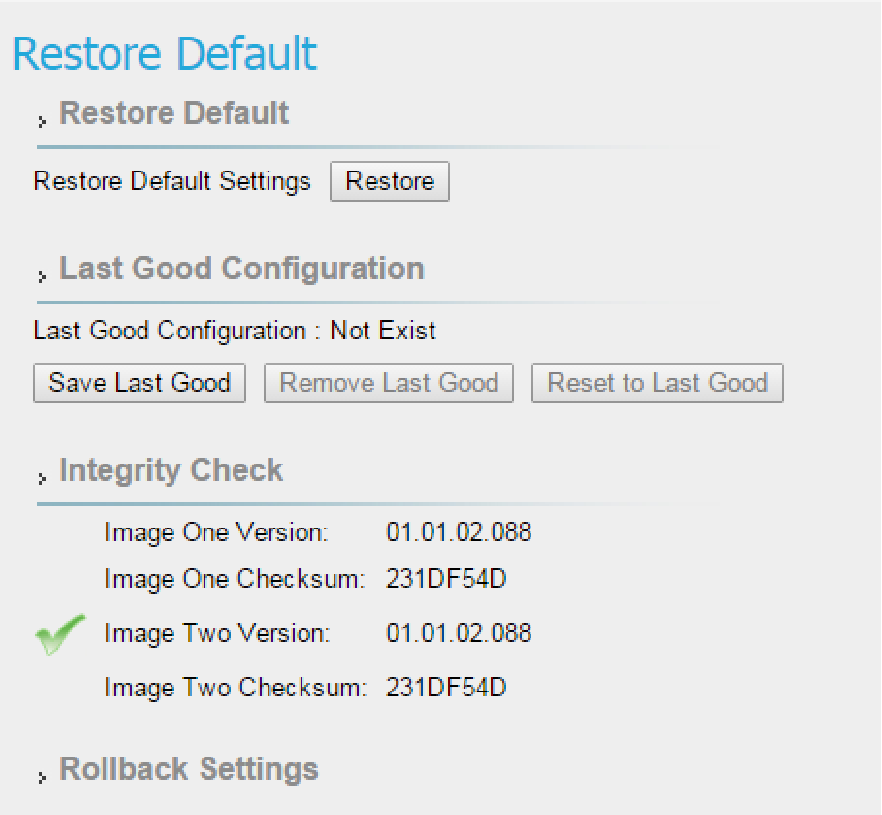
- **Device Time**
  - ➢ **Current Local Time:** Display current local time; or click **"Synchronize with PC"** button to synchronize the time of CPE with PC.
  - ➢ **Time Zone:** as titled.
  - ➢ **Auto Adjust for Daylight Saving Time:** Enable this option if your location observes Daylight Savings Time.
- **Timeout/Refresh Setting**
  - ➢ **Management Session Timeout:** Automatic logout after the period. (Range: 0-10 Minutes; 0 means never expired)
  - ➢ **GUI Refresh Time**: When users press "**auto**" button in any page, the page refresh

every the designated time. (Range: 5-60 Seconds)

- **Device Name:** The name of CPE. Users can log in to CPE from any device in the internal network by entering the device name on the address bar.
  - ➢ **Current Device Name:** Display the current device name.
  - ➢ **New Device Name:** A field to update your current device name.

Apply button	Commit the changes made and save them to the CPE device.
Cancel button	Reset fields to the last saved values

Management | Restore Default



Restore Default

Restore Default

Restore Default Settings: Restore

Last Good Configuration

Last Good Configuration : Not Exist

Save Last Good | Remove Last Good | Reset to Last Good

Integrity Check

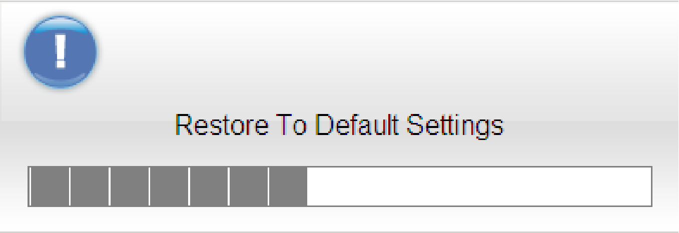
	Image One Version:	01.01.02.088
	Image One Checksum:	231DF54D
✓	Image Two Version:	01.01.02.088
	Image Two Checksum:	231DF54D

Rollback Settings

Management > Restore Default

Select ***Management > Restore* Default** to go back to the factory default settings.

- **Restore Default:** Click **"Restore"** button to clear all users' configuration and restore to factory default settings.



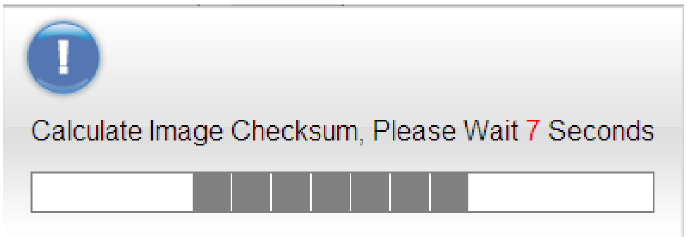
Restore To Default Settings

Restore to default settings Window

- **Last Good Configuration**.
  - ➢ **Save Last Good:** Save the current configuration.

- ➢ **Remove Last Good:** Remove the last saved configuration.
- ➢ **Reset to Last Good:** Load the last saved configuration.

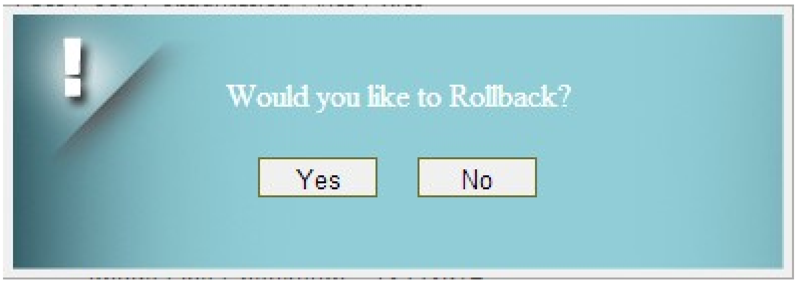
- **Integrity Check:** Integrity check for the software used in the device in case the storage device is broken**.** The green check ✓ indicates the investigation is passed.



Calculate Image Checksum, Please Wait 7 Seconds

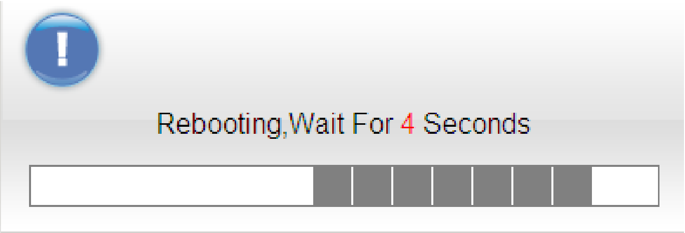
Integrity Check Window

- **Rollback Settings:** CPE saves two firmware with possible different versions in CPE. CPE would choose one of them. Users can press rollback to switch to use another firmware. A “Rollback confirming” window pops up and then starts rebooting to have change taken effect.



Would you like to Rollback?

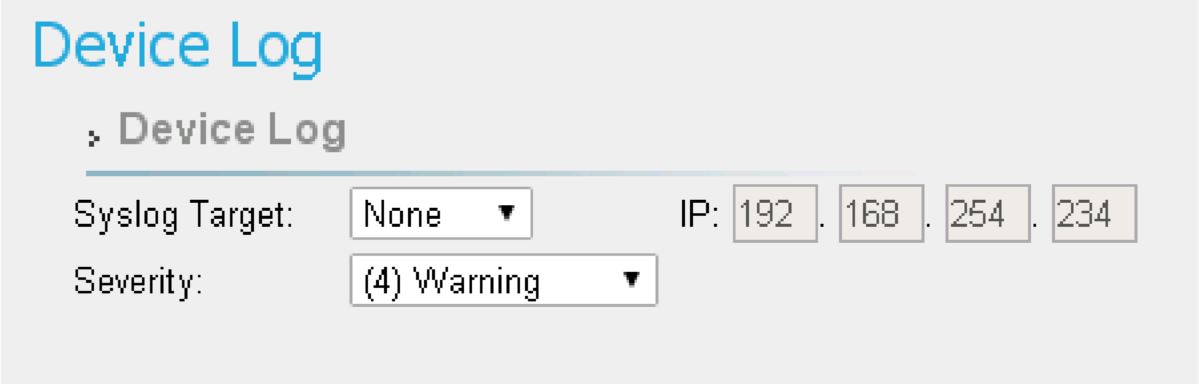
Rollback confirmation window



Rebooting,Wait For 4 Seconds

Rebooting window

Management | Device Log



Device Log

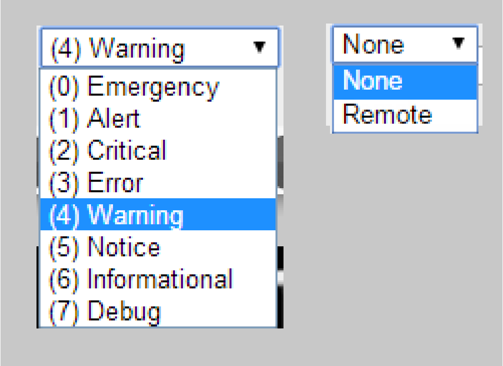
Device Log

Syslog Target: None

IP: 192 . 168 . 254 . 234

Severity: (4) Warning

Management >Device Log



Management >Device Log> Options of Severity & Syslog Target

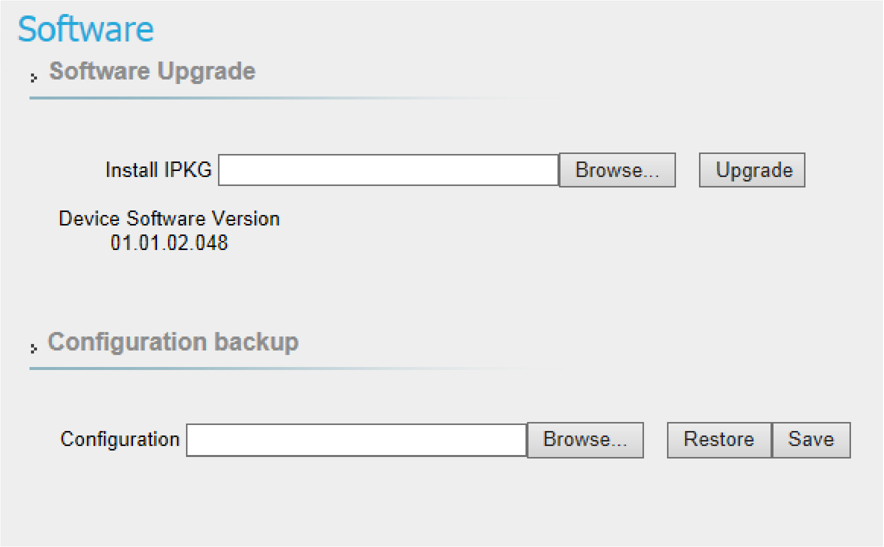
Syslog is an efficient tool for engineer debugging. CPE provide two kinds of ways to output its Syslog include output to Web and output to Remote server. And CPE also defines different Severity Level of output data, it can help engineer to get the specific logging data they want.

- **Syslog Target**: User can choose the output target to Web or Remote syslog server. **IP (Only available at "Remote Status"):** User can determine the Remote syslog server IP via this.
- **Severity:** User can log seven severity level of sys log for engineer to debug.

Save button	Click the "Save" button to save the option of Severity level.

Refresh button	Click the “Refresh” button to trigger refresh manually.
Auto button	This button will update the syslog information periodically.
Apply button	Commit the changes made and save them to the CPE device.

Management | Software


Software

Software Upgrade

Install IPKG

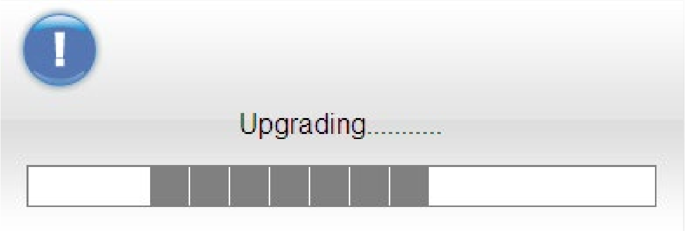
Device Software Version
01.01.02.048

Configuration backup

Configuration

Management > Software

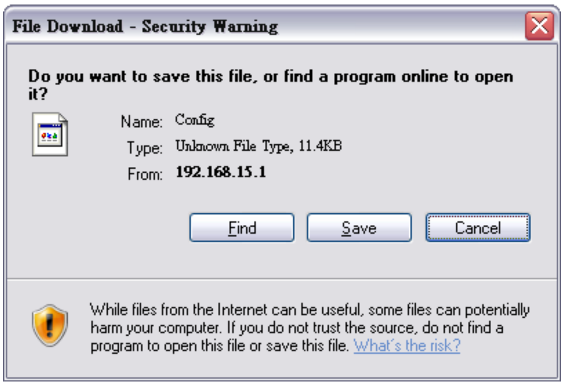
- **Software Upgrade:** Click ***"Browse"*** button to select the ipkg file to upload, and then click ***"Upgrade"*** to install the selected file. The Upgrading window will be shown as below and then the reboot process will be started to let the change taken effect. The ipkg file you have uploaded will be shown in the table below the device software version.



Management > Software > Upgrading Window

ℹ	After pressing the "Upgrade" button, it will automatically reboot the CPE and upgrade the firmware with the specified file. You will be prompted to re-login to the CPE after the upgrade is complete.

- **Configuration Backup:** Back up the current system configuration by clicking **"Save"** button.


File Download - Security Warning

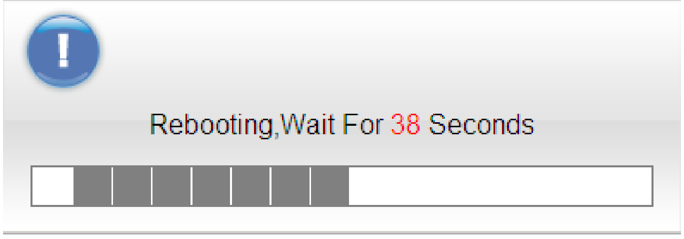
Do you want to save this file, or find a program online to open it?

Name: Config
Type: Unknown File Type, 11.4KB
From: 192.168.15.1

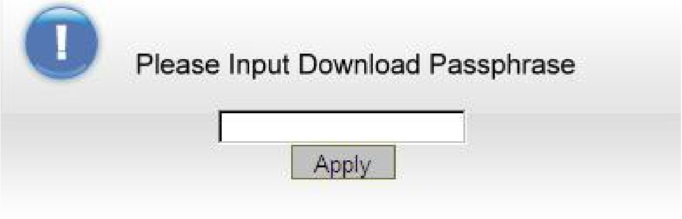
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

File Download Window

If user wants to restore the system to the restore the configuration, click **"Browse"** button to select the previously saved configuration file, and then click **"Restore"** button to restore the system to the previous settings.

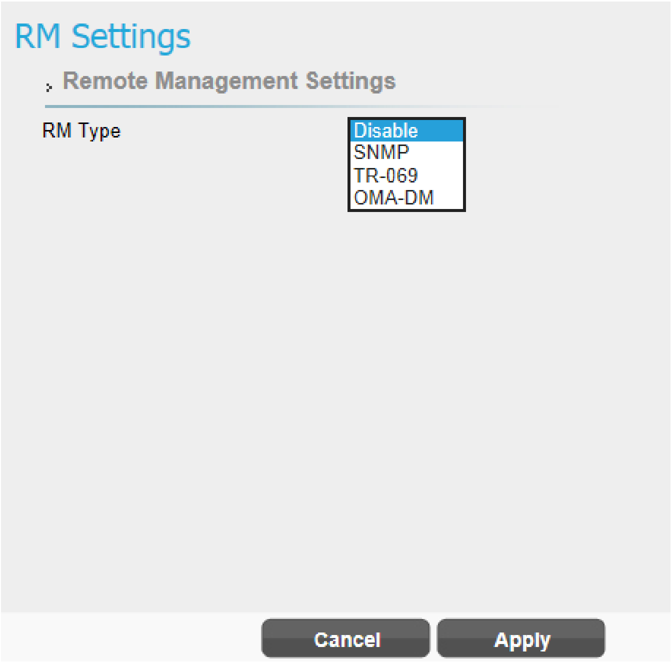

Rebooting,Wait For 38 Seconds

Management > Software > Upgrading Window

❗	A window will be popped up to let users to key in the passphrase when users save/restore the configuration. Please note that the entered passphrases need to be consistent when users do save/restore process.  Please Input Download Passphrase *Enter Passphrase Window*

ℹ	Press the “Restore” button, CPE will automatically reboot and adjust the configuration with the uploaded file. Users will be prompted to re-login to the CPE after the process is complete.

Management | RM Settings


RM Settings

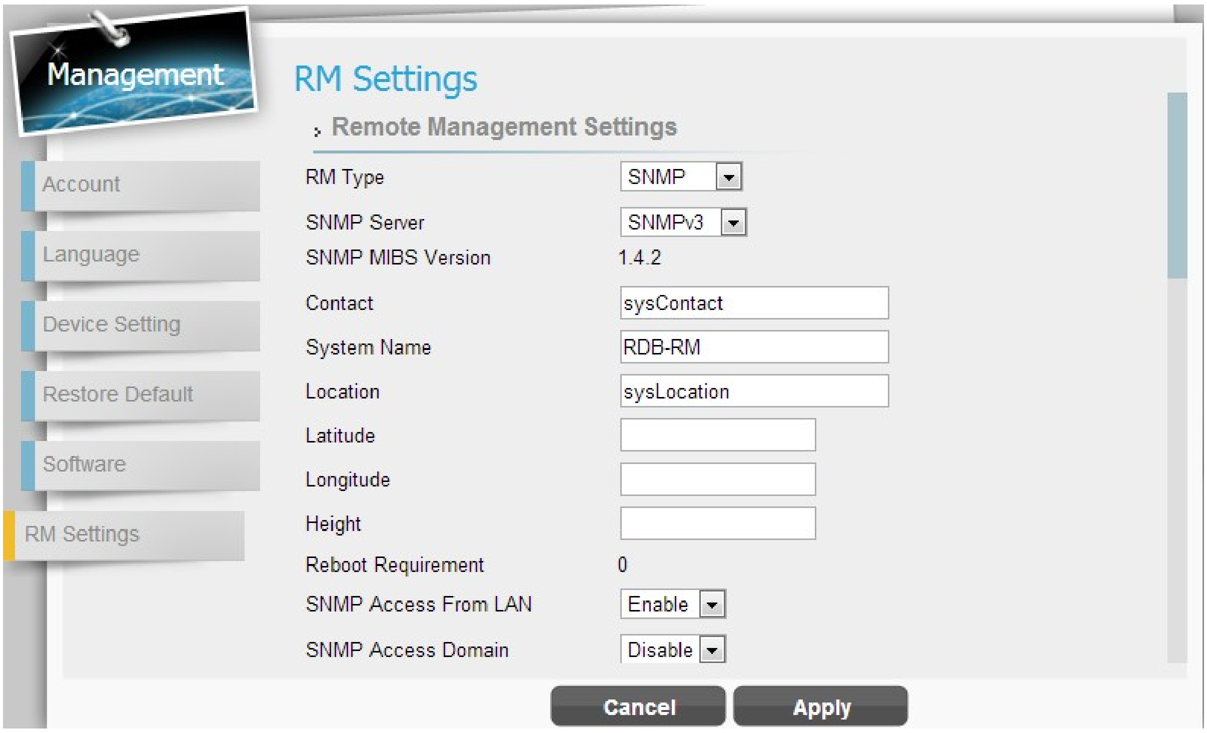
Remote Management Settings

RM Type: Disable (selected); SNMP; TR-069; OMA-DM

Management > RM Settings (Disable)

In this page, users can set up the remote management.

- **RM Type-Disable:** Select “Disable” to disable the remote management.
- **RM Type-SNMP (Simple Network Management Protocol)**



RM Settings

Remote Management Settings

RM Type	SNMP
SNMP Server	SNMPv3
SNMP MIBS Version	1.4.2
Contact	sysContact
System Name	RDB-RM
Location	sysLocation
Latitude	
Longitude	
Height	
Reboot Requirement	0
SNMP Access From LAN	Enable
SNMP Access Domain	Disable

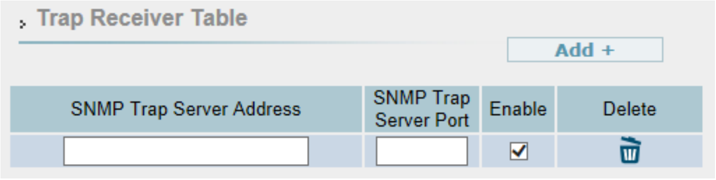
Management > RM Settings (SNMP)

For SNMP, CPE serves as the server, users can use the tool such as MIB browser as the client to connect to CPE and do remove control.

- **SNMP Server:** The type of the server. It includes SNMPv2c, SNMPv3.
- **SNMP MIBS Version:** 1.4.2
- **SNMP Read-Only Community (SNMPv2 only):** The “SNMP Community string” is like a user id or password that allows access to a router's or other device's statistics. If the community string is correct, the server responds with the requested information.
- **SNMP Read-Write Community (SNMPv2 only):** The “SNMP Community string” is like a user id or password that allows access to a router's or other device's statistics. If the community string is correct, the server responds with the requested information.
- **SNMP Trap (SNMPv2 only):** A way for an agent to send a asynchronous notification to the trap server. The traps that an agent can generate are defined by the MIBs it supports.
- **SNMP Trap Community (SNMPv2 only):** The “SNMP Community string” is like a user id or password that allows access to a router's or other device's statistics. If the

community string is correct, the server responds with the requested information.

- **SNMP Trap Server IP Address:** As titled.
- **SNMP Trap Server Port:** As titled.
- **Contact:** The name or organization responsible for the switch.
- **System Name:** The name that identifies the SNMP agent.
- **Location:** A location for the SNMP Agent.
- **Latitude:** A part of geo-location attributes.
- **Longitude:** A part of geo-location attributes.
- **Height:** A part of geo-location attributes.
- **Reboot Requirement:** A remainder to let users know that CPE needs to reboot to have something taken effect.
- **SNMP Access from LAN: Enable/Disable.**
- **SNMP Access Domain: Enable/Disable.**
  - **SNMP Access Domain IP Address:** The IP address of the access domain.
  - **SNMP Access Domain Netmask:** The subnet mask for the access domain.
- **SNMP Engine ID (SNMPv3 only):** A unique identifier for the agent.
- **SNMP Engine Boots (SNMPv3 only):** A count of the number of times the SNMP engine has re-booted/re-initialized since snmpEngineID was last configured.
- **SNMP Engine Time (SNMPv3 only):** The number of seconds since the snmpEngineBoots counter was last incremented
- **Trap Receiver Table (SNMPv3 only):**

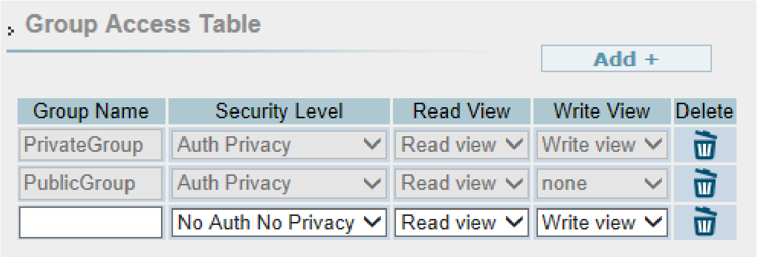


Trap Receiver Table

Add +

SNMP Trap Server Address	SNMP Trap Server Port	Enable	Delete
		☑	🗑

- **Group Access Table (SNMPv3 only):**

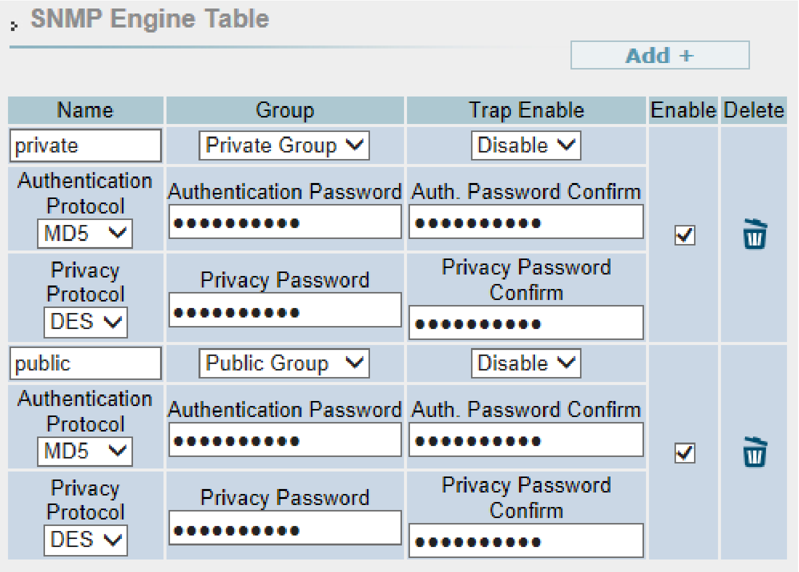


Group Access Table

Add +

Group Name	Security Level	Read View	Write View	Delete
PrivateGroup	Auth Privacy	Read view	Write view	🗑
PublicGroup	Auth Privacy	Read view	none	🗑
	No Auth No Privacy	Read view	Write view	🗑

- **SNMP Engine Table (SNMPv3 only):**

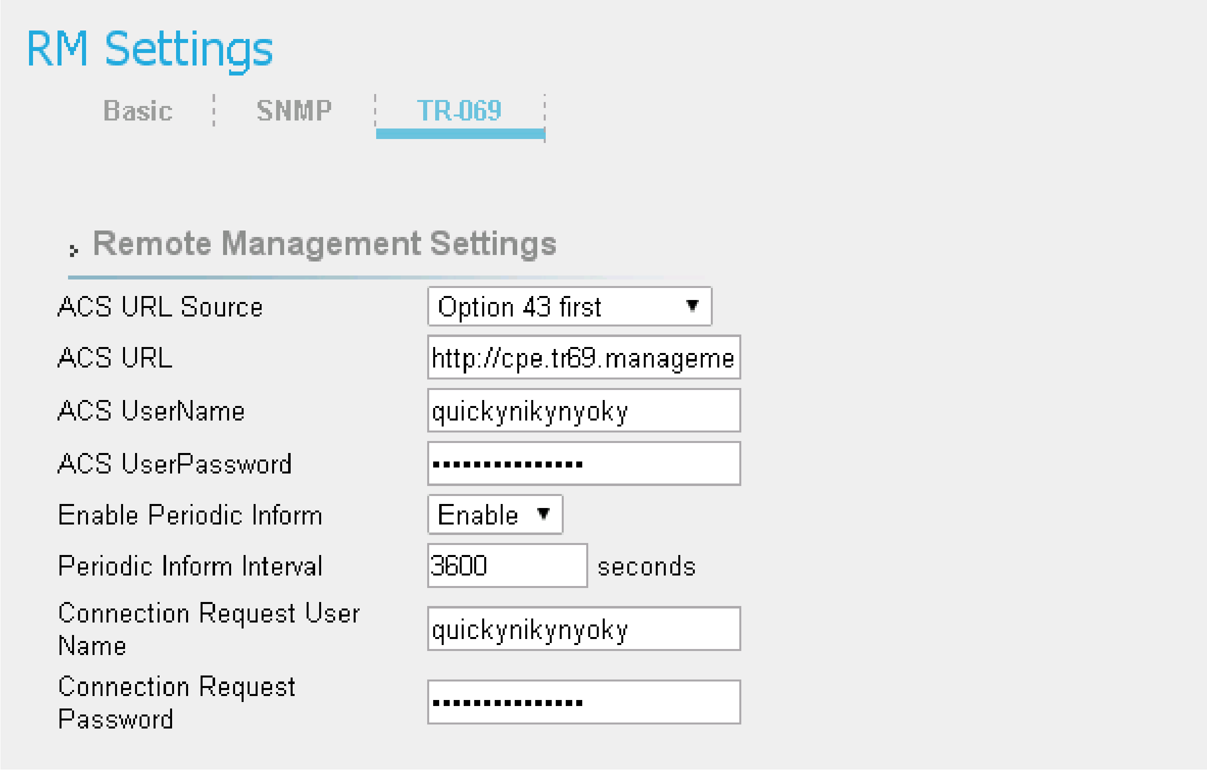


SNMP Engine Table

Add +

Name	Group	Trap Enable	Enable	Delete
private	Private Group	Disable	☑	🗑
Authentication Protocol MD5	Authentication Password ●●●●●●●●●●	Auth. Password Confirm ●●●●●●●●●●		
Privacy Protocol DES	Privacy Password ●●●●●●●●●●	Privacy Password Confirm ●●●●●●●●●●		
public	Public Group	Disable	☑	🗑
Authentication Protocol MD5	Authentication Password ●●●●●●●●●●	Auth. Password Confirm ●●●●●●●●●●		
Privacy Protocol DES	Privacy Password ●●●●●●●●●●	Privacy Password Confirm ●●●●●●●●●●		

- **RM Type-TR-069 (Technical Report 069)**



Remote Management Settings

ACS URL Source	Option 43 first ▼
ACS URL	http://cpe.tr69.manageme
ACS UserName	quickynikynyoky
ACS UserPassword	•••••••••••••••
Enable Periodic Inform	Enable ▼
Periodic Inform Interval	3600 seconds
Connection Request User Name	quickynikynyoky
Connection Request Password	•••••••••••••••

Management > RM Settings(TR-069)

TR-069 is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. In the following, the word ACS stands for Auto Configuration Server.

➢ **ACS URL:** The URL or IP address of the ACS.

➢ **ACS UserName:** The username for authentication when CPE connects to ACS. (20 alphanumeric characters allowed)

➢ **ACS UserPassword:** The password for authentication when CPE connects to ACS. (20 alphanumeric characters allowed)

➢ **Enable Periodic Inform:** Enable/Disable CPE to ask ACS periodically for configuration update.

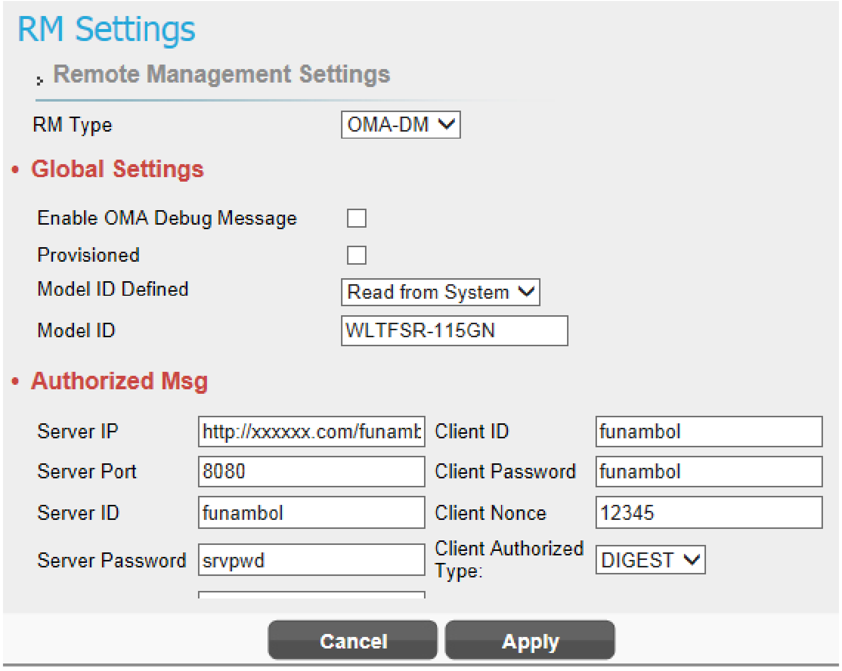
➢ **Periodical Inform Interval:** The period to update the configuration if the "**Enable**

Periodic Inform” is enabled.

- **Connection Request UserName:** When ACS connects to CPE, CPE also needs to challenge ACS for authentication. ACS has to provide the username which matches this field. (20 alphanumeric characters allowed)
- **Connection Request Password:** When ACS connects to CPE, CPE also needs to challenge ACS for authentication. ACS has to send the password which matches this field. (20 alphanumeric characters allowed)

If ACS does provisioning, there is no need for users to set connection request username/password because ACS would send that to users.

- **RM Type-ODM-DM (Open Mobile Alliance Device Management) – NOT SUPPORTED BY TELRAD**



RM Settings

Remote Management Settings

RM Type	OMA-DM

Global Settings

Enable OMA Debug Message	□
Provisioned	□
Model ID Defined	Read from System
Model ID	WLTFSR-115GN

Authorized Msg

Server IP	http://xxxxxx.com/funamb	Client ID	funambol
Server Port	8080	Client Password	funambol
Server ID	funambol	Client Nonce	12345
Server Password	srvpwd	Client Authorized Type:	DIGEST

Management > RM Settings (OMA-DM)

Using OMA-DM (OMA – Device Management) the terminals can communicate with the OMA DM Server and establish the configuration automatically. It's the current standard for activation of terminals in OMA (Open Mobile Alliance), it is designed for management of small mobile devices such as mobile phones, PDAs and palm top computers.

➢ **Global Settings**

- **Enable OMA Debug Message:** Enable it, and then the debug message is printed in the console.
- **Provisioned:** Configuration of the CPE, enabling and disabling features.
- **Model ID Defined:** Select "**customize**" or "**read from system**".
- **Model ID:** As titled.

➢ **Authorized Msg**

- **Server IP:** The IP address or URL of DM Server for the CPE to connect to.

- **Server Port:** Enter the port number of DM Server for the CPE to connect to.
- **Server ID:** The server ID for the CPE when connected to the DM Server.
- **Server Password:** The server password for the CPE when connected to the DM Server.
- **Server Nonce:** Nonce is an arbitrary number used only once to sign a cryptographic communication; the CPE and OMA-DM server use nonce to authenticate each other if user selects MD5 as an authentication algorithm in "***Server Auth Type"*** field. (20 alphanumeric characters allowed)
- **Server Authorized Type:** Select the encryption algorithm from dropdown list which used by DM Server to communicate with the client devices.
- **Client ID:** The ID of the CPE. It is used for DM server to connect to CPE.
- **Client Password:** The password of the CPE. It is used for DM server to connect to CPE.
- **Client Nonce:** The CPE and OMA-DM server use nonce to authenticate each other if user selects MD5 as an authentication algorithm in ***"Client Auth Type"*** field. (20 alphanumeric characters allowed)
- **Client Authorized Type:** Select the encryption algorithm used by DM server to communicate with the client devices.

➢ **Bootstrap Settings**

- **Bootstrapped:** To configure the CPE initially.
- **Bootstrap Encrypted:** To encrypt the bootstrap message.
- **Bootstrap Method:** To select bootstrap method.
- **WIB Retry:** The number of WIB retry.
- **WIB Retry Interval:** The interval of WIB retry.

➢ **Polling Settings**

- **Enable Client Polling:** The client can be able to do polling for tasks from server.
- **Enable Server Polling:** The server is able to dispatch works to the client directly without queuing the tasks.

- **Client Polling Interval:** As titled.
- **Client Polling Attempt:** As titled.

➢ **Client Initiated Session**

- **Client Initial Session:** If you press this button, the client would ask the server for tasks to do immediately.

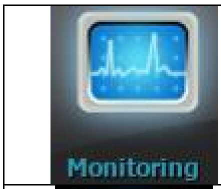
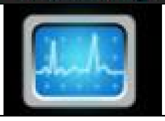
➢ **DRMD Authorized Msg**

- **Server URL:** Assign a hyperlink for server site.

Apply button	Click this button to reset the device settings to factory default
Cancel button	Reset fields to the last saved values

Monitoring

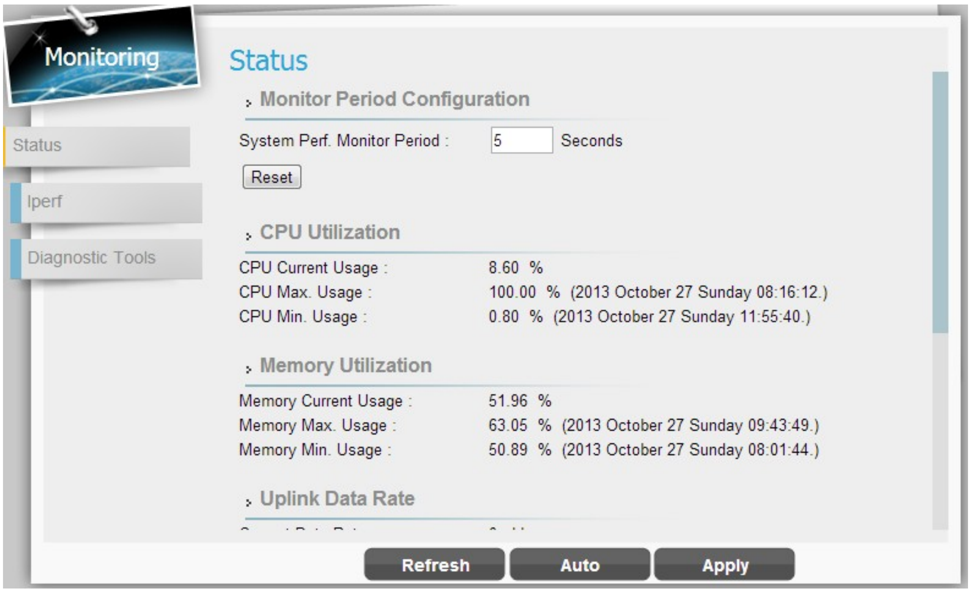
This section shows the device status such as CPU loading and memory usage and provides the interface to use the tools such as Iperf, ping and traceroute.

	Display in **Brief Summary Page**
	Display in “**Quick Panel**” of **Detailed Configuration Page**

- **Menu structure:**

Monitoring	Status
	Iperf
	Diagnostic Tools

Monitoring | Status



Status

Monitor Period Configuration

System Perf. Monitor Period : 5 Seconds

Reset

CPU Utilization

```
CPU Current Usage :     8.60  %
CPU Max. Usage :        100.00  %  (2013 October 27 Sunday 08:16:12.)
CPU Min. Usage :        0.80  %  (2013 October 27 Sunday 11:55:40.)
```

Memory Utilization

```
Memory Current Usage :  51.96  %
Memory Max. Usage :     63.05  %  (2013 October 27 Sunday 09:43:49.)
Memory Min. Usage :     50.89  %  (2013 October 27 Sunday 08:01:44.)
```

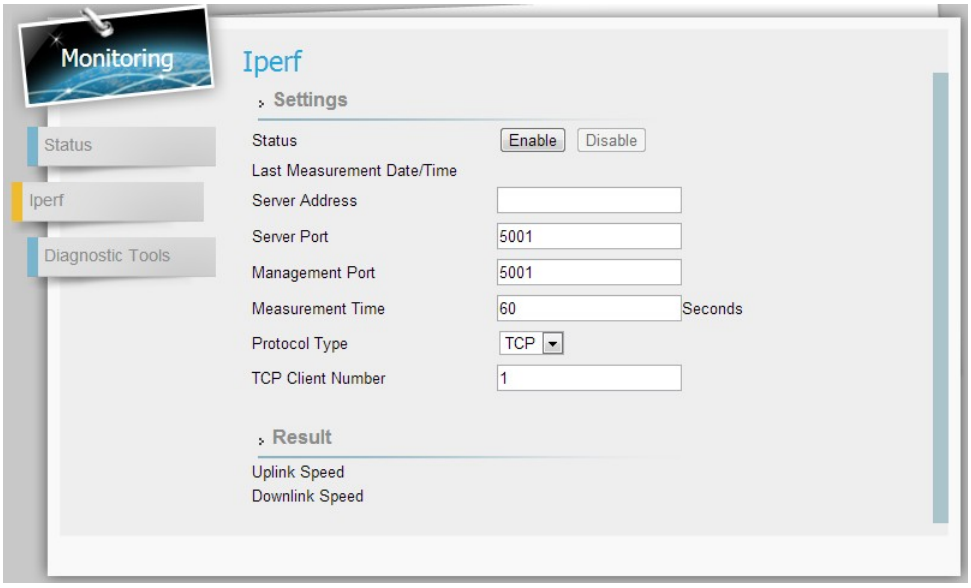
Uplink Data Rate

Monitor > Status

- **Monitor Period Configuration:** The period to record devices status. The recorded data is used to compute the CPU, memory and network statistics.
- **Reset button:** Reset CPU/Memory utilization and Uplink/Downlink data rate.
- **CPU Utilization:**
  - CPU Current Usage
  - CPU Max Usage
  - CPU Min Usage
- **Memory Utilization:**
  - Memory Current Usage
  - Memory Max Usage
  - Memory Min Usage:
- **Uplink Data Rate:**
  - Current Data rate
  - Max Data rate
  - Min Data rate.
- **Downlink Data Rate:**

        - Current Data rate
        - Max Data rate
        - Min Data rate.
- **System Information**
    - Firewall: The status of firewall. It is either ON or OFF.
    - Device Uptime. The accumulated time after the device is powered on.
    - Restart Reason
        - Device auto
        - User Forced
        - Operator Forced
        - Software Upgrade

Monitoring | Iperf



Iperf

Settings

Status

Last Measurement Date/Time

Server Address

Server Port 5001

Management Port 5001

Measurement Time 60 Seconds

Protocol Type TCP

TCP Client Number 1

Result

Uplink Speed

Downlink Speed

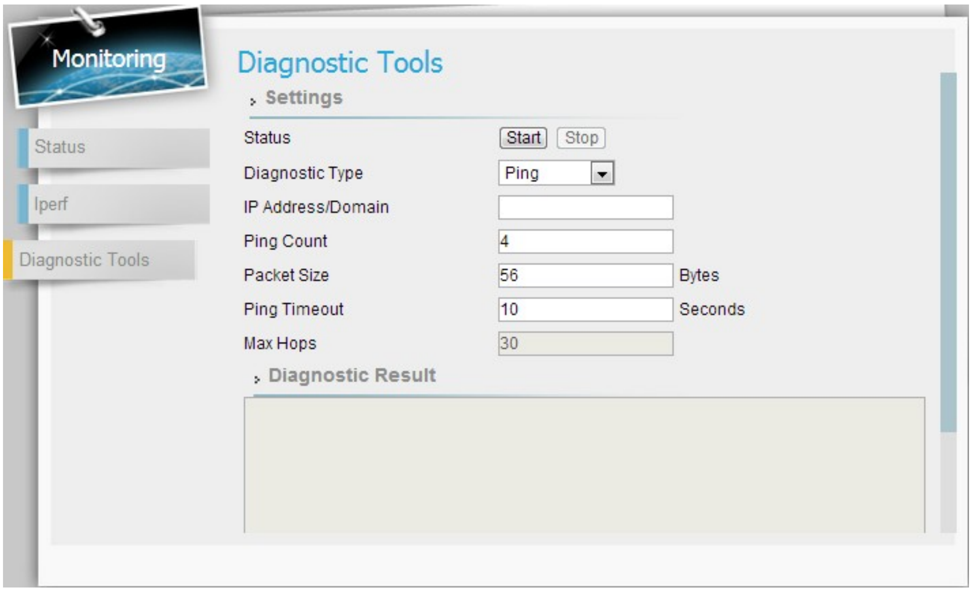
Monitor > Iperf

Iperf is a tool to measure network environment such as throughput, packet loss and delay jitter. Typically, to use Iperf, there should be a client and a server. The server opens a port and waits for clients to build the connection. Iperf in CPE only plays as a client.

- **Settings**
  - ➢ **Status:** Enable/Disable Iperf.
  - ➢ **Last Measurement Date/Time:** As titled.
  - ➢ **Server Address:** As titled.
  - ➢ **Server Port:** As titled.
  - ➢ **Management Port:** To do bi-directional transmission, CPE opens “management port” to let the server transmit data to itself.
  - ➢ **Management Time:** The time to do Iperf recording.
  - ➢ **Protocol Type: TCP** or **UDP**.
  - ➢ **TCP Client Number (Protocol Type: TCP):** The number of simultaneous TCP connection to the server.
  - ➢ **Data Length (Protocol Type: UDP):** The size of datagram.
  - ➢ **UDP Bandwidth (Protocol Type: UDP):** The UDP bandwidth to send in bits/sec.

- **Result**
  - ➢ Uplink Latency (only UDP)
  - ➢ Downlink Latency (only UDP)
  - ➢ Uplink Speed.
  - ➢ Downlink Speed.

Monitoring | Diagnostic Tools



Diagnostic Tools

Settings

Status: Start Stop

Diagnostic Type: Ping

IP Address/Domain:

Ping Count: 4

Packet Size: 56 Bytes

Ping Timeout: 10 Seconds

Max Hops: 30

Diagnostic Result

Monitor > Diagnostic Tools

CPE has built-in tools “ping” and “traceroute”. “Ping” is used to test if CPE can reach an IP address or domain by sending the ICMP “ECHO_REQUEST” packet and waiting for the ICMP “ECHO_RESPONSE” packet. “traceroute” records all the relay points from CPE to an IP address or domain. The result of “ping” and “traceroute” will be presented in “Diagnostic Result”.

- **Settings**
  - ➢ **Status:** Enable/Disable the tool.
  - ➢ **Diagnostic Type:** ping or traceroute.
  - ➢ **IP Address/Domain:** The IP address or domain name for CPE to connect.
  - ➢ **Ping Count (Diagnostic Type: Ping):** Stop after sending “Ping Count” packets.
  - ➢ **Packet Size (Diagnostic Type: Ping):** As titled.
  - ➢ **Ping Timeout (Diagnostic Type: Ping):** Time to wait for the response packet back to CPE.
  - ➢ **Max Hops (Diagnostic Type: Traceroute)**: The number of relay point that a packet can pass by.
- **Diagnostic Result**: The result of “Ping” or “Traceroute” will be shown here.

About

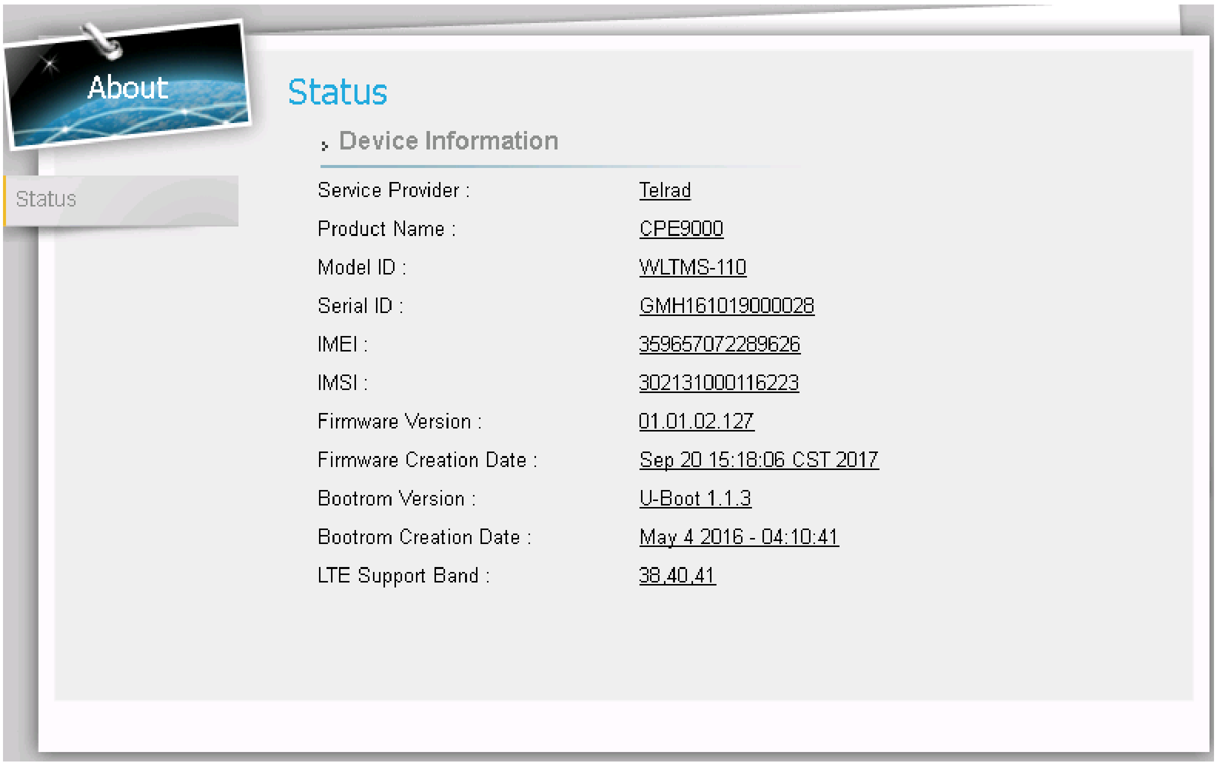
This section shows the device information such as Service Provider, Product Name, Model ID, Serial ID, IMEI, IMSI, Firmware version, Firmware Creation Date, Bootrom Version, Bootrom Creation Date and LTE Support Band.

ⓘ About	Display in **Brief Summary Page**
ⓘ	Display in “**Quick Panel**” of **Detailed Configuration Page**

- **Menu structure:**

About	Status

About | Status



Status

Device Information

Service Provider :	Telrad
Product Name :	CPE9000
Model ID :	WLTMS-110
Serial ID :	GMH161019000028
IMEI :	359657072289626
IMSI :	302131000116223
Firmware Version :	01.01.02.127
Firmware Creation Date :	Sep 20 15:18:06 CST 2017
Bootrom Version :	U-Boot 1.1.3
Bootrom Creation Date :	May 4 2016 - 04:10:41
LTE Support Band :	38,40,41

About > Status

This section shows CPE basic information.

- **Service Provider:** As titled.
- **Product Name:** The name is composed of functions provided by CPE.
- **Model ID:** The ID used by the manufacturer.
- **Serial ID:** The ID used by the operator.
- **IMEI:** International mobile equipment identity.
- **IMSI:** international mobile subscriber identity.
- **Firmware Version:** The version of the firmware.
- **Firmware Creation Date:** As titled.
- **Bootrom Version:** The version of the bootloader.
- **Bootrom Creation Date:** As titled.
- **LTE Support Band:** The supported LTE band.

Europe – EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN 301 908-1 V7.1.1
EN 301 908-13 V6.2.1
EN 62311:2008
EN 301 489-1 V1.9.2
EN 301 489-24 V1.5.1
EN60950-1:2006+A11:2009+A1:2010+A12:2011
EN60950-22 : 2006

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

The minimum distance between the user and/or any bystander and the radiating structure of the transmitter is 22 cm.

CE 0560

Česky [Czech]	*[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.

Latviski [Latvian]	Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	*[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.