LTE Outdoor CPE12000

User Manual

AUG 2019

Version: 2.5

Legal Rights

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.

Federal Communication Commission Interference Statement

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

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

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

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

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

IMPORTANT NOTE:

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 25cm between the radiator & your body.

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

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).

Table of Contents

Table of Contents 6

1. About this Guide 8

Prerequisite Skills and Knowledge 8

Conventions Used in this Document 8

2. Introduction 9

Product Highlights 9

3. Outdoor Specifications 10

3.1. LTE Specifications 10

3.2. Electrical / Physical Specifications 11

3.3. PoE Adapter Specification 11

4. Product Package 12

5. Connectors 13

6. LED Indicators 14

7. Installation 16

Connecting the Cables 17

8. Web Interface 23

8.1. Login to Web-GUI 23

Brief Summary Page 24

Detailed Configuration Page 27

8.2. Menu Structure 30

9. Reference Manual 31

9.1. LTE Network 31

LTE| Status| Basic 32

LTE | Status | Advance 35

LTE| Status| PDN 36

LTE | Cell Selection 37

LTE | Default PDN 40

LTE | Multiple PDN 41

LTE | Advanced 42

LTE | PIN 43

LTE | PLMN selection 45

LTE | Cell lock 46

9.2. Network 46

Network | Status 47

Network | WAN Setting (NAT Mode) 49
Network | WAN Setting (Tunnel Mode) 51
Network | WAN Setting (Bridge Mode) 54
Network | WAN Setting (Router Mode) 57
Network | LAN Setting 59
Network | Port Management | Port Forwarding (Available in NAT, Tunnel Mode) 63
Network | Port Management | Port Trigger (Available in NAT, Tunnel Mode) 65
Network | Routing(Available in Router, Tunnel Mode) 67
Network | DSCP 68
Network | MGMT Service 69
9.3. IPv6 70
IPv6| Status 71
IPv6 | Settings | Internet Connect Type 72
IPv6 | Settings | Extend WAN Prefix 73
IPv6 | Settings | Prefix Delegation 74
IPv6 | Settings | Static 75
9.4. Firewall: 76
Firewall | Basic 77
Firewall | Access Restriction 79
10. Management 81
Management | Account 82
Management | Device Setting 83
Management | Device Log 84
Management | Device Time 86
Management | Restore Default 87
Management | Software 89
Management | RM Settings 92
11. Monitoring 103
Monitoring | Status 104
Monitoring | Iperf 106
Monitoring | Diagnostic Tools 108
12. About 109
About | Status 110

1. About this Guide

This document provides information and procedures on the installation and configuration of CPE12000 LTE Outdoor CPE. Applicable products:

- CPE-12000SG-PRO-1D-3.x (for Bands 42&43)
- CPE-12000SG-PRO-1D-3.x-B48 (for Band 48)

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 Indoor 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

2. Introduction

Product Highlights

- Support TDD-LTE Mode Band 42,43 & 48 *
- Support 3GPP Release 12 compliant
- Support up to UE LTE Downlink Category 12 **
- Support 4x4 MIMO DL with 40MHz CA Maximum
- Support DL 256QAM with DL 2x2 MIMO only
- 2Tx &4Rx configuration support
- Support 1.8V and 3V SIM and USIM card for LTE Mode
- Supports Dynamic Host Configuration Protocol
- Built-in web server for web-based configuration
- Password protected access and configuration
- Supports IEEE 802.3, IEEE 802.3u, 802.3ab (10/100/1000 Mbps)
- Support Power over Ethernet of Outdoor WAN port {802.3 at} Supports
- Supports VPN pass-through& End Point
- Support IP67 Environmental Proof

* B48 support is subject to FCC certification with a dedicated P/N please refer to the release notes

** TDD Cat 12 with 4x4 + 40MHz carrier aggregation

3. Outdoor Specifications

3.1. LTE Specifications

Item	Description
Standard Compliance	3GPP Rel. 12
Duplex Mode	TDD
Frequency Bands	42, 43, 48*
Channel bandwidth (MHz)	5, 10, 15, 20
Modulation	DL: QPSK, 16QAM, 64QAM, 256QAM UL: QPSK, 16QAM, 64QAM
Transmit Modes (TM's)	TM1, TM2, TM3, TM4, TM8
Carrier Aggregation	Downlink Carrier Aggregation support
Tx/Rx Ports	2 Tx / 4 Rx
Maximum Transmit Power	23 dBm Per Port
Antenna	13 ± 1 dBi
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

* B48 ordering with B48 suffix to the P/N

Note: for actual supported features please refer to the software Release Notes.

3.2. Electrical / Physical Specifications

Item	Description
Dimensions (HxWxD)	277 x 140 x 75 mm
Weight	0.6 Kg | 1.3 lbs.
Physical Interface	LAN - 10/100/1000
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

3.3. PoE Adapter Specification

Item	Description
Power Source	100~240VAC
Output Power (PoE)	56V / 0.27A
User Interfaces	Data only : 1xLAN RJ45
Maximum cable length	100m

4. 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

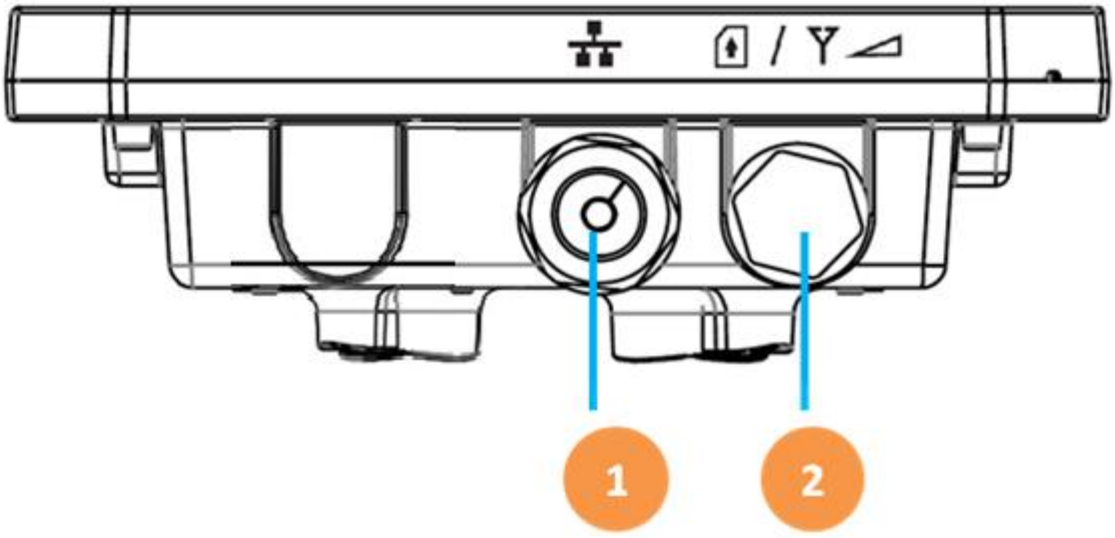
!	If any item of mentioned above is missing or damaged, please contact our customer support immediately.

5. Connectors

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

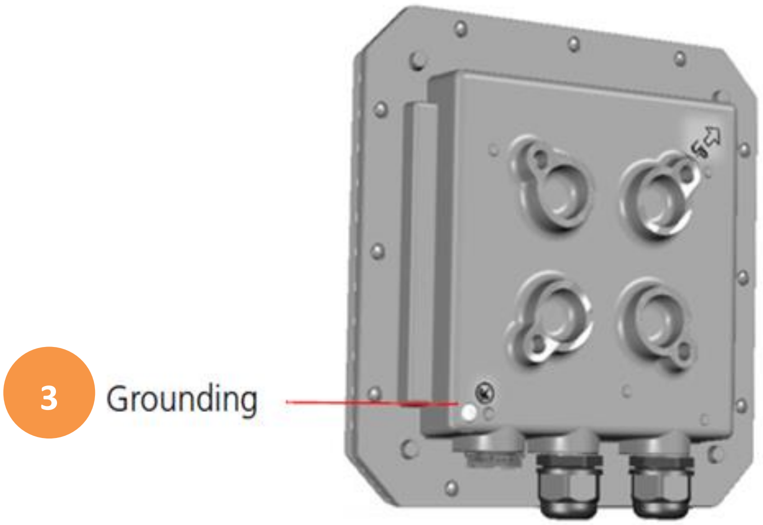
1. One RJ-45 connector for connecting to the PoE adaptor.

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.



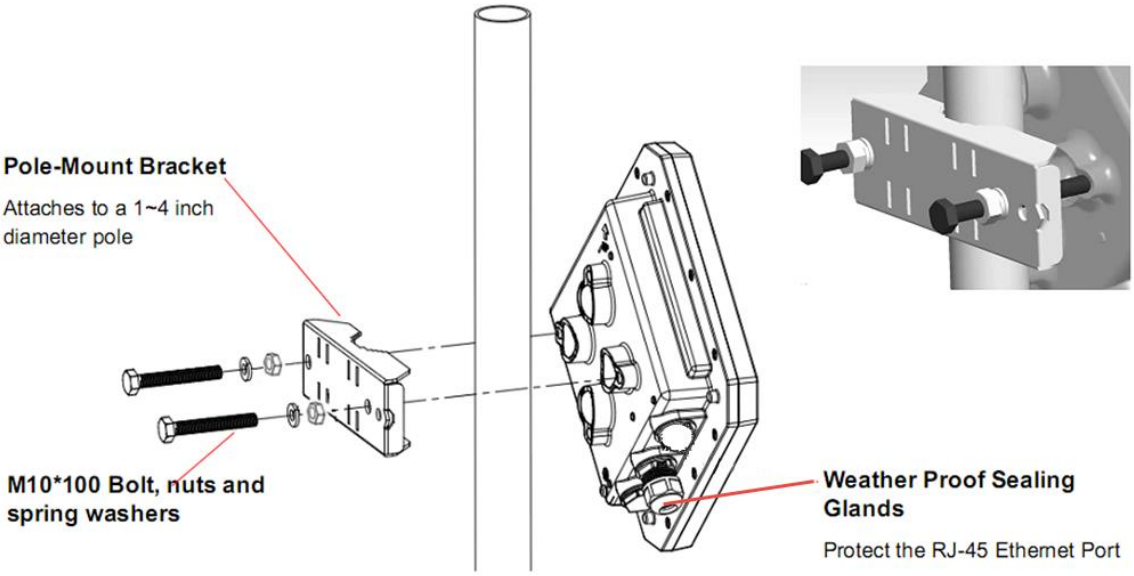
6.LED Indicators

LED name	Location	Color	LED Behavior	Status Indication
LED List	●●● ●●●●●			
MAIN power	●○○ ○○○○○	**Blue**	**ON**	Power On
			OFF	Power Off
Ethernet status	○●○ ○○○○○	**Orange**	**Steady ON**	Detect Ethernet Device Connected
			Blinking	N/A
			OFF	No Ethernet action
SIM status	○○● ○○○○○	**Green**	**Steady ON**	SIM Detected and LTE connected
			Blinking when On-hook	No SIM Detected
			OFF	SIM Detected and No LTE connection
LTE Status LED : Link Status			When CPE is power on, each LED indicates each link status; change upon customer requirement	
LTE 1	○○○ ●○○○○	**Blue**	**Steady ON**	Signal is poor SINR ≤ 3dB
LTE 2	○○○ ●●○○○	**Blue**	**Steady ON**	Signal is weak 3dB <SINR ≤ 11dB
LTE 3	○○○ ●●●○○	**Blue**	**Steady ON**	Signal is Good 11dB < SINR ≤ 18dB

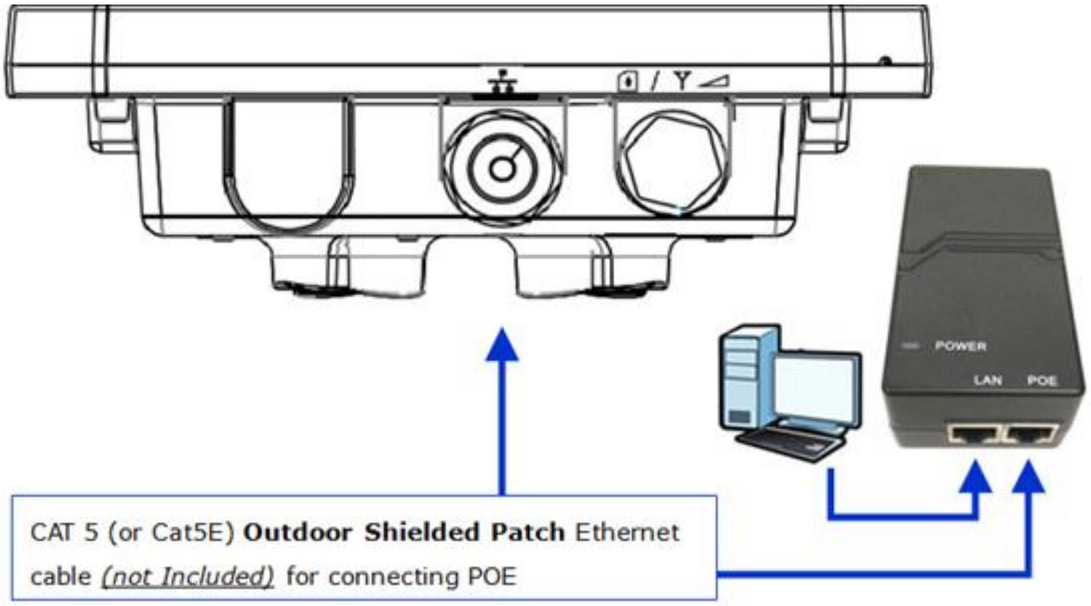
LTE 4	○○○ ●●●●○	**Blue**	**Steady ON**	Signal is very good 18dB < SINR ≤ 23dB
LTE 5	○○○ ●●●●●	**Blue**	**Steady ON**	Signal is Excellent 23dB < SINR

7. 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 good ground 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

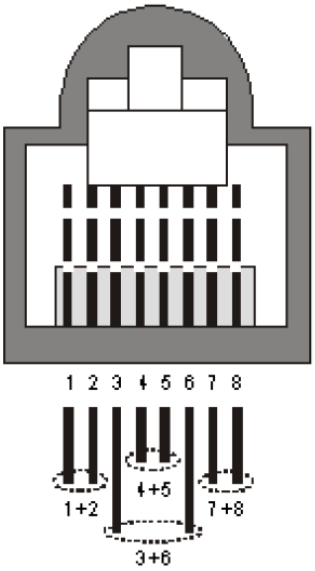

POWER
LAN
POE
CAT 5 (or Cat5E) **Outdoor Shielded Patch** Ethernet cable *(not Included)* for connecting POE

- **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.

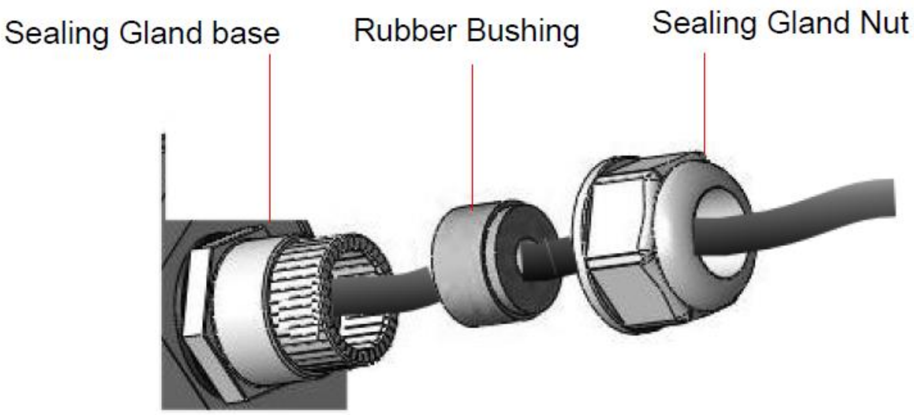
The following figure shows the required wire pair connections. The color codes used in standard cables supplied by the manufacturer are as listed in the table.

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**

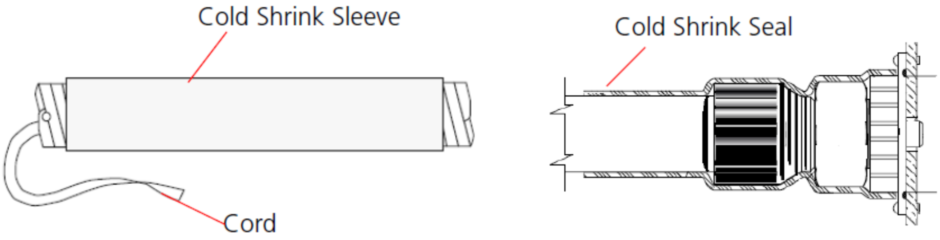
- Remove the sealing cable gland plug from the gland nut.
- Open the sealing gland nut and remove it. Don not disassembles the gland base from the bracket.
- Insert the cable into the sealing gland base and connect it to the RJ-45 connector at the bottom of the CPE. Make sure the connector is completely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

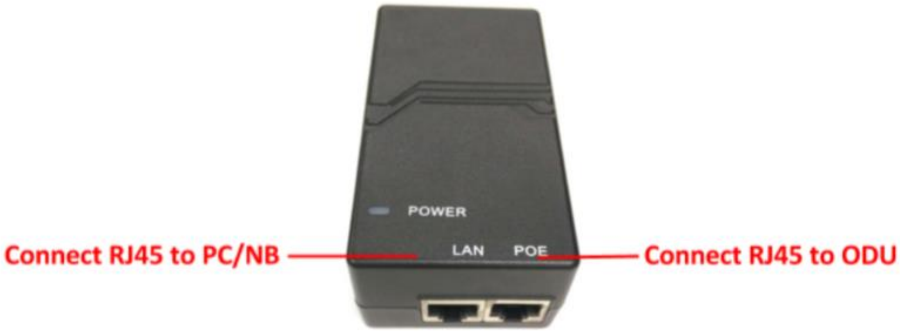
- Attach the mastic tape (Scotchfil™ Electrical Insulation Putty) and wrap it around the connector butting up against the connector. Do not over stretch.
- Squeeze to tighten the mastic sealer. Make sure there are no air bubbles.
- Slide the cold shrink sleeve on top of the connector. Make sure that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



- Pull the cord slowly to shrink the sleeve.

PoE 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.



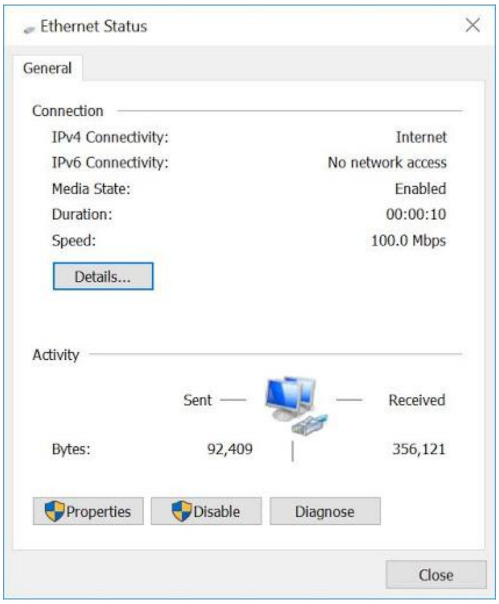
Connect RJ45 to PC/NB

Connect RJ45 to ODU

!	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**.



Ethernet Status

General

Connection

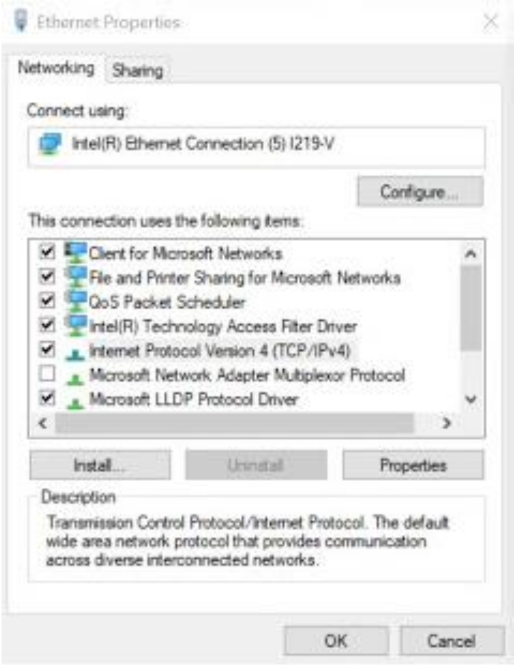
IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:00:10
Speed: 100.0 Mbps

Activity

Sent — — Received
Bytes: 92,409 | 356,121

Local Area Connection Status

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



Ethernet Properties

Networking Sharing

Connect using:
Intel(R) Ethernet Connection (5) I219-V

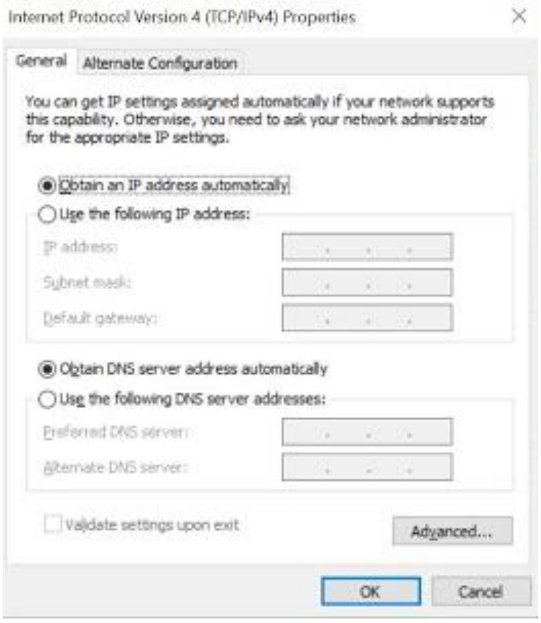
This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Intel(R) Technology Access Filter Driver
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver

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

Local Area Connection Properties

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



Internet Protocol Version 4 (TCP/IPv4) 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:

□ Validate settings upon exit

Advanced...

OK Cancel

Internet Protocol (TCP/IP) Properties

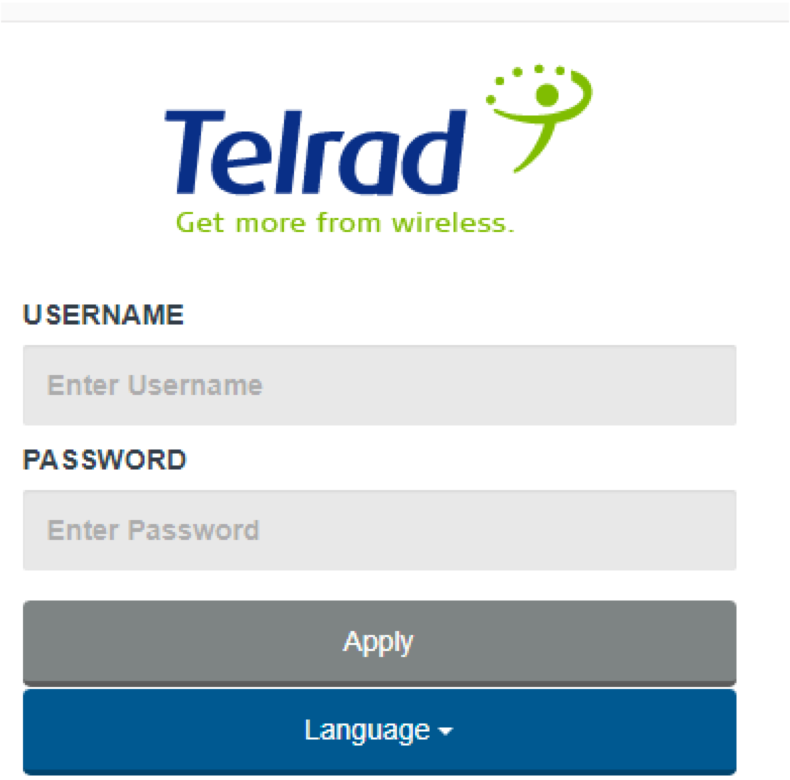
8. In order to verify CPE has a successful connection to the LTE eNodeB please observe the signal strength LEDs (Please refer **LED Indications** section in **Introduction** chapter of this manual to find the location of these LEDs on the device). At least one of these LEDs glowing continuously is an indication of successful connection to the eNodeB. Now you can start browsing the Internet.

8. Web Interface

8.1. 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 : 192.168.254.251



Web browser

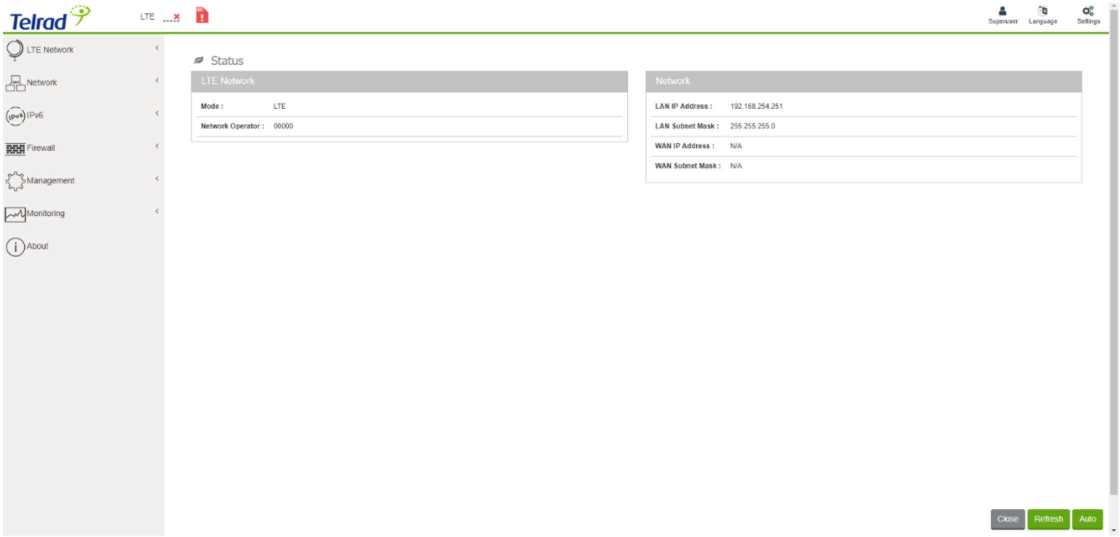
Step2: Enter USERNAME/PASSWORD to access the web management interface.

The default USERNAME/PASSWORD of "super user" is **operator/Telrad4G.**

The default USERNAME/PASSWORD of "end-user" is **admin/admin.**

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.



Status

LTE Network

Mode : LTE

Network Operator : 00000

Network

LAN IP Address : 192.168.254.251

LAN Subnet Mask : 255.255.255.0

WAN IP Address : N/A

WAN Subnet Mask : N/A

Brief Summary Page

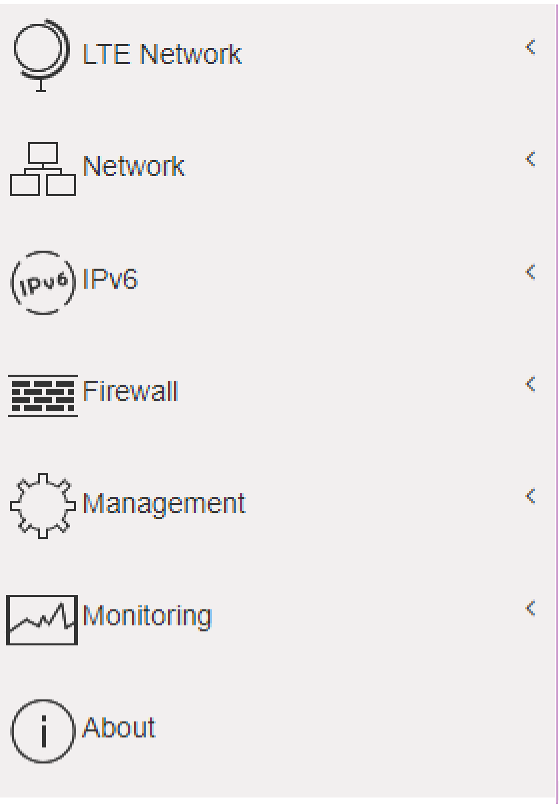
Brief Summary Page

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 indoor 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)

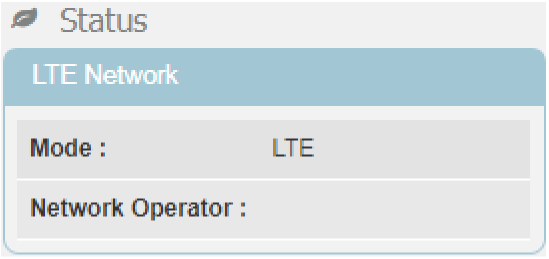
Detailed information for each block is in the below table.



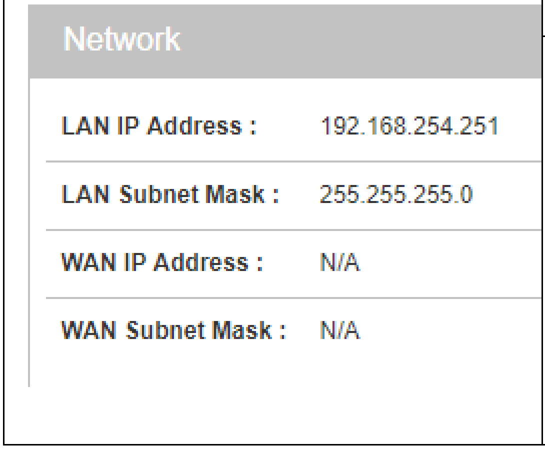
[y1]

GUI Interface

Please see below logo photo	Logo of Service Provider.
Superuser	Login Identity, could be **Superuser** or **Enduser**.
Language	Button of **Language** could be change language.
Settings	Button of **Settings** could be display Settings list.
Summary	Button of **summary**.
Reboot	Button of **Reboot**.
Logout	Button of **Logout**.

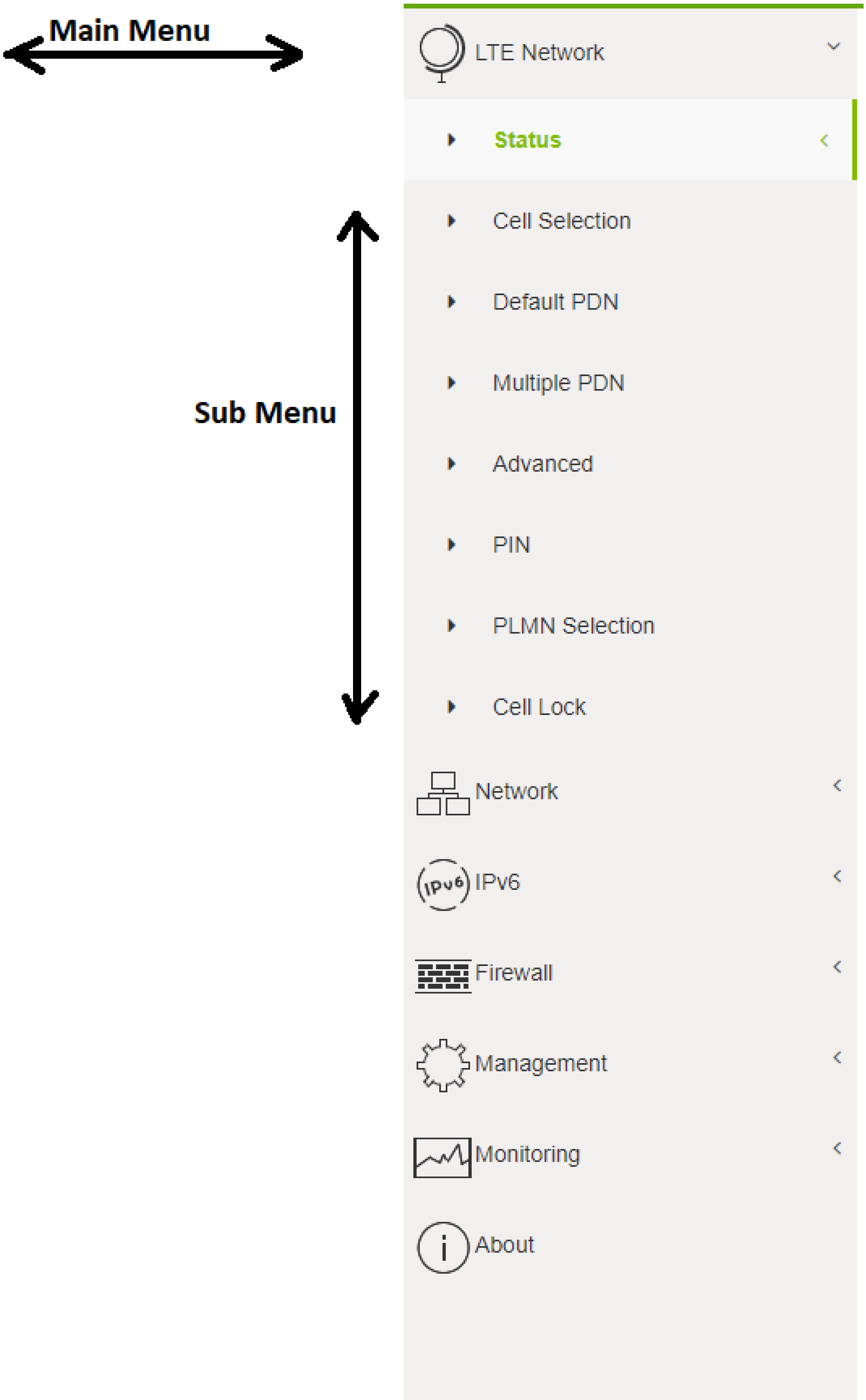
 Status LTE Network Mode : LTE Network Operator :	Mode:	**LTE**
	Operator:	Either **APN Name**
	Signal:	▂▄▆█ ▂▄▆_ ▂▄__ ▂___ ▪---- ----- (More bar means better signal) ----✕ (Disconnect, no signal)

!	▂▄▆█ 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 : N/A WAN Subnet Mask : N/A	LAN IP:	LAN IP of CPE
	WAN IP:	WAN IP of CPE

Detailed Configuration Page

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



[y2]

Detailed Configuration Page

Main Menu	Show the current main menu
Sub Menu	Clickable, can jump to another Sub Menu under the same Main Menu

LTE	Current service, could be **LTE**
📶	Signal bar, more bar means better signal ----✗ no signal or disconnection.
⚠	When CPE cannot Detect SIM card, the ICON will appear.
Superuser	Login identity, could be **Superuser** or **Enduser**
Language	Button of **Language** could be change language.
Settings	Button of **Settings** could be display Settings list.
Summary	Button of **summary**.
Reboot	Button of **Reboot**.
Logout	Button of **Logout**.

8.2. 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
	Default PDN
	Multiple PDN
	Advanced
	PIN
	PLMN Selection
	Cell Lock
Network	Status
	WAN Setting
	LAN Setting
	Port Management
	DSCP
	MGMT Service
IPv6	Status
	Settings
Firewall	Basic
	Access Restriction
Management	Account
	Device Setting
	Device Log
	Time Settings
	Restore Default
	Software
	RM Settings
Monitoring	Status
	Iperf
	Diagnostic Tools
About	Status

9.Reference Manual

9.1. LTE Network

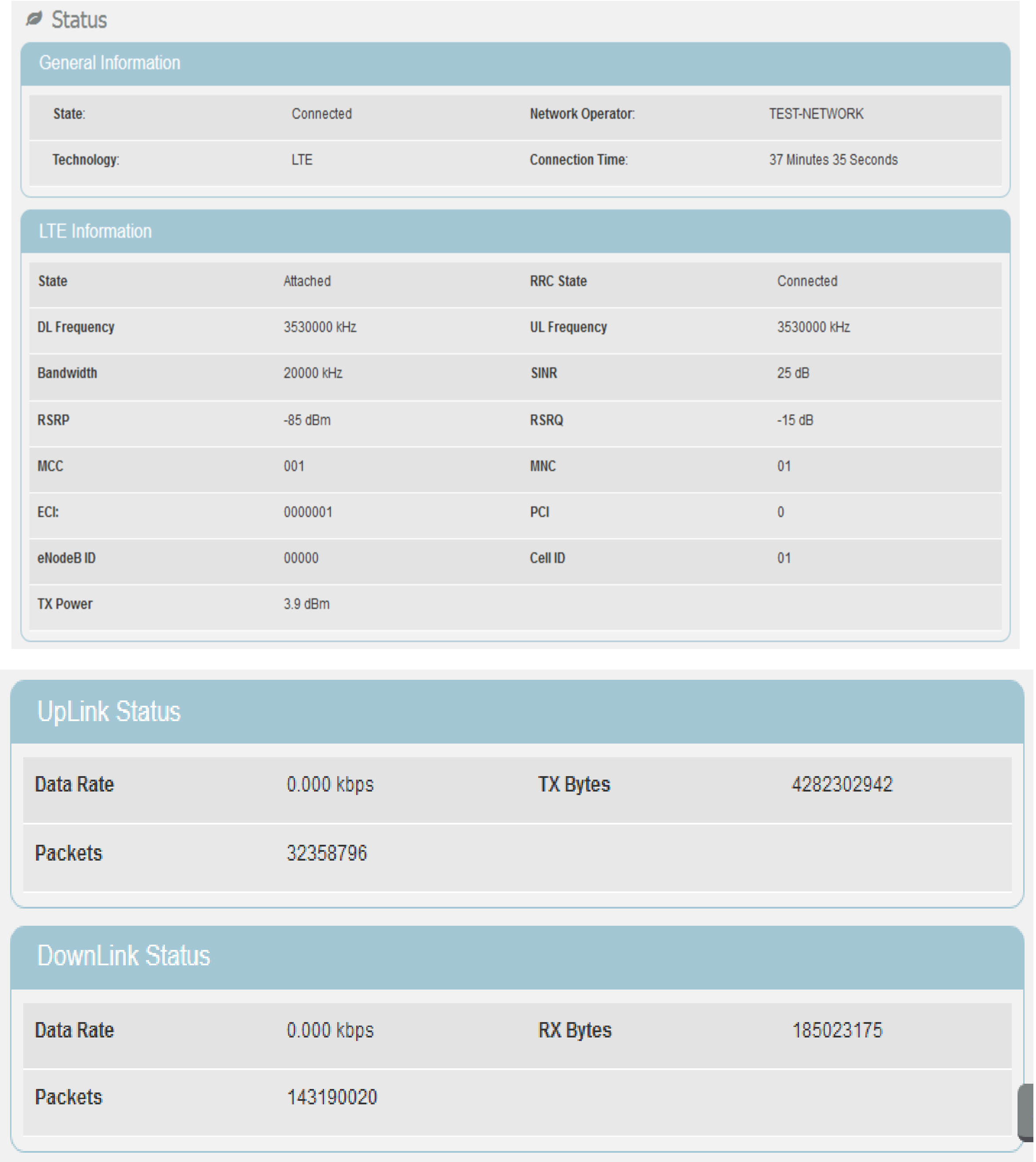
In “**LTE Network**” main menu, user can see the LTE basic information and uplink/downlink status. All the setting about LTE placed here such as LTE Earfcn and PIN code, PDN, multiple PDN, PLMN search.

LTE Network	Display in **Brief Summary Page**

- Menu Structure:

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

LTE| Status| Basic



Status

General Information

State:	Connected	Network Operator:	TEST-NETWORK
Technology:	LTE	Connection Time:	37 Minutes 35 Seconds

LTE Information

State	Attached	RRC State	Connected
DL Frequency	3530000 kHz	UL Frequency	3530000 kHz
Bandwidth	20000 kHz	SINR	25 dB
RSRP	-85 dBm	RSRQ	-15 dB
MCC	001	MNC	01
ECI:	0000001	PCI	0
eNodeB ID	00000	Cell ID	01
TX Power	3.9 dBm		

UpLink Status

Data Rate	0.000 kbps	TX Bytes	4282302942
Packets	32358796		

DownLink Status

Data Rate	0.000 kbps	RX Bytes	185023175
Packets	143190020		

LTE> Status

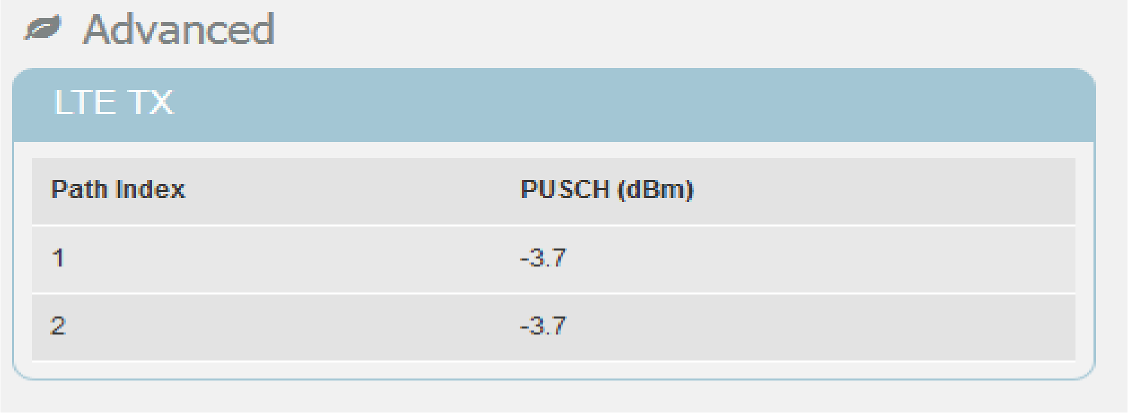
General Information

- **State:** Possible states are connecting and connected.
- **Network Operator:** It shows Operator’s name or PLMN ID.
- **Technology:** LTE.
- **Connection Time:** the accumulated time after the state is “connected”.

- **LTE Information**
  - **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.
  - **SINR:** Signal to interference plus noise ratio.
  - **RSRP:** Reference signal receiving power.
  - **RSRQ:** Reference signal receive quality.
  - **MCC:** As titled.
  - **MNC:** As titled.
  - **ECI:** As titled.
  - **PCI:** Physical cell identity.
  - **Cell ID:** Cell Identity, a part of cell global identification.
  - **eNodeB ID:** Identity of connected eNodeB.
  - **TX Power:** Transmission power.
- **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.

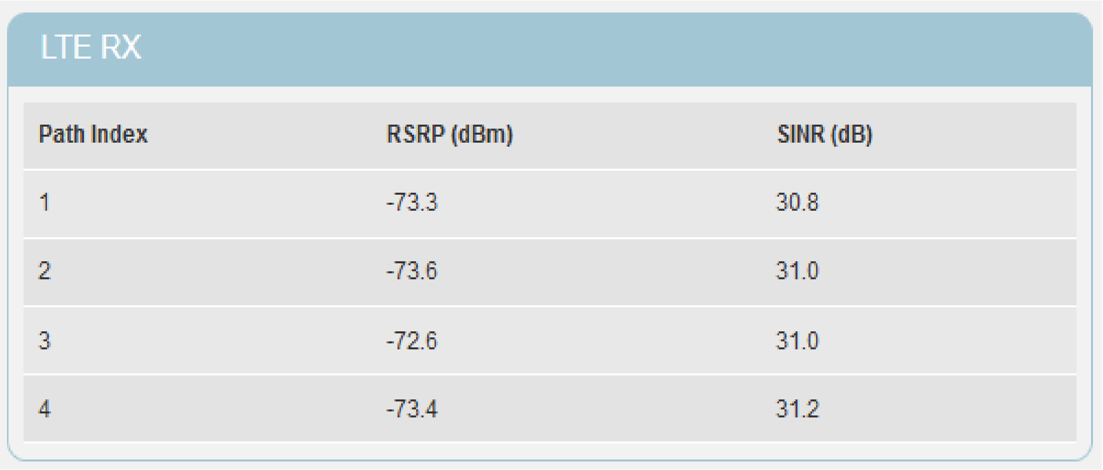
LTE | Status | Advance



Advanced

LTE TX

Path Index	PUSCH (dBm)
1	-3.7
2	-3.7

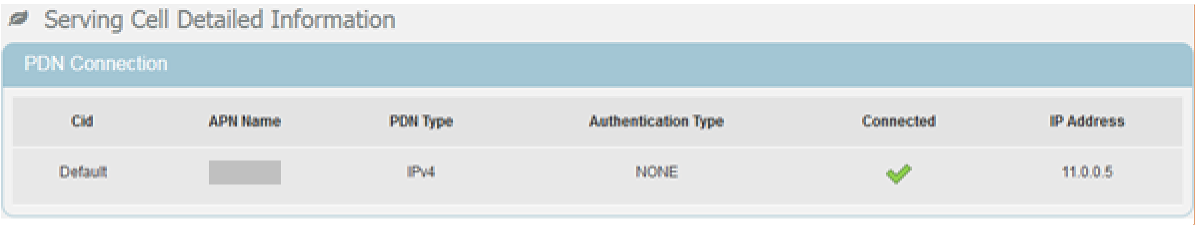


LTE RX

Path Index	RSRP (dBm)	SINR (dB)
1	-73.3	30.8
2	-73.6	31.0
3	-72.6	31.0
4	-73.4	31.2

- **LTE TX**
  - **Path Index:** Transmitter path.
  - **PUSCH:** Physical Uplink Shared Channel power.
- **LTE RX**
  - **Path Index:** Receiver path.
  - **RSRP:** Reference Signal Receiving Power.
  - **SINR:** Signal to Interference plus Noise Ratio.

LTE| Status| PDN



Serving Cell Detailed Information

PDN Connection

Cid	APN Name	PDN Type	Authentication Type	Connected	IP Address
Default	[redacted]	IPv4	NONE	✓	11.0.0.5

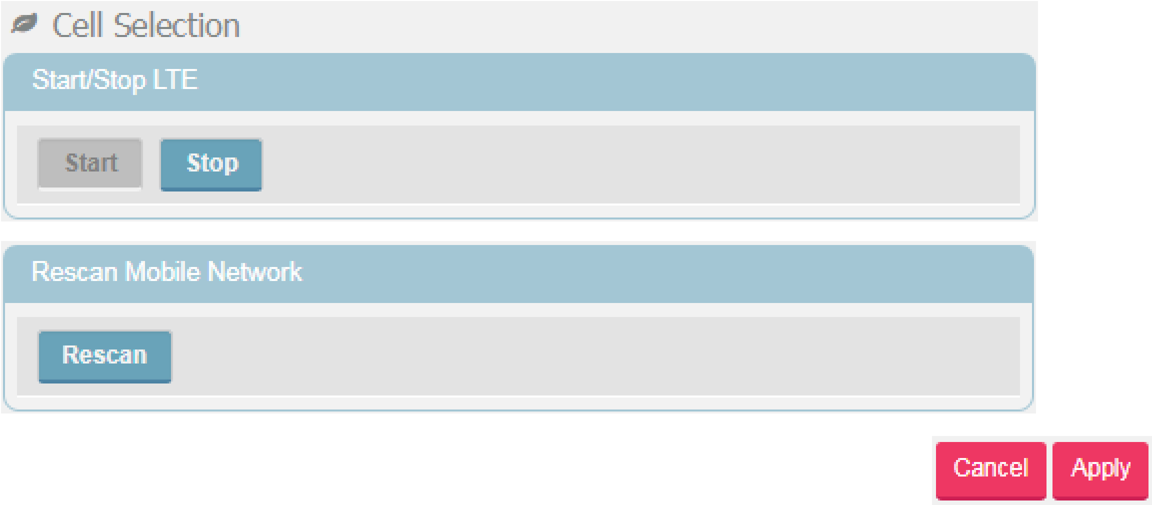
[a3]

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.

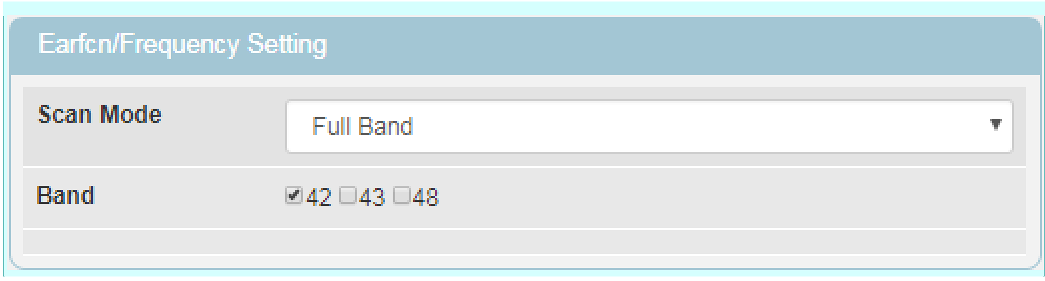
!	The first Cid of PDN should be considered as default. The Cid sequence would be started from 2.

LTE | Cell Selection



LTE>Cell Selection

- **Start / Stop LTE**: stop and start the radio.
- **Rescan Mobile Network**: manual scanning, the radio link is dropped when using the Rescan.



Scan Mode: Full Band

Band ☑42 □43 □48

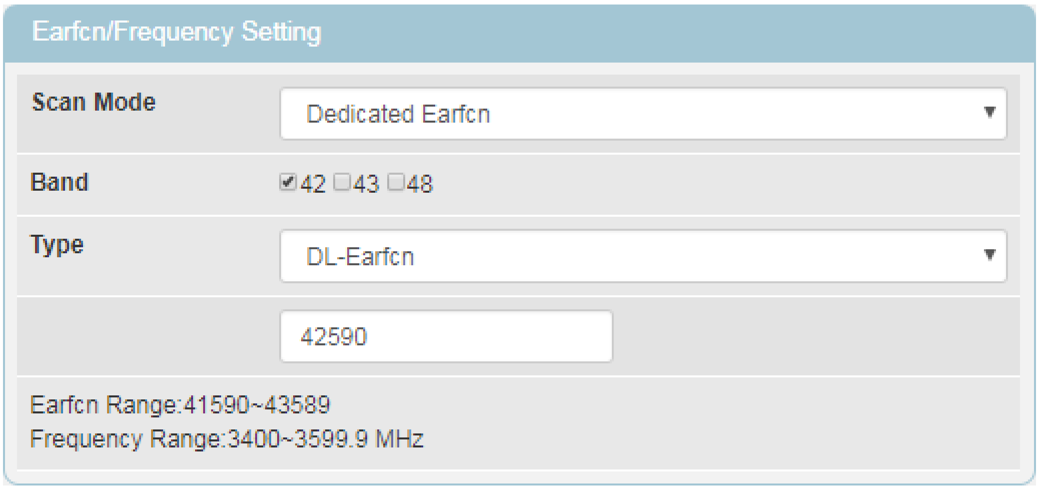
[MD4]

LTE>Cell Selection>Earfcn/Frequency Setting>Scan Mode>Full Band

- **Scan Mode:** Full Band, Dedicated Earfcn and Dedicated Earfcn List.

  Searching full band would take much longer time than Dedicated Earfcn and Dedicated Earfcn List.

  - **Full Band:** According to the selected band of the device to do "Full band" scanning**.**
  - **Dedicated Earfcn:** LTE connection according to Dedicated Earfcn/Frequency.



Earfcn/Frequency Setting

Scan Mode: Dedicated Earfcn

Band: ☑42 □43 □48

Type: DL-Earfcn

42590

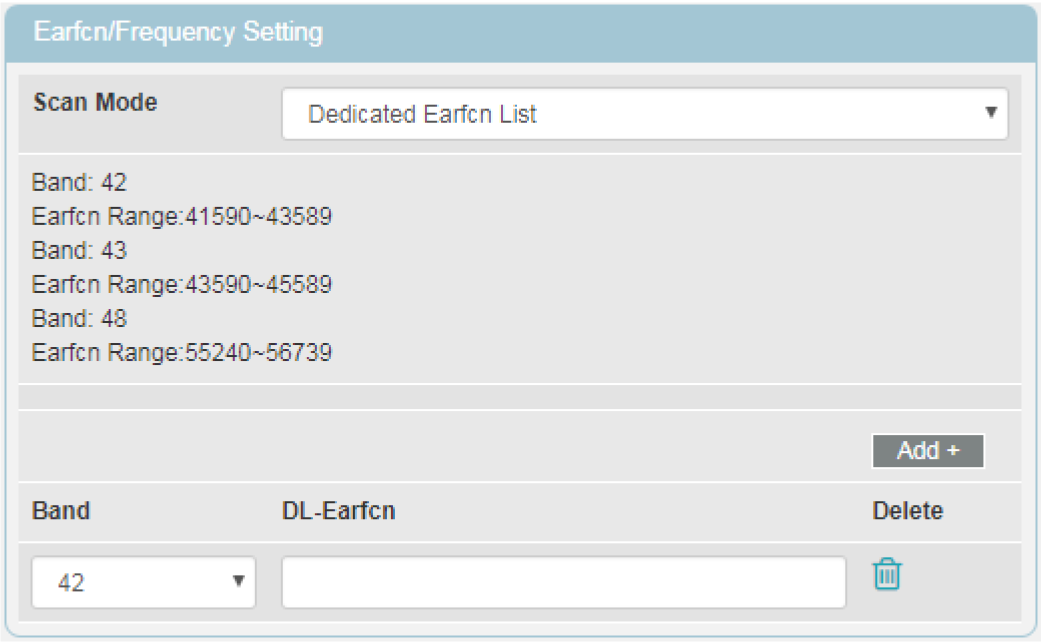
Earfcn Range:41590~43589

Frequency Range:3400~3599.9 MHz

LTE>Cell Selection>Earfcn/Frequency Setting>Scan Mode>Dedicated Earfcn

- **Band:** Chose device band.
- **Type**: Set band Earfcn or Frequency

- **Dedicated Earfcn list:** LTE connection according to the Dedicated Earfcn list



Earfcn/Frequency Setting

Scan Mode: Dedicated Earfcn List

Band: 42
Earfcn Range:41590~43589
Band: 43
Earfcn Range:43590~45589
Band: 48
Earfcn Range:55240~56739

Band	DL-Earfcn	Delete
42		🗑

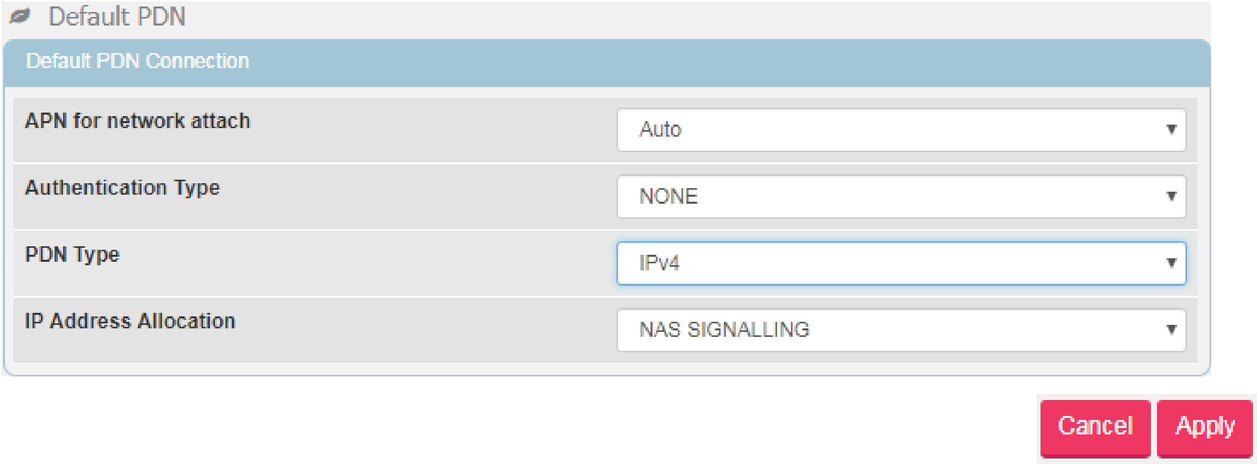
LTE>Cell Selection>Earfcn/Frequency Setting>Scan Mode> Dedicated Earfcn List

- **Band:** Chose device band.
- **DL-Earfcn**: Set dedicated DL-Earfcn.

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 42** are just an example. Real number is determined by the user's requirement.

LTE | Default PDN



Default PDN

Default PDN Connection

APN for network attach	Auto
Authentication Type	NONE
PDN Type	IPv4
IP Address Allocation	NAS SIGNALLING

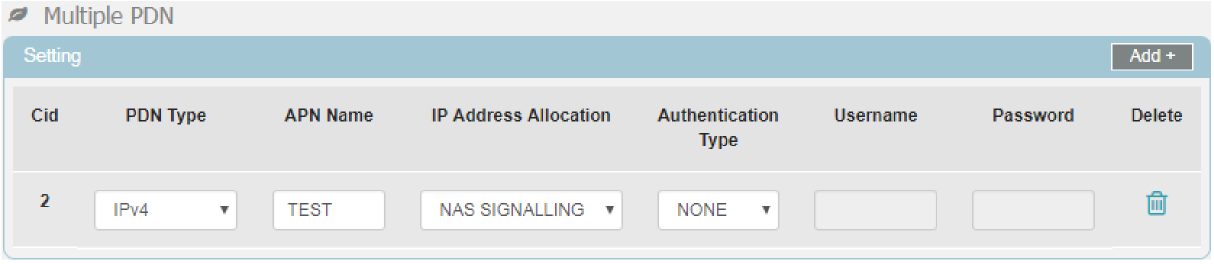
LTE>Default PDN

- **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:** Support IPv4 and / or IPv6 .
- **IP Address Allocation: NAS SIGNALLING and DHCP option.**

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



Multiple PDN

Setting

Cid	PDN Type	APN Name	IP Address Allocation	Authentication Type	Username	Password	Delete
2	IPv4	TEST	NAS SIGNALLING	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.

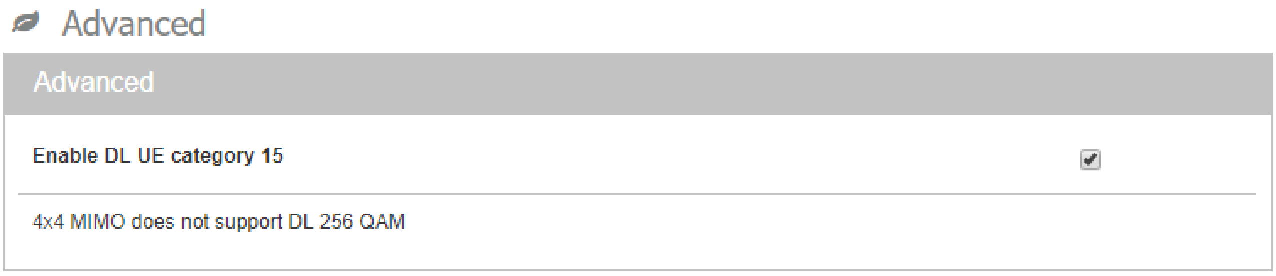
- **PDN Type:** Support IPv4 and / or Ipv6.
- **APN Name:** The PDN name in the service (in BreezeWAY).
- **IP Address Allocation: NAS SIGNALLING and DHCP option.**
- **Authentication Type:** There are **"None"**, ***"PAP (Password authentication protocol)"***, or ***"CHAP (Challenge Handshake Authentication 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.

!	LTE CPE supports at most 8 PDNs connections, default and (Cid 2 to 8)

LTE | Advanced



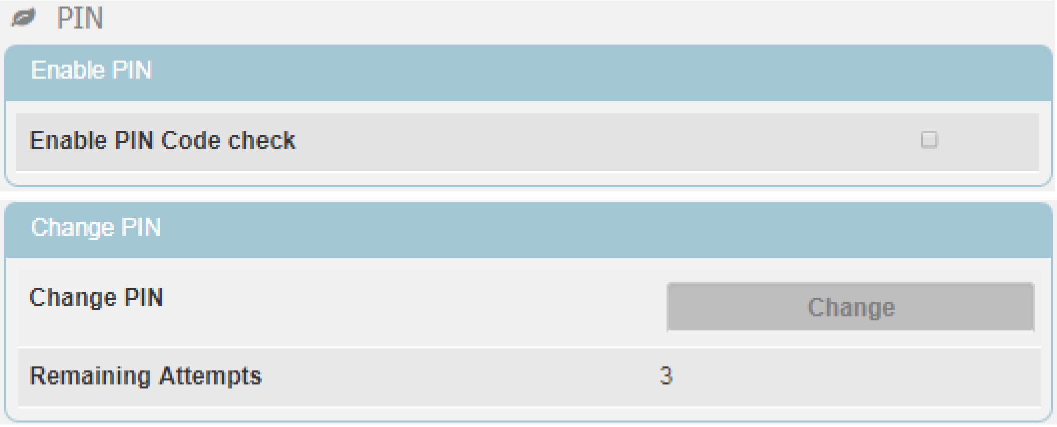
Advanced

Advanced

Enable DL UE category 15 ☑

4x4 MIMO does not support DL 256 QAM

LTE | PIN



PIN

Enable PIN

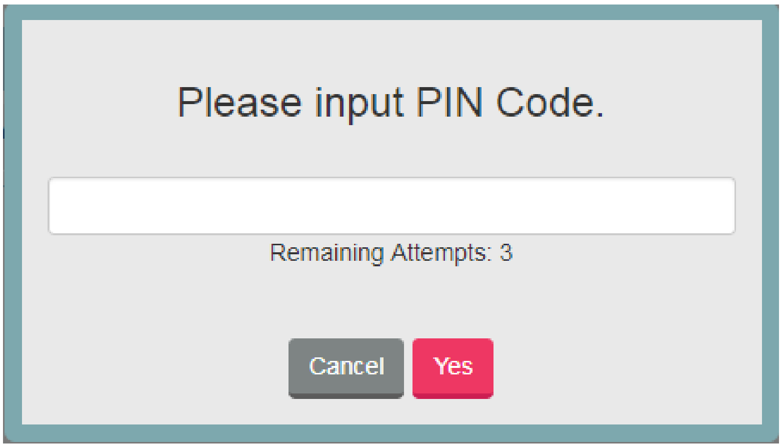
Enable PIN Code check □

Change PIN

Change PIN

Remaining Attempts 3

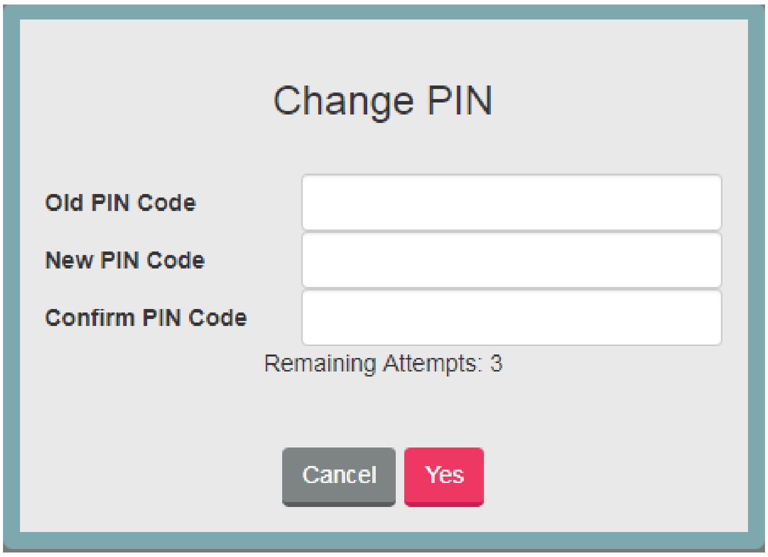
LTE>PIN



Please input PIN Code.

Remaining Attempts: 3

LTE>PIN >Enable PIN



Change 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.

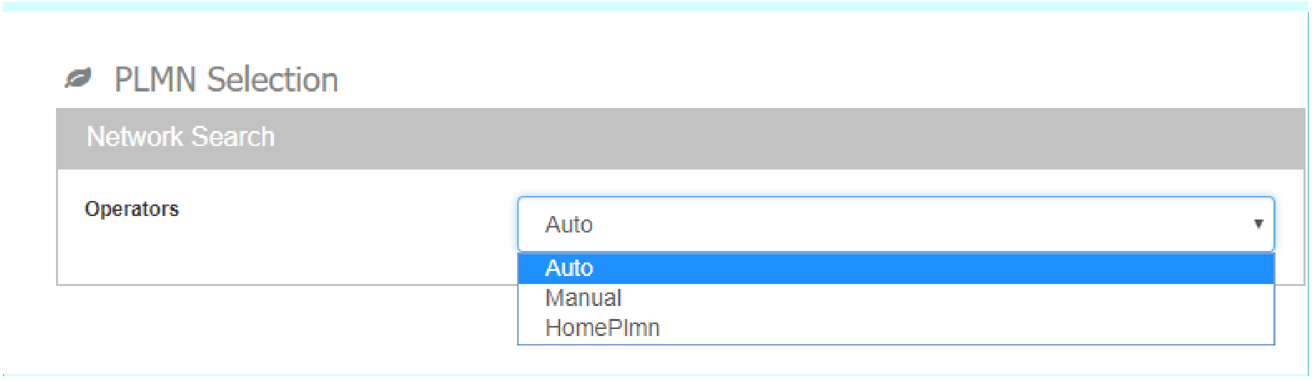
!	Please make sure the current technology is **LTE**. It can be checked from upper left corner of Web-GUI.

!	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 | PLMN selection



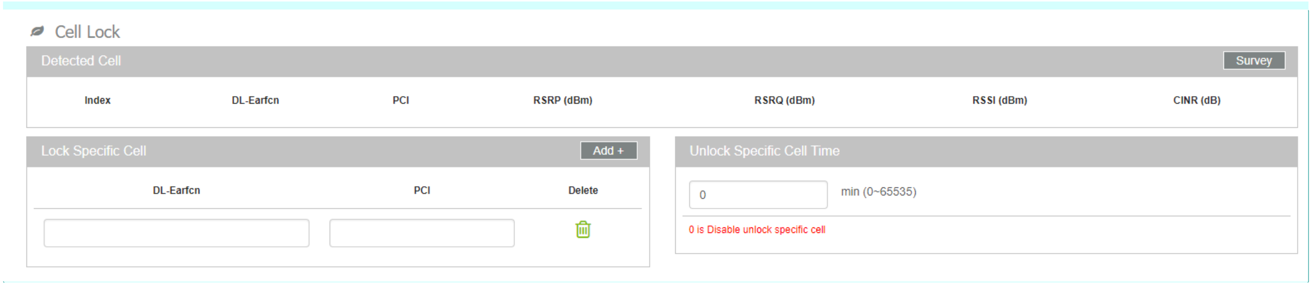
PLMN Selection

Network Search

Operators: Auto

[MD5]

LTE | Cell lock



Cell Lock

Detected Cell

Index	DL-Earfcn	PCI	RSRP (dBm)	RSRQ (dBm)	RSSI (dBm)	CINR (dB)

Lock Specific Cell

DL-Earfcn	PCI	Delete
		🗑

Unlock Specific Cell Time

0 min (0~65535)

0 is Disable unlock specific cell

[MD6]

9.2. Network

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

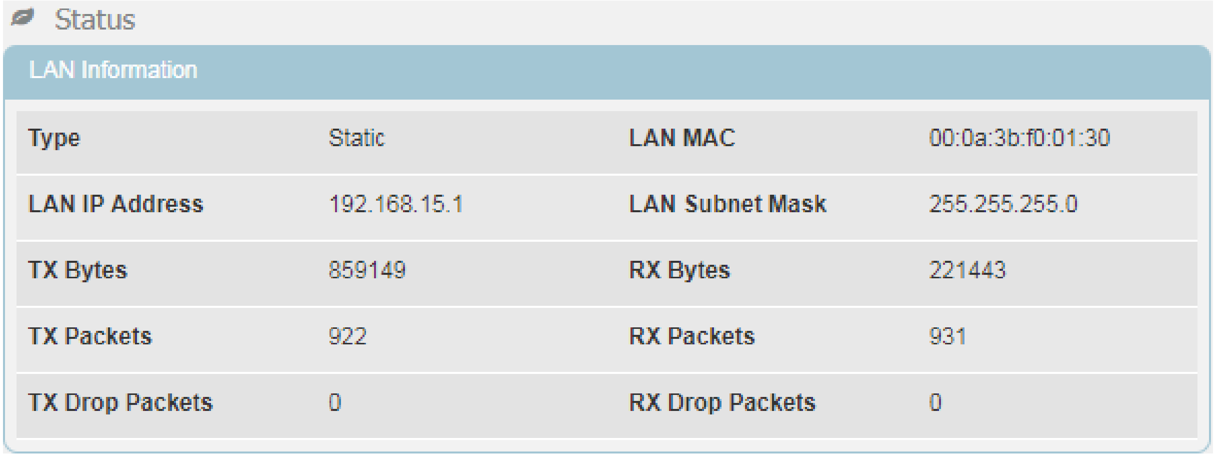
	Display in **Brief Summary Page**

- **Menu Structure:**

Network	Status
	WAN Setting
	LAN Setting
	Port Management
	DSCP
	MGMT Service

Network | Status

- **LAN Information**



Status

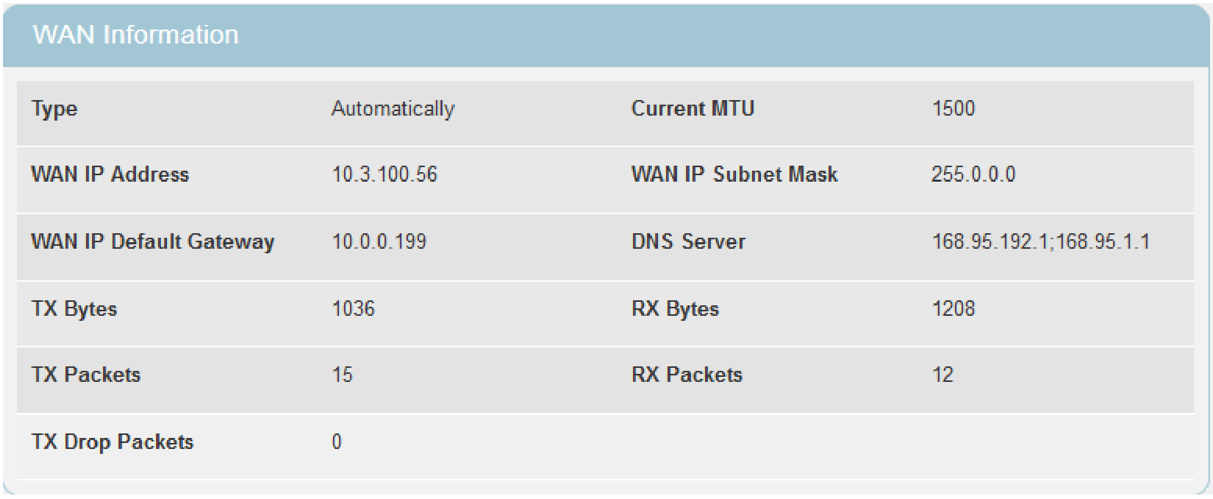
LAN Information

Type	Static	LAN MAC	00:0a:3b:f0:01:30
LAN IP Address	192.168.15.1	LAN Subnet Mask	255.255.255.0
TX Bytes	859149	RX Bytes	221443
TX Packets	922	RX Packets	931
TX Drop Packets	0	RX Drop Packets	0

Network> Status > LAN Information

- **WAN Information:** This section shows WAN IP, MAC, Gateway, DNS Server, Time Server of LTE indoor CPE and statistics of TX and RX Bytes and Packets of WAN interface.

Network > Status > WAN Information

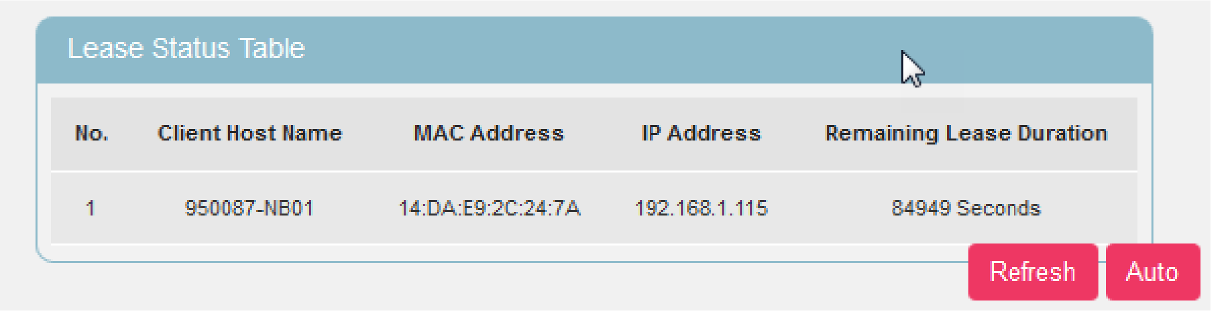


WAN Information

Type	Automatically	Current MTU	1500
WAN IP Address	10.3.100.56	WAN IP Subnet Mask	255.0.0.0
WAN IP Default Gateway	10.0.0.199	DNS Server	168.95.192.1;168.95.1.1
TX Bytes	1036	RX Bytes	1208
TX Packets	15	RX Packets	12
TX Drop Packets	0		

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

CPE.



Lease Status Table

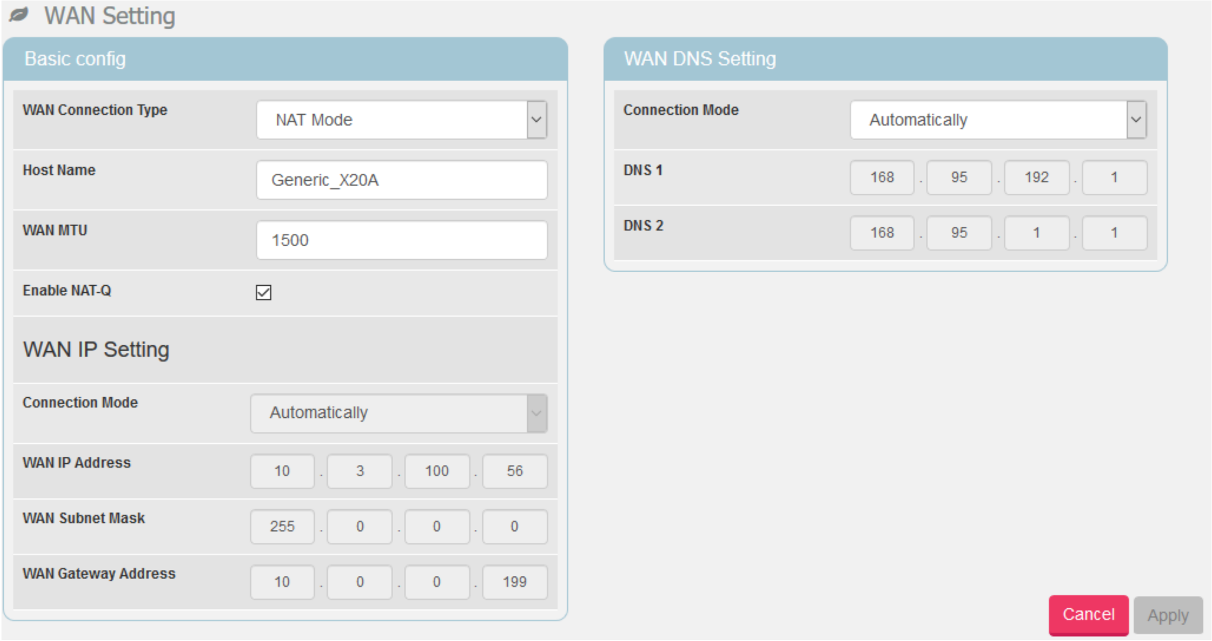
No.	Client Host Name	MAC Address	IP Address	Remaining Lease Duration
1	950087-NB01	14:DA:E9:2C:24:7A	192.168.1.115	84949 Seconds

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

Basic config

WAN Connection Type	NAT Mode
Host Name	Generic_X20A
WAN MTU	1500
Enable NAT-Q	☑

WAN IP Setting

Connection Mode	Automatically
WAN IP Address	10 . 3 . 100 . 56
WAN Subnet Mask	255 . 0 . 0 . 0
WAN Gateway Address	10 . 0 . 0 . 199

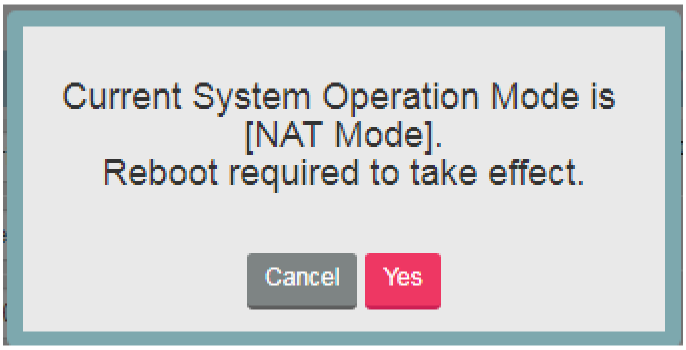
WAN DNS Setting

Connection Mode	Automatically
DNS 1	168 . 95 . 192 . 1
DNS 2	168 . 95 . 1 . 1

Network > WAN Setting

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

!	Changing the "**WAN Connection Type**" 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.

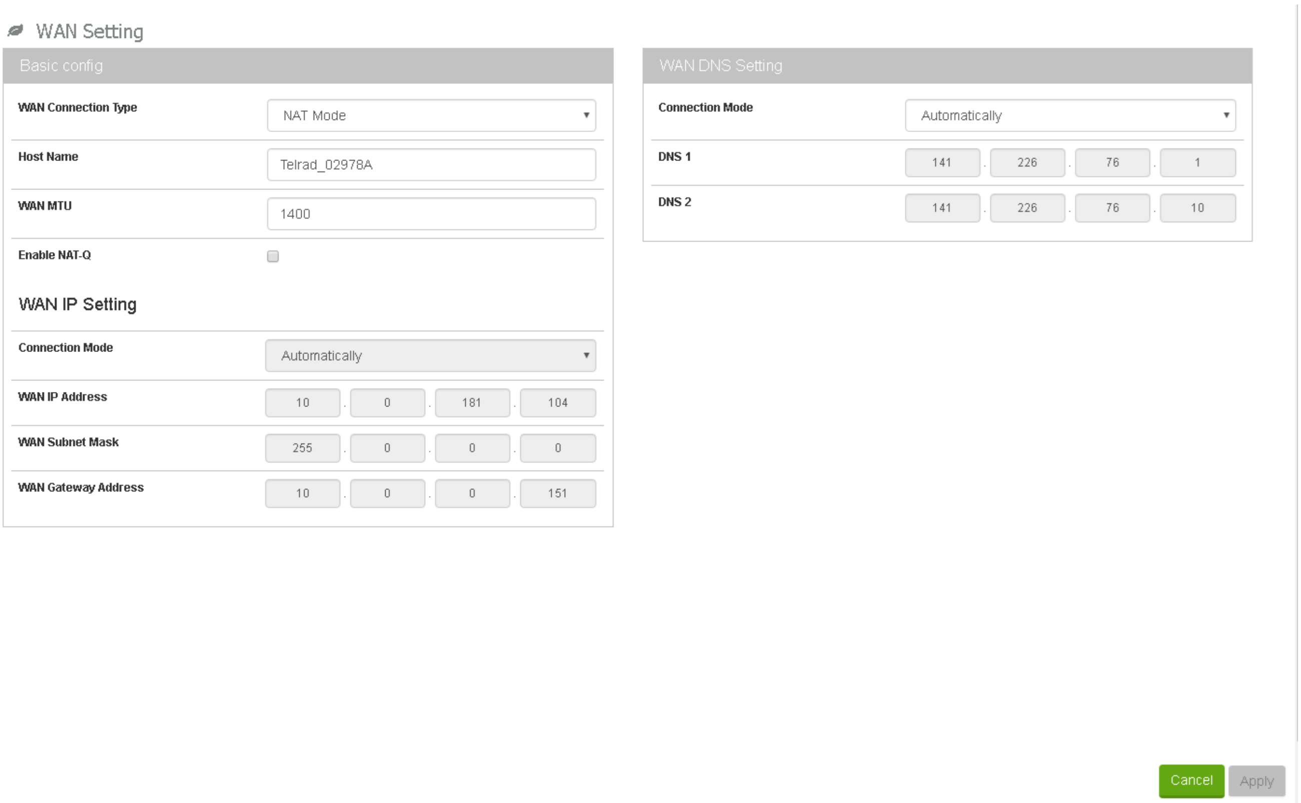
Pop-up windows to confirm reboot

- **Connection Mode:** "Automatically" or "**Static**".
  - ➢ If "Automatically" mode is selected, CPE would automatically acquire configuration

information.

➢ 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 the connection mode is “Automatically” and editable when the mode is “**Static**”.



WAN Setting

Basic config

WAN Connection Type: NAT Mode

Host Name: Telrad_02978A

WAN MTU: 1400

Enable NAT-Q: □

WAN IP Setting

Connection Mode: Automatically

WAN IP Address: 10 . 0 . 181 . 104

WAN Subnet Mask: 255 . 0 . 0 . 0

WAN Gateway Address: 10 . 0 . 0 . 151

WAN DNS Setting

Connection Mode: Automatically

DNS 1: 141 . 226 . 76 . 1

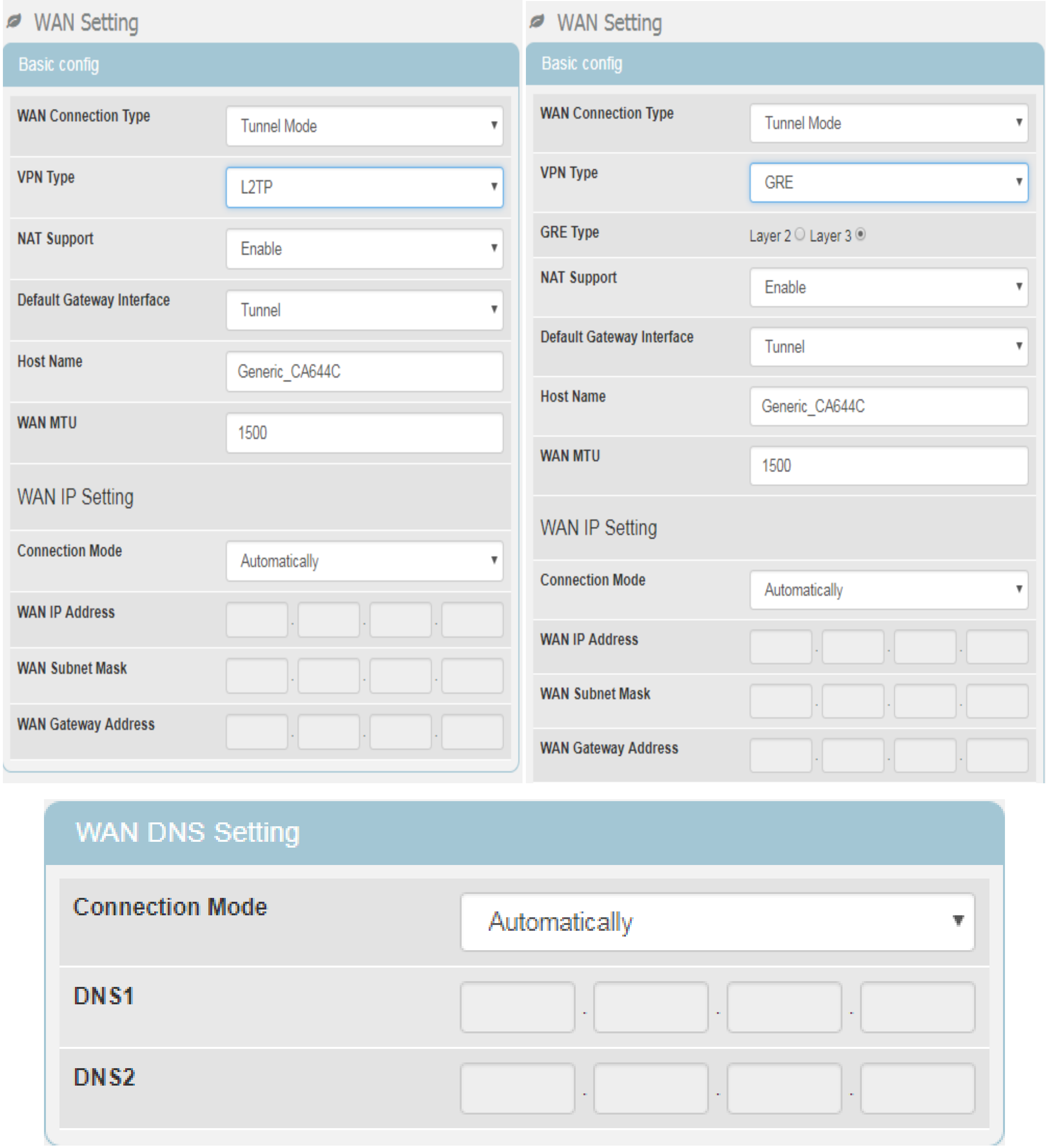
DNS 2: 141 . 226 . 76 . 10

Two WAN IP, DNS

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

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)



WAN Setting

Basic config

WAN Connection Type	Tunnel Mode
VPN Type	L2TP
NAT Support	Enable
Default Gateway Interface	Tunnel
Host Name	Generic_CA644C
WAN MTU	1500

WAN IP Setting

Connection Mode	Automatically
WAN IP Address	. . .
WAN Subnet Mask	. . .
WAN Gateway Address	. . .

WAN Setting

Basic config

WAN Connection Type	Tunnel Mode
VPN Type	GRE
GRE Type	Layer 2 ○ Layer 3 ●
NAT Support	Enable
Default Gateway Interface	Tunnel
Host Name	Generic_CA644C
WAN MTU	1500

WAN IP Setting

Connection Mode	Automatically
WAN IP Address	. . .
WAN Subnet Mask	. . .
WAN Gateway Address	. . .

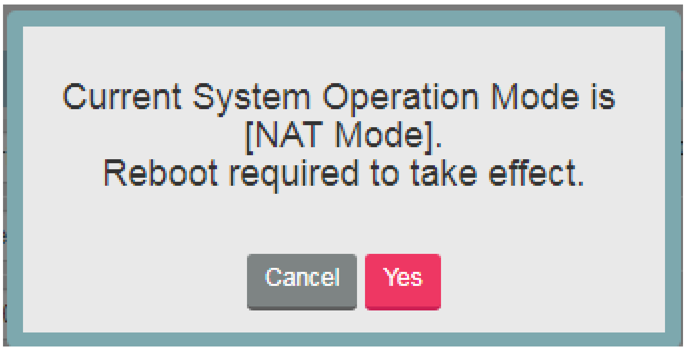
WAN DNS Setting

Connection Mode	Automatically
DNS1	. . .
DNS2	. . .

Network > WAN Setting > PPTP, L2TP, GRE

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

!	Changing the "**WAN Connection Type**" 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:** L2TP (with IPsec)

  GRE (Layer2/ Layer3) Tunnel Mode
- **NAT Support:** CPE will do network address translation for its clients in LAN.
- **Default Gateway Interface:** Users can select which interface as the default gateway. The default is "**Tunnel**" Interface.
- **L2TP Server/ User/ Password (Only in L2TP):**The IP address of server and username and password for authentication.
- **GRE Type (Layer 2)/ Destination IP Address:** The IP address of the peer to build GRE tunnel with CPE.
- **GRE Type (Layer 3)/Tunnel IP Address/ Subnet Mask:** The IP address of the peer to build GRE tunnel with CPE**.** The subnet mask is used to determine the traffic sent to the peer.

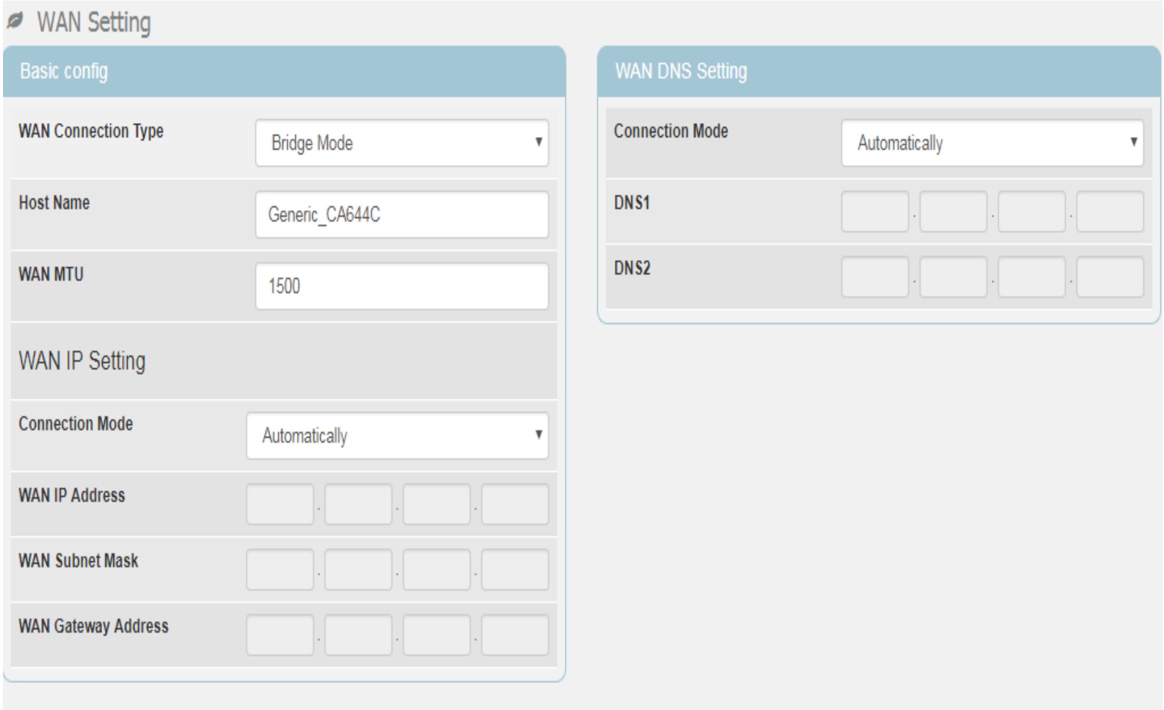
!	All information need in this page are assigned by "Tunnel Server". Like Server IP, Username and Password.

- **Connection Mode:** "Automatically" or "Static".
  - If "Automatically" mode is selected, CPE would automatically acquire configuration information.
  - 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 “Automatically” 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 “**ConnectionMode**”. Otherwise, these values will be given by DHCP server.

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)



WAN Setting

Basic config

WAN Connection Type	Bridge Mode
Host Name	Generic_CA644C
WAN MTU	1500

WAN IP Setting

Connection Mode	Automatically
WAN IP Address	. . .
WAN Subnet Mask	. . .
WAN Gateway Address	. . .

WAN DNS Setting

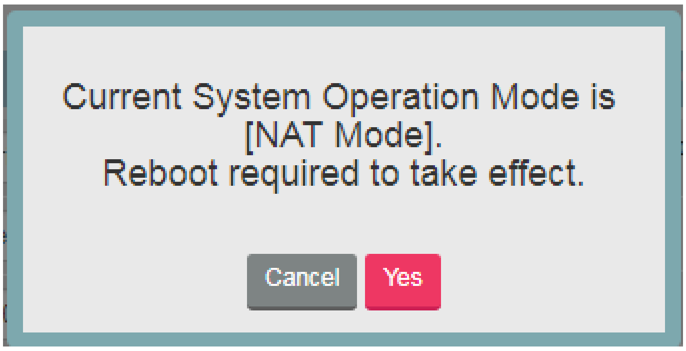
Connection Mode	Automatically
DNS1	. . .
DNS2	. . .

Network >WAN Setting

- **WAN Connection Type: users have NAT**, **Tunnel**, **Bridge** and **Router** Mode to choose from.

  The following pages show how to configure "**Bridge mode**".

!	Changing the "**WAN Connection Type**" 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.



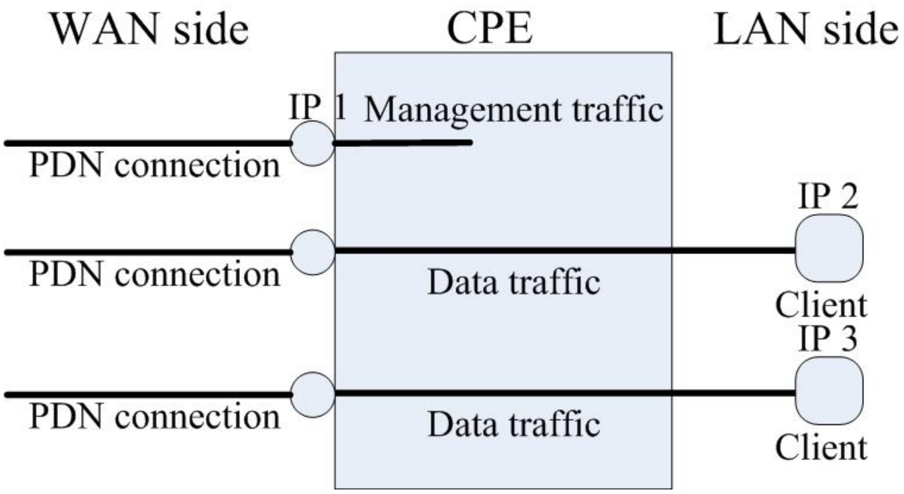
Current System Operation Mode is [NAT Mode].
Reboot required to take effect.

Pop-up windows for reboot confirm

- **Host Name:** Currently no function.

- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when "**Connection Mode**" is "**Automatically**" 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 "**ConnectionMode**". Otherwise, these values will be given by DHCP server.
- In single PDN connection mode, CPE is in "IP pass through" (IPPT) mode. The device behind CPE would get the IP which is allocated from eNB directly. If user wants to change the device behind CPE, user could do the either way of following:
  - User would need a complete process of IP release on the device, then user can switch to another device. (only support IPv4)
  - User could reboot the CPE after connecting to another device.
- In Multi-PDN connections mode (Only in Bridge Mode): If user set the Multi-PDN connections, CPE will pre-create PDN connections for local clients. Thus, clients request IP addresses from CPE, CPE will reply an IP address got from one of PDN connections. The IP address of the first PDN connection is always allocated to the management of CPE.

  Below is an example for "enabled" case.(only support IPv4)

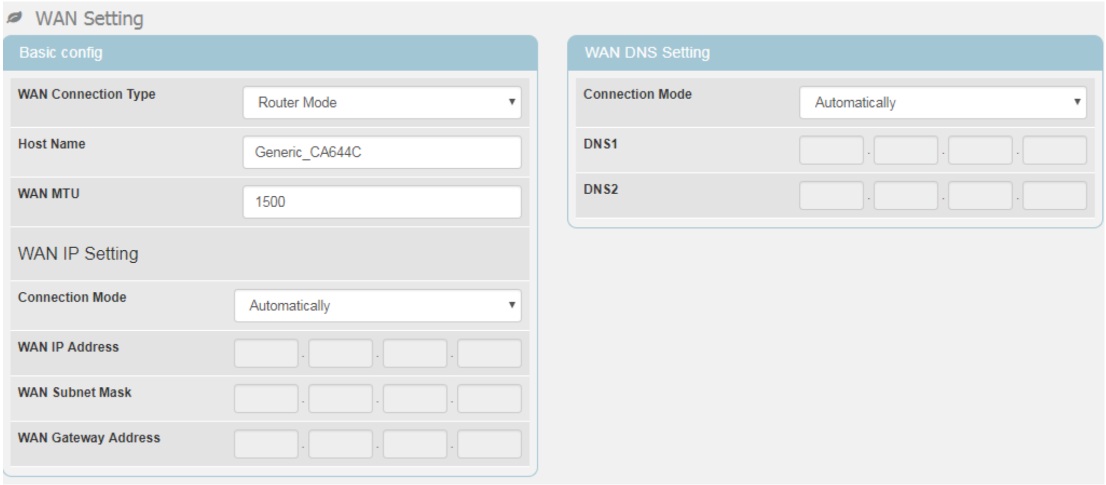


Multi-PDN in Bridge Mode

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)

- **WAN Connection Type:** users have **NAT**, **Tunnel**, **Bridge** and **Router** mode to choose from.The following pages will show how to configure "**Router mode**".



WAN Setting

Basic config

WAN Connection Type: Router Mode

Host Name: Generic_CA644C

WAN MTU: 1500

WAN IP Setting

Connection Mode: Automatically

WAN IP Address: . . .

WAN Subnet Mask: . . .

WAN Gateway Address: . . .

WAN DNS Setting

Connection Mode: Automatically

DNS1: . . .

DNS2: . . .

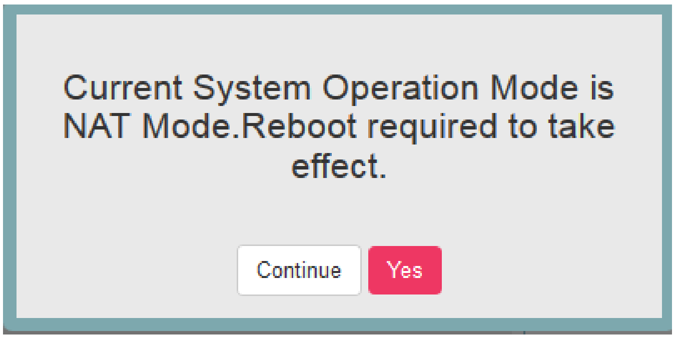
Network >WAN Setting

- **Connection Mode:** "Automatically" or "Static".
  - If "Automatically" mode is selected, CPE would automatically acquire configuration information.
  - 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 "**Connection mode**" is "Automatically" 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.

!	Changing the “**WAN Connection Type**” 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.

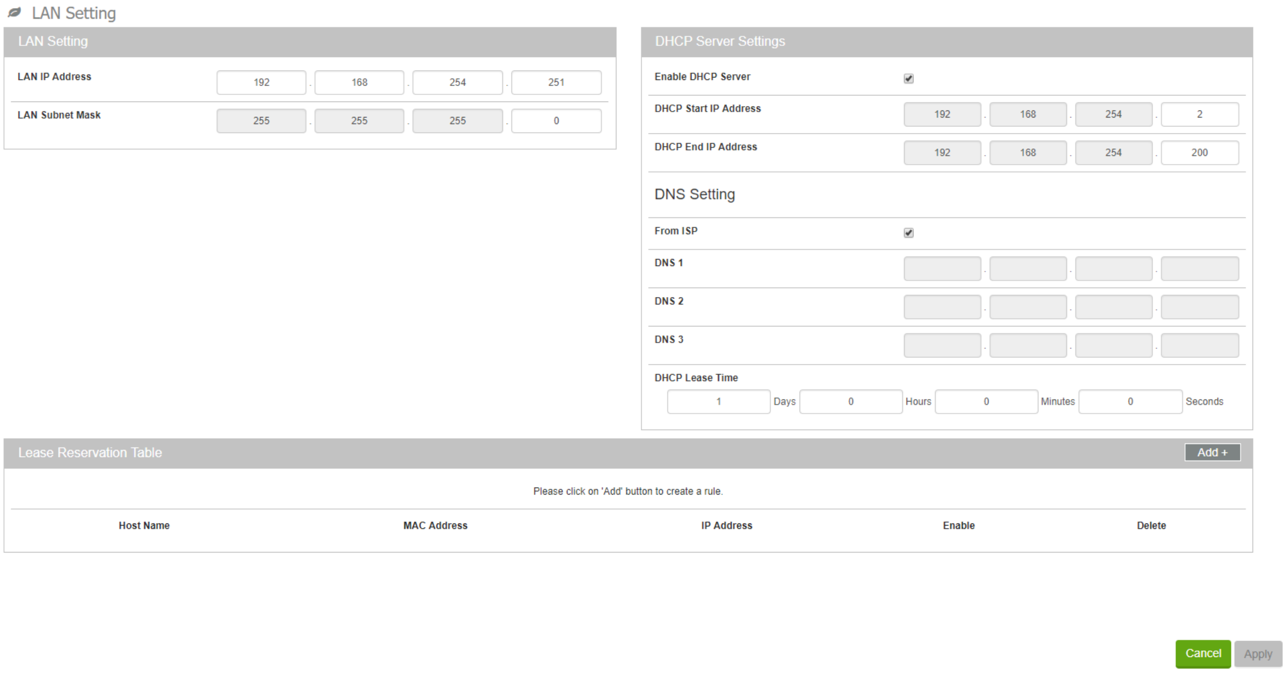


Current System Operation Mode is NAT Mode.Reboot required to take effect.

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 Start IP Address	192 . 168 . 254 . 2
DHCP End IP Address	192 . 168 . 254 . 200

DNS Setting

From ISP	☑
DNS 1	
DNS 2	
DNS 3	
DHCP Lease Time	1 Days 0 Hours 0 Minutes 0 Seconds

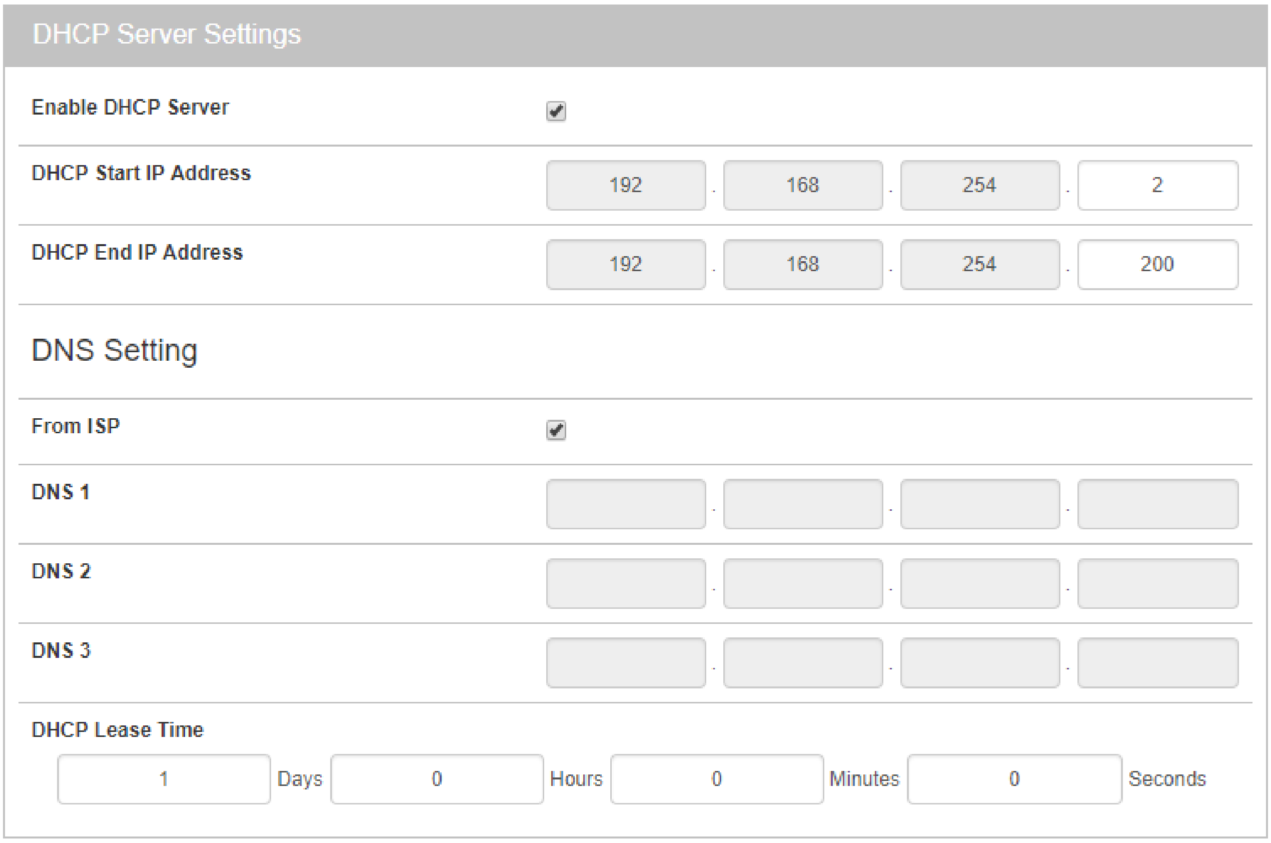
Lease Reservation Table

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

Host Name	MAC Address	IP Address	Enable	Delete

Network >LAN Setting

- **LAN Setting:**
  - **LAN IP Address / Subnet Mask:** The IP address and subnet mask used by CPE in LAN
    - 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)



DHCP Server Settings

Enable DHCP Server ☑

DHCP Start IP Address 192 . 168 . 254 . 2

DHCP End IP Address 192 . 168 . 254 . 200

DNS Setting

From ISP ☑

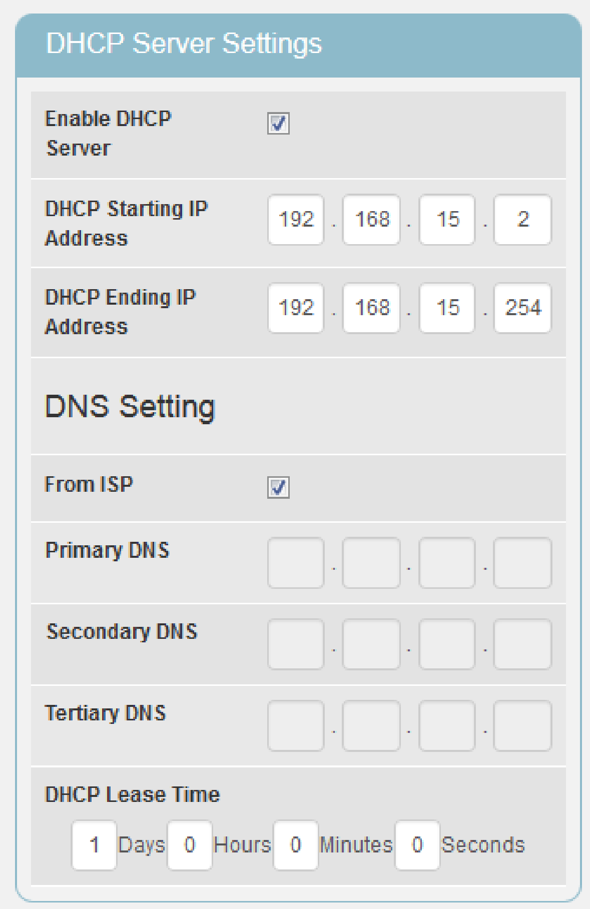
DNS 1 . . .

DNS 2 . . .

DNS 3 . . .

DHCP Lease Time

1 Days 0 Hours 0 Minutes 0 Seconds



DHCP Server Settings

Enable DHCP Server ☑

DHCP Starting IP Address 192 . 168 . 15 . 2

DHCP Ending IP Address 192 . 168 . 15 . 254

DNS Setting

From ISP ☑

Primary DNS . . .

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 or WiFi would obtain a dynamic IP address from CPE.

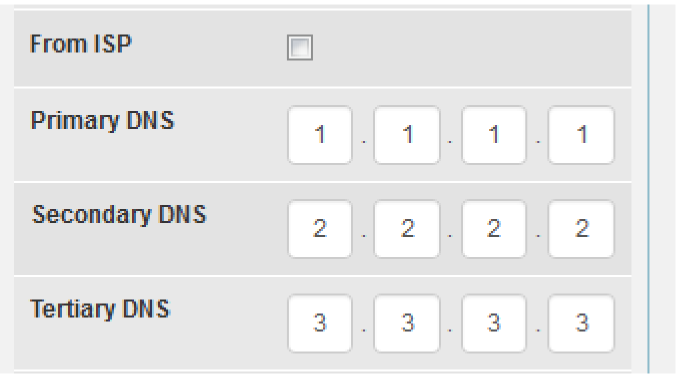
- **Enable DHCP Server:** enable/disable DHCP server
- **DHCP Starting IP Address:** The starting IP address assigned by DHCP server.
- **DHCP Ending IP Address:** The ending IP address assigned by DHCP server.

!	Notice that WiFi and 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**".

!	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.



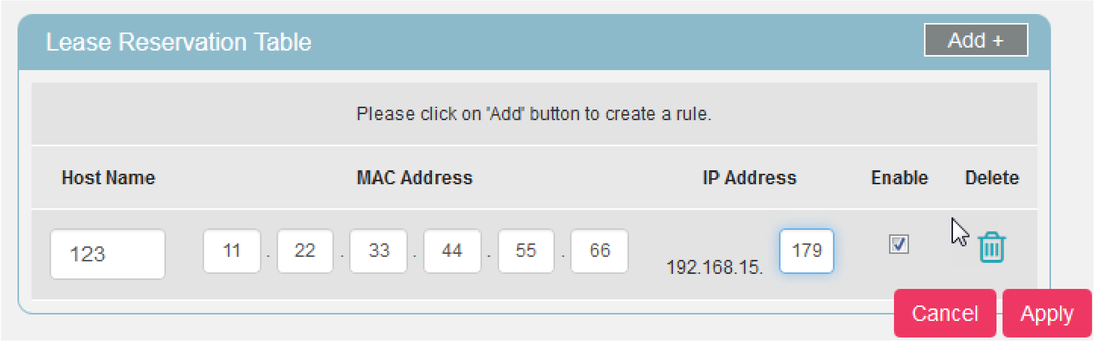
From ISP	☐
Primary DNS	1 . 1 . 1 . 1
Secondary DNS	2 . 2 . 2 . 2
Tertiary DNS	3 . 3 . 3 . 3

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 "**192.168.15.123**" and the host name "**Example**" to it.



Lease Reservation Table

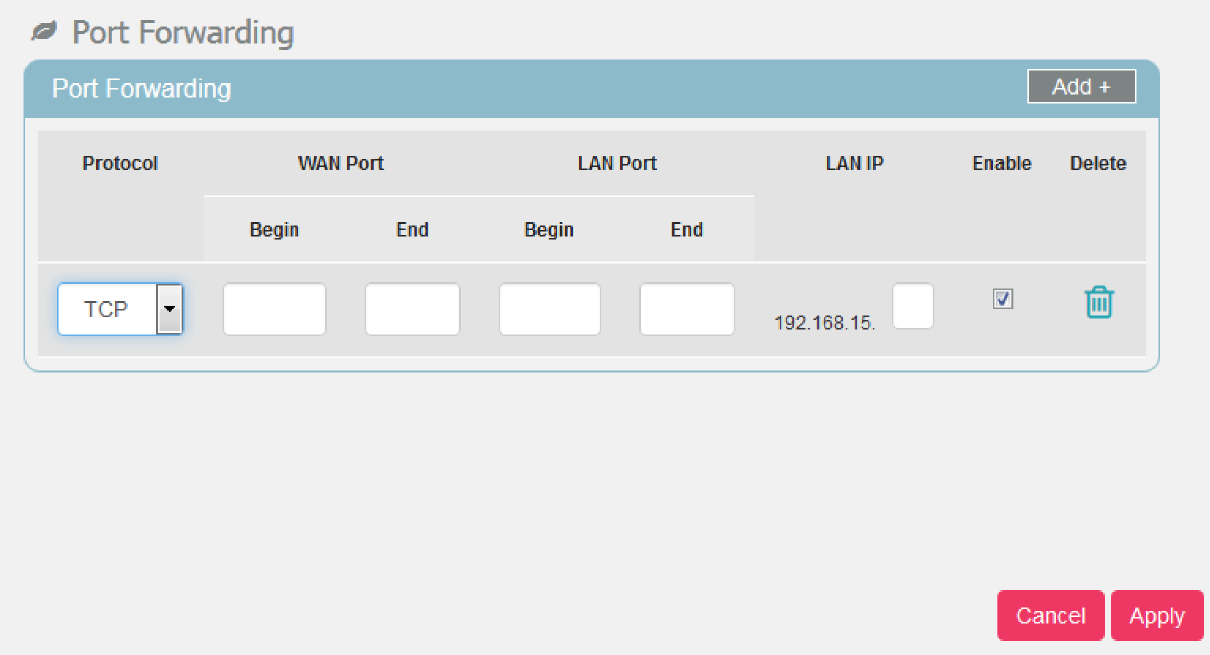
Please click on 'Add' button to create a rule.

Host Name	MAC Address	IP Address	Enable	Delete
123	11 . 22 . 33 . 44 . 55 . 66	192.168.15. 179	☑	🗑

!	"Example", "11:22:33:44:55:66", "192.168.15.179" 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 | Port Management | Port Forwarding (Available in NAT, Tunnel Mode)



Protocol	WAN Port		LAN Port		LAN IP	Enable	Delete
	Begin	End	Begin	End			
TCP					192.168.15.	☑	🗑

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 setup in LAN side like FTP server.

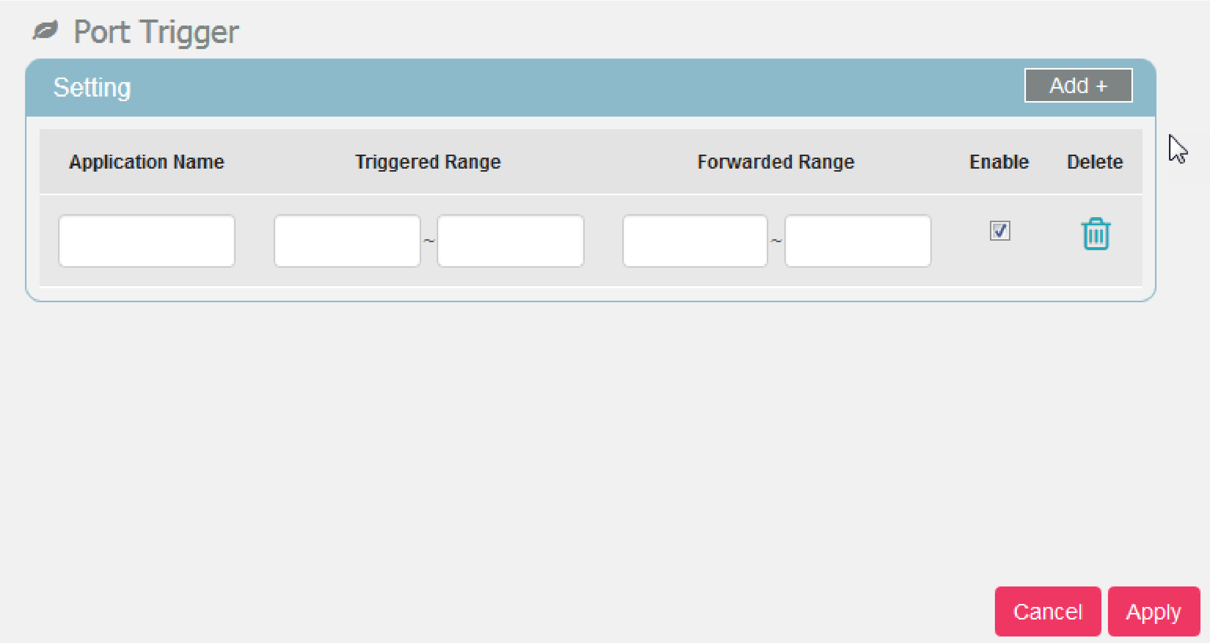
- Click **"Add +"** button to add a new rule, clicking **"Delete"** icon (🗑) to delete the rule.
- **Protocol:** TCP or UDP.
- **WAN Port:** The range of WAN port.
- **LAN Port:** The range of LAN port.
- **LAN IP:** Enter the IP which desires to receive forwarded packets.
- **Enable:** Enable/Disable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

!	WAN Port 53, 68,123, 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)



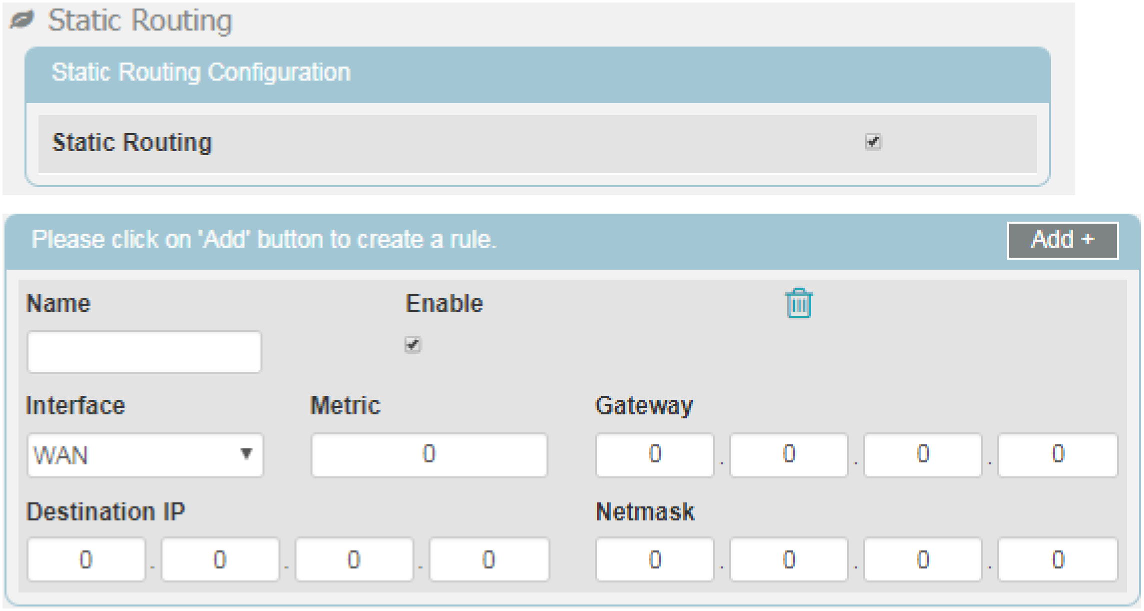
Network > Port Management >Port Trigger

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 | Routing(Available in Router, Tunnel Mode)



Static Routing ☑

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

Name:

Enable ☑

Interface: WAN

Metric: 0

Gateway: 0 . 0 . 0 . 0

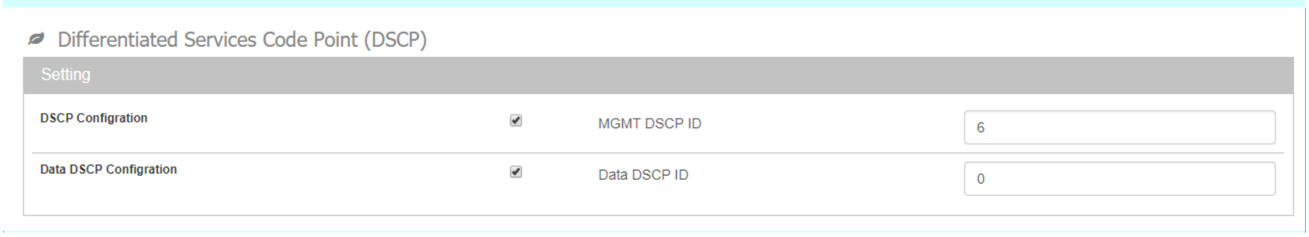
Destination IP: 0 . 0 . 0 . 0

Netmask: 0 . 0 . 0 . 0

Network > Static Routing

- **Static Routing:** Enable/Disable static routing.
- **When Static Routing is enabled,** you can add/del routing item from the drop-down l ist, and configure the following parameters:**Name,Interface,Metric,Geteway,Destination IP and Netmask**.

Network | DSCP



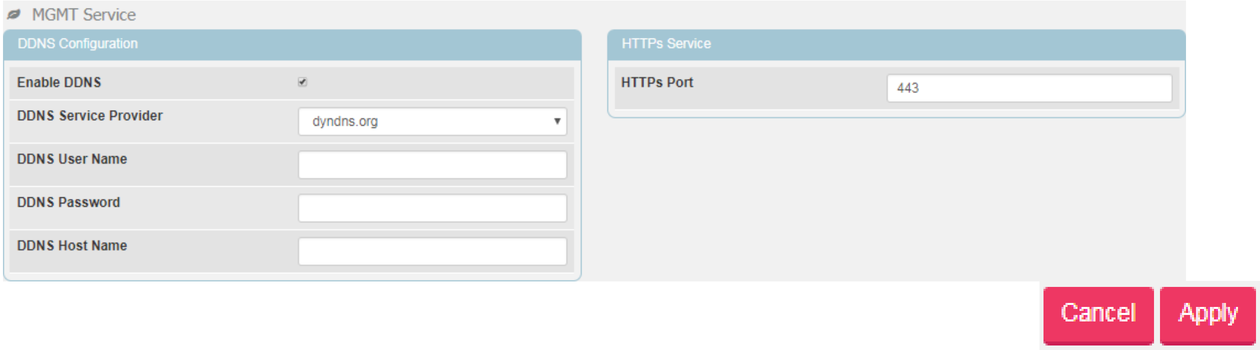
Differentiated Services Code Point (DSCP)

Setting

DSCP Configration	☑	MGMT DSCP ID	6
Data DSCP Configration	☑	Data DSCP ID	0

[MD7]

Network | MGMT Service



MGMT Service

DDNS Configuration

Enable DDNS	☑
DDNS Service Provider	dyndns.org
DDNS User Name	
DDNS Password	
DDNS Host Name	

HTTPs Service

HTTPs Port	443

Network > MGMT Service

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**.
- **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.

!	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.

9.3. IPv6

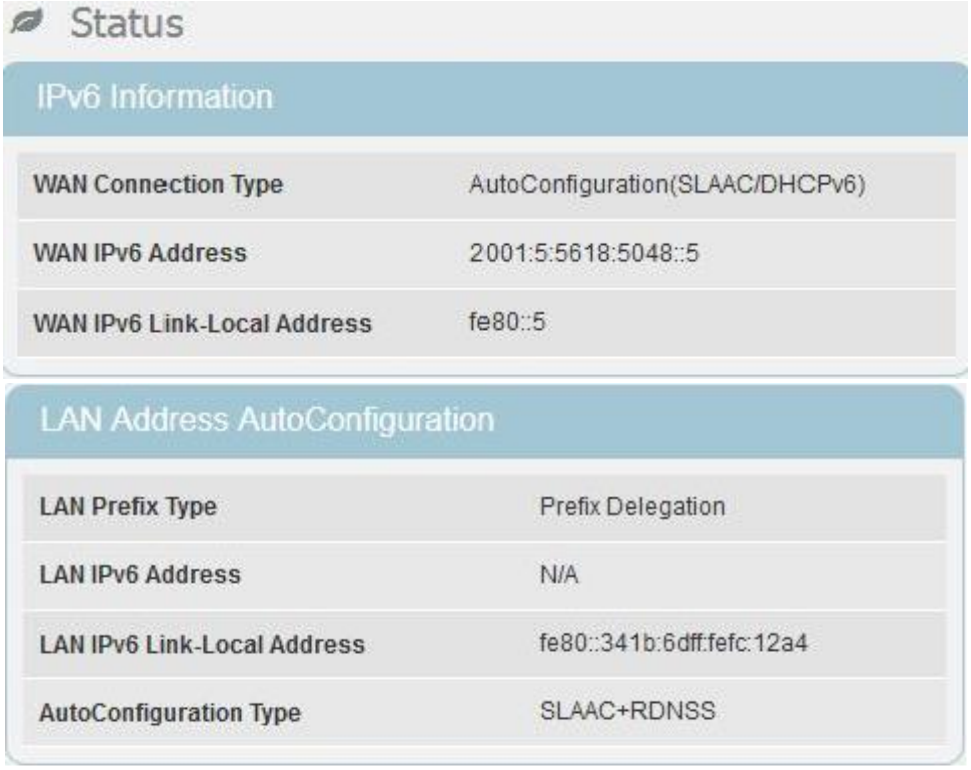
IPv6 provides other technical benefits in addition to a larger addressing space.

	Display in **Brief Summary Page**

- **Menu Structure:**

IPv6	Status
	Settings

IPv6| Status



Status

IPv6 Information

WAN Connection Type	AutoConfiguration(SLAAC/DHCPv6)
WAN IPv6 Address	2001:5:5618:5048::5
WAN IPv6 Link-Local Address	fe80::5

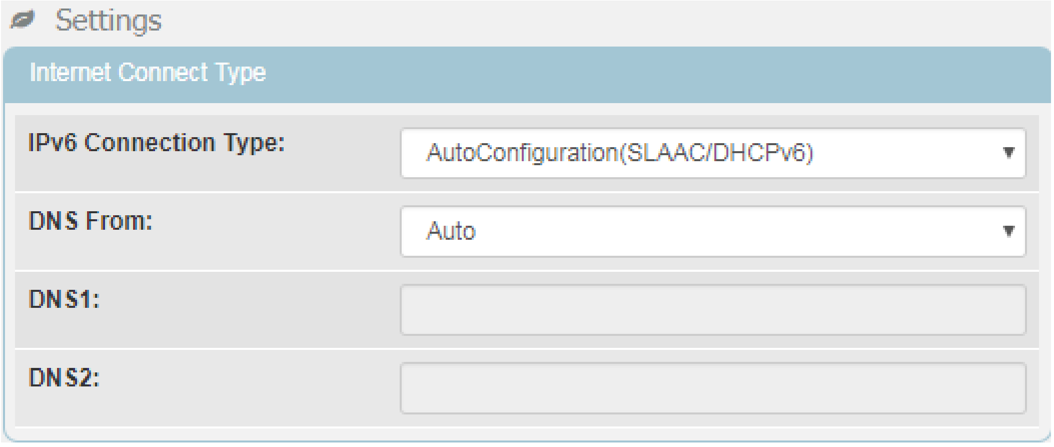
LAN Address AutoConfiguration

LAN Prefix Type	Prefix Delegation
LAN IPv6 Address	N/A
LAN IPv6 Link-Local Address	fe80::341b:6dff:fefc:12a4
AutoConfiguration Type	SLAAC+RDNSS

IPv6>Status

- **IPv6 Information:** This section shows WAN Connection Type, WAN IPv6 Address and WAN IPv6 Link-Local Address
- **LAN Address AutoConfiguration:** This section shows LAN Prefix Type, LAN IPv6 Address, LAN IPv6 Link-Local Address and AutoConfiguration Type.

IPv6 | Settings | Internet Connect Type



Settings

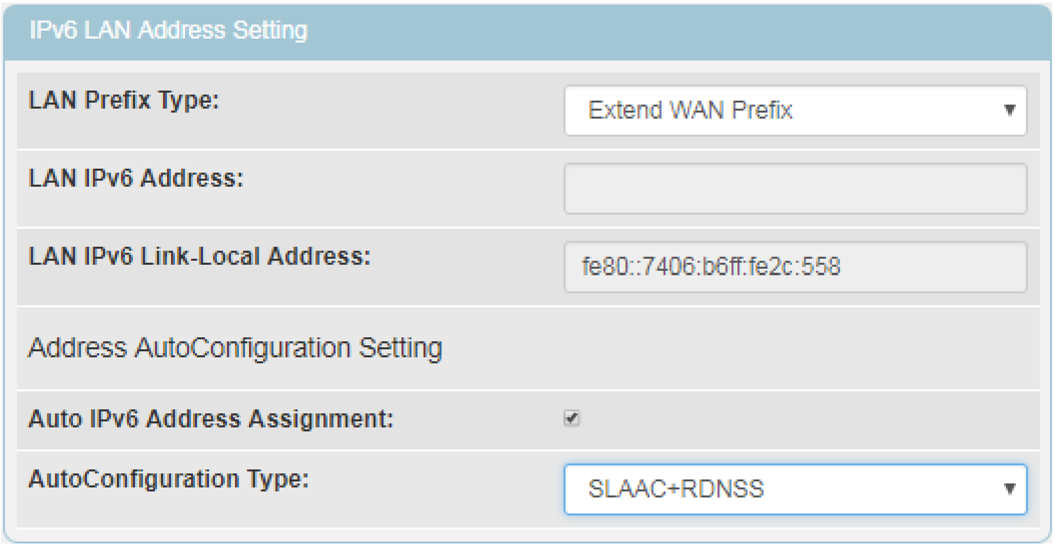
Internet Connect Type

IPv6 Connection Type:	AutoConfiguration(SLAAC/DHCPv6) ▾
DNS From:	Auto ▾
DNS1:	
DNS2:	

IPv6> Settings

- **IPv6 Connect Type:** Choose SLAAC+DHCPv6 for CPE's clients to get IPv6 IP.
- **DNS from:** Choose Auto or Static option.
- **DNS 1:** Enter the IPv6 DNS1 record in IPv6 DHCP Server.
- **DNS 2:** Enter the IPv6 DNS2 record in IPv6 DHCP Server.

IPv6 | Settings | Extend WAN Prefix



IPv6 LAN Address Setting

LAN Prefix Type:	Extend WAN Prefix ▾
LAN IPv6 Address:	
LAN IPv6 Link-Local Address:	fe80::7406:b6ff:fe2c:558

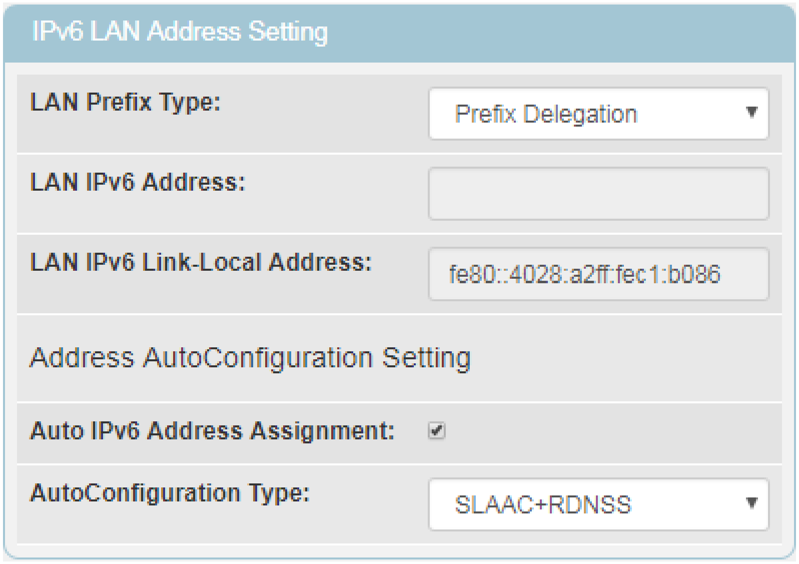
Address AutoConfiguration Setting

Auto IPv6 Address Assignment:	☑
AutoConfiguration Type:	SLAAC+RDNSS ▾

IPv6> Settings

- **LAN Prefix Type(Extend Wan Prefix) :**Assign a network address prefix and automate configuration and provisioning of the public routable addresses for the network
- **LAN IPv6 Link-Local Address**: Use this address to connection CPE’s Web-GUI.
- **Auto IPv6 Address Assignment:** Enable/Disable.
- **Auto Configuration Type :** Choose SLAAC+RDNSS, SLAAC+DHCP or Automatically for CPE’s clients to get IPv6 IP

IPv6 | Settings | Prefix Delegation



IPv6 LAN Address Setting

LAN Prefix Type: Prefix Delegation ▾

LAN IPv6 Address:

LAN IPv6 Link-Local Address: fe80::4028:a2ff:fec1:b086

Address AutoConfiguration Setting

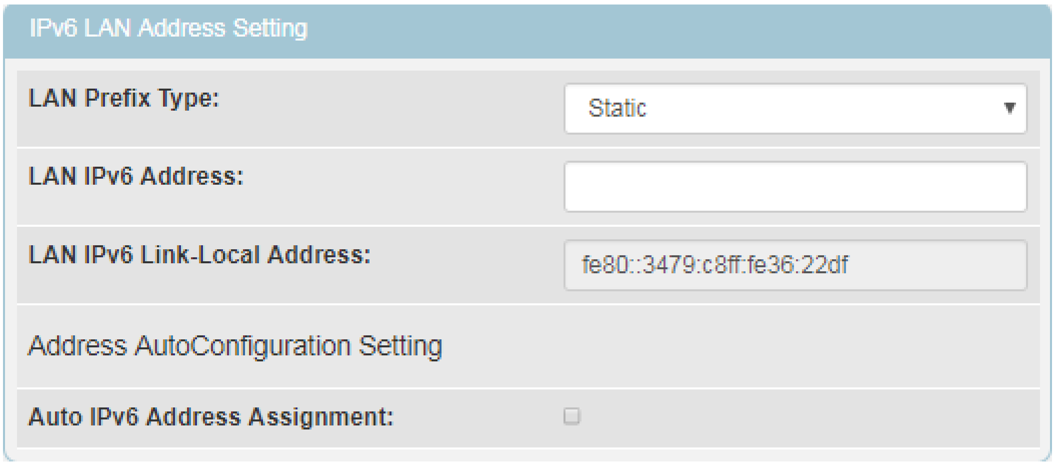
Auto IPv6 Address Assignment: ☑

AutoConfiguration Type: SLAAC+RDNSS ▾

IPv6> Settings

- **LAN Prefix Type (Prefix Delegation): Supported** by most ISPs who provide native IPv6 for consumers on fixed networks.
- **LAN IPv6 Link-Local Address**: Use this address to connection CPE's Web-GUI.
- **Auto IPv6 Address Assignment:** Enable/Disable.
- **Auto Configuration Type :** Choose SLAAC+RDNSS, SLAAC+DHCP or Automatically for CPE's clients to get IPv6 IP

IPv6 | Settings | Static


IPv6 LAN Address Setting

LAN Prefix Type: Static ▾

LAN IPv6 Address:

LAN IPv6 Link-Local Address: fe80::3479:c8ff:fe36:22df

Address AutoConfiguration Setting

Auto IPv6 Address Assignment: □

IPv6> Settings

- **LAN Prefix Type(Static): This** type can Enter LAN IPv6 Address as follow.
- **LAN IPv6 Address:** Enter the IPv6 address.
- **LAN IPv6 Link-Local Address**: Use this address to connection CPE's Web-GUI.
- **Auto IPv6 Address Assignment:** Enable/Disable.
- **Auto Configuration Type:** Choose SLAAC+RDNSS, SLAAC+DHCP or Automatically for CPE's clients to get IPv6 IP.

9.4. Firewall:

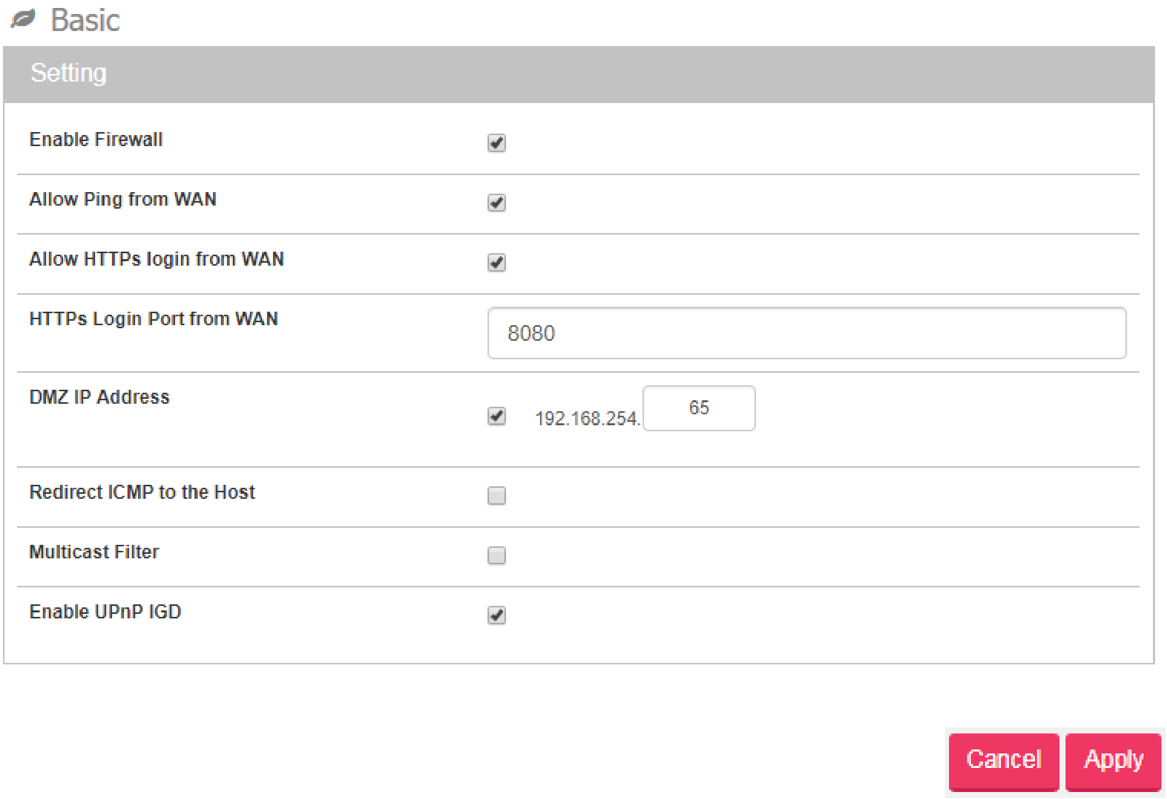
The “Firewall” page allows user to configure firewall to block and grant some network access.

	Display in **Brief Summary Page**

- **Menu structure:**

Firewall	Basic
	Access Restriction

Firewall | Basic



Basic

Setting

Enable Firewall	☑
Allow Ping from WAN	☑
Allow HTTPs login from WAN	☑
HTTPs Login Port from WAN	8080
DMZ IP Address	☑ 192.168.254. 65
Redirect ICMP to the Host	□
Multicast Filter	□
Enable UPnP IGD	☑

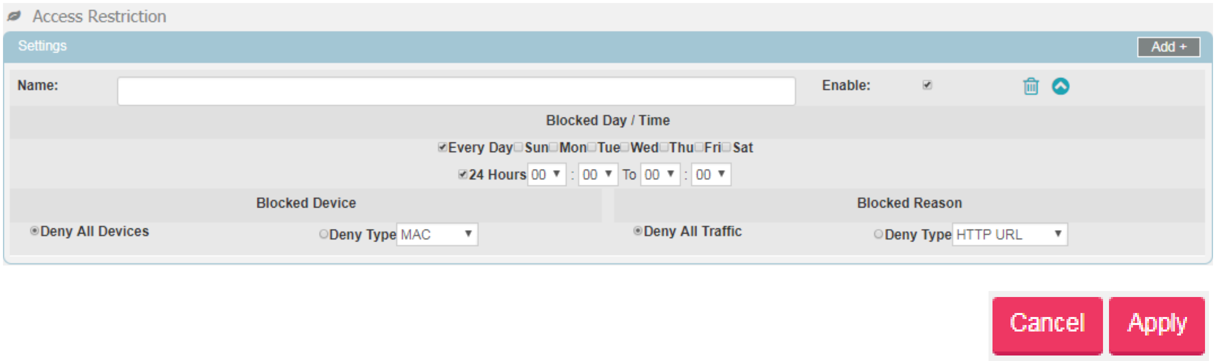
Firewall > Basic

- **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:** Enable/Disable Internet Gateway Device.

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 | Access Restriction



Access Restriction

Settings — Add +

Name: ____ Enable: ☑

Blocked Day / 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

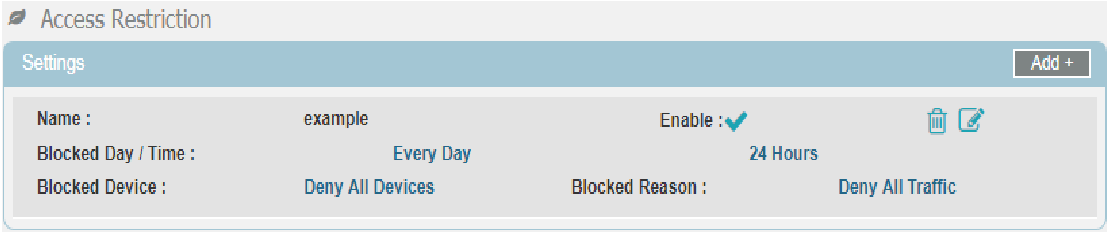
Blocked Reason: ●Deny All Traffic ○Deny Type HTTP URL

Cancel Apply

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.



Access Restriction

Settings — Add +

Name : example Enable : ✓

Blocked Day / Time : Every Day 24 Hours

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

Firewall > Access Restriction (Digest)

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

10. Management

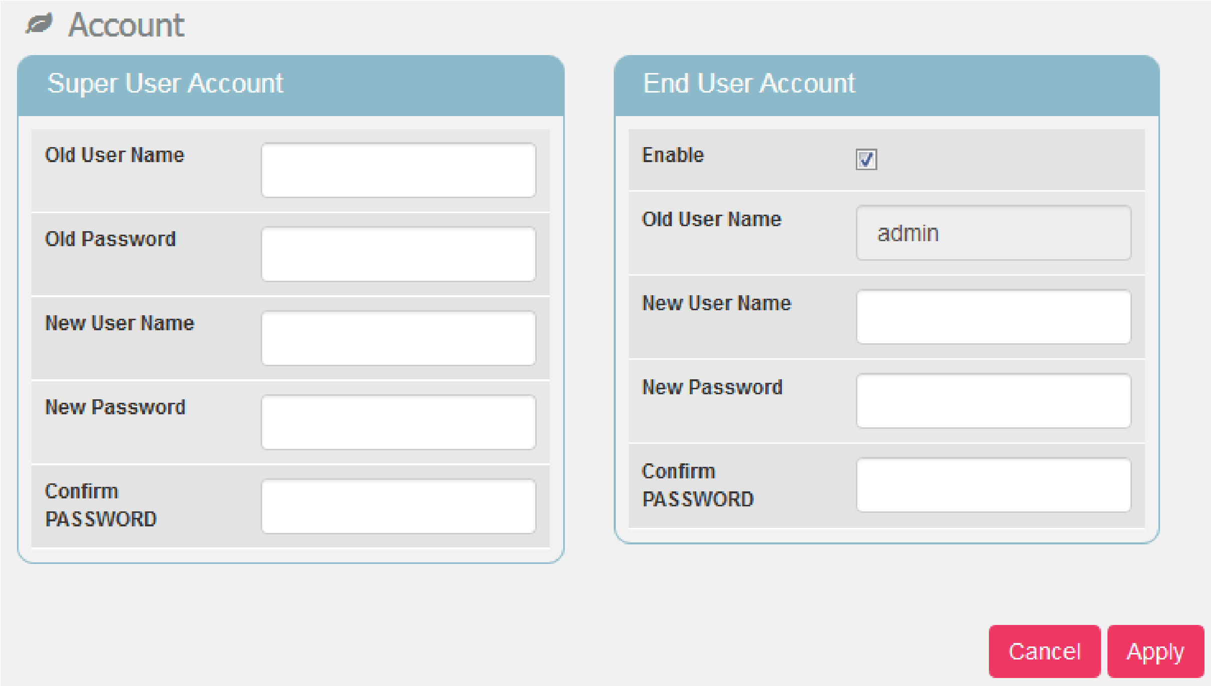
The “Management” page allows user to configure the main system parameters such as password, language, device time/name …etc.

Management	Display in **Brief Summary Page**

- **Menu structure:**

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

Management | Account



Account

Super User Account

Old User Name

Old Password

New User Name

New Password

Confirm PASSWORD

End User Account

Enable ☑

Old User Name: admin

New User Name

New Password

Confirm PASSWORD

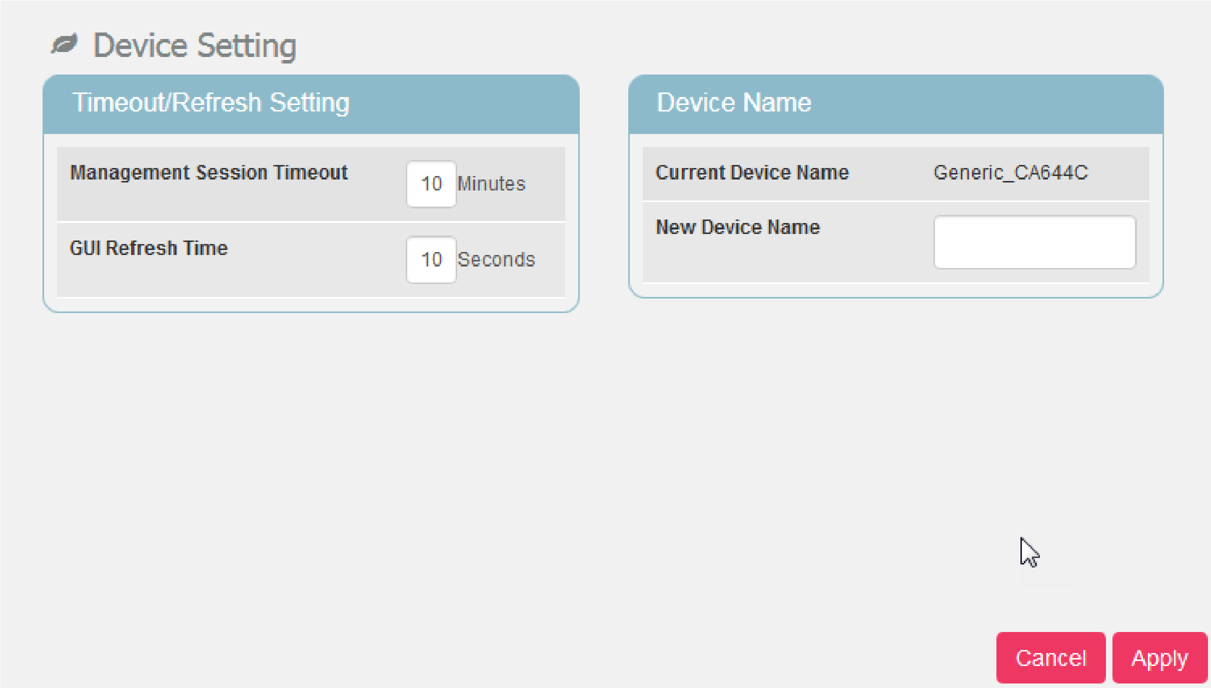
Management > Account Management

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 | Device Setting



Device Setting

Timeout/Refresh Setting

Management Session Timeout: 10 Minutes

GUI Refresh Time: 10 Seconds

Device Name

Current Device Name: Generic_CA644C

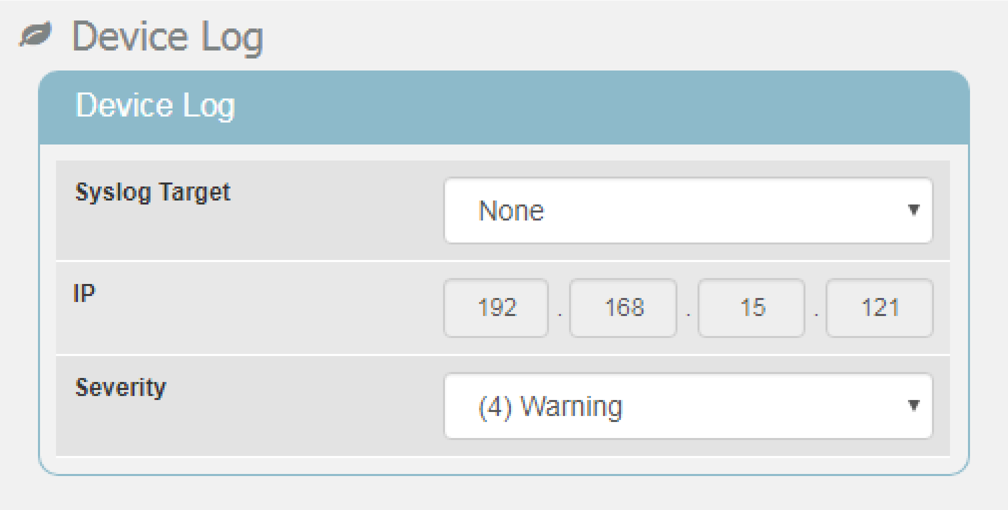
New Device Name:

Management > Device Setting

- **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 refreshes ay the designated time. (Range: 5-60 Seconds)
- **Device Name:** The name of CPE. Users can login 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 | Device Log



Device Log

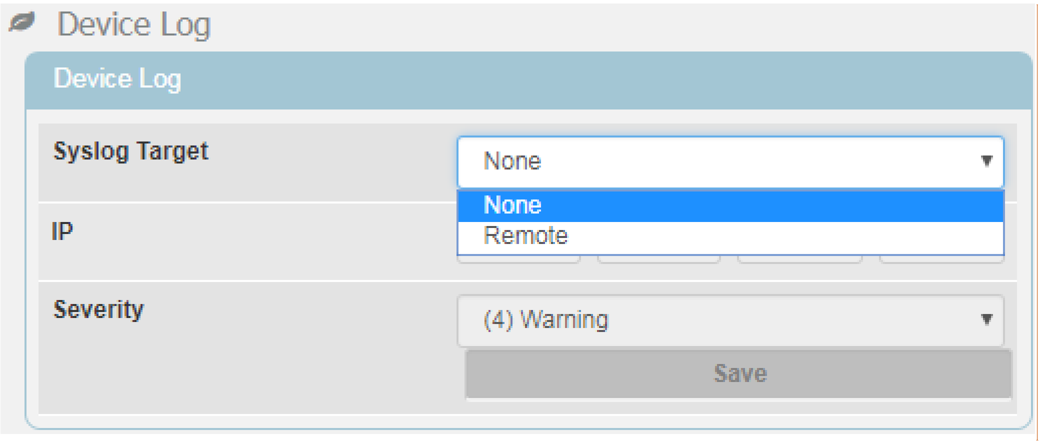
Device Log

Syslog Target: None

IP: 192 . 168 . 15 . 121

Severity: (4) Warning

Management >Device Log



Device Log

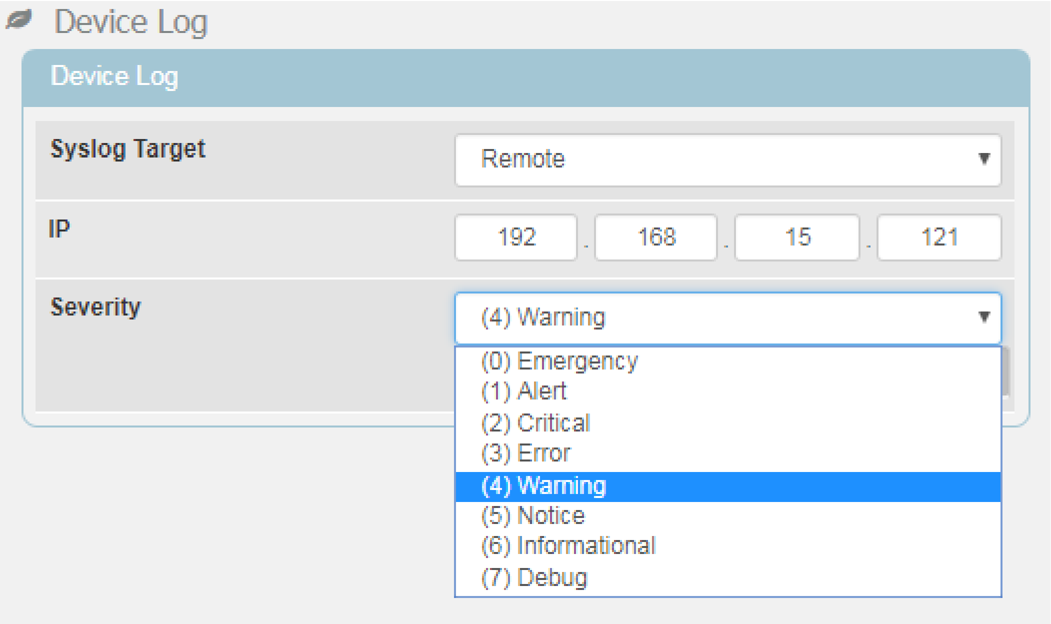
Device Log

Syslog Target: None

IP

Severity: (4) Warning

[a8]



Device Log

Device Log

Syslog Target: Remote

IP: 192 . 168 . 15 . 121

Severity: (4) Warning

Management >Device Log> Options of Severity & Syslog Target

Syslog is an efficient tool for engineer debugging. 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 Remote syslog server.

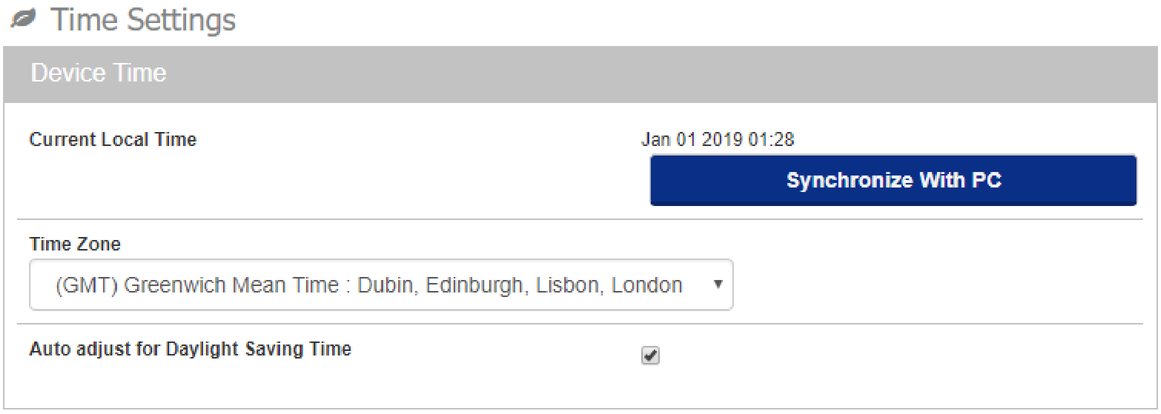
  IP (Only available at "Remote Status"): User can determine the Remote syslog server IP via this.

- **Severity:** User can log eight 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 | Device Time



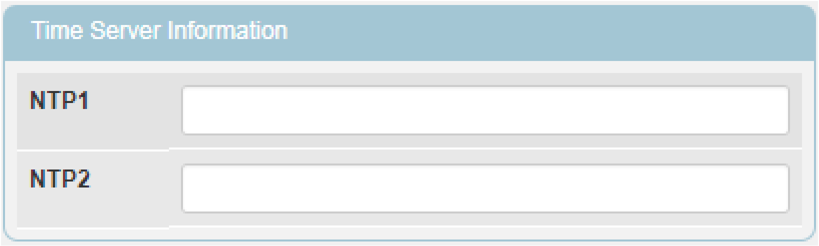
Time Settings

Device Time

Current Local Time: Jan 01 2019 01:28

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

Auto adjust for Daylight Saving Time ☑



Time Server Information

NTP1:

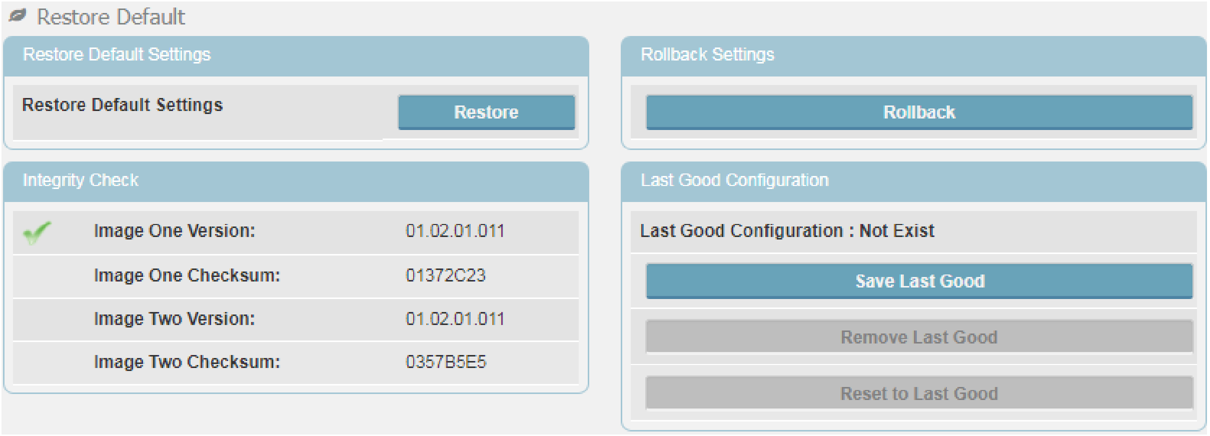
NTP2:

Management >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.
- ➢ **Time Server Information:** Setting the NTP server.
- ➢ **NTP1/2:** Users can specify two NTP servers in "IP" or "Domain name" format.

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 Settings

Restore Default Settings

Rollback Settings

Integrity Check

✓	Image One Version:	01.02.01.011
	Image One Checksum:	01372C23
	Image Two Version:	01.02.01.011
	Image Two Checksum:	0357B5E5

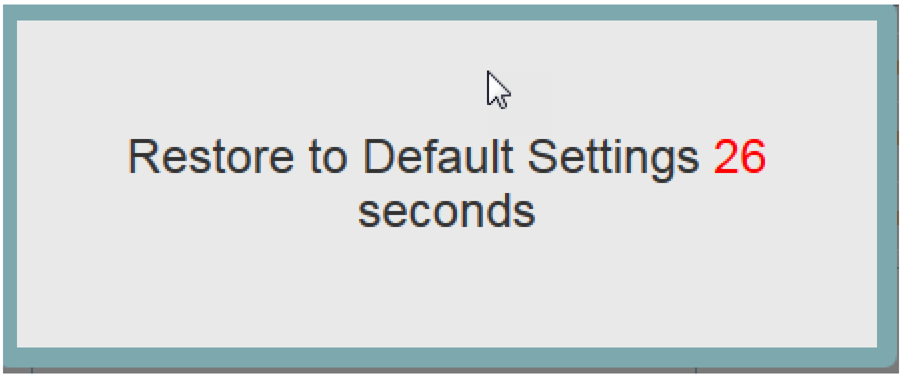
Last Good Configuration

Last Good Configuration : Not Exist

Management > Restore Default

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

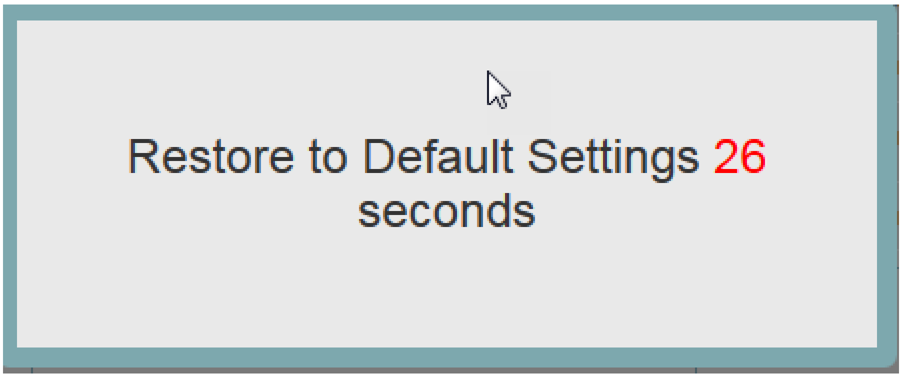
- **Restore Default:** Click **"Restore"** button to clear all users' configuration and restore to factory default settings.



Restore to Default Settings 26 seconds

Restore to default settings Window

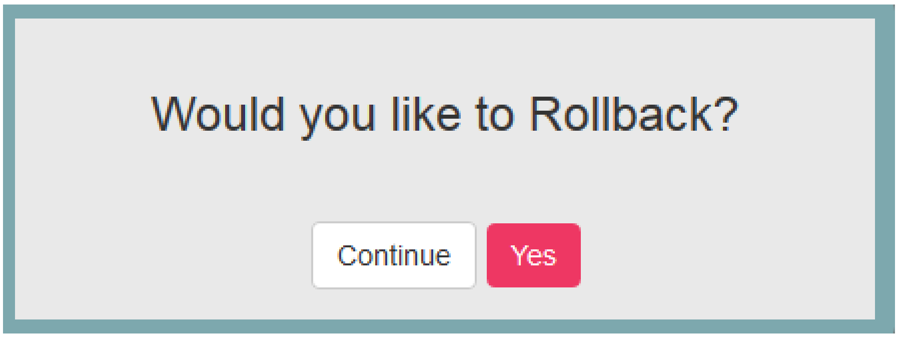
- **Integrity Check:** Integrity check for the software used in the device in case the storage device is broken**.** The green check ✓ indicates the investigation is passed.



Restore to Default Settings 26 seconds

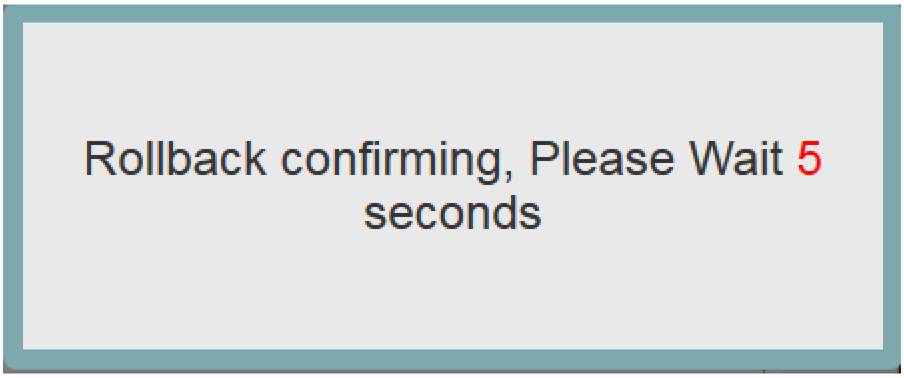
Integrity Check WindoW

- **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

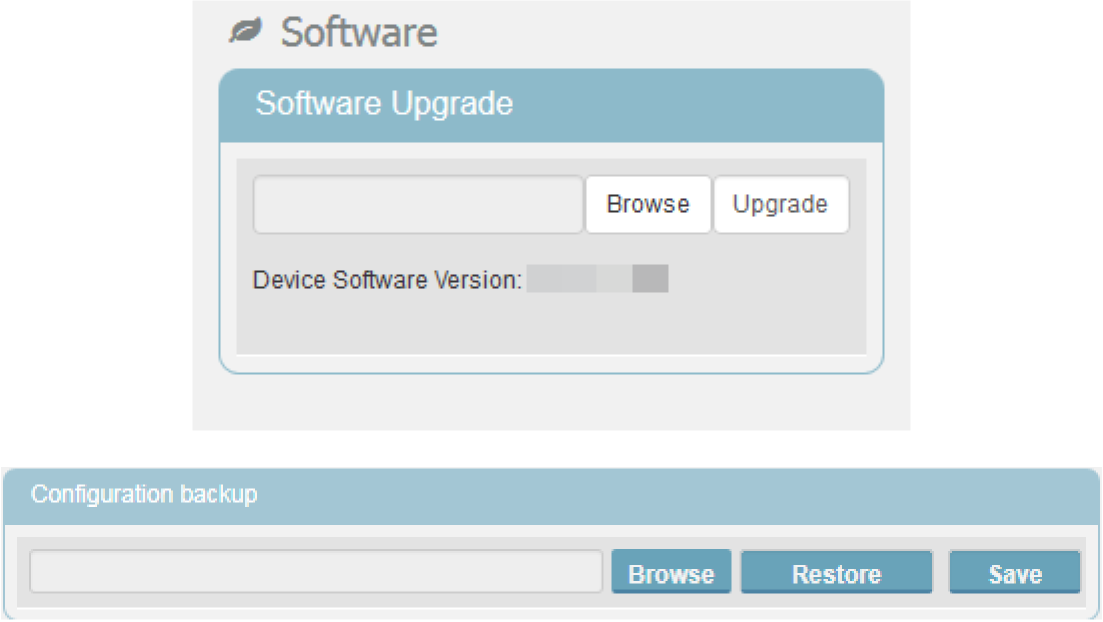


Rollback confirming, Please Wait 5 seconds

Rebooting 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.

Management | Software



Software

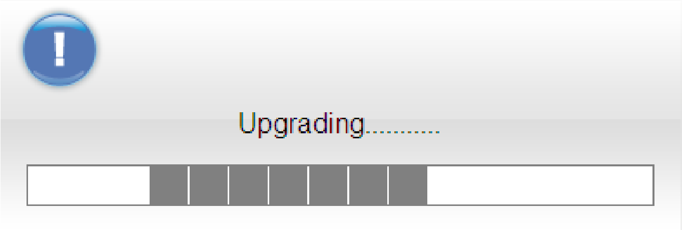
Software Upgrade

Device Software Version: [redacted]

Configuration backup

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.

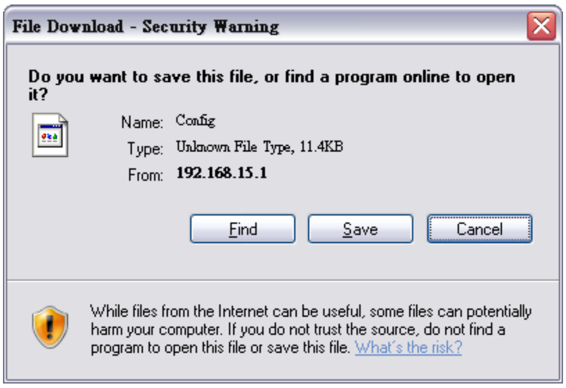


Upgrading...........

Management > Software> Upgrading Window

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

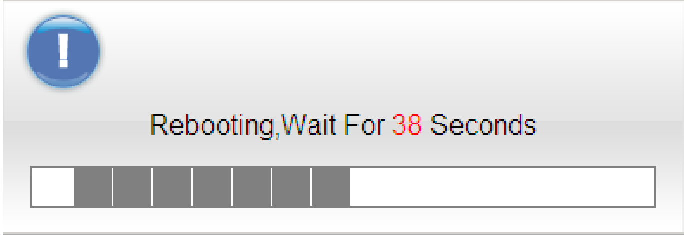
Type: Unknown File Type, 11.4KB

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?

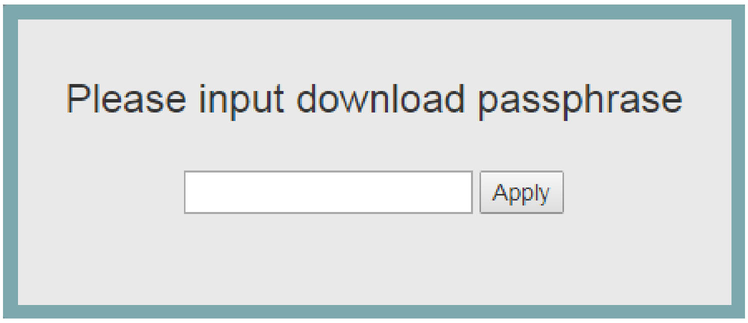
File Download Window

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.



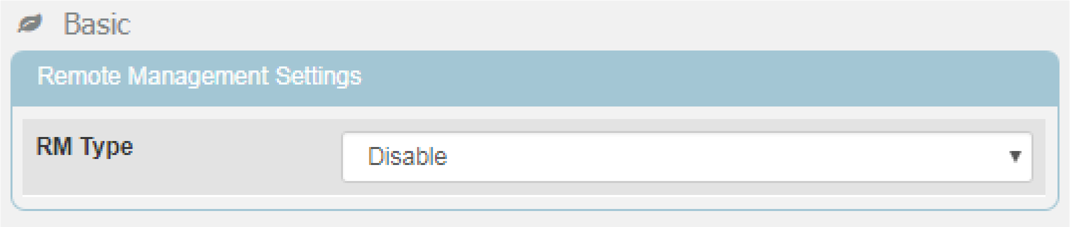
Rebooting,Wait For 38 Seconds

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 Apply *Enter Passphrase Window*

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



Basic

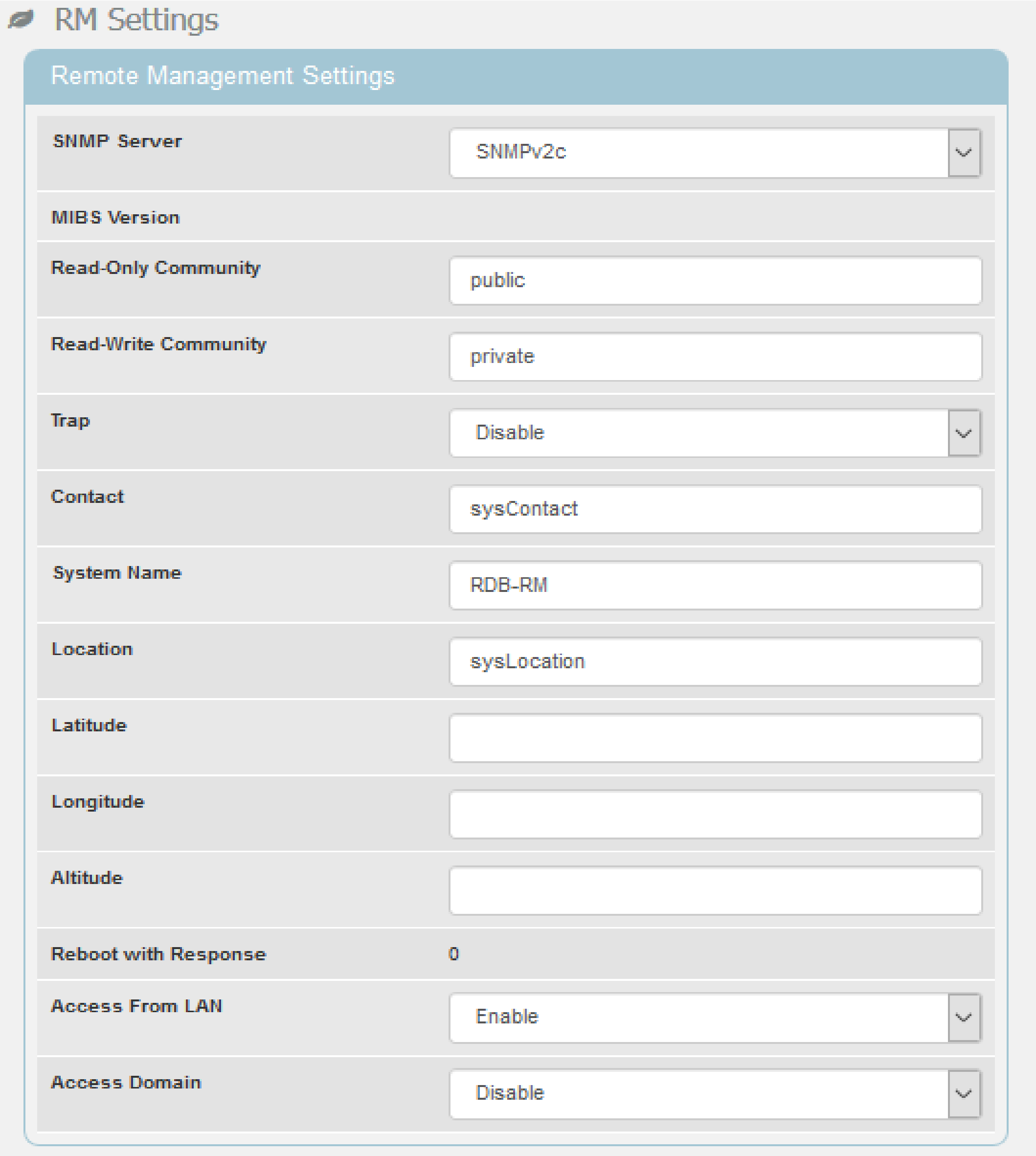
Remote Management Settings

RM Type	Disable

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

SNMP Server	SNMPv2c
MIBS Version	
Read-Only Community	public
Read-Write Community	private
Trap	Disable
Contact	sysContact
System Name	RDB-RM
Location	sysLocation
Latitude	
Longitude	
Altitude	
Reboot with Response	0
Access From LAN	Enable
Access Domain	Disable

Management > RM Settings (SNMP)

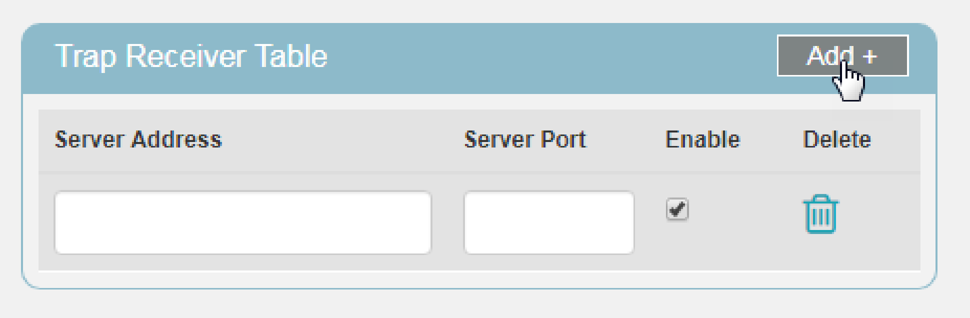
For SNMP, CPE serves as the server, users can use the tool such as MIB browser as the client to connect to CPE and do remove control.

- **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 an 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 SNMP Engine ID was last configured.
- **SNMP Engine Time (SNMPv3 only):** The number of seconds since the

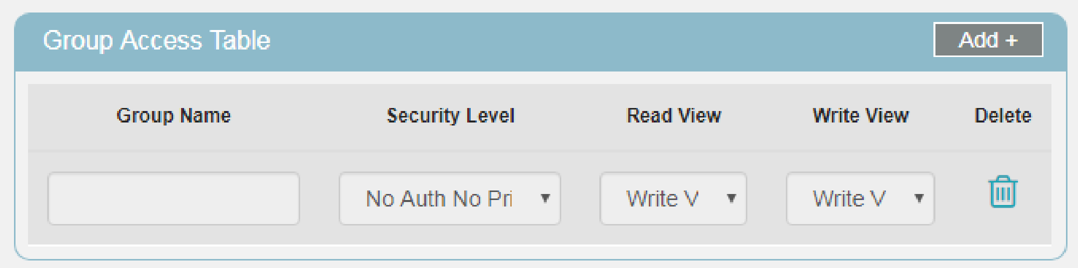
  SNMP Engine Boots counter was last incremented
- **Trap Receiver Table (SNMPv3 only):**



Trap Receiver Table

Server Address	Server Port	Enable	Delete
		☑	🗑

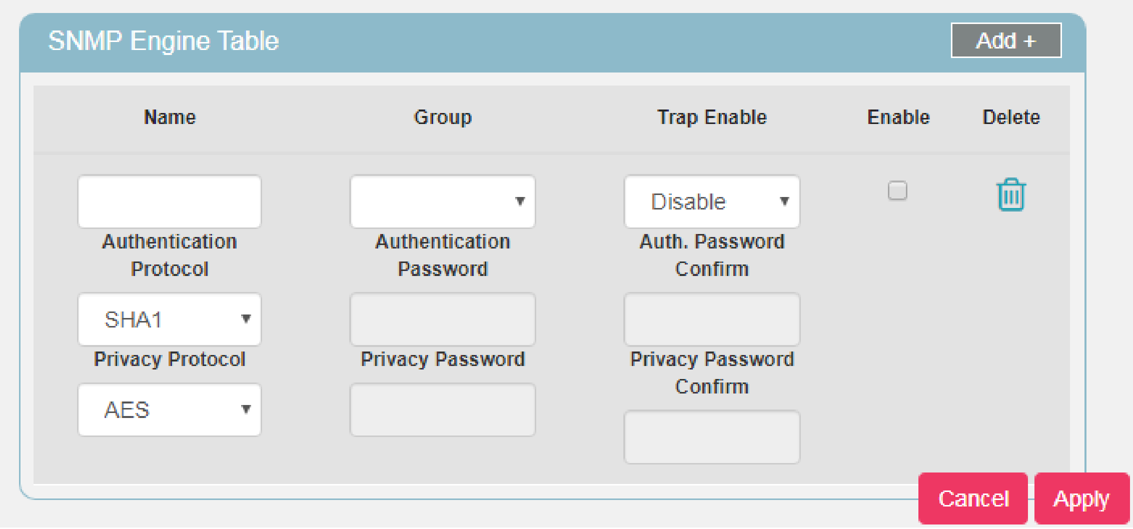
- **Group Access Table (SNMPv3 only):**



Group Access Table

Group Name	Security Level	Read View	Write View	Delete
	No Auth No Pri ▾	Write V ▾	Write V ▾	🗑

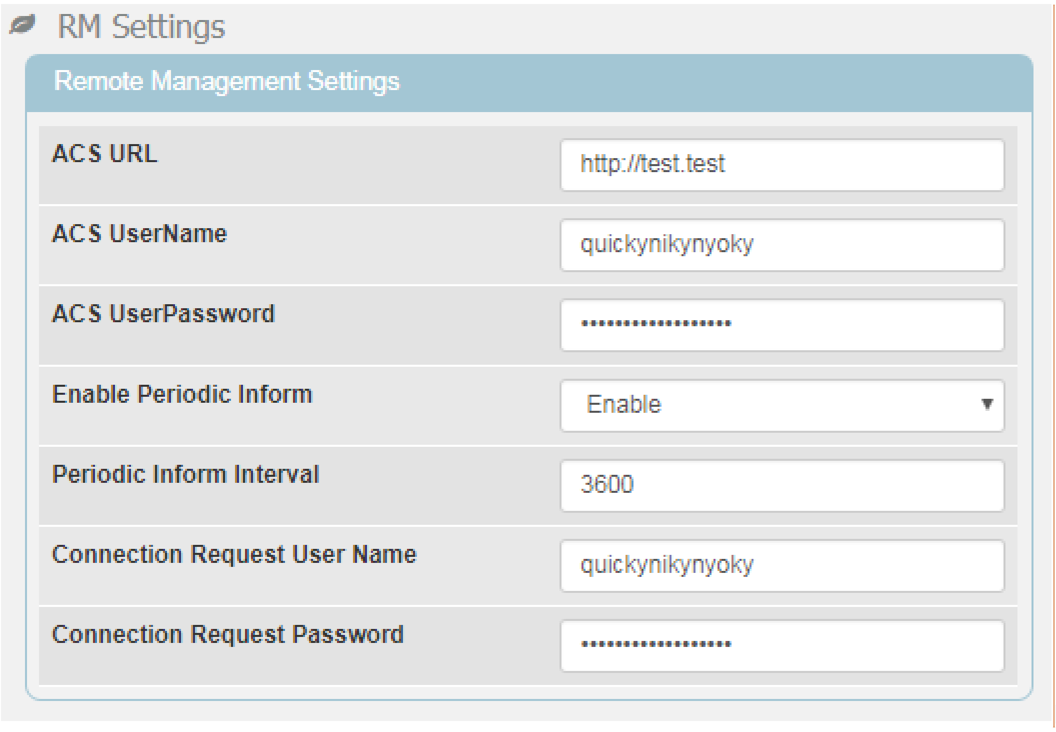
- **SNMP Engine Table (SNMPv3 only):**



SNMP Engine Table

Name	Group	Trap Enable	Enable	Delete
		Disable	□	🗑
Authentication Protocol	Authentication Password	Auth. Password Confirm		
SHA1				
Privacy Protocol	Privacy Password	Privacy Password Confirm		
AES				

RM Type-TR-069 (Technical Report 069)



RM Settings

Remote Management Settings

ACS URL	http://test.test
ACS UserName	quickynikynyoky
ACS UserPassword	••••••••••••••••••
Enable Periodic Inform	Enable ▾
Periodic Inform Interval	3600
Connection Request User Name	quickynikynyoky
Connection Request Password	••••••••••••••••••

[a9]

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.

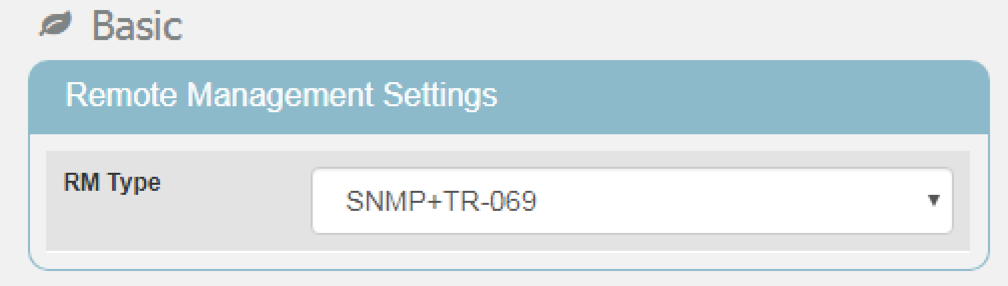
- **ACS URL:** The URL or IP address of the ACS.
- **ACS Username:** The username for authentication when CPE connects to ACS. (20 alphanumeric characters allowed)
- **ACS UserPassword:** The password for authentication when CPE connects to ACS. (20 alphanumeric characters allowed)
- **Enable Periodic 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-SNMP+TR-069**



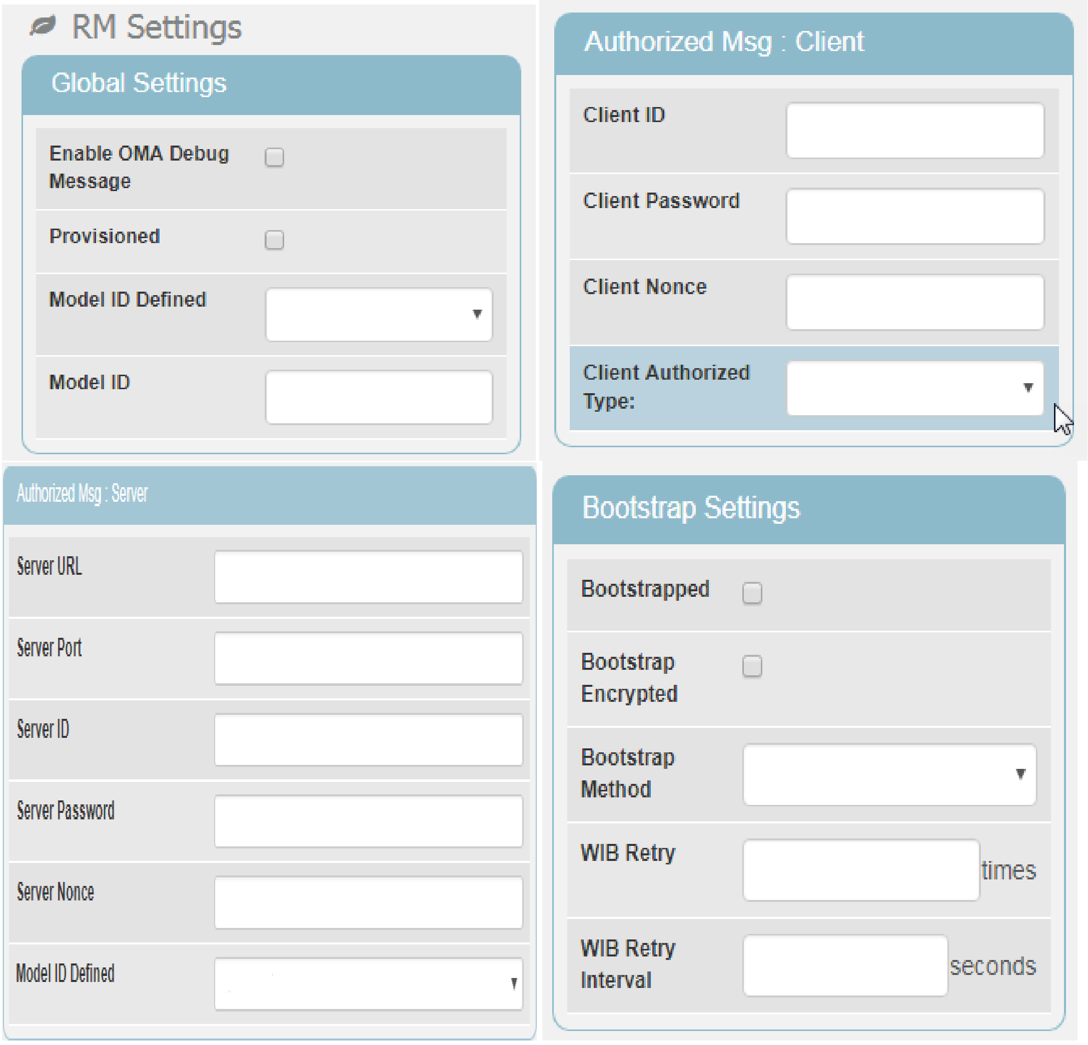
Basic

Remote Management Settings

RM Type: SNMP+TR-069 ▾

SNMP with TR-069: User need to set the configuration of RM type(both SNMP and TR-069) first.

- **RM Type-OMA-DM (Open Mobile Alliance Device Management)**



RM Settings

Global Settings

Enable OMA Debug Message □

Provisioned □

Model ID Defined ▾

Model ID

Authorized Msg : Client

Client ID

Client Password

Client Nonce

Client Authorized Type: ▾

Authorized Msg : Server

Server URL

Server Port

Server ID

Server Password

Server Nonce

Model ID Defined ▾

Bootstrap Settings

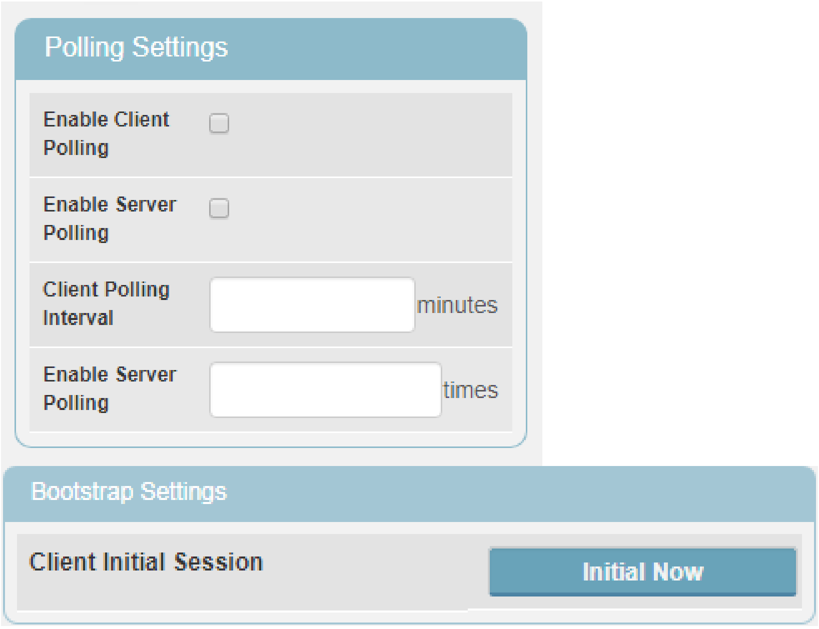
Bootstrapped □

Bootstrap Encrypted □

Bootstrap Method ▾

WIB Retry times

WIB Retry Interval seconds



Polling Settings

Enable Client Polling □

Enable Server Polling □

Client Polling Interval ▭ minutes

Enable Server Polling ▭ times

Bootstrap Settings

Client Initial Session

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**

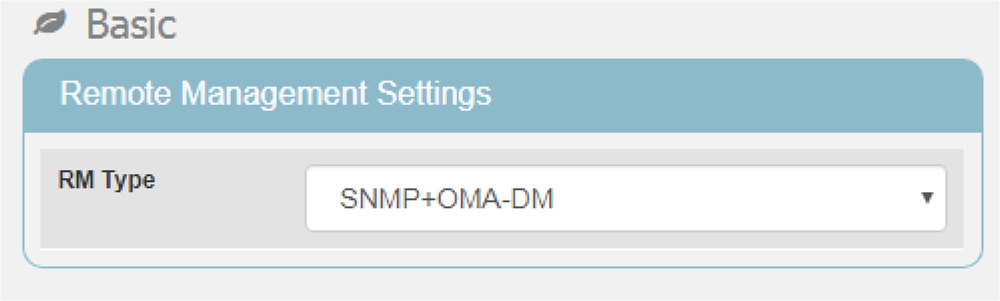
- **Enable Client Polling:** The client can be able to do polling for tasks from server.
- **Enable Server Polling:** The server is able to dispatch works to the client directly without queuing the tasks.
- **Client Polling Interval:** As titled.

- **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.

◆ **RM Type-SNMP+OMA-DM**



Basic

Remote Management Settings

RM Type: SNMP+OMA-DM

SNMP+OMA-DM: User need to set the configuration of RM types (both SNMP and OMA-DM) first.

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

11. Monitoring

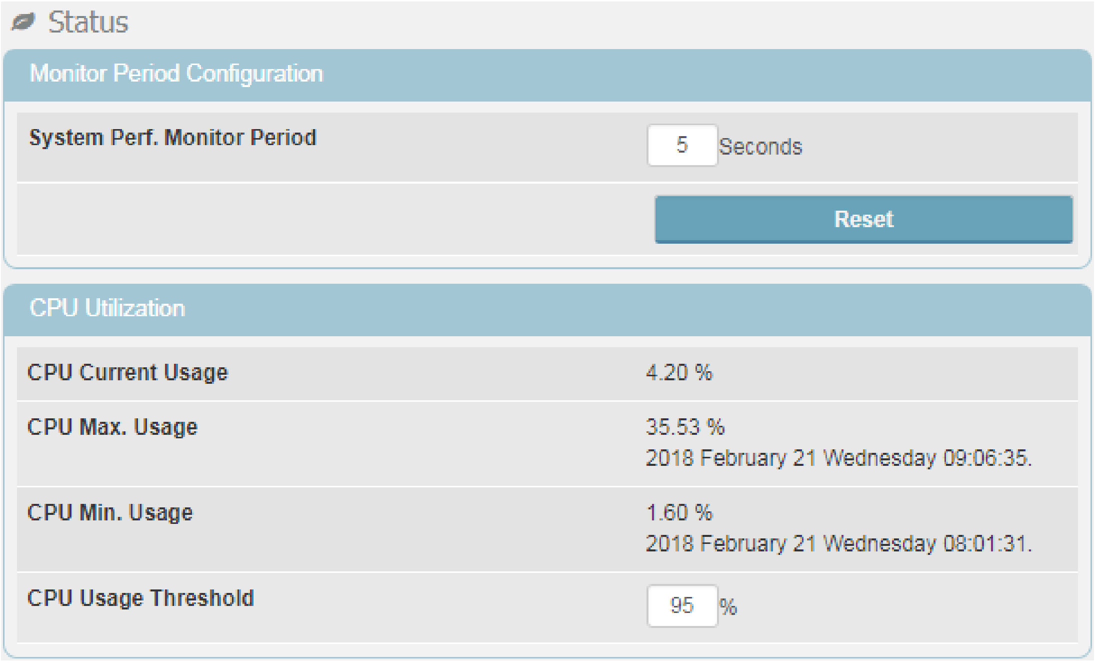
This section shows the device status such as CPU loading and memory usage and provides the interface to use the tools such as Iperf, ping and traceroute.

	Display in **Brief Summary Page**

- **Menu structure:**

Monitoring	Status
	Iperf
	Diagnostic Tools

Monitoring | Status



Monitor Period Configuration

System Perf. Monitor Period	5 Seconds

CPU Utilization

CPU Current Usage	4.20 %
CPU Max. Usage	35.53 % 2018 February 21 Wednesday 09:06:35.
CPU Min. Usage	1.60 % 2018 February 21 Wednesday 08:01:31.
CPU Usage Threshold	95 %

Monitor > Status

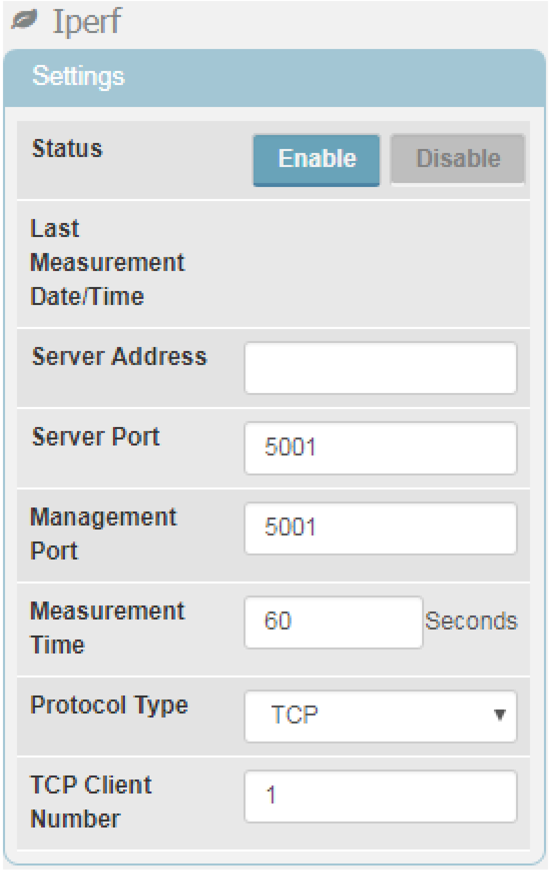
- **Monitor Period Configuration:** The period to record devices status. The recorded data is used to compute the CPU, memory and network statistics.
- **Reset button:** Reset CPU/Memory utilization and Uplink/Downlink data rate.
- **CPU Utilization:**
  - CPU Current Usage
  - CPU Max Usage
  - CPU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

  - Current Data rate

- **Downlink Data Rate:**
  - Current 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	Enable / Disable
Last Measurement Date/Time	
Server Address	
Server Port	5001
Management Port	5001
Measurement Time	60 Seconds
Protocol Type	TCP
TCP Client Number	1

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.

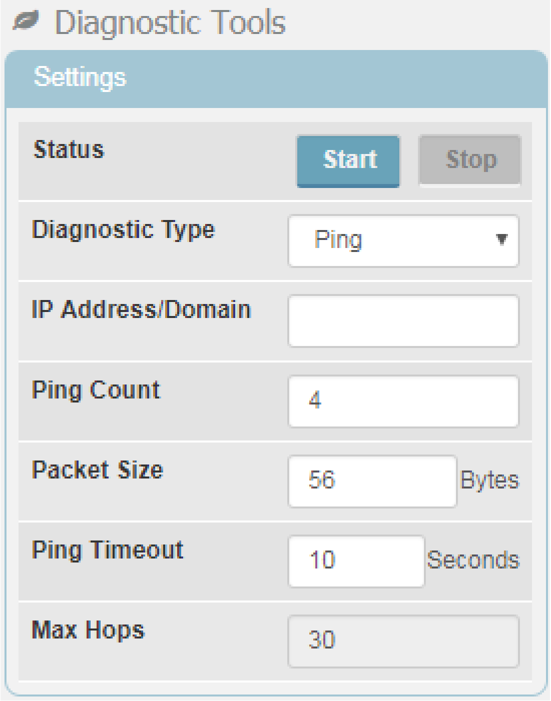
- **Settings**
  - **Status:** Enable/Disable Iperf.
  - **Last Measurement Date/Time:** As titled.
  - **Server Address:** As titled.
  - **Server Port:** As titled.
  - **Management Port:** To do bi-directional transmission, CPE opens “management port” to let the server transmit data to itself.
  - **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



Status	Start / Stop
Diagnostic Type	Ping
IP Address/Domain	
Ping Count	4
Packet Size	56 Bytes
Ping Timeout	10 Seconds
Max Hops	30

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.

12. About

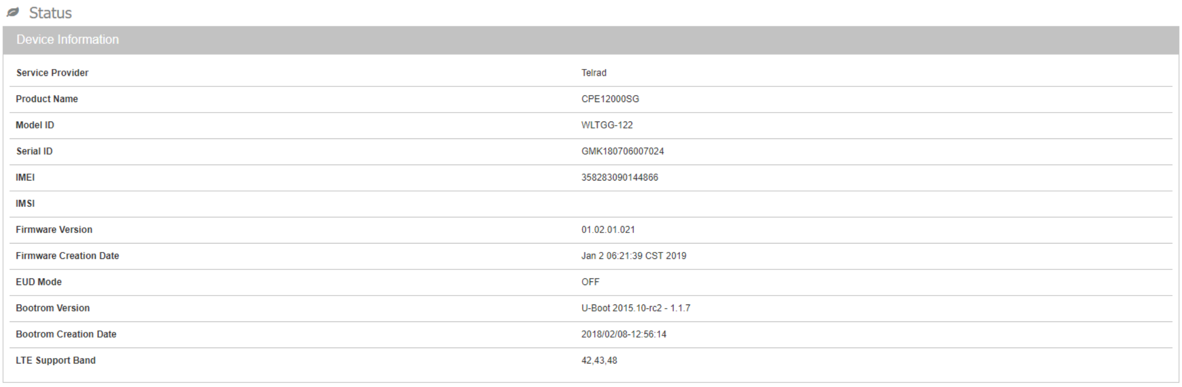
This section shows the device information such as Service Provider, Product Name, Model ID, Serial ID, IMEI, IMSI, Firmware version, Firmware Creation Date, Bootrom Version, Bootrom Creation Date and LTE Support Band.

	Display in **Brief Summary Page**

- **Menu structure:**

About	Status

About | Status



Status

Device Information	
Service Provider	Telrad
Product Name	CPE12000SG
Model ID	WLTGG-122
Serial ID	GMK180706007024
IMEI	358283090144866
IMSI	
Firmware Version	01.02.01.021
Firmware Creation Date	Jan 2 06:21:39 CST 2019
EUD Mode	OFF
Bootrom Version	U-Boot 2015.10-rc2 - 1.1.7
Bootrom Creation Date	2018/02/08-12:56:14
LTE Support Band	42,43,48

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