Telrad
We're on your wavelength.

Dual Mode CPE7000

USER MANUAL

Release Version: 01.01.02.009
August 2014
DN 151201

Telrad LTE/WiMAX DM ODU User Manual

Copyright

Notice

Telrad reserves the right to change specifications without prior notice.

While the information in this document has been compiled with great care, it may not be deemed an assurance of product characteristics. Telrad shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Telrad.

Contents

About this Guide

This document provides information and procedures on the installation and configuration of Telrad LTE/WiMAX Indoor CPE. You could utilize the information in this guide to set up your device.

Prerequisite Skills and Knowledge

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

- Hardware installers should have a working knowledge of basic electronics and mechanical assembly, and should understand related local building codes.
- Network administrators should have a solid understanding of software installation procedures for network operating system and troubleshooting knowledge. LTE/WiMAX 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.
	Additional information that may be helpful but not required.

bold	Menu commands, buttons and input fields are displayed in bold

Introduction

Product Overview

Introduction

Telrad's Dual Mode Outdoor CPE 7000 solution is a premium unit designed to suport a seamless migration from WiMAX to TD-LTE for operators and ISPs. The cost-effective, rugged outdoor CPE supports both Data and VoIP, offering the folowing benefits:

- Dual Mode WiMAX/LTE solution enabling transition from WiMAX to TD-LTE
- TD-LTE – 3GPP Release 9, UE Category 4
- Supports wired (LAN) and wireless (WiFi) Data ports and VoIP port
- High gain 15dBi embedded Antenna
- Easy installation saves time and money
- Device Management – Web and TR69
- IP67 environmental rating – fully ruggedized, suitable for the harshest outdoor deployment scenarios

The Dual Mode Outdoor CPE 7000 has two installation options using different indoor PoE accessories as follow:

1. **PoE Adapter** with one LAN/RJ45 and two VoIP/POTS interfaces (included in outdoor CPE PN)

2. **Residential Gateway** with WiFi AP, two LAN/RJ45 and one one VoIP/POTS interfaces (dedicated PN, should be purchased separately – when required)

Outdoor CPE 7000 - WiMAX & LTE Specifications

	LTE Interface	WiMAX Interface
Standard Compliance	3GPP Rev. 9, UE Cat 4	IEEE 802.16e-2005
Duplex Mode	TDD	TDD
Frequency Bands	40, 41, 42, 43	PN 725060: 2.3-2.4 and 2.5-2.7 GHz PN 735060: 3.4-3.6 and 3.6-3.8 GHz
Channel bandwidth (MHz)	5, 10, 20	5, 7, 10
Modulation	DL: MCS1 - MCS28 (QPSK, 16QAM, 64QAM) UL: MCS1 – MCS16 (QPSK, 16QAM)	DL: QPSK, 16QAM, 64QAM UL: QPSK, 16QAM, 64QAM
L1	MIMO TM1, TM2, TM3	MIMO A/B

L2 & L3	Multiple APN PLMN and Cell Selection	IP and Eth CS
Authentication	USIM and SIM function	EAP-TTLS, EAP-TLS
QoS	Non-GBR, GBR	BE, UGS, rtPS, ertPS, nrtPS
MTU Size	1,500 bytes	1,500 bytes

Outdoor CPE 7000 – Mechanical / Electrical / Physical Specifications

Dimensions (HxWxD)	260 x 250 x 80 mm / 10.2 x 9.8 x 3.1 in
Weight	1.2 Kg | 2.6 lbs
Physical Interface	LAN - 100 Base-T port Voice - RJ11/RJ14 SIM - 1.8V and 3.3V
Maximum Transmit Power	2.X GHz: 23 dBm 3.X GHz: 27dBm for WiMAX, 23 dBm for TD-LTE
Antenna	1TX/2RX, 15dBi
Power Source	PoE
Environmental	IP67 - withstands harsh weather and outdoor environments
Operating Temperature	-40° to 55 C | -40° to 131° F
Humidity	5% to 95% non-condensing
ESD Rating	+/-15KV
Power Consumption	6.7W
Regulatory Compliance	2.X GHz: • CE: 2.3-2.4 GHz and 2.5-2.7 GHz • FCC: 2.5-2.7 GHz • IC: 2.3-2.4 GHz 3.X GHz: • CE: 3.4-3.8 GHz • FCC: 3.65-3.7 GHz • IC: 3.475-3.7 GHz

PoE Adapter Specification

Power Source	100~240VAC
Output Power (PoE)	56V / 0.45A
User Interfaces	2xVoIP POTS ports + 1xLAN RJ45 Cable
To Outdoor CPE Interfaces	1xPoE (RJ45) port + 1xVoIP (RJ14) port

Residential Gateway Specifications

Power Source	56VDC using the supplied PSU adapter
Output Power (WAN - PoE)	56VDC / 0.45A
User Interfaces	Embedded WiFi AP + 1xVoIP POTS (RJ11) ports + 2xLAN RJ45 Cable
To Outdoor CPE Interfaces	1xPoE (RJ45) port
Embedded WiFi AP	2.4 GHz (2x2 MIMO) with IEEE 802.11 b/g/n fully compliant
LED Indicators	Status indicators about: Power / System / LTE signal Strength / LAN1 & LAN2 / WAN / WLAN / WPS / Phone
Environmental	Indoor
Operating Temperature	0° to 40 C
Humidity	0% to 95% non-condensing
Regulatory Specification	Radio-WiFi EN 300 328 (V1.8.1) Safety EN 60950-1 EMC EN 301 489-1/-4/-17/-24
Dimensions (HxWxD)	173 x 128 x 34 mm

Product Package

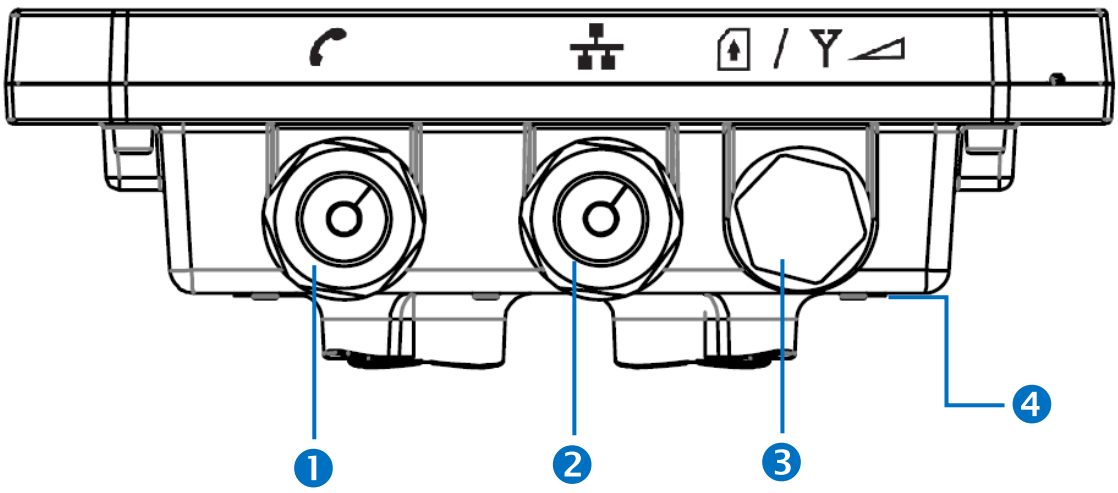
	Item	Qty
1	LTE/WiMAX Outdoor CPE	1
2	Quick Installation Guide	1
3	Power Adapter	1
4	Pole installation kit	1

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

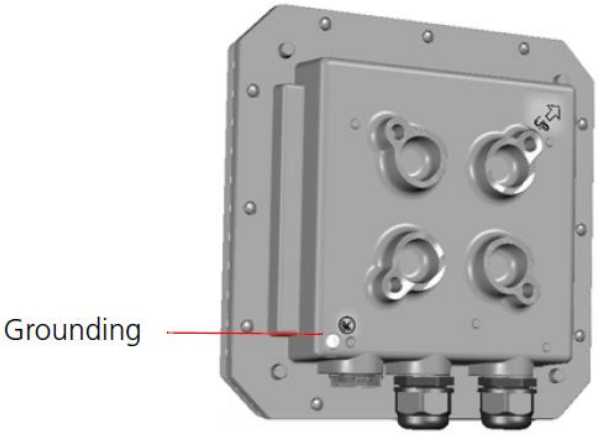
Connectors

The CPE7000 Outdoor has the following connectors (from left to right):

1. One RJ-14 connector for connecting to a telephone line.
2. One RJ-45 connector for connecting to the PoE adaptor.
3. LED indicator inside and SIM card slot for inserting SIM card.
4. A grounding screw on the rear panel.



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



LED Indicators

LED name	Location	Color	LED Behavior	Status Indication
LED List				
MAIN power		**Blue**	**ON**	Power On
			OFF	Power Off
Ethernet Status		**Yellow**	**Steady ON**	Ethernet connected
			Blinking	Data transmission
			OFF	No Ethernet action
SIM status		**Green**	**Steady ON**	SIM Detected
			Blinking when On-hook	PUK / PIN Code
			OFF	No SIM Detected
4G Status LED : Link Status			When CPE is power on, each LED indicates each link status	
4G- 1		**Red**	**Steady ON**	CINR < 8dB
4G- 2		**Red/ Yellow**	**Steady ON**	8dB < CINR < 24dB
4G- 3		**Red/ Yellow/ Green**	**Steady ON**	24dB <= CINR

Installation

Before installing the WiMAX / LTE outdoor CPE, verify that you have all the items listed in the package checklist. If any of the items are missing or damaged, contact your service provider.

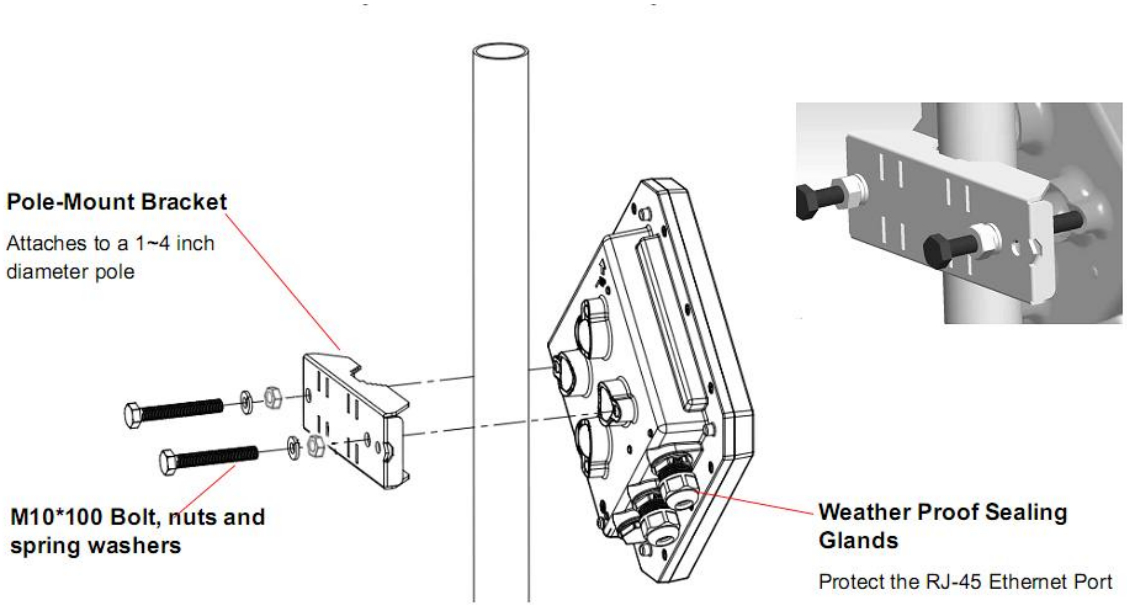
	Only experienced installation professionals who are familiar with local building and safety codes and, where applicable, are licensed by the appropriate government regulatory authorities should install outdoor units and antennas.

Installing WiMAX/LTE Outdoor CPE

- **Selecting a Location:** WiMAX / LTE Outdoor CPE should be pole-mounted outdoors and aligned so its antenna faces the nearest LTE eNodeB / WiMAX BS. When selecting a suitable location for the unit, consider these guidelines:
  - Place WiMAX / LTE Outdoor CPE as high as possible to achieve the best possible link quality.
  - Place the WiMAX / LTE Outdoor CPE away from power and telephone lines.
  - Avoid placing WiMAX / LTE Outdoor CPE close to any metallic reflective surfaces.
  - Be sure to ground WiMAX / 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 WiMAX / LTE Outdoor CPE on a 1-4” pole using the supplied kit, or the optional tilt accessory.

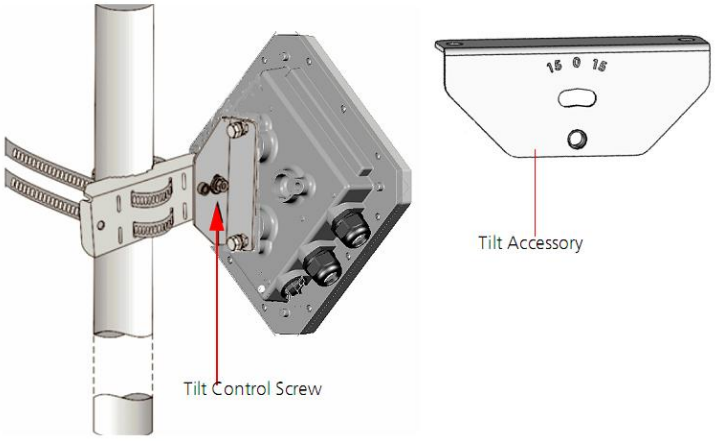
- **Using the clamp**

1. Thread the M10*100mm bolt through a spring washer, flat washer and the bracket holes.
2. With the connector facing downward, attach the WiMAX / 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.

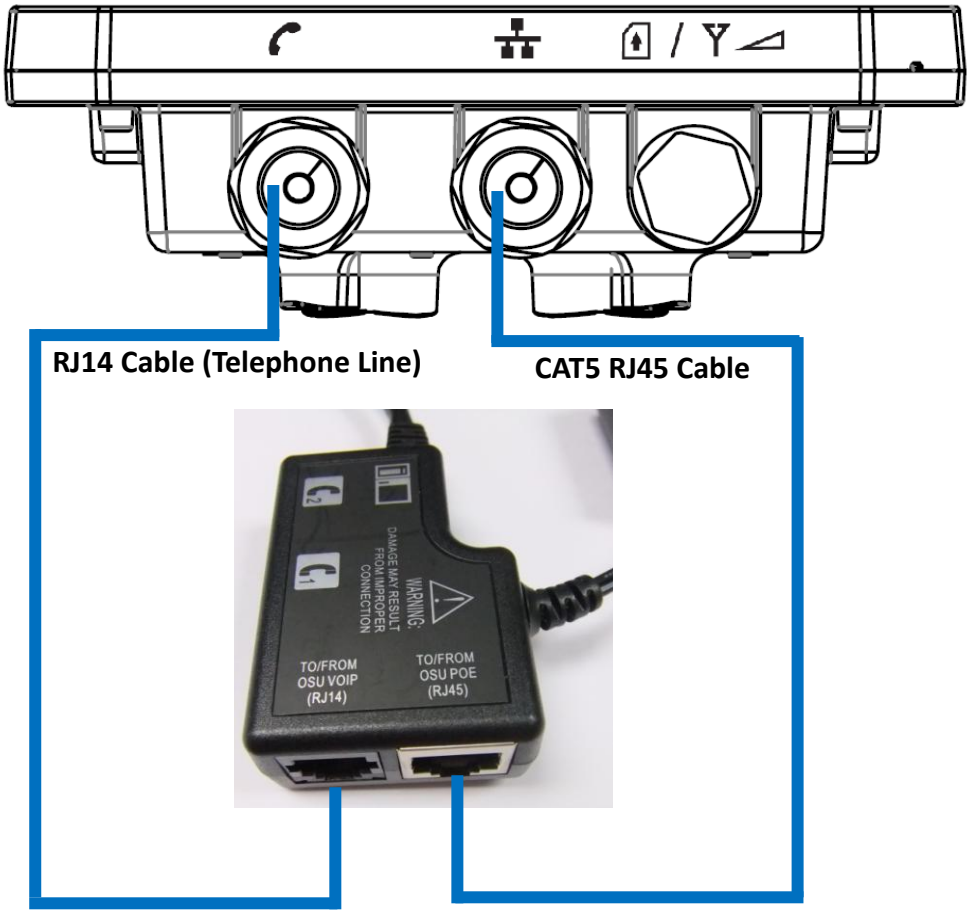


- **Using the tilt accessory (optional)**

1. Attach the tilt accessory to WiMAX / LTE Outdoor CPE using two pairs of flat washers, spring washers and nuts supplied in the tilt kit.
2. Mount the tilt accessory on a 1-4” pole using two 9/16” metal bands.
3. Slightly release the tilt control screw, tilt LTE Outdoor CPE downward/upward as required, and re-tighten the screw.



- **Connecting the Cables**

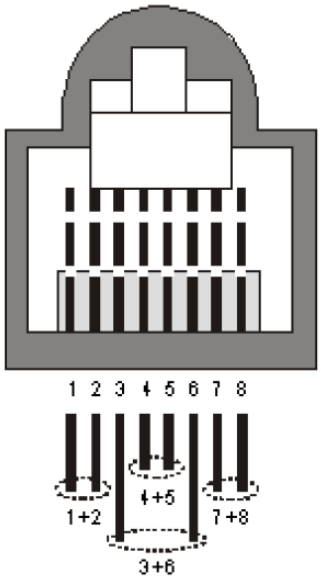


- **Outdoor Connection:** Connect a grounding cable between the Ground terminal of the WiMAX / LTE outdoor CPE and a good ground connection.
- **Preparing and connecting the cable:** Use only UTP-FTP 4x2x24AWG CAT. 5E outdoor cable from an approved manufacturer. The cable provides pin-to-pin connection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

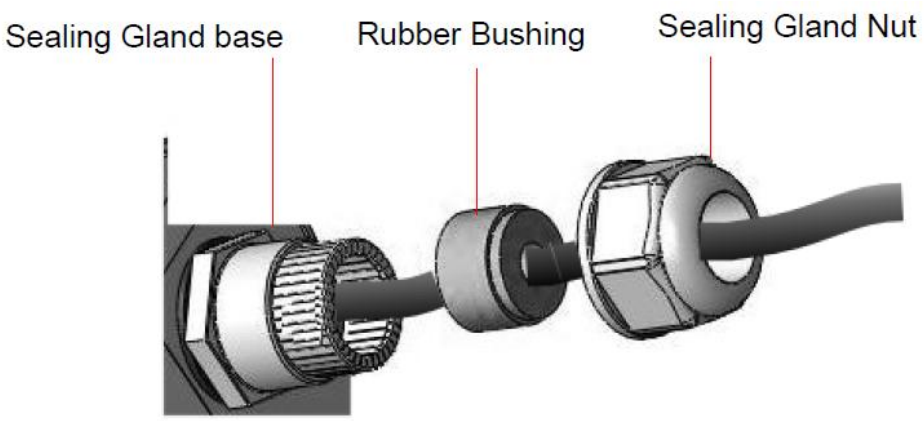
The following figure shows the required wire pair connections. The color codes used in standard cables supplied by the manufacturer are as listed in the following table.

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



2. Connect the cable

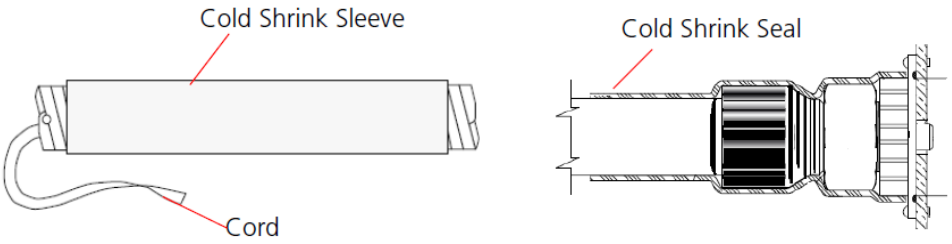
- Remove the sealing cable gland plug from the gland nut.
- Open the sealing gland nut and remove it. Don not disassembles the gland base from the bracket.
- Insert the cable into the sealing gland base and connect it to the RJ-45 connector at the bottom of the CPE. Make sure the connector is completely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



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

3. Seal the connector

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



- Pull the cord slowly to shrink the sleeve.

- **Indoor Connection**

1. It is assumed that the RJ-45 and telephone line cables are already connected to the WiMAX / LTE outdoor CPE. Assemble an RJ-45 connector with a protective cover on the other end of the WiMAX / LTE outdoor CPE cable.
2. Connect the other end of the cable to the PoE adaptor which labeled **"TO/FROM OSU POE (RJ45)"**.
3. Connect telephone line cable from WiMAX / LTE outdoor CPE to PoE adaptor which labeled "**TO/FROM OSU VOIP (RJ14)**"
4. Use a telephone cable to connect a phone to RJ-11 port on PoE adaptor with a telephone illustration.
5. Connect RJ45 cable from PoE adaptor to a PC/NB/Hub/Switch.

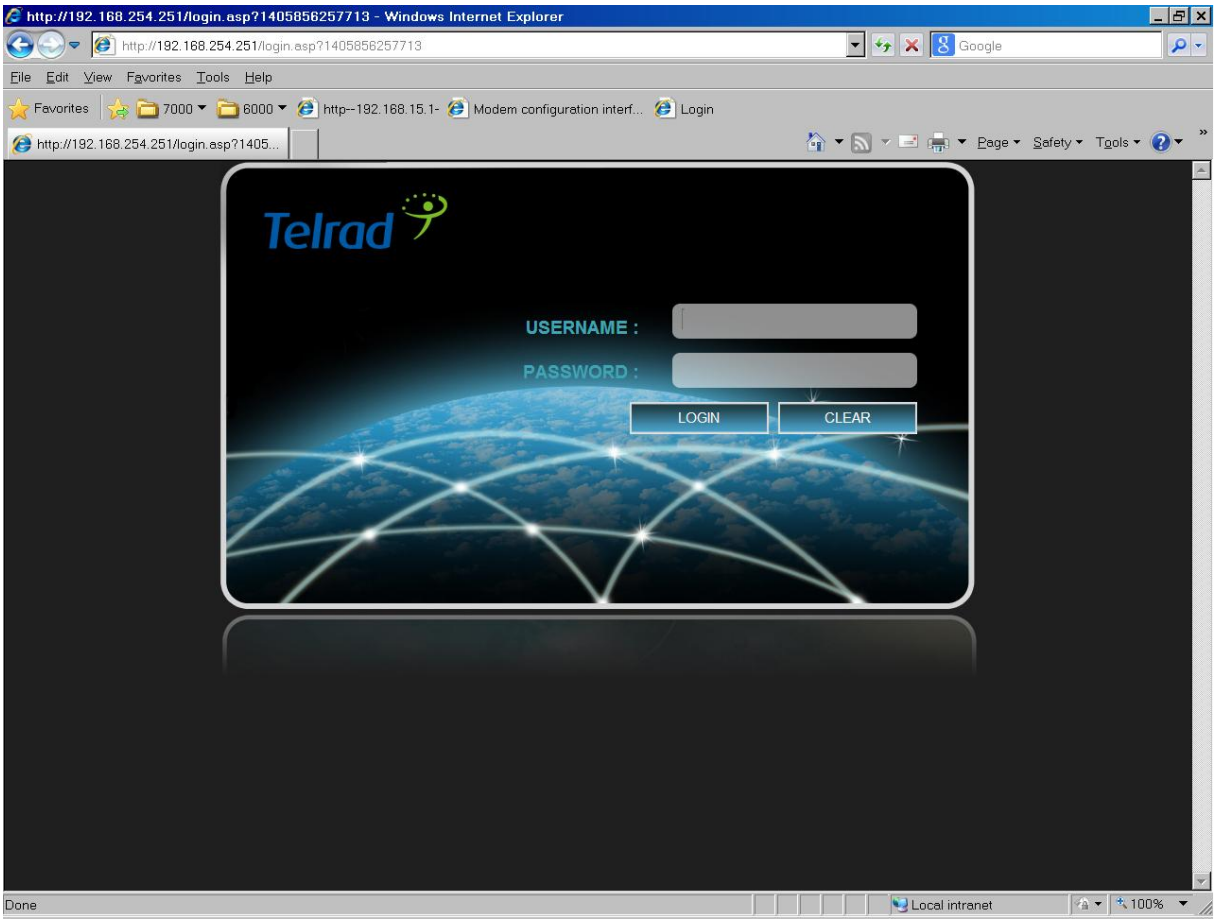
!	Use **ONLY** the PoE adaptor which supplied with the ODU. Otherwise, WiMAX / LTE outdoor CPE may be damaged.

Web Interface

Login to Web-GUI

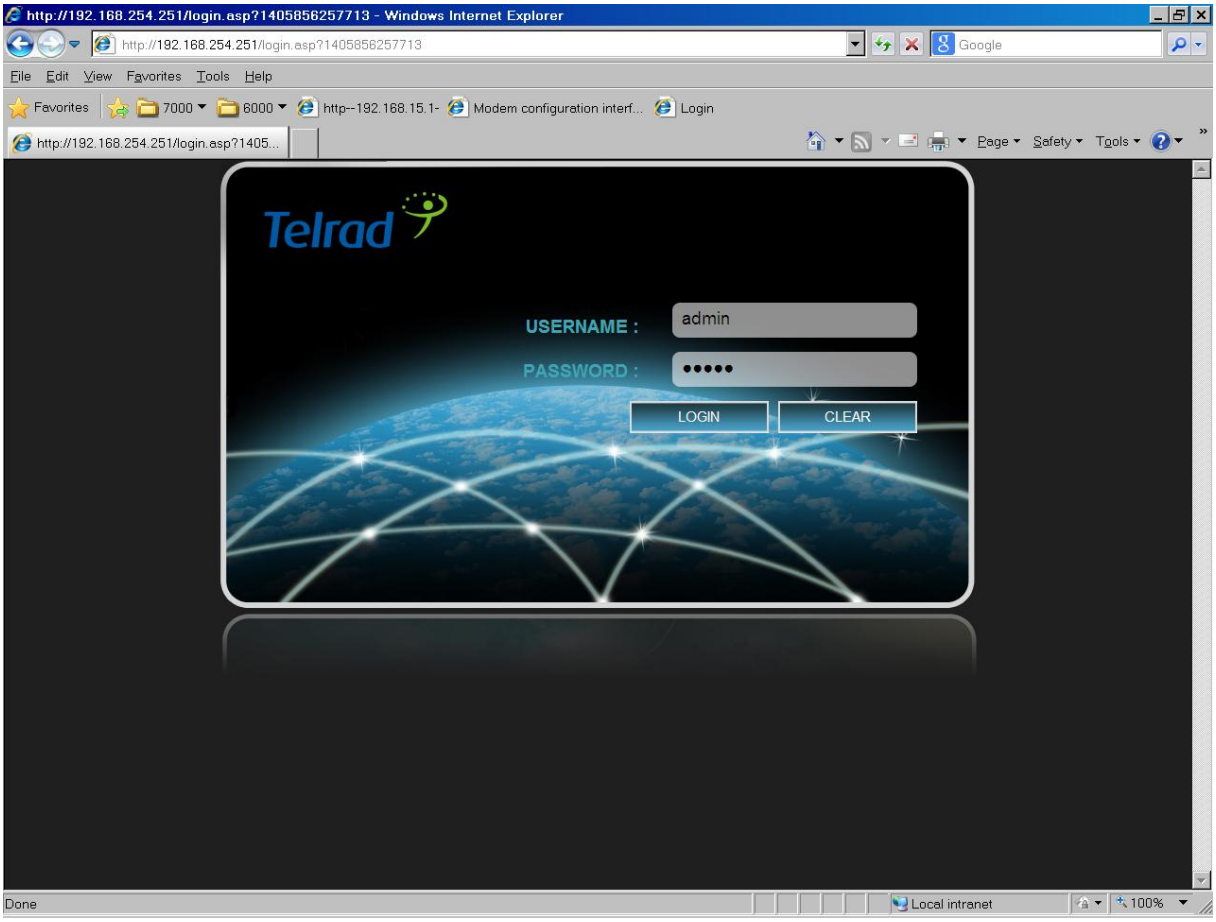
User's devices are assumed to be connected to CPE LAN side. Please follow the steps below to configure your device through WEB interface:

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



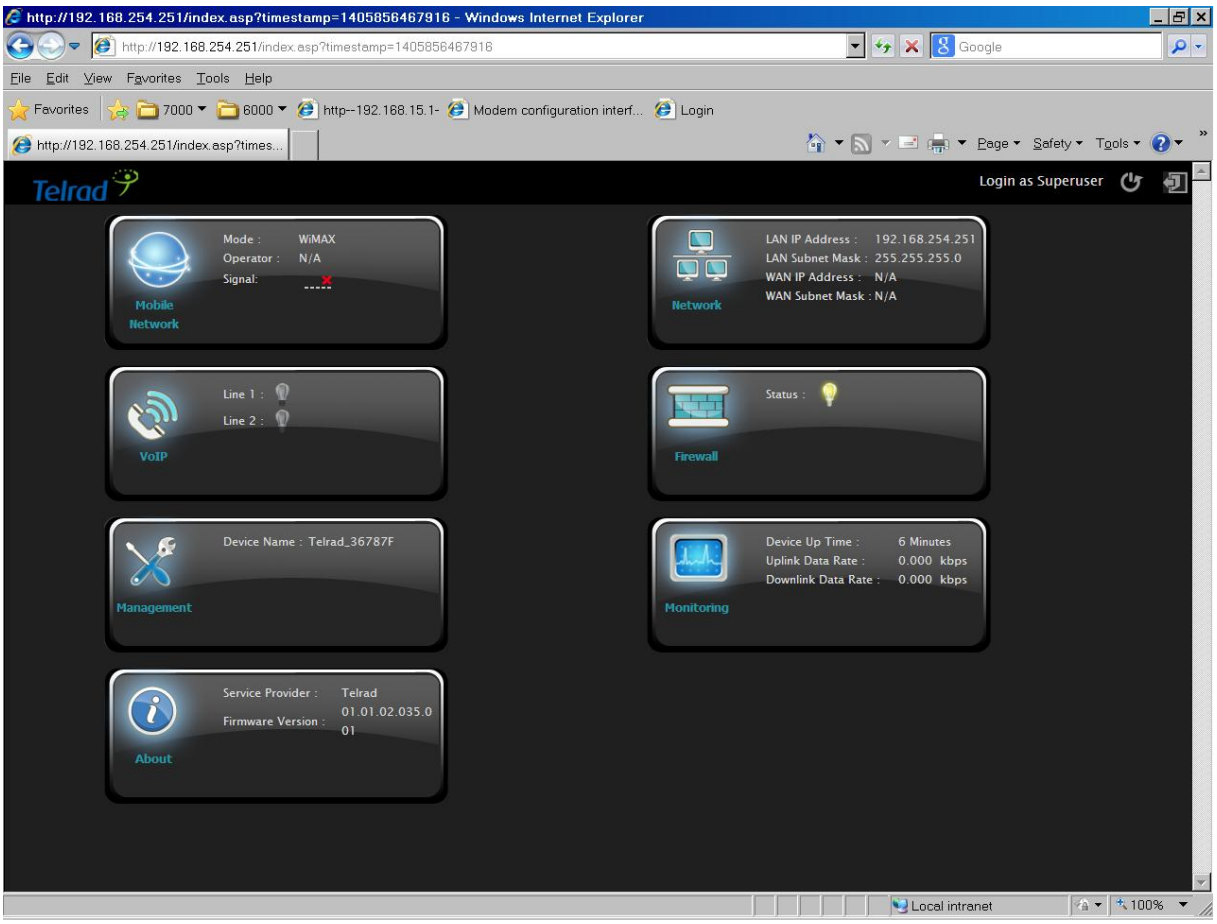
Web browser

Step2: Enter USERNAME/PASSWORD to access the web management interface. The default USERNAME/PASSWORD of superuser is **operator / wimax.**



Web management interface

Step3: After successful login, “Brief Summary Page” is displayed. 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.



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.

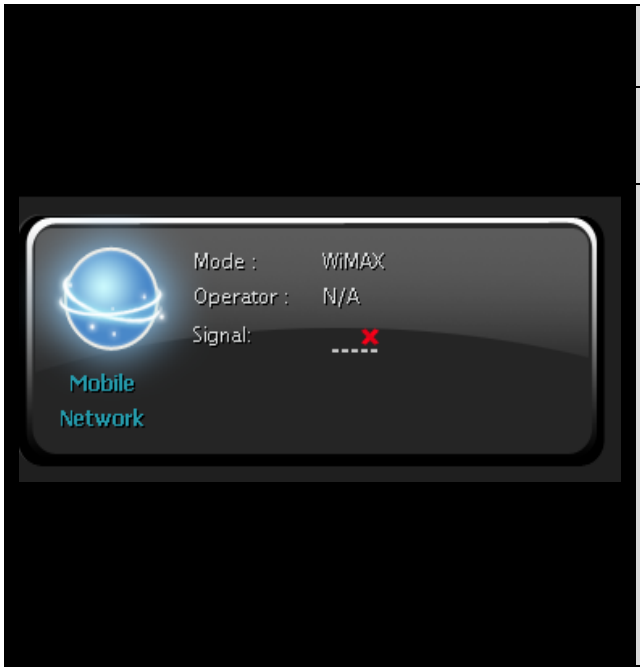
After login, users can see a "**Brief Summary Page**" about all functions of LTE/WiMAX outdoor CPE, each block is a link to "**Detailed Configuration Page**".

(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.

GUI Interface

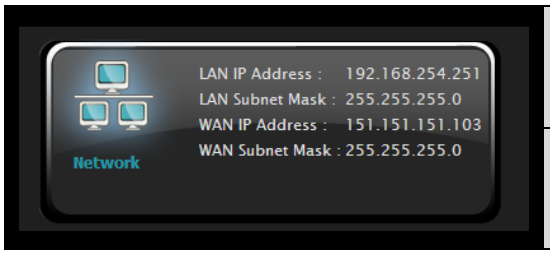
	Logo of Service Provider.
	Login Identity, could be **Superuser** or **Enduser**
	Button of **REBOOT**
	Button of **LOGOUT**



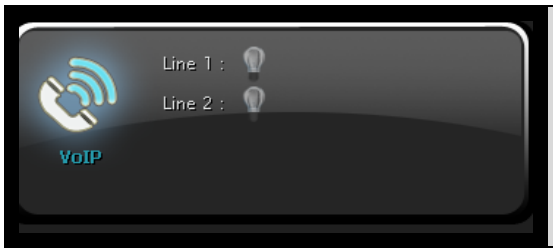
Mode:	**LTE** or **WiMAX**
Operator:	Either **APN Name** (LTE mode) or **BSID** (WiMAX mode)
Signal:	CINR <=0 ==>0 bar 0<CINR<8 ==>1 bar 8<=CINR<12 ==>2 bars 12<=CINR<16 ==>3 bars 16<=CINR<24 ==>4 bars CINR>=24 ==>5 bars (Disconnect, no signal)

!	Mode: WiMAX Only an example, the real mode depends on the local service.

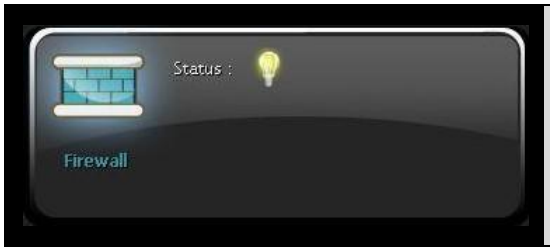
!	Signal: Only an example, the real signal depends on local connection environment.



LAN IP:	LAN IP of CPE
WAN IP:	WAN IP of CPE

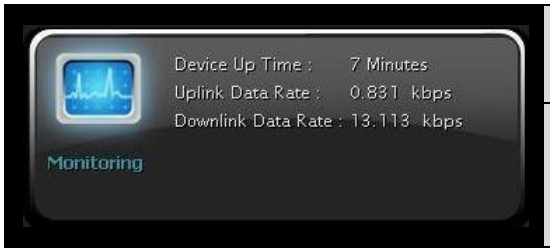


Line 1: Line 2:	means VoIP is registered means VoIP is not registered



Status:	means Firewall is enabled means Firewall is disabled.

Device Name:	Name of LTE/WiMAX outdoor CPE in LAN side



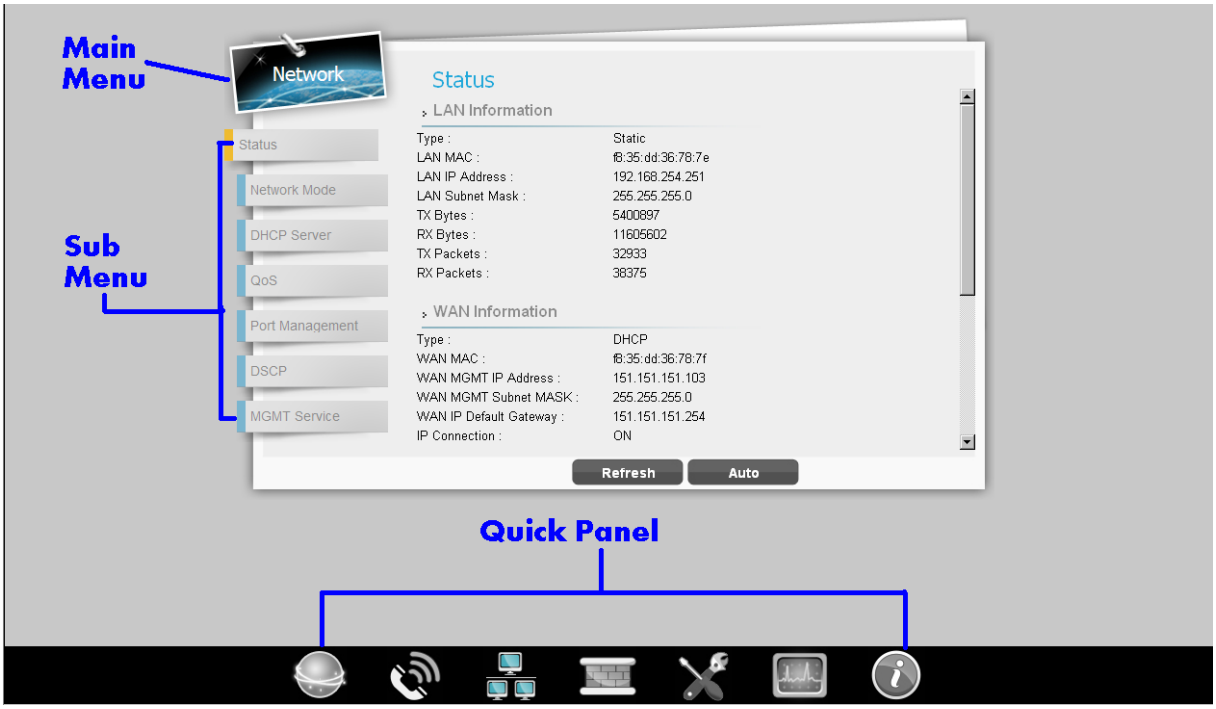
Device Up Time:	The uptime from the boot up of LTE/WiMAX outdoor CPE
Uplink / Downlink Data Rate:	Uplink / Downlink Rate of LTE/WiMAX outdoor CPE

Service Provider:	The service provider of this LTE/WiMAX outdoor CPE.
Firmware Version:	Firmware Version of this LTE/WiMAX outdoor CPE.

!	Firmware Version: **01.01.02.028** is just an example here; the real firmware version is based on the firmware provided by Telrad.

Detailed Configuration Page

After clicking any block in “Brief Summary Page”, the webpage would be switched to the “Detailed Configuration Page”. (e.g. “Network”)



Detailed Configuration Page

Main Menu	Show the current Main Menu
Sub Menu	Clickable, can jump to another Sub Menu under the same Main Menu
Quick Panel	Each icon in **Quick Panel** represents a “Main Menu”, when users click it, a list of “Sub Menu” will be popped up. By using **Quick Panel**, users can quickly jump to the desired Sub Menu under other Main Menu. (For example, to perform “Restore Default”, Click “**Management**” icon , then click “**Restore Default**”)

Pop up Sub Menu in Quick Panel

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:

Mobile Network	Status		
	Technology	Basic	
		LTE	Cell Selection
			PIN
			Default PDN
			Multiple PDN
			PLMN Selection
		WiMAX	Scanner
			Authentication
VoIP	Status		
	Basic		
	Advanced		
Network	Status		
	Network Mode		
	DHCP Server (Not available in **Bridge** Mode)		
	QoS (Not available in **Bridge** Mode)		
	Routing (Available in **Router** Mode)		
	Port Forwarding (Available in **NAT**、**Tunnel** Mode)		

	Port Trigger (Available in **NAT**、**Tunnel** Mode)
	DSCP
	Vlan (only in ETH-CS)
	MGMT Service
Firewall	Basic
	L3 MGMT Filter
	L3 DATA filter
	L2 Filter
	Access Restriction
Management	Account
	Language
	Device Setting
	Restore Default
	Software
	RM Settings
Monitoring	Status
	Iperf
	Diagnostic Tools
About	Status

Reference Manual

Mobile Network

	Display in **Brief Summary Page**
	Display in "**Quick Panel**" of **Detailed Configuration Page**

- In "**Mobile Network**" main menu, the user can see the status like RSSI and CINR which are link quality and strength.
- All the setting about LTE and WiMAX are placed here such as WIMAX frequency and LTE Earfcn and PIN code
- Menu Structure:

<table>
<tr><td rowspan="10">Mobile Network</td><td colspan="3">Status</td></tr>
<tr><td rowspan="9">Technology</td><td colspan="2">Basic</td></tr>
<tr><td rowspan="5">LTE</td><td>Cell Selection</td></tr>
<tr><td>PIN</td></tr>
<tr><td>Default PDN</td></tr>
<tr><td>Multiple PDN</td></tr>
<tr><td>PLMN Selection</td></tr>
<tr><td rowspan="3">WiMAX</td><td>Scanner</td></tr>
<tr><td>Authentication</td></tr>
<tr><td>Advanced</td></tr>
</table>

Mobile Network | Status

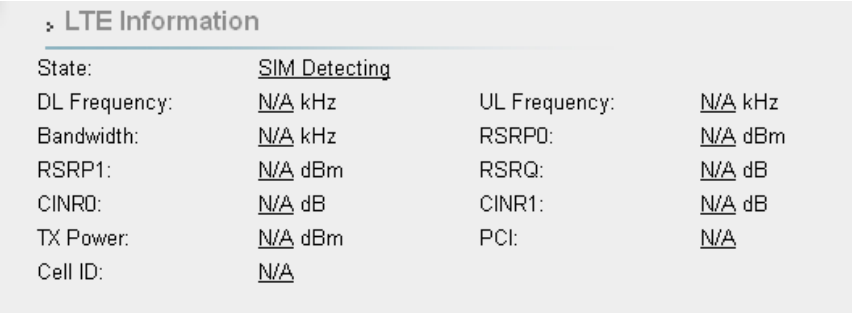
Mobile Netwrok > Status

- Status page is divided into two parts. The first one is “General Information”, the second one is “LTE Information” or “WiMAX Information”.

  The content of the second part depends on the technology used then.

- **General Information** (both available in LTE or WiMAX mode)
  - **State:** Possible states are connecting and connected.
  - **Network Operator:** When CPE is in LTE mode, it shows APN name; when CPE is in WiMAX mode, it shows BSID.
  - **Technology:** LTE or WiMAX.
  - **Connection Time:** the accumulated time after the state is connected.

- **LTE Information** (Only in LTE mode)



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.
- **Bandwidth:** As titled.
- **RSRP1:** Reference signal receiving power of path 1.
- **CINR0:** The quality of the signal of path 0.
- **Tx Power:** Transmission power.
- **Cell ID:** Cell Identity, a part of cell global identification.
- **UL Frequency:** Uplink frequency.
- **RSRP0:** Reference Signal Receiving Power Path 0.
- **RSRQ:** Reference signal receive quality.
- **CINR1:** The quality of the signal of path 1.
- **PCI:** Physical cell identity.

- **WiMAX Information** (Only in WiMAX mode)

WiMAX Information

  - **State**
    - **INIT:** Detect WiMAX module.
    - **READY:** Has detected WiMAX module.
    - **SCAN:** Scan available BS.
    - **NETWORK_ENTRY:** Target a base station but not connected.
    - **OPERATOINAL:** Connected to the BS.
  - **Security:** Possible states are unauthorized and authorized. This depends on whether the authentication is used or not.
  - **Center Frequency:** As titled.
  - **RSSI:** Received signal strength indication.
  - **CINR Reuse1:** A kind of signal quality.
  - **Tx Power:** Transmission power.
  - **BSID:** As titled.
  - **Bandwidth:** As titled.
  - **CINR: as titled.** A kind of signal quality.
  - **CINR Reuse3:** A kind of signal quality.
  - **Max Tx Power:** As titled.

- **WiMAX TX** (Only in WiMAX mode)

WiMAX TX

- **Data Rate:** Transmission data rate.
- **Packets:** Number of transmitted packets.
- **TX Bytes:** Number of transmitted bytes.
- **UL MCS:** Uplink Modulation and coding sequence. This includes qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-1/2, qam64-ctc-2/3, qam64-ctc-3/4 and qam64-ctc-5/6.

- **WiMAX RX** (Only in WiMAX mode)

WiMAX RX

- **Data Rate:** Receiving data rate.
- **Packets:** Number of received packets.
- **MIMO Mode:** Matrix B is for increasing the data rate whereas Matrix A is for increasing the coverage area or distance.
- **RX Bytes:** Number of received bytes.
- **DL MCS:** Downlink modulation and coding sequence. This includes qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-1/2, qam64-ctc-2/3, qam64-ctc-3/4 and qam64-ctc-5/6.

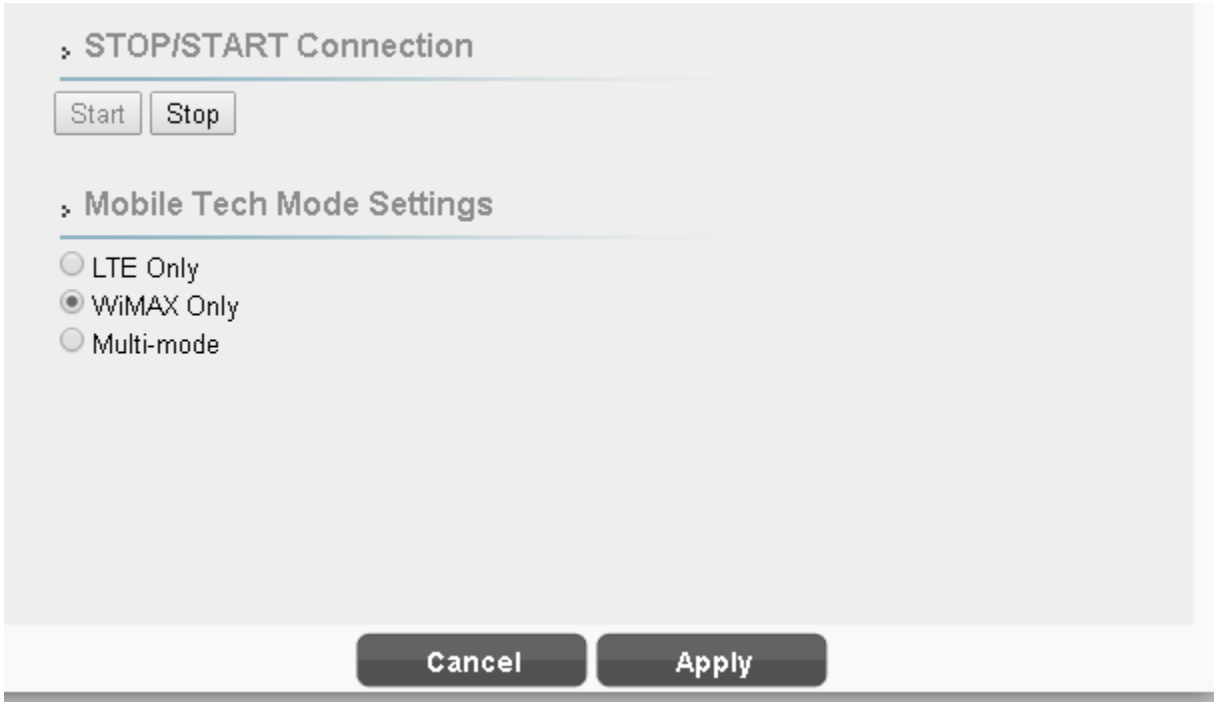
- **Service Flow** (Only in WiMAX mode)**:** This Field shows detailed information about "Service Flow" dispatched by WiMAX base station.

Service Flow

SFID	CID	BID	Type	State	Direction	Scheduling	MaxRate	ARQ	HARQ	Rules
0	120	120	basic	active	bidirectional	best-effort	0	no	no	0
0	632	120	primary	active	bidirectional	best-effort	0	no	no	0
1009	4188	120	data	active	downlink	best-effort	256000	no	yes	1
1010	4189	120	data	active	uplink	best-effort	256000	no	no	1
1011	4772	120	data	active	downlink	best-effort	20000000	no	yes	1
1012	4773	120	data	active	uplink	best-effort	10000000	no	no	1

Service Flow Table

Mobile Network | Technology | Basic



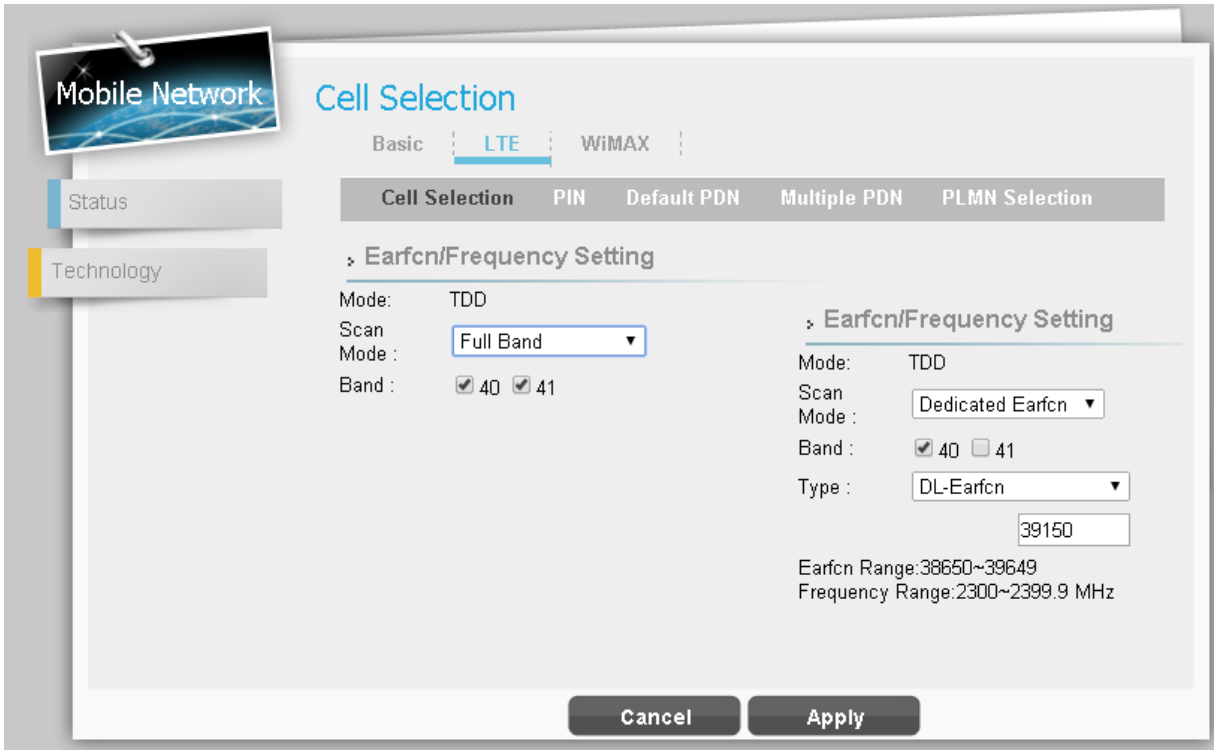
Mobile Network > Technology > Basic

- **STOP/START Mobile Network:** Click button "**Start**"/"**Stop**" to start/terminate the WAN connection.
- **Mobile Tech Mode Settings:** This option chooses the WAN connection mode of CPE.
  - If you choose **LTE Only** or **WiMAX Only**, CPE will only seek LTE or WiMAX service.

    If you choose **Multi-mode**, Both LTE and WiMAX service would be searched but one at a time. The user can choose **LTE First** or **WiMAX First**, CPE would interchangeably search LTE and WiMAX service but search the one you specify first. The searching process would repeat until CPE is connected to eNodeB or BS.

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.

Mobile Network | Technology | LTE | Cell Selection



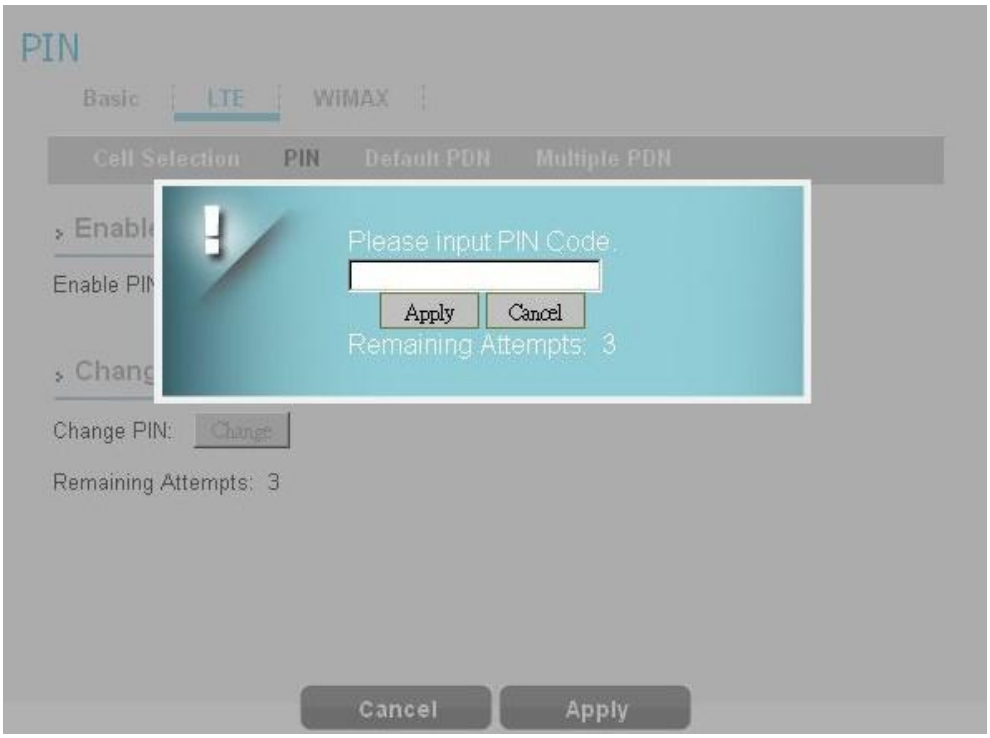
Mobile Network > Technology > LTE > Cell Selection

- **Mode:** TDD only.
- **Scan Mode:** Full Band or Dedicated Earfcn. Searching full band would take much longer time than Dedicated Earfcn.
- **Band:** (40 and / or 41), (42 and / or 43) depend on CPE band.

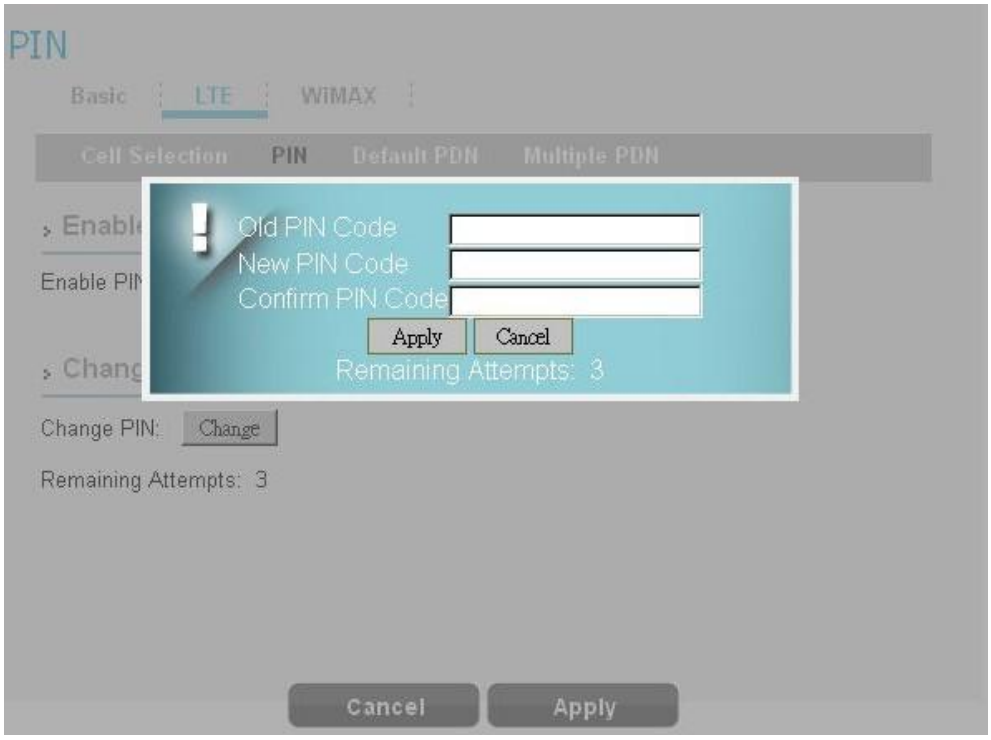
➢ **Type: DL-Earfcn or Dl-Frequency**

Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.
!	**LTE Band 40, 41 and Earfcn/Frequency Range** are just an example. Real number is determined by the user's requirement.

Mobile Network | Technology | LTE | PIN



Mobile Network > Technology > LTE > PIN > Enable PIN



Mobile Network > Technology > LTE > PIN > Change PIN

- **Enable PIN:** Enable/Disable PIN code protection.
- **Change PIN:** Change the PIN code.

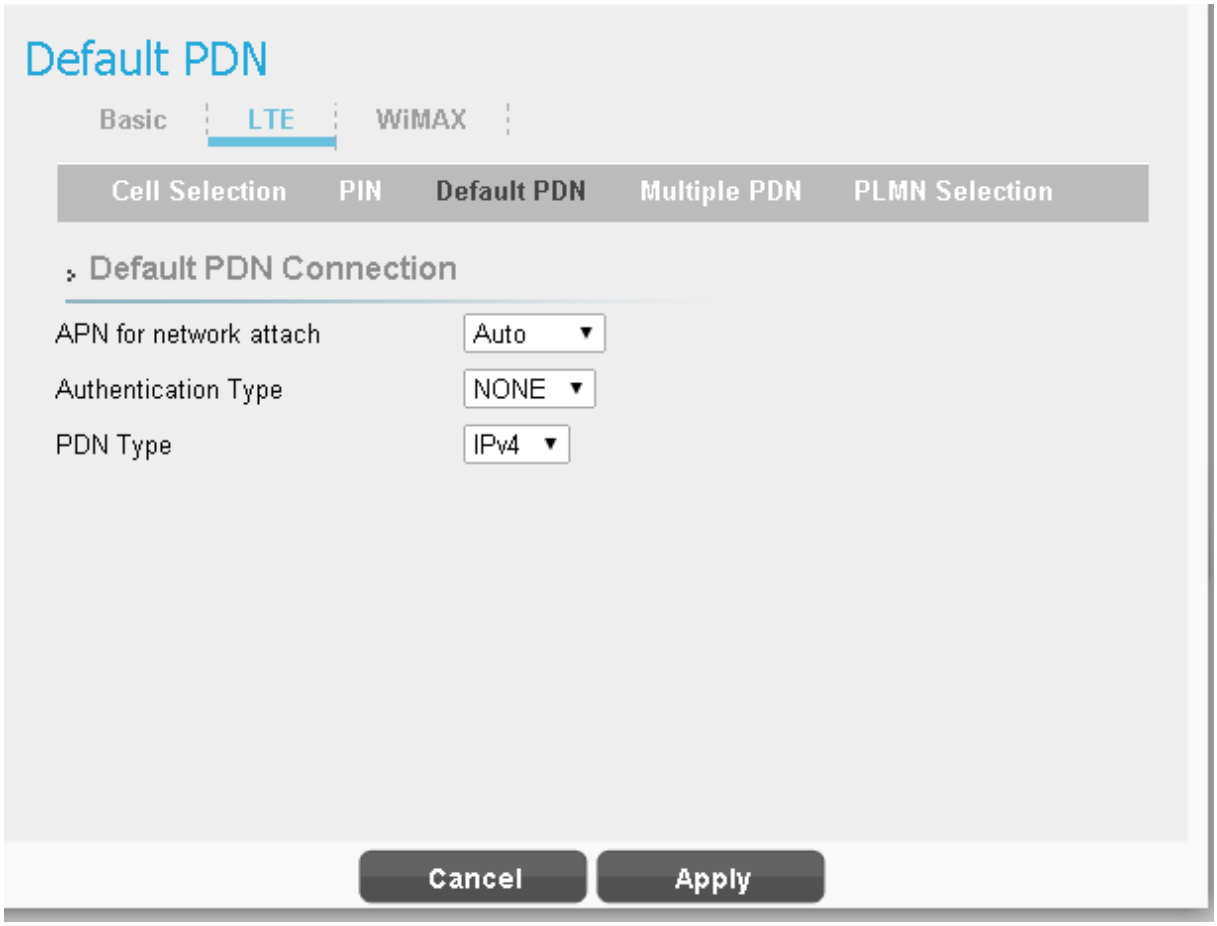
Cancel button	Reset fields to the last saved values.
Apply button	Commit the changes made and save to the CPE device, some services will be reloaded.

	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.

Mobile Network | Technology | LTE | Default PDN

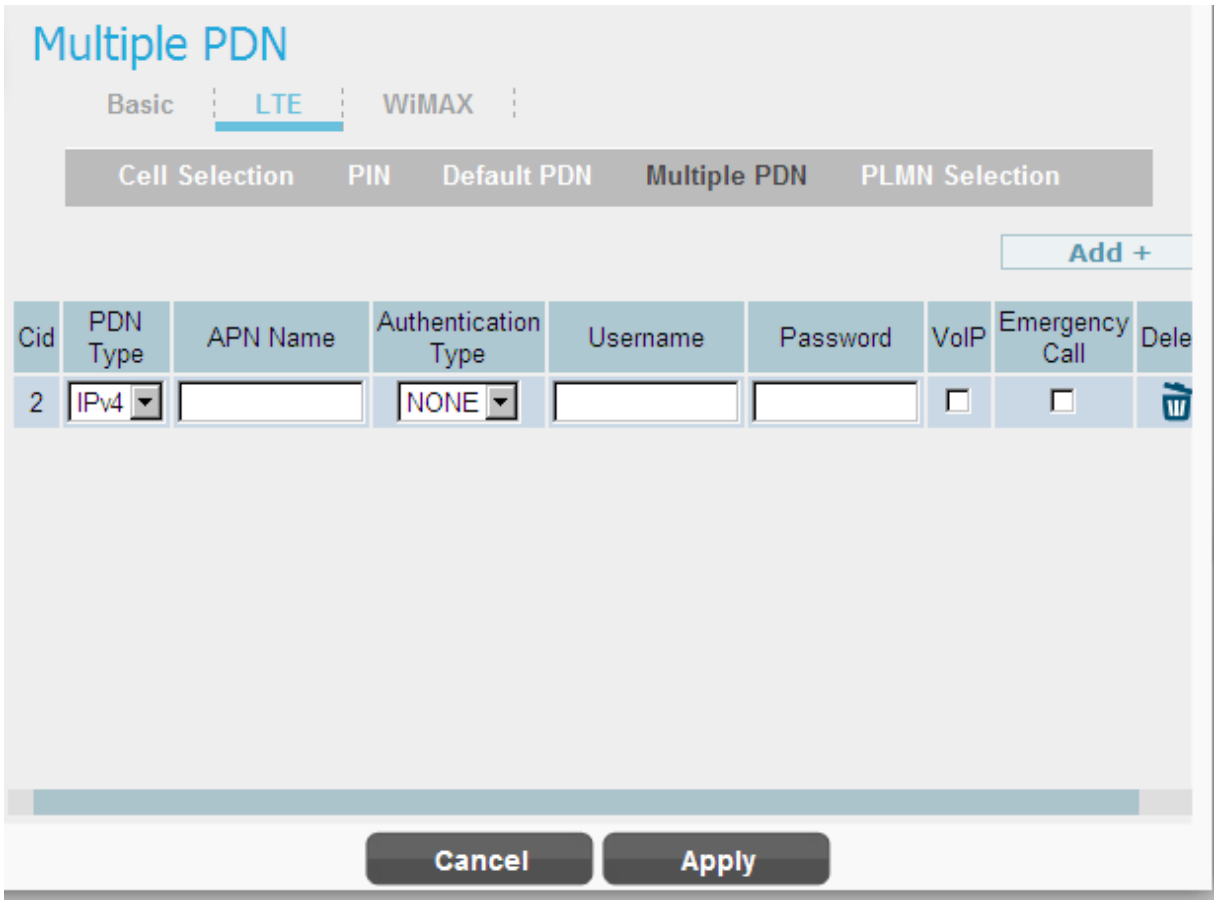


Mobile Network > Technology > LTE > Default PDN

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

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

Mobile Network | Technology | LTE | Multiple PDN



Mobile Network > Technology > LTE > Multiple PDN

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

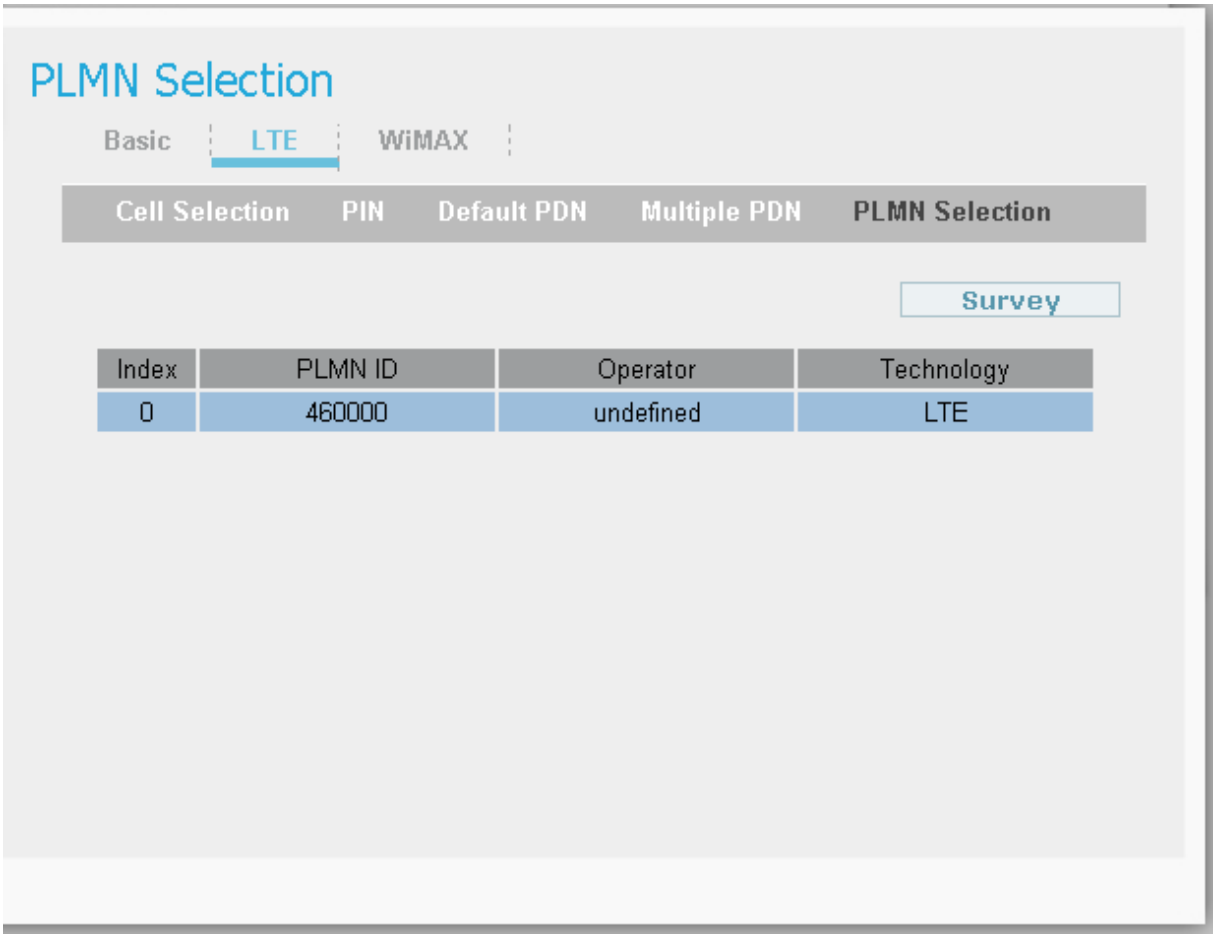
- **PDN Type:** Only support IPv4 right now.
- **APN Name:** As titled.
- **Authentication Type:** There are **"None"**, ***"PAP (Password authentication protocol)"***, or ***"CHAP (Challenge Handshake Authentication Protocol)"*** to choose from. If choosing PAP or CHAP, users need to specify the username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

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

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

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

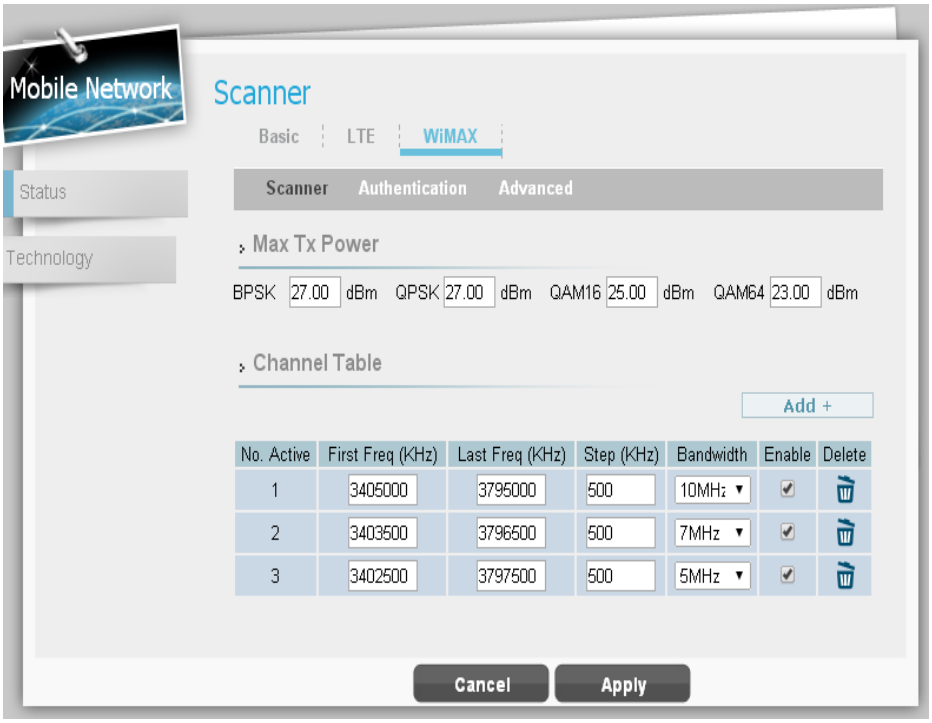
Mobile Network | Technology | LTE | PLMN Selection



In this screen the LTE outdoor CPE survey all available operators and their PLMN ID according to the standard MCC/MNC (also called PLMN code) for each supported network.

!	The PLMN ID 460000 is an example (no operator have this code).

Mobile Network | Technology | WiMAX | Scanner



Mobile Network > Technology > WiMAX > Scanner

- **Max Tx Power:** Users can define the maximum Tx power for different modulations.
- **Channel Table:** Users can modify the WiMAX frequency which CPE scan in this table.
  - If users only want a specific frequency, just set **First Freq** and **Last Freq** to the same value and **Step** can be any value.
  - If users want to scan a range of frequency, users can use Step to achieve this.

    Ex: **First Freq**=2300000, **Last Freq**=2350000, **Step**=10000

    CPE will scan 2300000, 2310000, 2320000, 2330000, 2340000 and 2350000.

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.

Mobile Network | Technology | WiMAX | Authentication

Mobile Network > Technology > WiMAX > Authentication

The base station that users connect to may require authentication. In this section, users can set the parameters for the authentication.

- The authentication type includes **NONE**, **EAP-TLS**, **EAP-TTLS**.
- **None:** The authentication is not needed.
- **EAP-TLS**
  - **Identity:** The identity of the clients. Chances are that different clients may use the same certificate. The server differentiates different clients from the identity in this case. You may use random identity if the server does not care about that.
    - **Use Realm:** If the server only allows the identity that goes with a realm, you need to fill in the realm.
  - **Enable WiMAX Supplicant chain:** The uploaded certificate file may contain device

certificate and the chain certificates. When the option is enabled, the whole file is sent to the server. When the option is disabled, only the device certificate in the file is sent to the server.

- **Root/Device Certificate Passphrase:** The passphrase to protect the certificate. Although the certificate is public, it still can be protected.
- **Validate the Date Duration of CA Certificate:** Test if the uploaded CA certificate has expired. This is optional because the time of CPE may be incorrect.
- **Validate the Server Certificate:** Verify the server certificate through CA certificate.

- **EAP-TTLS**
  - **Phase2:** Use the mechanism of either **CHAP** or **MSCHAPV2** to authenticate the user with username and password.
  - **Use Device Certificate:** In EAP-TTLS, the server can authenticate the client by either username/password or certificate. If this option is enabled, CPE would ignore the username/password fields.
  - **Identity:** The identity of the clients. Chances are that different clients may use the same certificate. Servers differentiate the different clients from the identity in this case. You may use random identity if the server does not care about that.
    - **Use Realm:** If the server only allows the identity that goes with a realm, you need to fill in the realm.
  - **Root Certificate Passphrase:** The passphrase to protect the certificate. Although the certificate is public, it still can be protected.
  - **Validate the Date Duration of CA Certificate:** Test if the uploaded CA certificate has expired. This is optional because the time of CPE may be incorrect
  - **Validate the Server Certificate:** Verify the server certificate through CA certificate.

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

	The Device certificate and chain certificate(s) are merged into a single file. The order of the content is important. The device certificate should be placed before chain certificate(s) in the file. Beware that the **Line feed** should be "\n" (UNIX style), not "\r\n"(Windows Style). We recommend using the text editor "MadEdit" to do it. The order is like below. ➢ Device Cert ➢ Chain Cert
	The authentication information in this page is just an example.

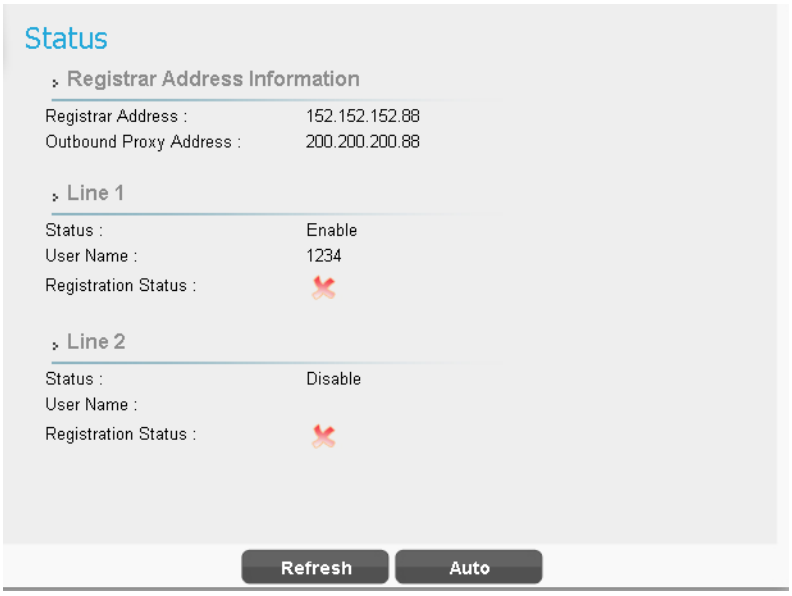
VoIP

	Display in **Brief Summary Page**
	Display in "**Quick Panel**" of **Detailed Configuration Page**

- In VoIP main menu, users can see and tweak parameters of VoIP.
- Users can set **User Name**, **User Account**, **User Password** and others in VoIP registration process.
- Menu Structure:

VoIP	Status
	Basic
	Advanced

VoIP | Status



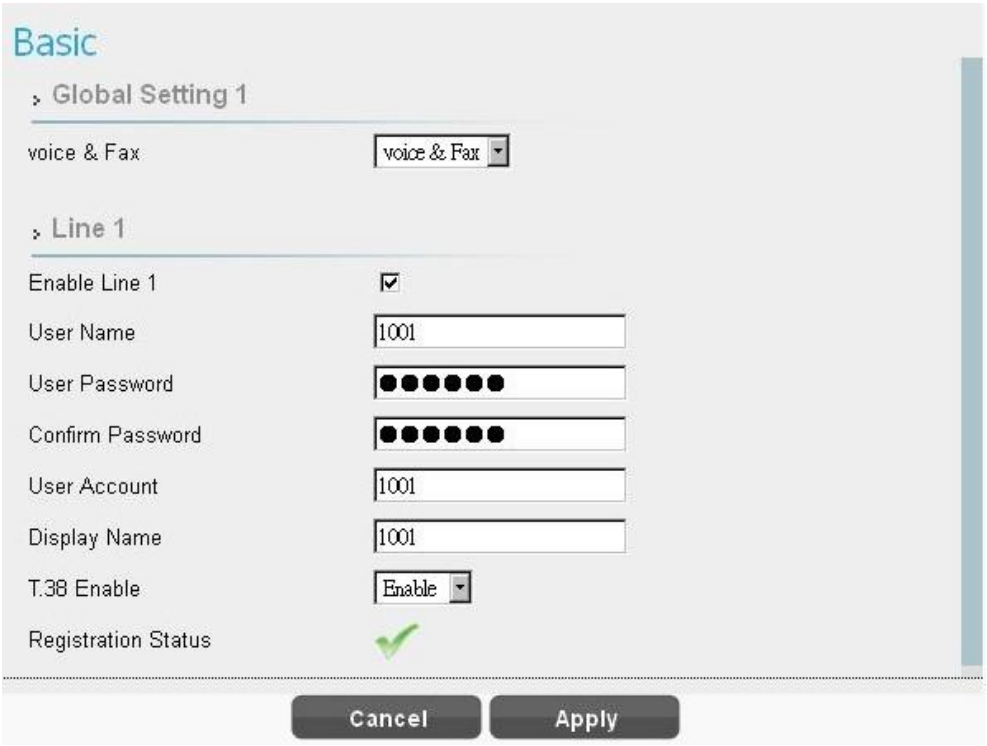
VoIP > Status

- Users can know the status of VoIP in this page. Like Enable / Disable, Registrar Address and Registration Status.
- **Line 1 / Line 2**
  - **Status**: VoIP is enabled or disabled.
  - **UserName**: Username of Line.
  - **Registration Status**: show a green check ✔ if the registration is successful; otherwise, show a red cross ✘.
- The upper left part of the page shows  if VoIP Line 1 is registered successfully; otherwise, it shows  .

Refresh button	Click the "Refresh" button to refresh the page manually.
Auto button	This button will update the status information periodically. (The period is controlled by "GUI Refresh Time" in page **Management / Device Setting**)

!	Address and User Name are all examples here.

VoIP | Basic



VoIP > Basic

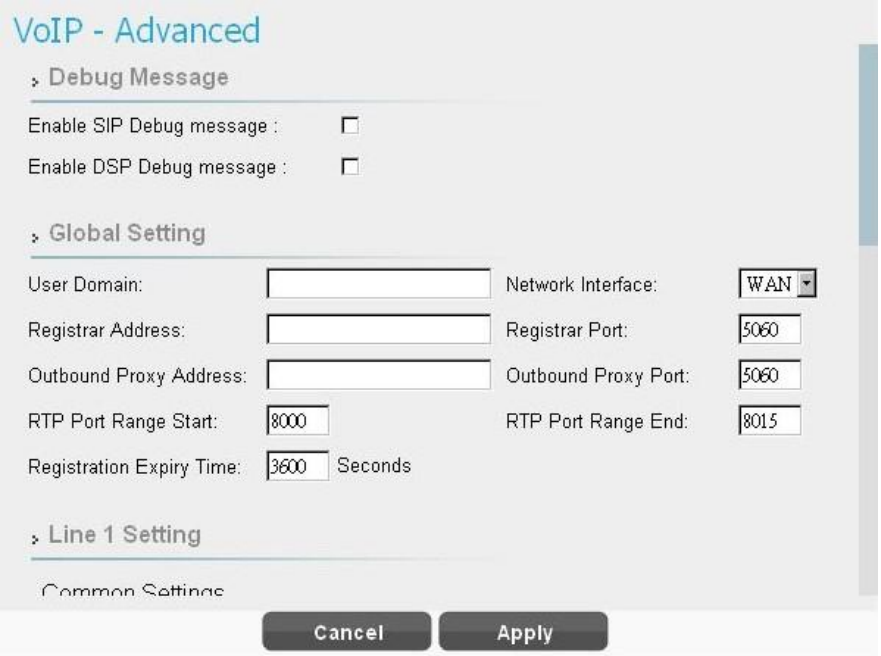
- **Global Setting 1:** Select from the dropdown list to enable "Voice Only" or "Voice & Fax".
- **Line 1**
  - **Enable Line 1:** Tick the checkbox to enable VoIP.
  - **User Name: authentication.** Enter the user name provided by your VoIP service provider.
  - **User Password:** Enter the user password provided by your VoIP service provider.
  - **Confirm Password:** Enter the password again for confirmation.
  - **User Account:** It serves as a telephone number.
  - **Display Name:** caller name. A part of Caller ID. Caller ID is composed of display name, telephone number, the current time. Not every device can show "**Display Name**". Regular devices should be able to show telephone number and the current time.

- **T.38 Enable:** T.38 is an ITU-T standard for allowing transmission of fax over IP networks in real time. Select ***"Enable"*** from the dropdown list to enable T.38. If T.38 is not enabled, Fax is sent as voice. If the network is congested, it is suggested to use T.38.
- **Registration Status:** If VoIP Line 1 is registered successfully, it will show a green check  , otherwise it will show a red cross  .

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.

	WiMAX / LTE outdoor CPE has two separate lines for Voip.

VoIP | Advanced

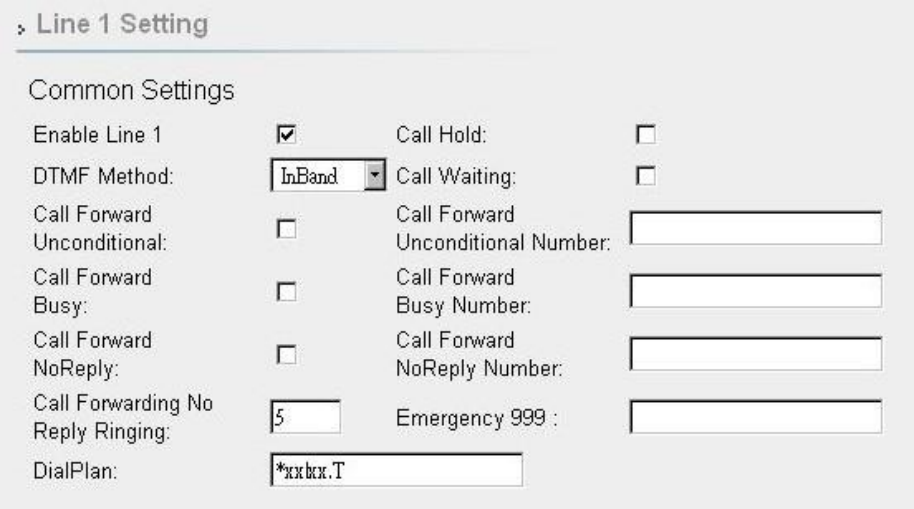


VoIP > Advanced

- **Debug Message**
  - **Enable SIP Debug Msg:** Tick the checkbox to enable session initiation protocol debugging; the debug message will be displayed in the console.
  - **Enable DSP Debug Msg:** Tick the checkbox to enable digital signal processor debugging; the debug message will be displayed in the console.
- **Global Setting**
  - **User Domain:** your SIP user domain.
  - **Network Interface:** Select the network interface for SIP service.
  - **Registrar Address:** Enter your SIP registrar address.
  - **Registrar Port:** Enter your SIP registrar port number. (default:5060)
  - **Outbound Proxy Address:** Enter your SIP outbound proxy address if there is a proxy server.
  - **Outbound Proxy Port:** Enter your SIP outbound proxy port number. (default:5060)

- **RTP Port Range Start:** Enter the starting port number of Real-time Transport Protocol (RTP).
- **RTP Port Range End:** Enter the ending port number of Real-time Transport Protocol (RTP).
- **Registration Expiry Time:** The valid period of registration.

◆ **Line Setting**

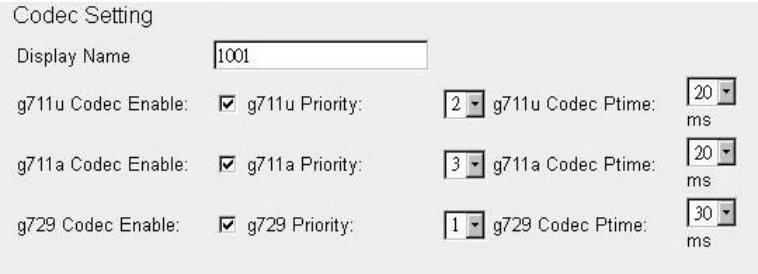


- **Common Settings**
  - **Enable Line 1:** Tick the checkbox to enable Line 1 VoIP service.
  - **CallHold:** Users can place the call on hold if this checkbox is ticked.
  - **DTMF Method:** Select Dual-tone multi-frequency signaling (DTMF) from the drop-down list. (CPE supports In-Band, RFC2833, RFC2833_In-Band, and SIP Info.) SIP info: key tone is indicated in the SIP packet. RFC2883: It is like SIP Info. In-Band: treat it as voice.
  - **Call Waiting: If it is enabled, when the line is busy, the user can hear the tone that indicates a new call is coming; otherwise, there is no tone and the user does not know a new call is coming at that time.**
  - **Call Forward Unconditional:** Tick the checkbox to let CPE automatically forward

all calls to another phone number.

- **Call Forward Unconditional Number:** If ***"Call Forward Unconditional"*** is enabled, enter the phone number that you'd like your phone call to be redirected to.
- **Call Forward Busy:** Redirects your incoming calls to another phone number when your line is busy.
- **Call Forward Busy Number:** If ***"Call Forward Busy"*** is enabled, enter the phone number that you'd like your phone call to be redirected to.
- **Call Forward Noreply:** Redirects all calls to another phone number when there is no reply.
- **Call Forward Noreply Number:** If ***"Call Forward Noreply"*** is enabled, enter the phone number that you'd like your phone call to be redirected to.
- **Call Forward No Reply Ringing:** The value defines the state "No Reply" by the number of ringing.
- **Emergency 999:** A mapping to a real emergency phone number. This option is for emergency use. When the user dial 999 and this call will be routed to the emergency service.
- **Dial Plan:** Allow users to establish the expected number or pattern for a telephone number.

➢ **Codec Setting**

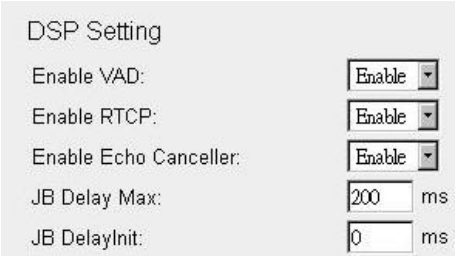


There are 3 codec here, when the checkbox of any of them is ticked, it is put in the codec candidate list, and sent to the server to coordinate which codec to use. Please note that

g711u, g711a do not compress the data, but g729 does. Thus, using g729 would distort the signal.

- **g711u/g711a/g729 Codec Enable:** Tick the checkbox to enable it.
- **g711u/g711a/g729 priority:** An indicator of which codec to use first.
- **g711u/g711a/g729 Codec Ptime:** A data packet corresponds to the duration of voice.

➢ **DSP Setting**



- **Enable VAD:** Enable or disable VAD (Voice Activity Detection) for voice transmission. When VAD is enabled, if the voice signal is smaller than a threshold, no voice packet is transmitted.
- **Enable RTCP:** Enable or disable RTCP (Real Time Transport Protocol). This is used to exchange control information between sender and receiver, works in conjunction with RTP. It offers end-to-end monitoring, data delivery, and QoS.
- **Enable Echo Canceller:** Enable Echo canceller to remove echo from a voice communication in order to improve voice quality on a telephone call.
- **JB Delay Max:** Specify the maximum jitter buffer delay in milliseconds.
- **JB DelayInit:** The size of the jitter buffer is variable, this value is its initial value.

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

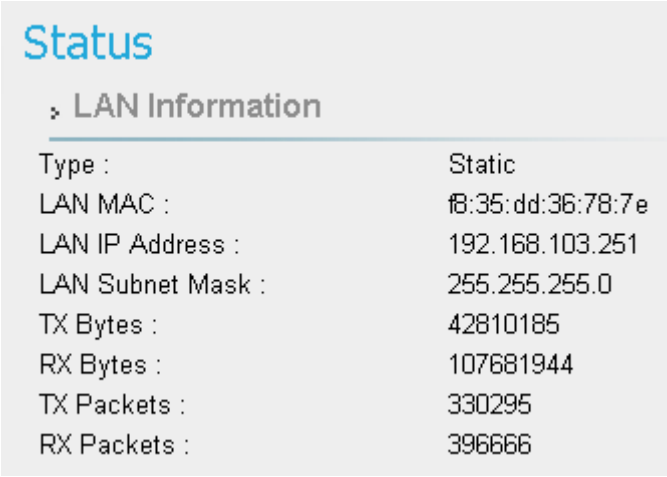
	Display in **Brief Summary Page**
	Display in "**Quick Panel**" of **Detailed Configuration Page**

- **Menu Structure:**

Network	Status
	Network Mode
	DHCP Server (Not available in **Bridge** Mode)
	QoS (Not available in **Bridge** Mode)
	Routing (Available in R**outer** Mode)
	Port Forwarding (Available in **NAT**、**Tunnel** Mode)
	Port Trigger (Available in **NAT**、**Tunnel** Mode)
	DSCP
	Vlan (only in ETH-CS)
	MGMT Service

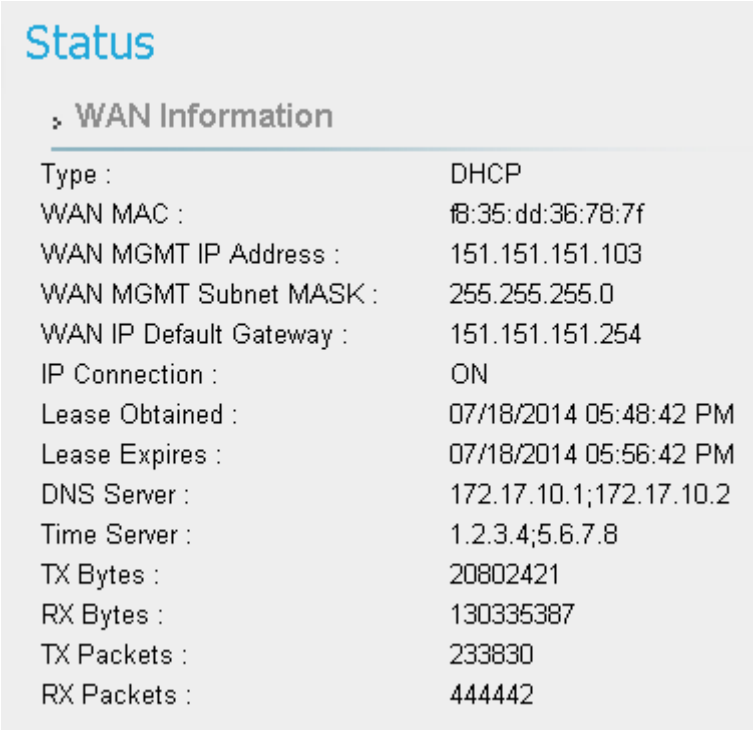
Network | Status

- **LAN Information**: This section shows LAN MAC and IP address of LTE / WiMAX outdoor CPE and statistics of TX and RX Bytes and Packets of LAN interface.



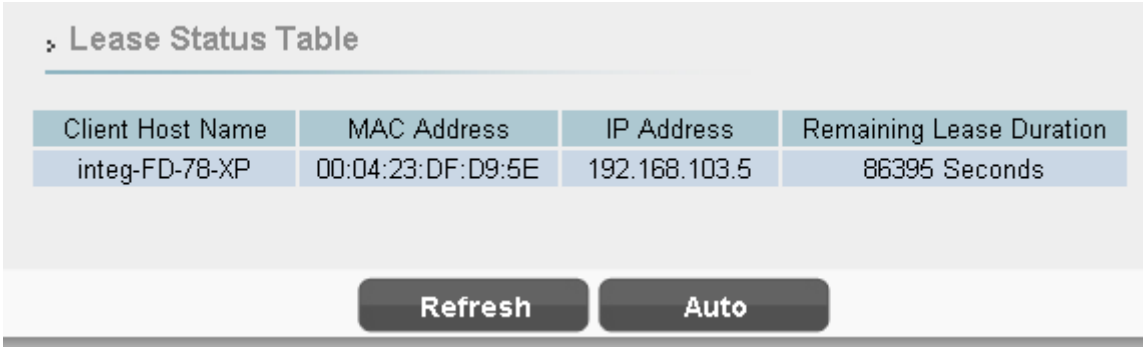
Network > Status > LAN Information

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



Network > Status > WAN Information

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

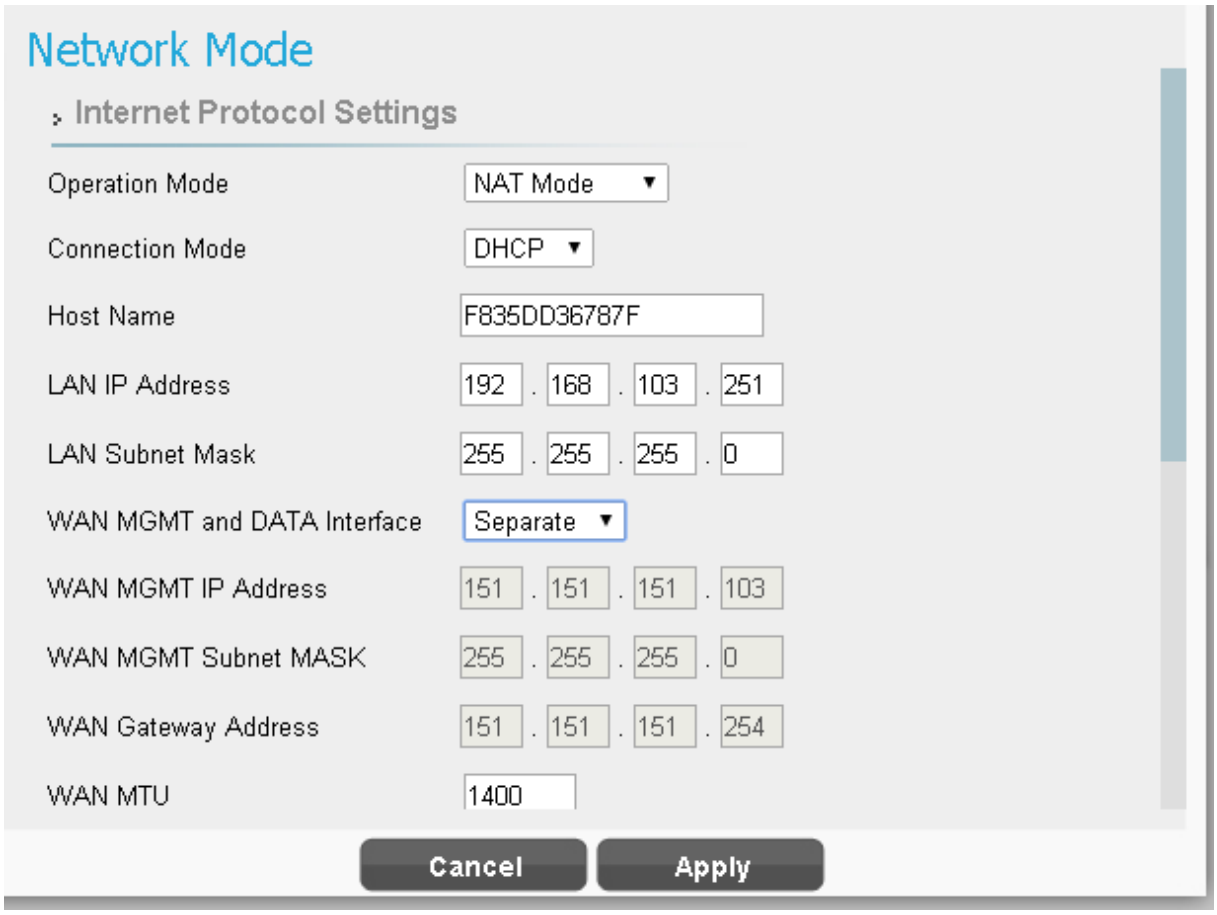


Network > Status > Lease Status Table

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 | Network Mode (NAT Mode)



Network > Network Mode

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

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

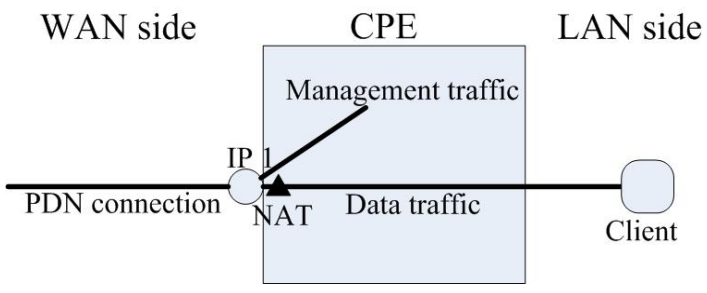
Pop-up windows to confirm reboot

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

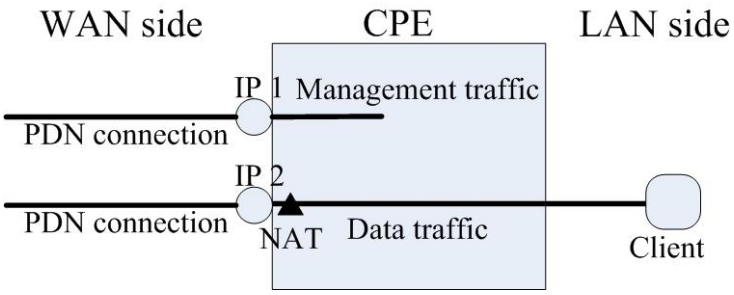
!	Host Name"**<F835DD36787F>"** Just an example here, in general, it will be WAN MAC.

- **LAN IP Address / Subnet Mask:** As titled. This IP will change IP prefix in "**DHCP Server**" , "**Port Forwarding**" and "**Port Trigger**"
- **WAN MGMT and DATA Interface:** Users can choose "**Separate**" to use different Interface for MGMT and Data traffic, or just use "**Combine**" which means using same interface for MGMT and Data.

  Below are two simple pictures that describe this function.



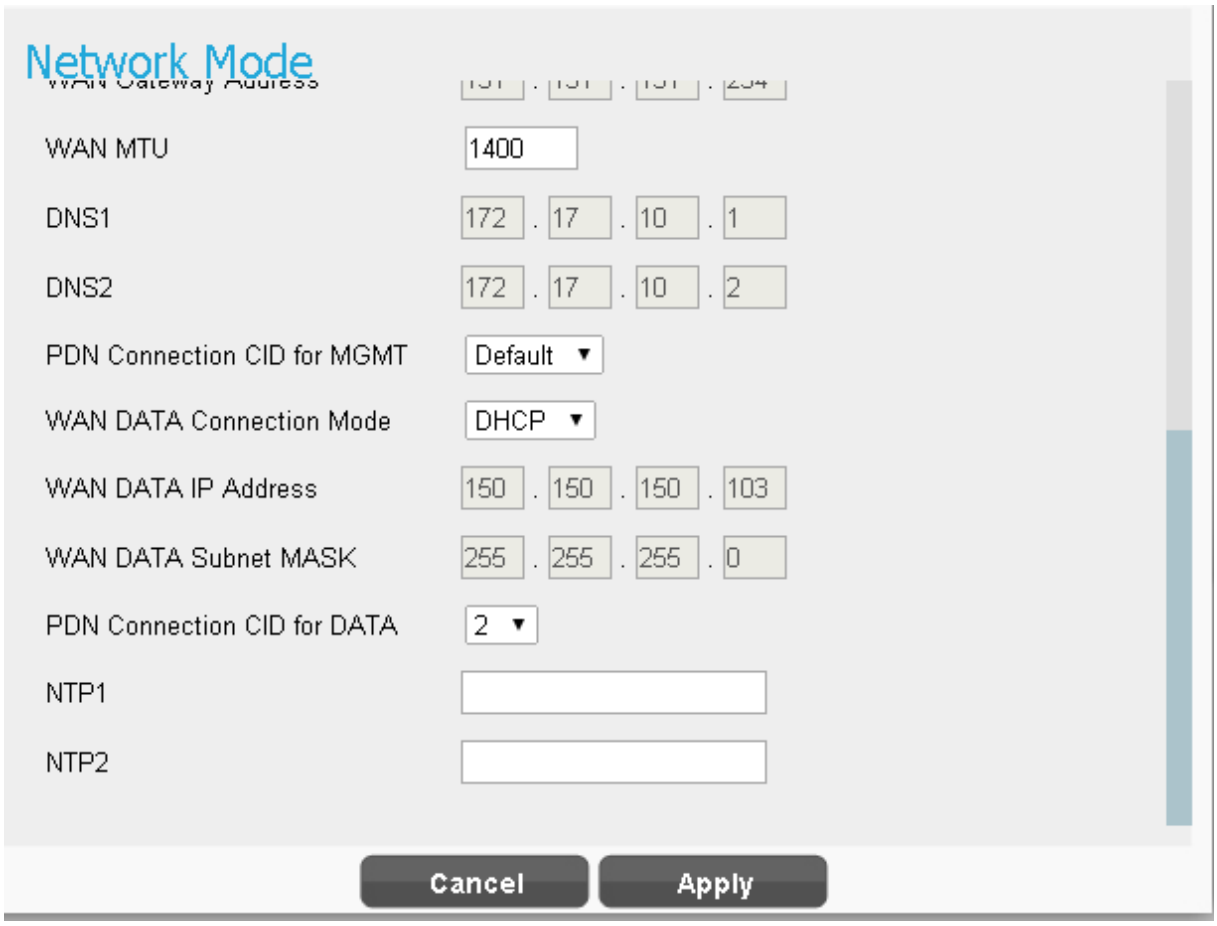
*NAT mode, choosing "**Combine**" in WAN MGMT and Data Interface*



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

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

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



Two WAN IP, one for MGMT, other for DATA

- **WAN MTU:** This value is "Maximum Transmission Unit". The size of a single packet can only be as large as MTU. If the size of the packet exceeds MTU, the packet would be fragmented. No fragmentation in bridge mode.

- **DNS:** Domain Name Server, editable when users select "Static" in "Connection Mode". Otherwise, DNS information will be given by DHCP server.
- **PDN connection CID for MGMT:** If selecting "**Separate**" in "**WAN MGMT and DATA Interface**", users need to assign the PDN used as MGMT. By now, the only option is "Default".
- **PDN connection CID for DATA:** If selecting "**Separate**" in "**WAN MGMT and DATA**

Interface", users need to choose from 2-8 for WAN DATA connection. Please make sure this PDN is configured beforehand in page ***Mobile Network > Technology > LTE > Multiple PDN***.

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

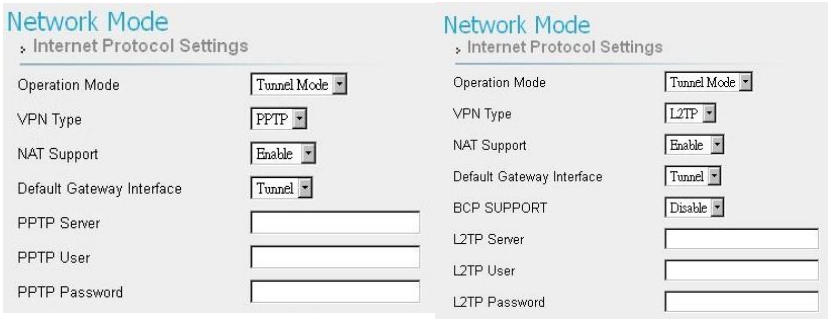
  For example **220.130.158.72** or **tw.pool.ntp.org**

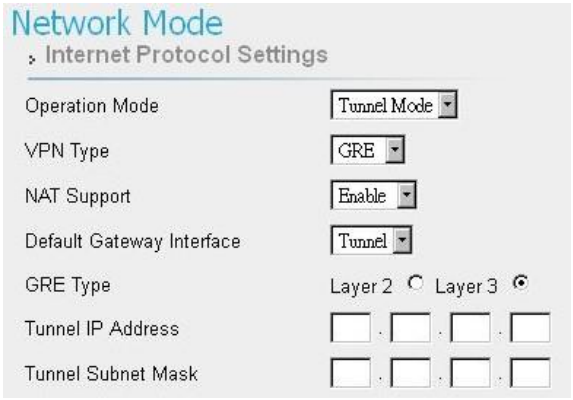
  These NTP are additional to time server that CPE get via DHCP option 42.

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 | Network Mode (Tunnel Mode)

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





Network > Network Mode > PPTP, L2TP, GRE

Pop-up windows for reboot confirm

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

- **VPN Type:** PPTP (with IPsec)
  L2TP (with IPsec & BCP Disable/Enable)
  GRE (Layer2/ Layer3) Tunnel Mode
- **NAT Support (except L2TP with BCP Enabled):** CPE will do network address translation for its clients in LAN.
- **Default Gateway Interface (except L2TP with BCP Enabled):** Users can select which interface as the default gateway. The default is "**Tunnel**" Interface.
- **BCP SUPPORT (Only in L2TP):** If it is enabled, CPE will bridge "**WAN**", "**Tunnel**" and "**LAN**" interface together. Client in LAN side will get IP from Tunnel rather than from CPE's DHCP Server. The traffic to WAN for clients in LAN would not be directed to CPE WAN interface. It would be directed to the gateway at the other end of the tunnel.
- **PPTP Server/ User/ Password (Only in PPTP):** The IP address of PPTP server and username and password for authentication.
- **L2TP Server/ User/ Password (Only in L2TP):** The IP address of PPTP 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:** "DHCP" or "Static".
  - If "DHCP" mode is selected, CPE would automatically acquire configuration information from a DHCP server.

- If "Static" mode is selected, users have to manually enter the required information in below fields.

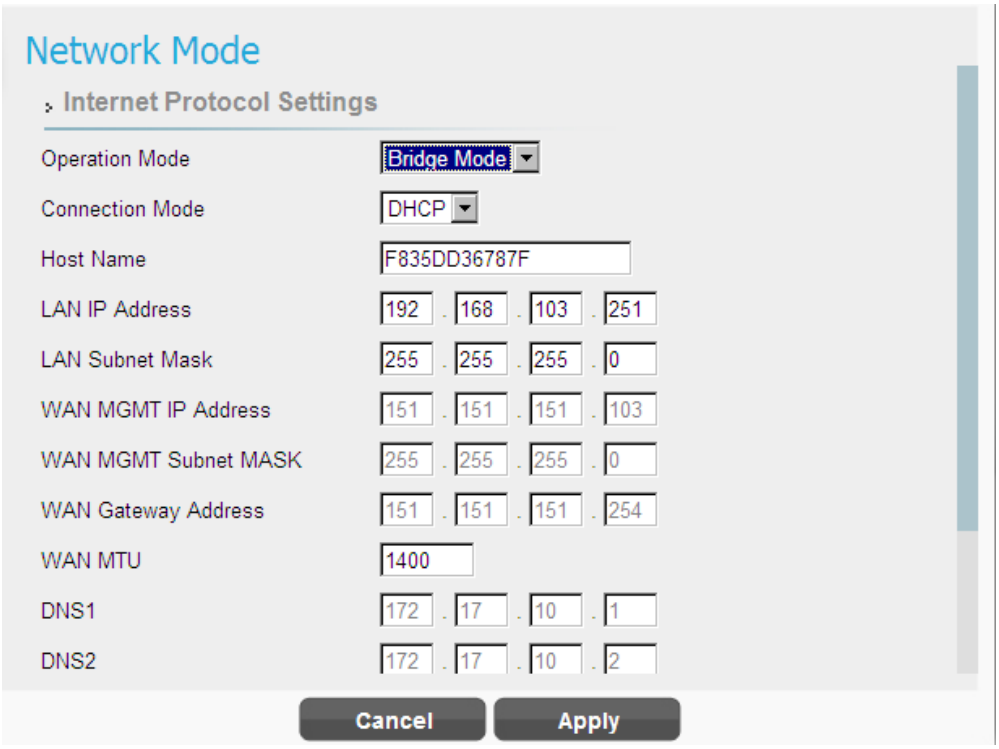
- **Host Name:** Currently no function.
- **LAN IP Address / Subnet Mask:** The IP address and subnet mask used by CPE in LAN
  - If users choose "**L2TP with BCP Enabled**" in "**Operation Mode**", this IP only means a back-up IP address. When users cannot link to CPE web GUI due to the dynamic IP address, users can use the back-up IP address to link to CPE web GUI instead.
  - If users choose other tunnel mode, this IP means LAN side domain and Web GUI IP address.(This IP will change IP prefix in "**DHCP Server**" , "**Port Forwarding**" and "**Port Trigger**")
- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when users select "**DHCP**" in "**Connection Mode**".
- **WAN MTU:** This value is "Maximum Transmission Unit". It is the largest size of a single packet.
- **NTP:** Users can specify two NTP servers in "IP" or "Domain name" format.
  For example **220.130.158.72** or **tw.pool.ntp.org**
  These NTP are additional to time server that CPE get via DHCP option 42.
- **DNS:** Domain Name Server, editable when users select "Static" in "Connection Mode". Otherwise, DNS information will be given by DHCP server.
- **IPsec Tunnel (PPTP and L2TP):** encrypt/decrypt the packet flow.
- **Pre-Shared Key**: the key used for authentication in IPsec.

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 | Network Mode (Bridge Mode)

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

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



Network > Network Mode

Pop-up windows for reboot confirm

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

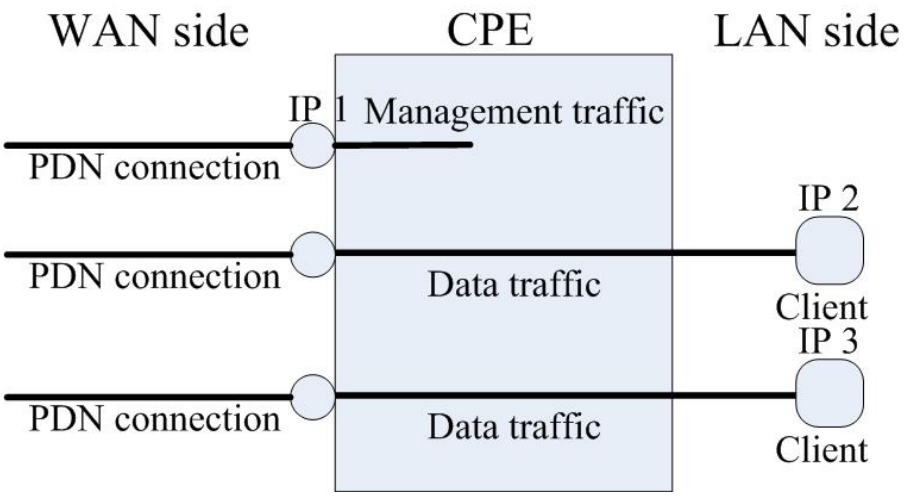
- **Connection Mode:** “DHCP” or “Static”.
  - If “DHCP” mode is selected, CPE would automatically acquire configuration information from a DHCP server.
  - If “Static” mode is selected, users have to manually enter the required information in below fields.
- **Host Name:** Currently no function.

!	Host Name“**<F835DD36787F>”** Just an example here, in general, it will be WAN MAC.

- **LAN IP Address / Subnet Mask:** The IP address and subnet mask used by CPE in LAN
  - This IP only means a back-up IP address. When users cannot link to CPE web GUI due to the dynamic IP address, users can link to CPE web GUI through the back-up IP address.
- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when “**Connection Mode**” is “**DHCP**” and editable when “**Connection Mode**” is “**Static**”.
- **WAN MTU:** This value is “Maximum Transmission Unit”. It is the largest size of a single packet.
- **DNS:** Domain Name Server. It is editable when users select “**Static**” in “**Connection Mode**”. Otherwise, these values will be given by DHCP server.
- **MultiPDN connection for Data (Only in Bridge Mode):** If it is enabled, CPE will pre-create PDN connections for local clients. Thus, a client requests IP address from CPE, CPE will reply an IP gotten from one of APN.

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

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



Multi-PDN in Bridge Mode

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

  For example **220.130.158.72** or **tw.pool.ntp.org**

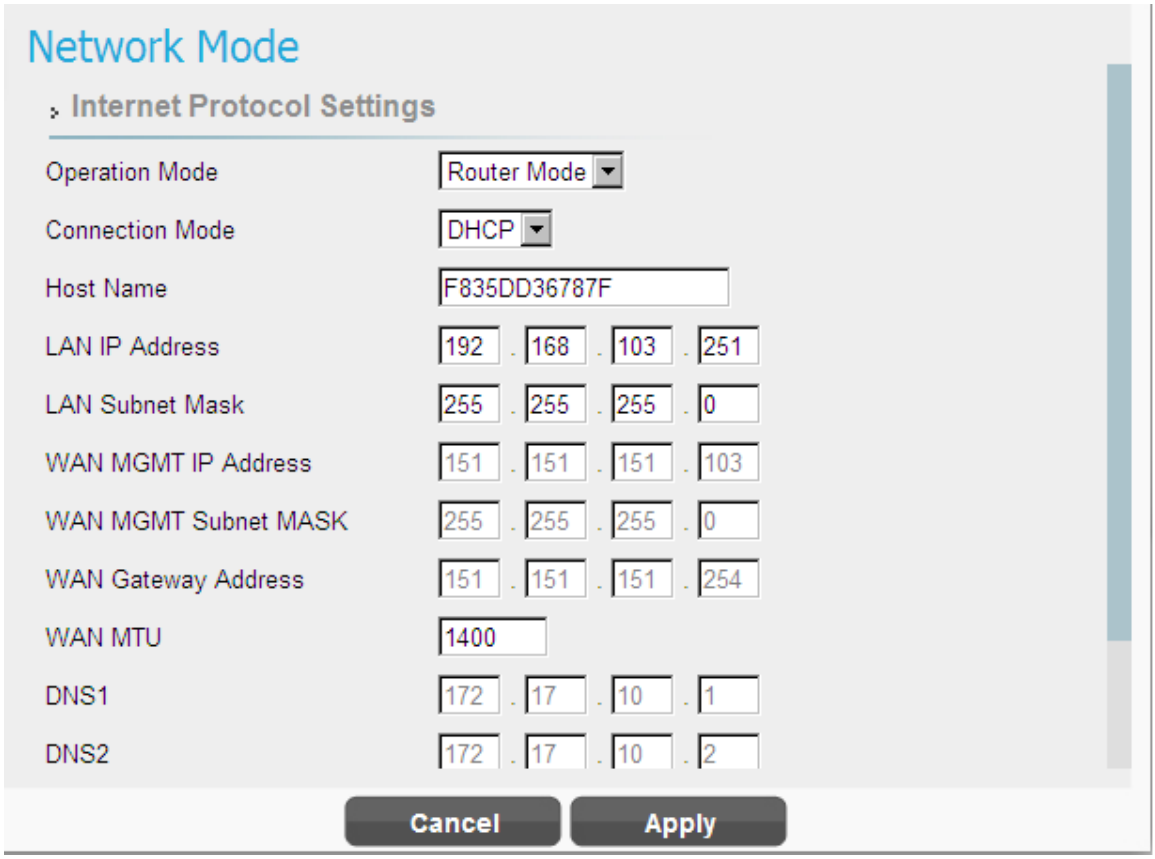
  These NTP are additional to time server that CPE get via DHCP option 42.

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 | Network Mode (Router Mode)

- **Operation Mode:** users have **NAT**, **Tunnel**, **Bridge** and **Router** mode to choose from.

  The following pages will show how to configure "**Router mode**".



Network > Network Mode

Change a picture to Router Mode

Pop-up windows for reboot confirm

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

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

	Host Name“**<F835DD36787F>”** Just an example here, in general, it will be WAN MAC.

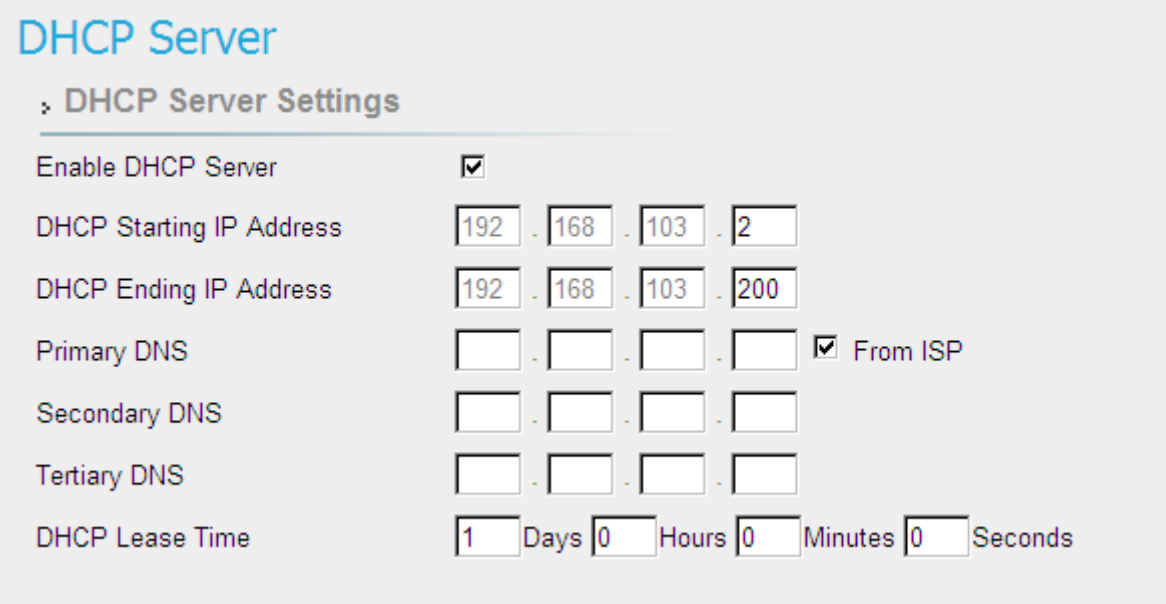
- **LAN IP Address / Subnet Mask:** The IP address and subnet mask used by CPE in LAN
- **WAN IP Address/ Subnet Mask/ Gateway Address:** These values are un-editable when “**Connection mode**” is “**DHCP**” and editable when “**Connection mode**” is “**Static**”.
- **WAN MTU:** This value is “Maximum Transmission Unit”. It is the largest size of a single packet.
- **DNS:** Domain Name Server. It is editable when users select “**Static**” in “**Connection Mode**”. Otherwise, these values will be given by DHCP server.
- **NTP:** Users can specify two NTP servers in “IP” or “Domain name” format.

  For example **220.130.158.72** or **tw.pool.ntp.org**

  These NTP are additional to time server that CPE get via DHCP option 42.

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 | DHCP Server (not available on bridge mode)



Network > DHCP Server

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

- **Enable DHCP Server:** enable/disable DHCP server
- **DHCP Starting IP Address:** The starting IP address assigned by DHCP server.
- **DHCP Ending IP Address:** The ending IP address assigned by DHCP server.
- **From ISP:** When the checkbox is ticked, clients set CPE as DNS server, but CPE will only act as a "**DNS relay**". The following picture is captured from a PC in LAN; DNS Server field is 192.168.103.251 (LAN IP of CPE). DNS request will be sent to 192.168.103.251 then forwarded to ISP DNS Server.

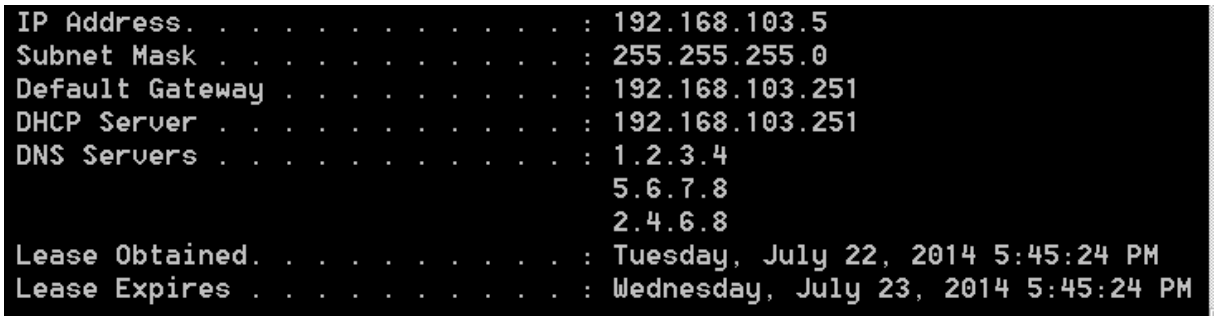
```
IP Address. . . . . . . . . . . . : 192.168.103.5
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.103.251
DHCP Server . . . . . . . . . . . : 192.168.103.251
DNS Servers . . . . . . . . . . . : 192.168.103.251
Lease Obtained. . . . . . . . . . : Tuesday, July 22, 2014 5:35:19 PM
Lease Expires . . . . . . . . . . : Wednesday, July 23, 2014 5:35:19 PM
```

Network > DHCP Server > From ISP

!	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.

Network > DHCP Server > not From ISP

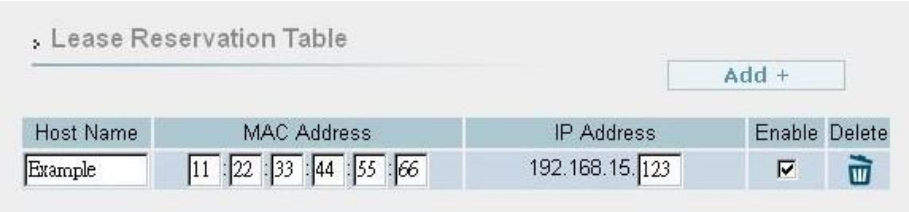


Network > DHCP Server > not From ISP

!	"1.2.3.4", "5.6.7.8" and "2.4.6.8" 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.

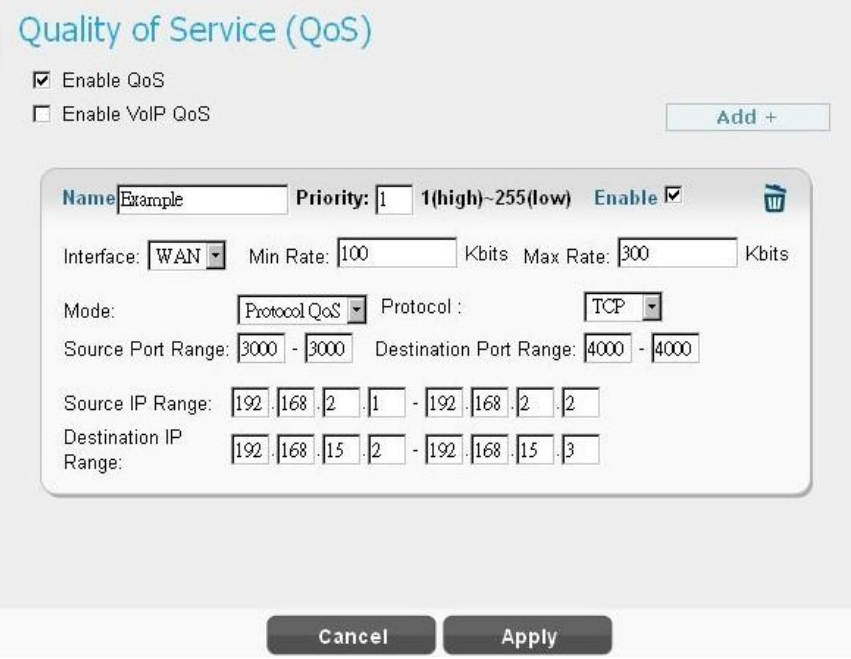
  An example is illustrated below. If a client with MAC Address "**11:22:33:44:55:66**" requests IP, DHCP server will assign IP "**192.168.15.123**" and the host name "**Example**" to it.



!	"Example", "11:22:33:44:55:66", "192.168.15.123" are examples here.

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

Network | QoS (Not available in bridge mode)



Network > QoS

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

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

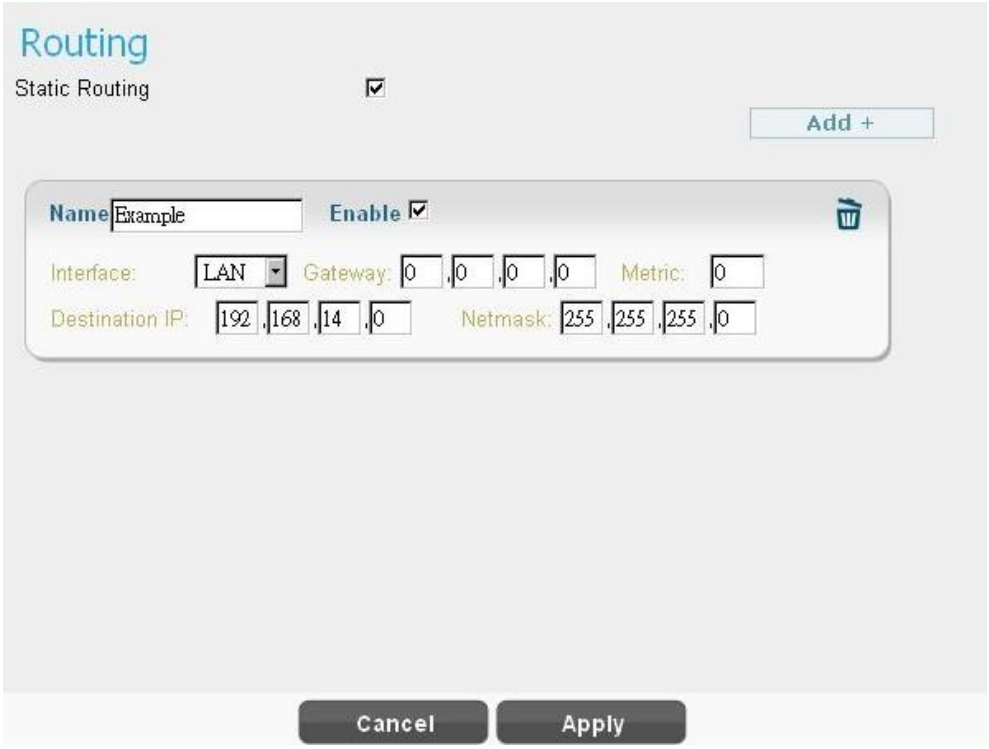
!	About **Min Rate** and **Max Rate**, we can discuss this in 3 cases. For example, Min Rate=**50** kbps Max Rate=**100** kbps 1. If **20** kbps is needed, the traffic will only get **20** kbps, CPE will not give it **50** kbps (50 kbps=Min Rate, this can prevent wasting bandwidth) 2. If **60** kbps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

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

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

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

Network | Routing (Available in Tunnel、Router Mode)

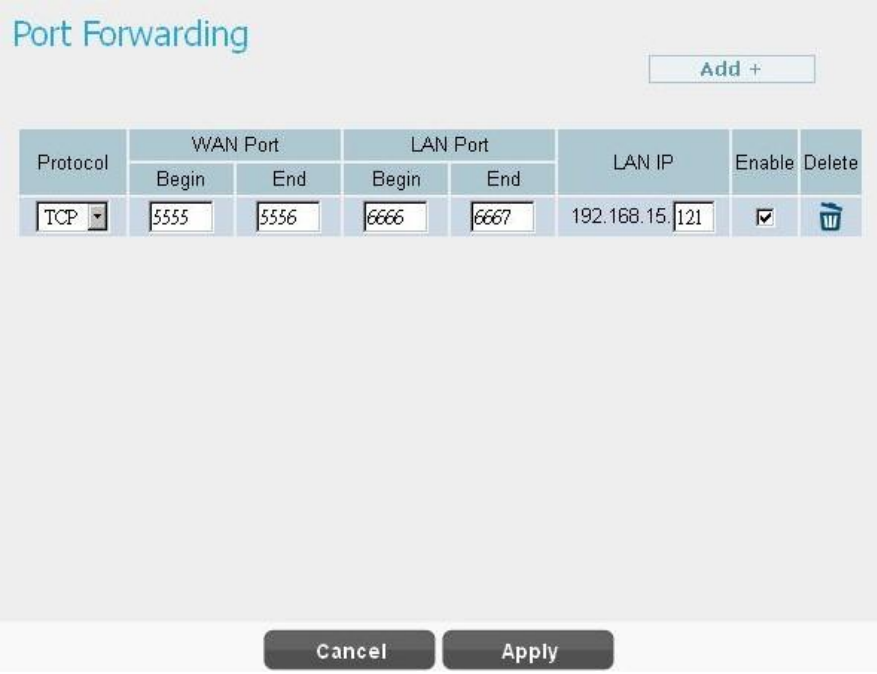


Network > Routing

Users can designate routing rules of CPE

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

Network | Port Forwarding (Available in NAT、Tunnel Mode)



Network > Port Forwarding

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

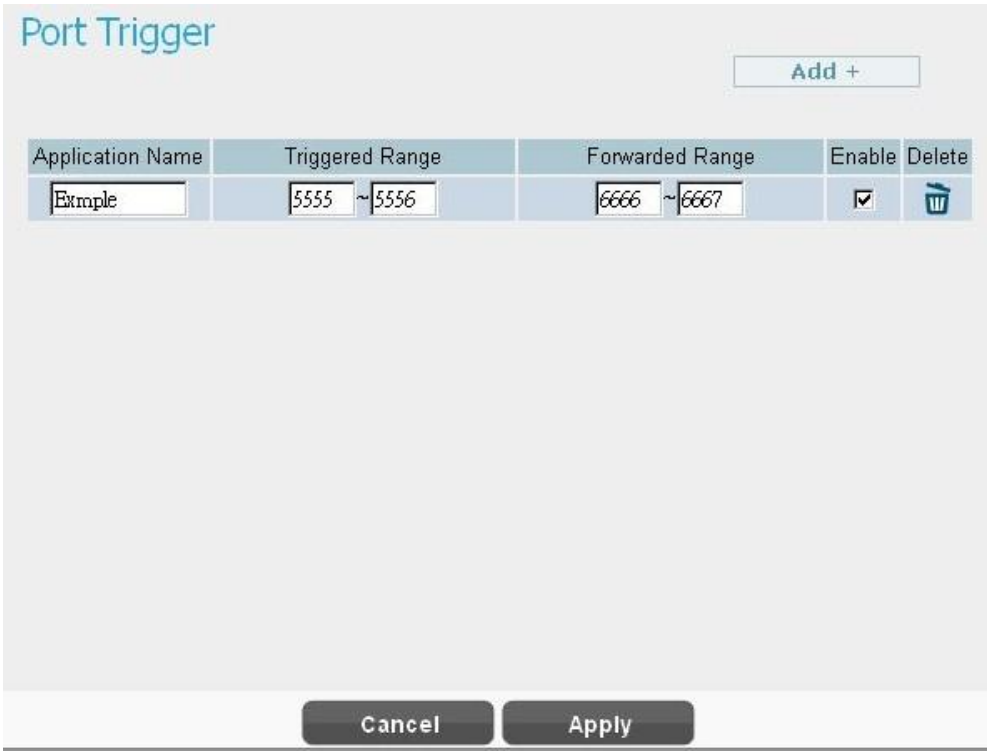
- Click **"Add +"** button to add a new rule, clicking **"Delete"** icon ( ) to delete the rule.
- **Protocol:** TCP or UDP.
- **WAN Port:** The range of WAN port.
- **LAN Port:** The range of LAN port.
- **LAN IP:** Enter the IP which desires to receive forwarded packets.
- **Enable:** Enable/Disable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

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

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

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

Network | Port Trigger (Available in NAT、Tunnel Mode)



Network > Port Trigger

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

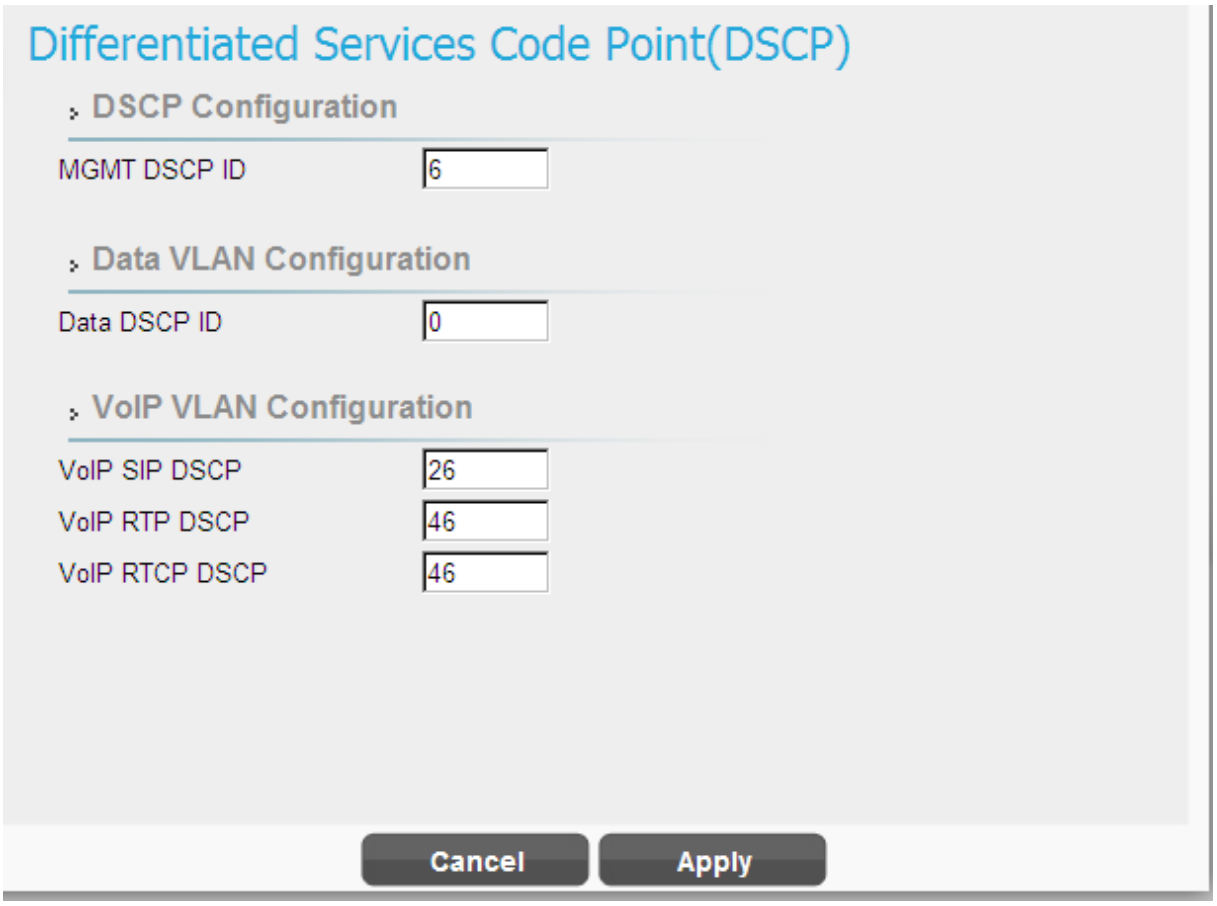
- **Application Name:** Name of the port trigger rule.
- **Triggered Range:** Traffic passing through **t**he port in the triggered range would automatically open the forwarded port in the forwarded range. The ports in the triggered range are LAN ones.
- **Forwarded Range:** The ports that would be automatically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

through ports in the triggered range. The ports in the triggered range are WAN port.

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

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

Network | DSCP

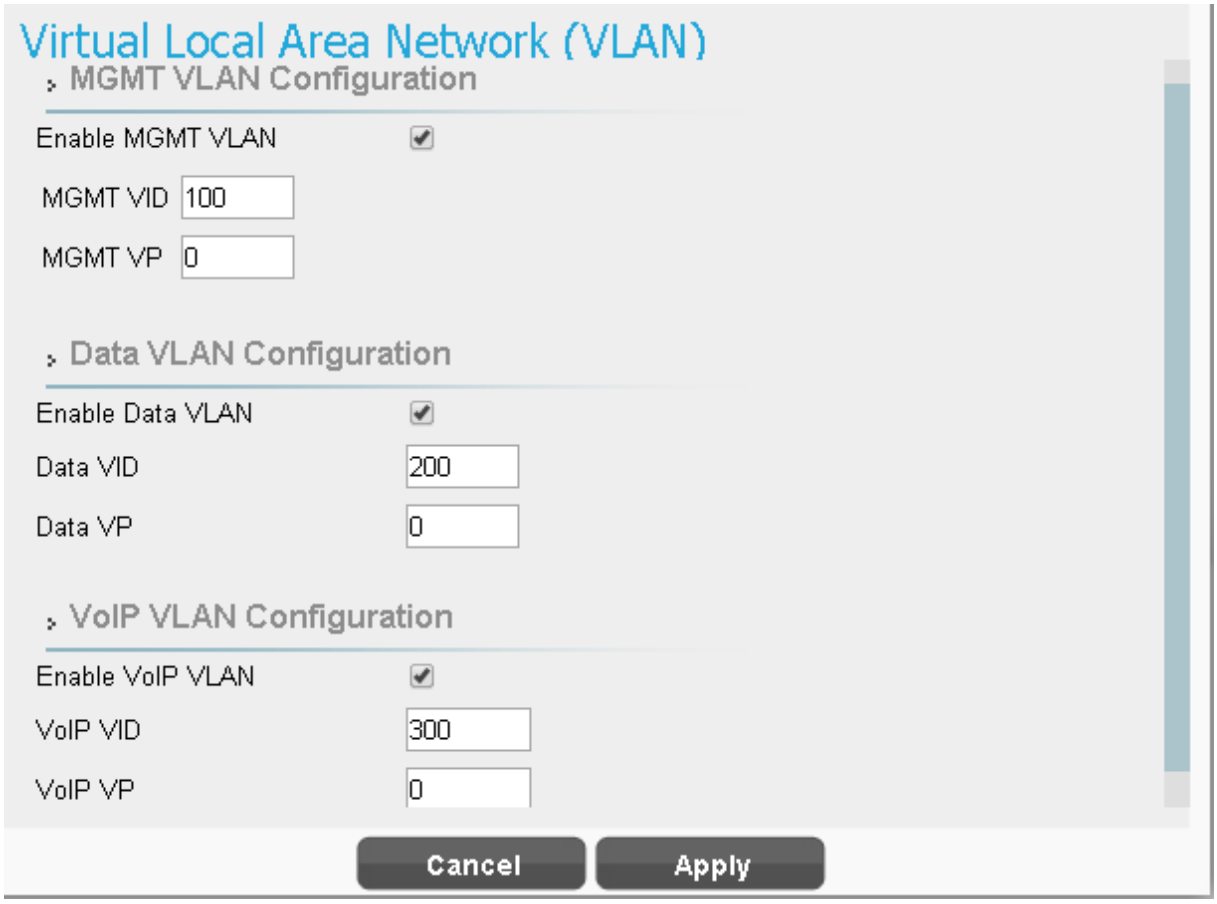


- **MGMT DSCP ID:** UL DSCP that LTE / WiMAX outdoor CPE mark the management packets.
- **Data DSCP ID:** UL DSCP that LTE / WiMAX outdoor CPE mark the data packets.
- **VoIP SIP DSCP ID:** UL DSCP that LTE / WiMAX outdoor CPE mark the VoIP SIP packets.
- **VoIP RTP DSCP ID:** UL DSCP that LTE / WiMAX outdoor CPE mark the VoIP RTP packets.
- **VoIP RTCP DSCP ID:** UL DSCP that LTE / WiMAX outdoor CPE mark the VoIP RTCP packets.

!	DSCP 0,6,26,46 are examples.

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 | Vlan (available in ETH-CS only)



In ETH-CS mode the LTE / WiMAX outdoor CPE has 3 interfaces.
Management, data and VoIP;

- **Enable MGMT VLAN:** this option allow configuring MGMT Vlan ID and Vlan priority. The interface is layer 2 (Vlan-cs).
- **Enable DATA VLAN:** this option allow configuring DATA Vlan ID and Vlan priority. The interface is layer 2 (Vlan-cs). If this option is disable it means that LET / WIMAX outdoor CPE delivers the packets as is (transparent), if this option is enable it means that the CPE

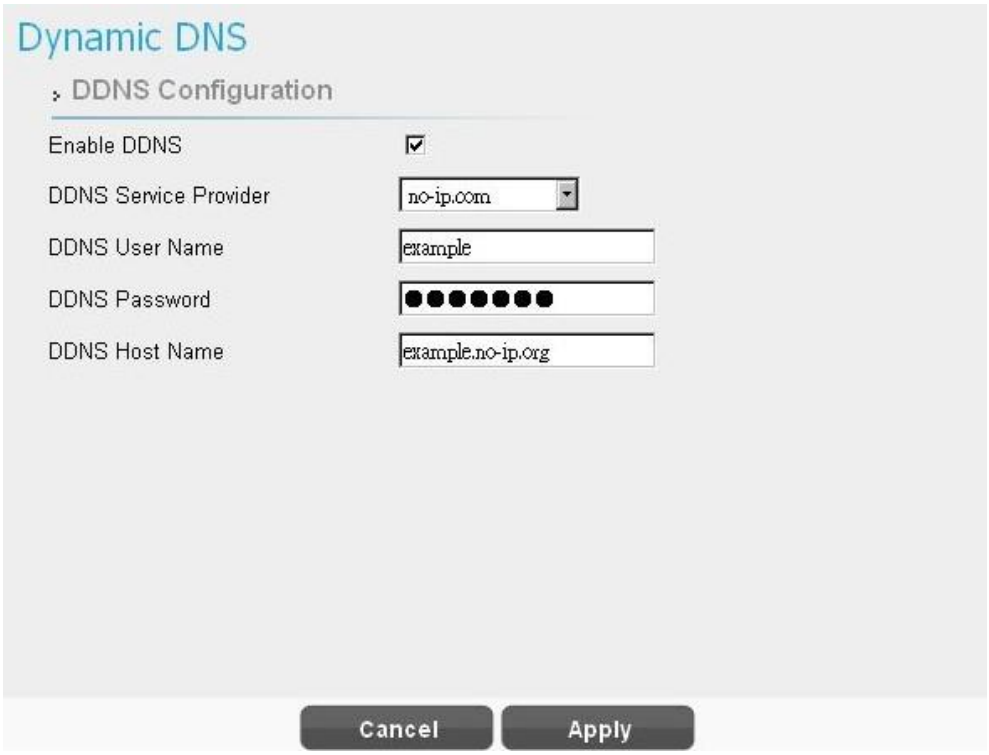
retag the Vlan to untag packet (on LAN side). The interface is layer 2 (Vlan-cs). There is no option to use untag and transparent in same time.

- **Enable VoIP VLAN:** this option allow configuring VoIP Vlan ID and Vlan priority. The interface is layer 2 (Vlan-cs).

!	Vlan 100, 200, 300 are examples.

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 | Dynamic DNS



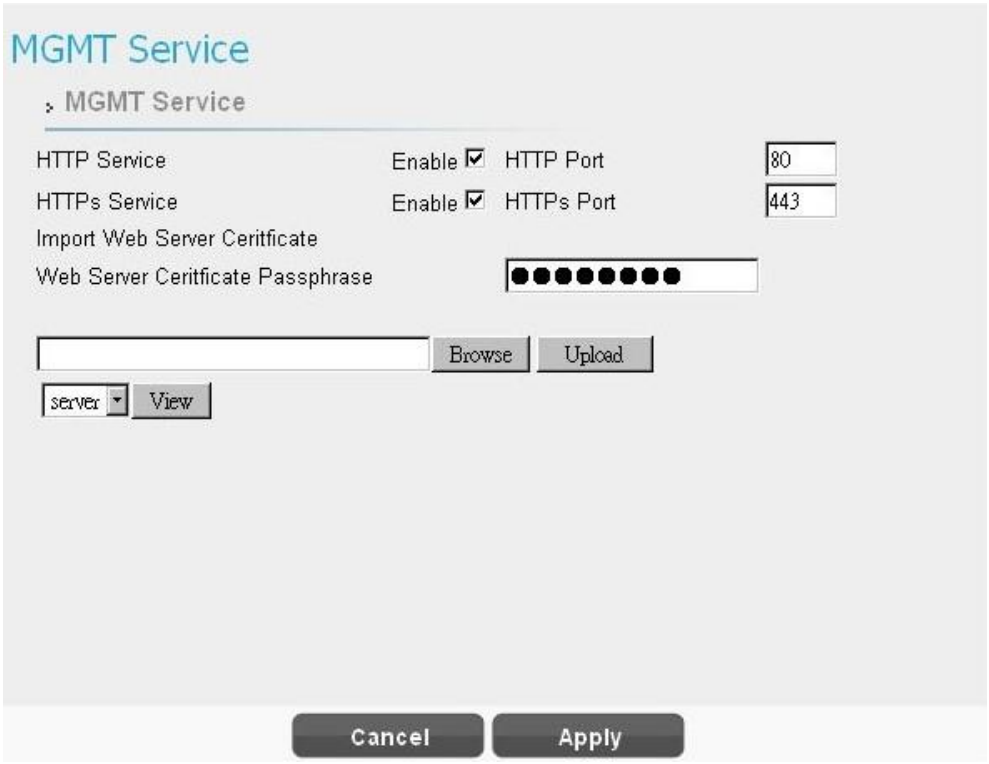
Network > Dynamic DNS

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

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

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

Network | MGMT Service



Network > MGMT Service

MGMT service is about HTTP and HTTPs configuration.

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

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

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

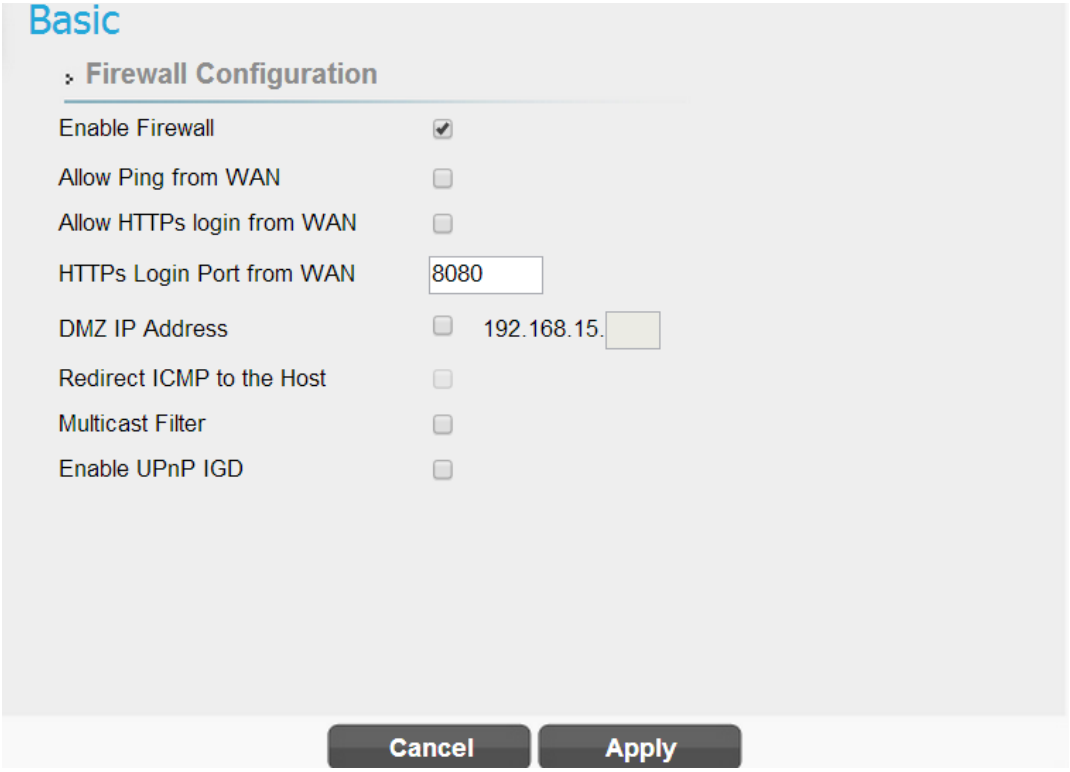
Firewall

	Display in **Brief Summary Page**
	Display in "**Quick Panel**" of **Detailed Configuration Page**

- The firewall is used to block and grant some network access.
- **Menu structure:**

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

Firewall | Basic

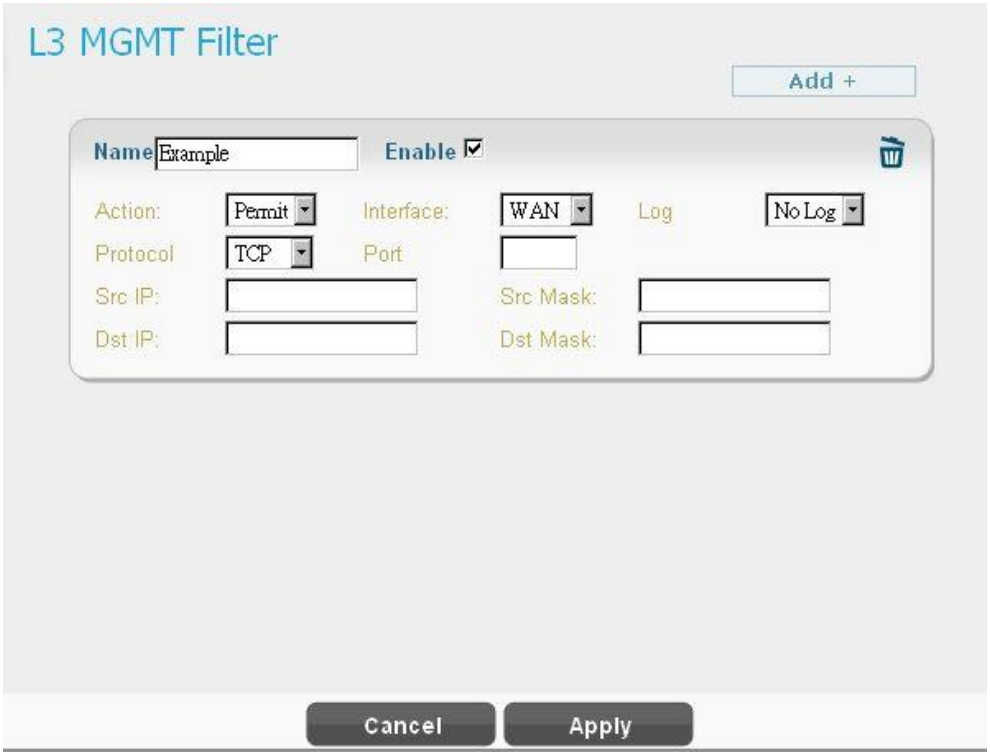


Firewall > Basic

- **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.

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

Firewall | L3 MGMT Filter



Firewall > L3 MGMT Filter

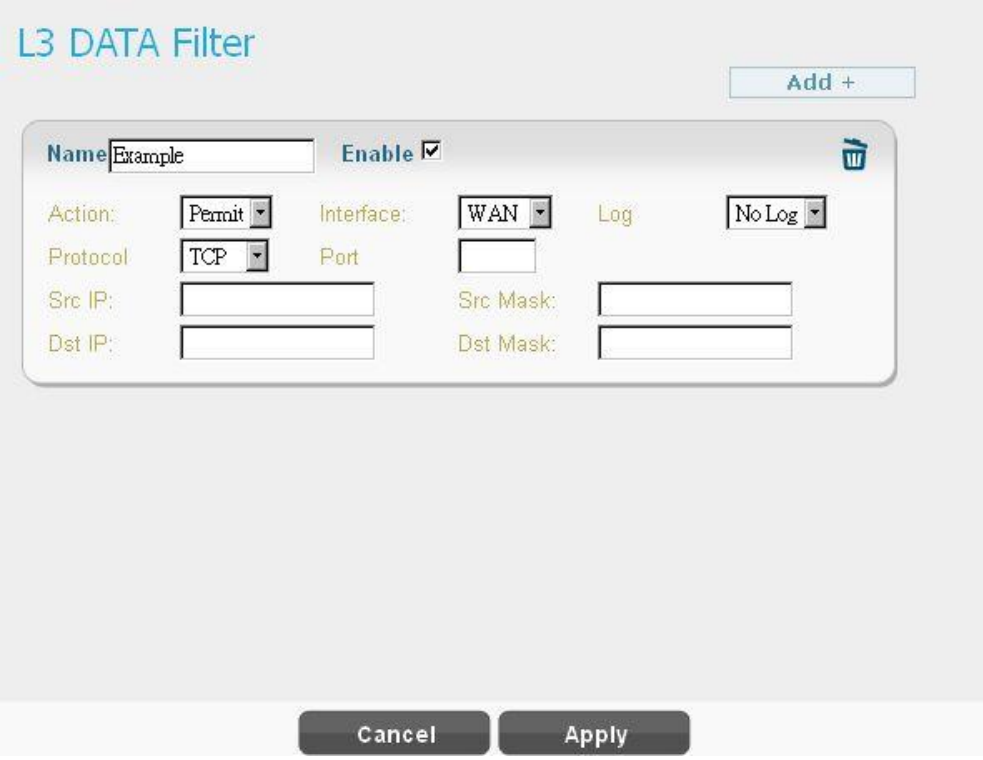
L3 MGMT filter disallow/allows packets with certain ports and IP address which is sent to CPE.

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

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

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

Firewall | L3 DATA Filter



Firewall > L3 DATA Filter

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

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

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

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

Firewall | L2 Filter

Firewall > L2 Filter

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

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

identifier, the number range is from 0 to 4095.

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

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

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

Firewall | Access Restriction

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.

Firewall > Access Restriction (Digest)

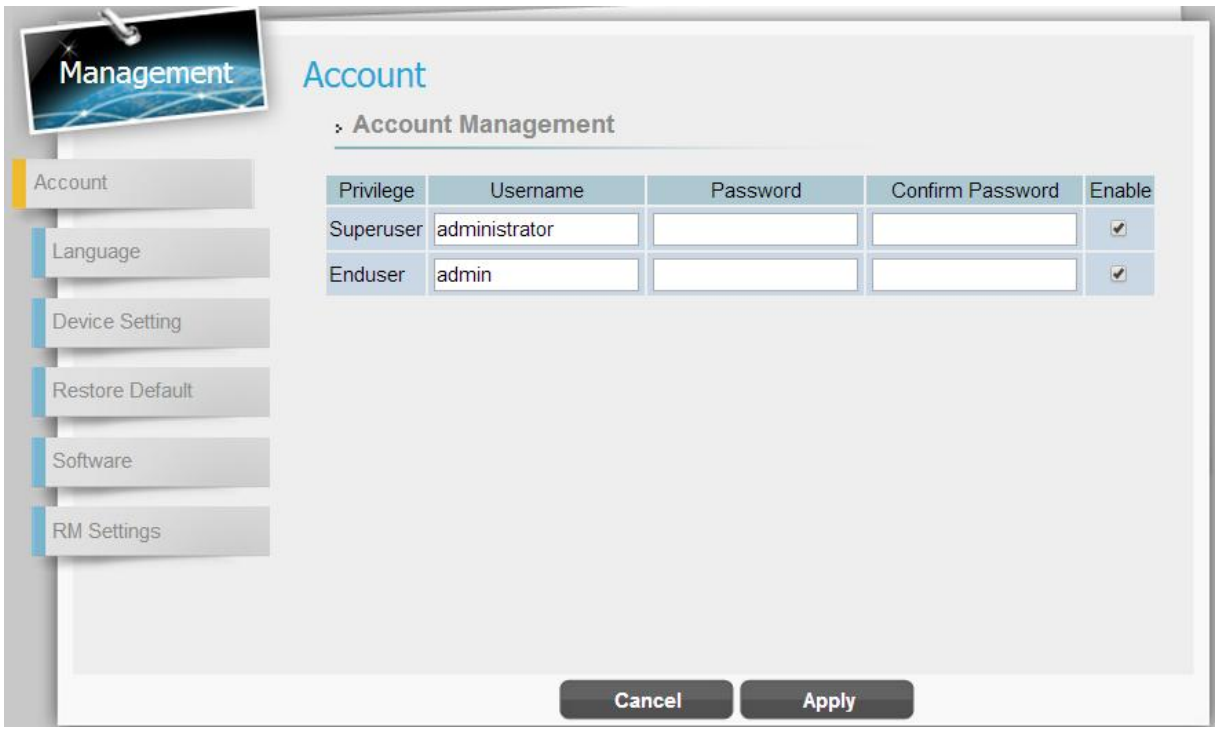
- **Name:** The name of the rule.
- **Enable: E**nable/Disable the rule.
- **Blocked Day / Blocked Time:** The day and time to block the network.
- **Blocked Device:** Block the device with specified MAC address or block packets with specified IP range.
- **Blocked Reason:** (1) block all traffic (2)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

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

Management

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

Management | Account



Management > Account Management

The Account Management page lets you change the default username and password for superuser and enduser.

- There should be at least 9 characters for the password. Click ***“Apply”*** to save this change.

  Tick the checkbox ***“Enable”*** to enable the account.

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

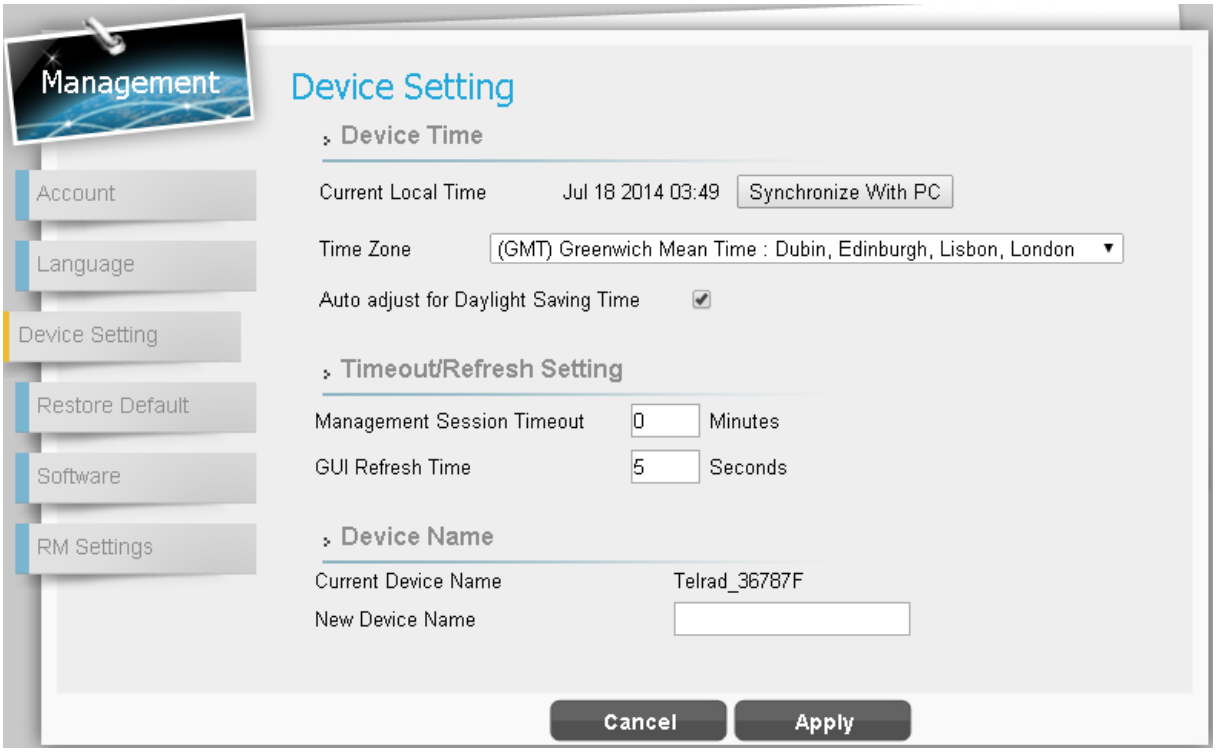
Management | Language

Management > Language

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

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

Management | Device Setting



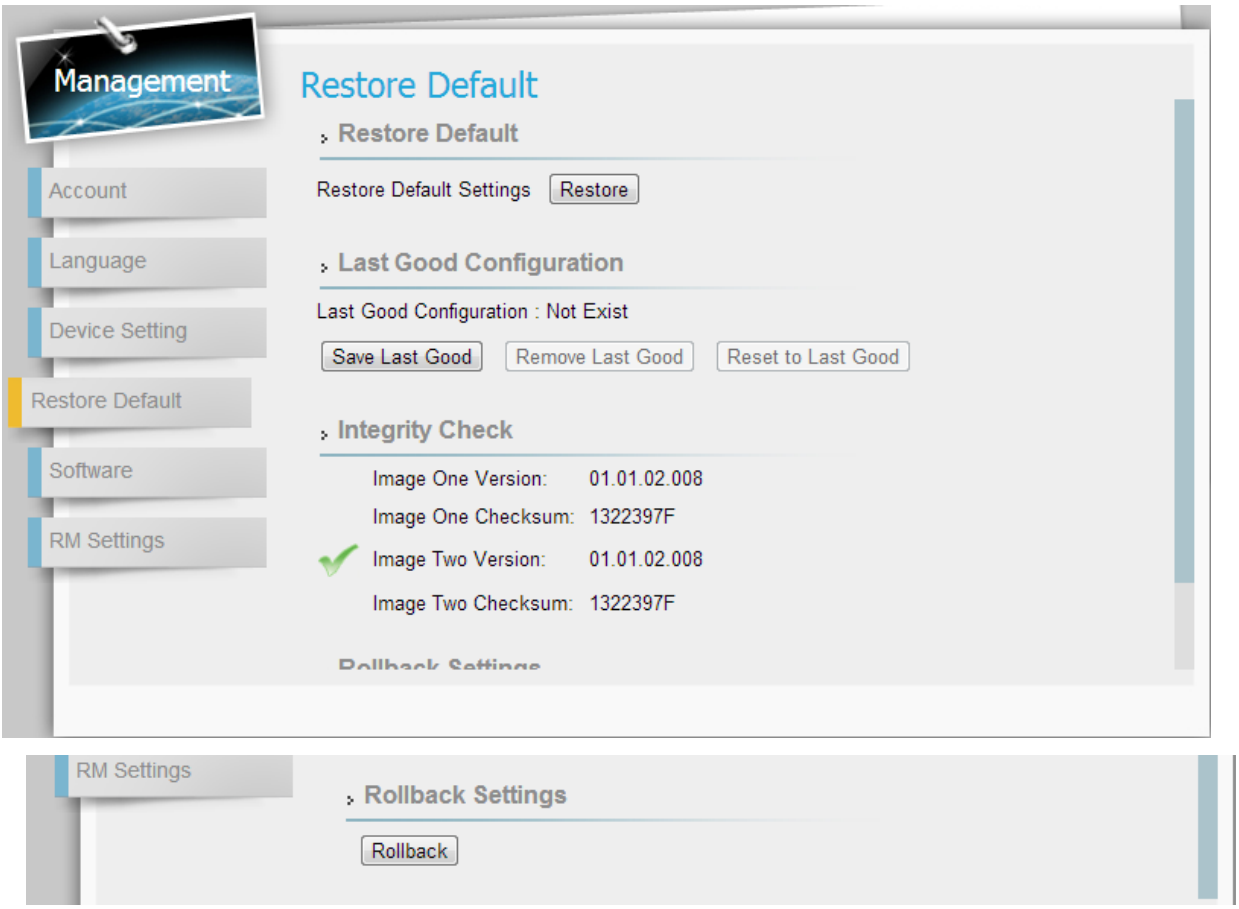
Management > Device Time

- **Device Time**
  - **Current Local Time:** Display current local time; or click **"Synchronize with PC"** button to synchronize the time of CPE with PC.
  - **Time Zone:** as titled.
  - **Auto Adjust for Daylight Saving Time:** Enable this option if your location observes Daylight Savings Time.
- **Timeout/Refresh Setting**
  - **Management Session Timeout:** Automatic logout after the period. (Range: 0-10 Minutes; 0 means never expired)
  - **GUI Refresh Time**: When users press "**auto**" button in any page, the page refresh every the designated time. (Range: 5-60 Seconds)

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

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

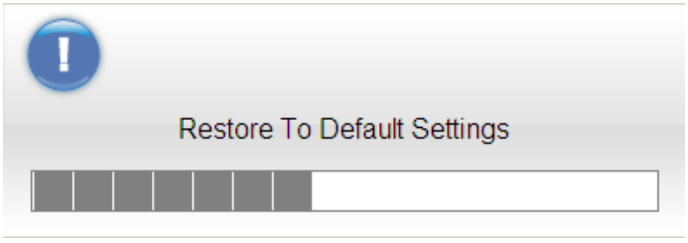
Management | Restore Default



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.

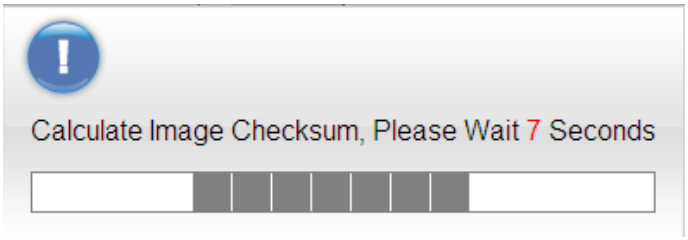


Restore to default settings Window

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

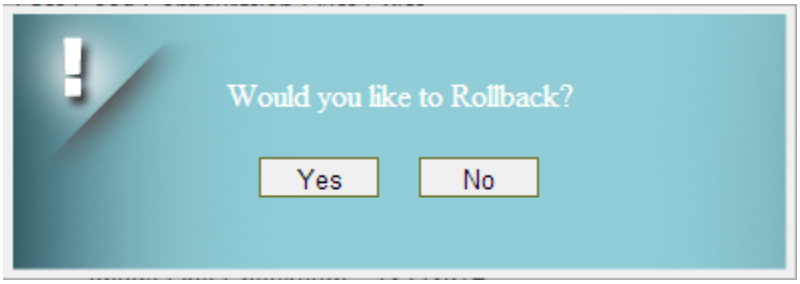
- **Remove Last Good:** Remove the last saved configuration.
- **Reset to Last Good:** Load the last saved configuration.

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

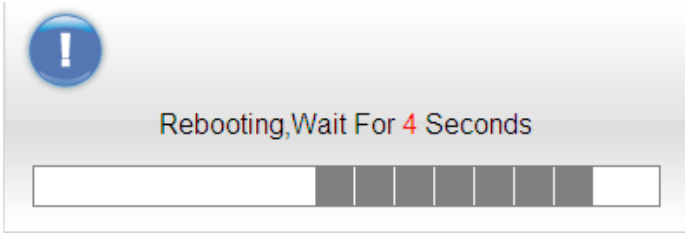


Integrity Check Window

- **Rollback Settings:** CPE saves two firmware with possible of 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.

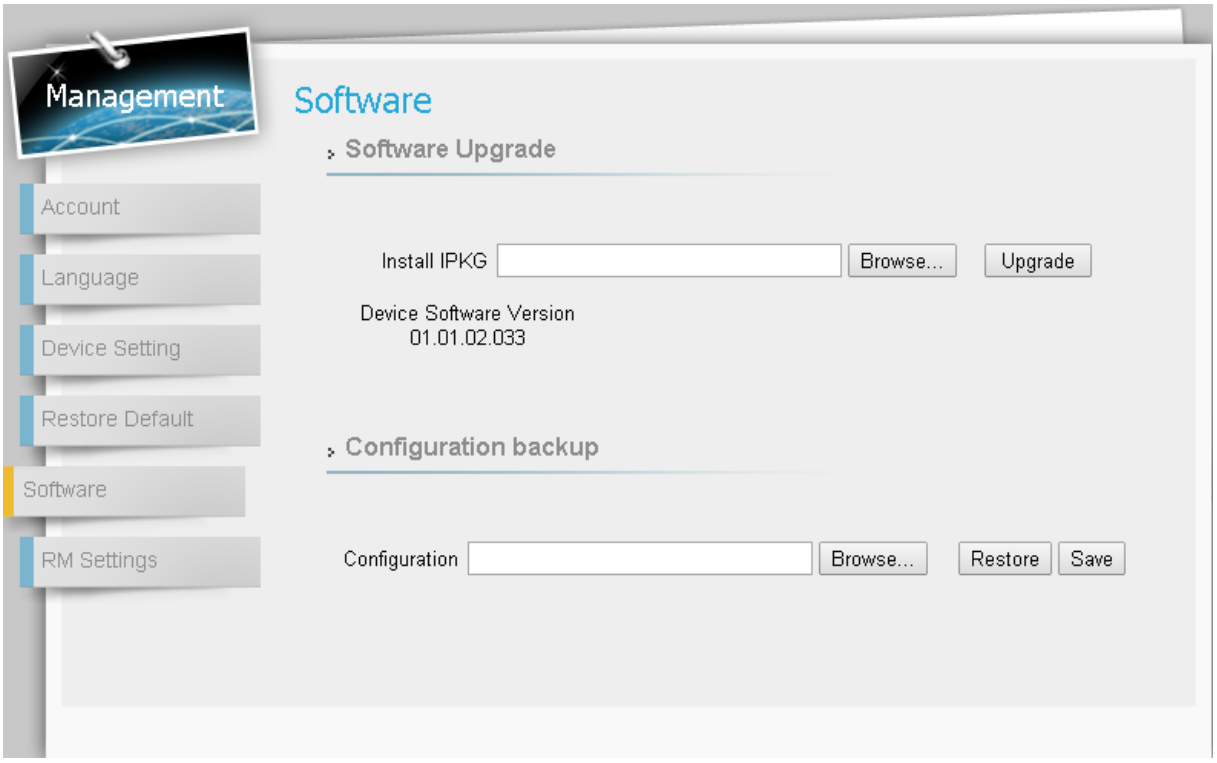


Rollback confirmation window



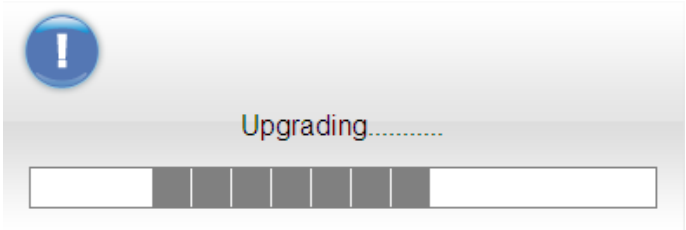
Rebooting window

Management | Software



Management > Software

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

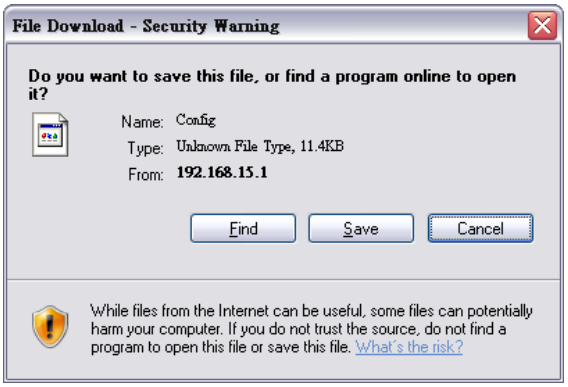


Management > Software > Upgrading Window

i	After pressing the "Upgrade" button, it will automatically reboot the CPE and upgrade the firmware with the specified file. You will be

	prompted to re-login to the CPE after the upgrade is complete.

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



File Download 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.

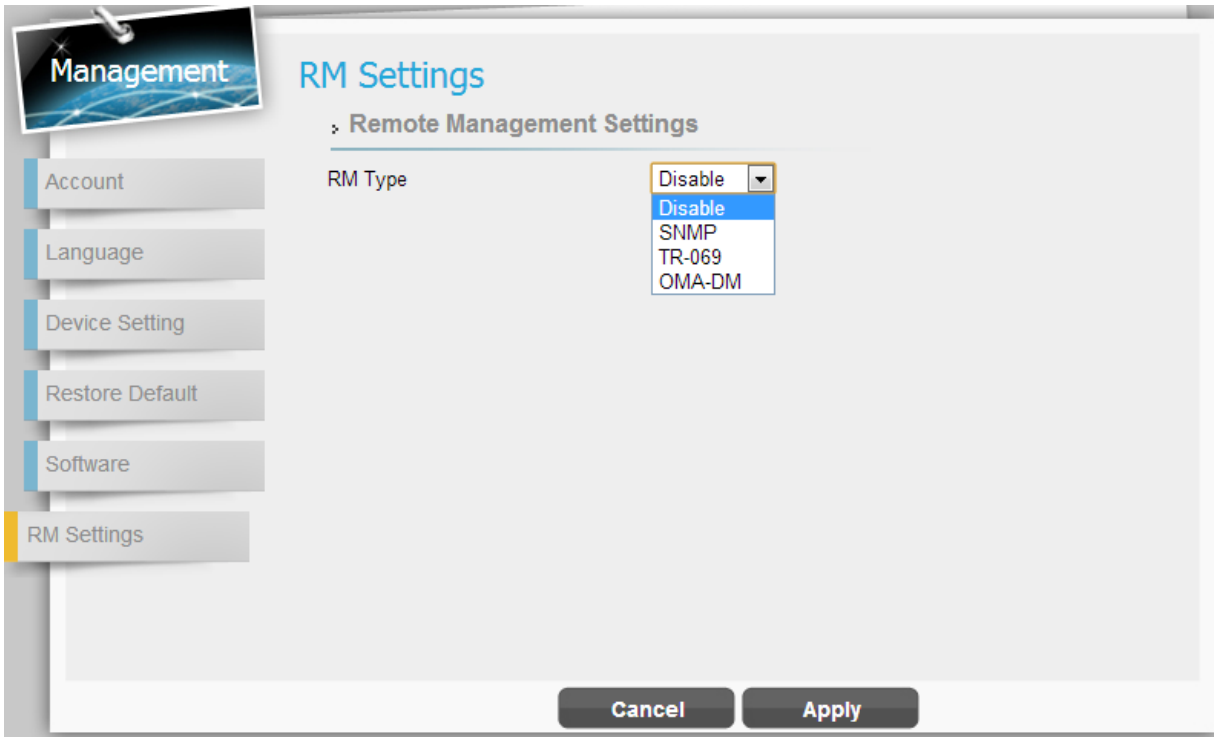
Management > Software > Upgrading Window

!	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.

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.

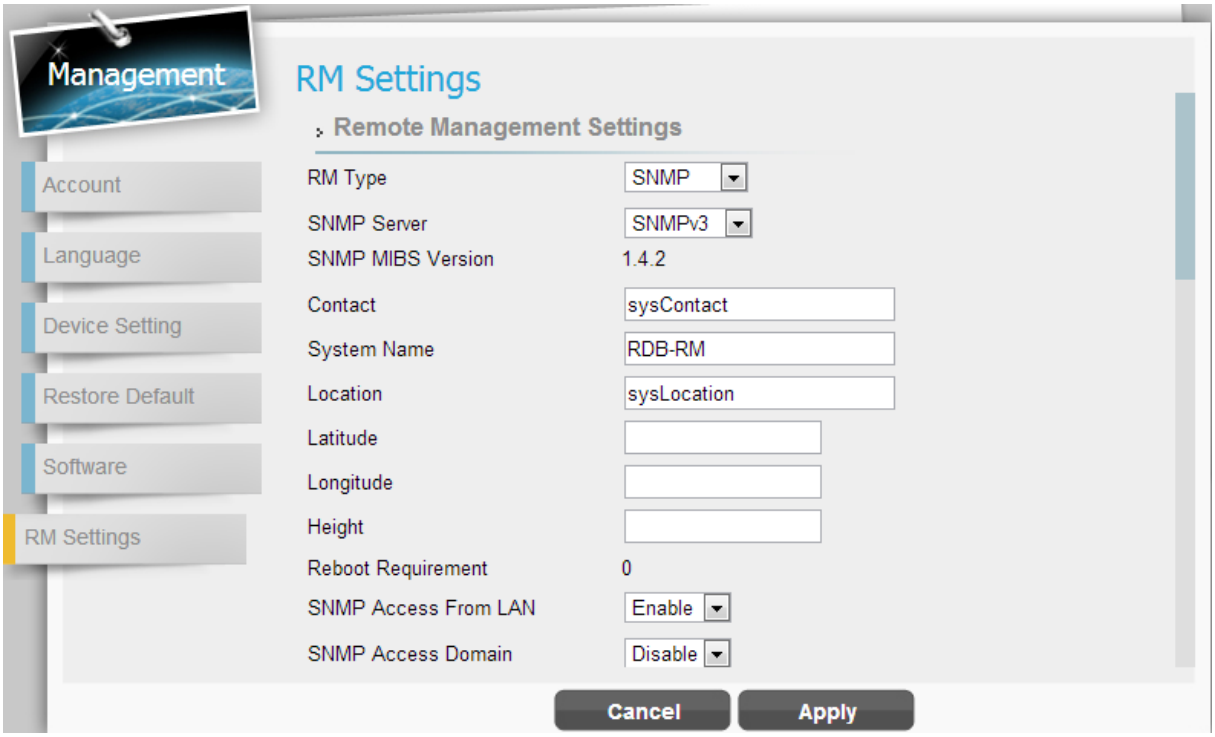
Management | RM Settings



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)**



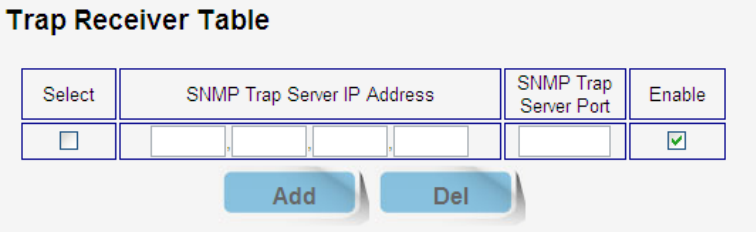
Management > RM Settings(SNMP)

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

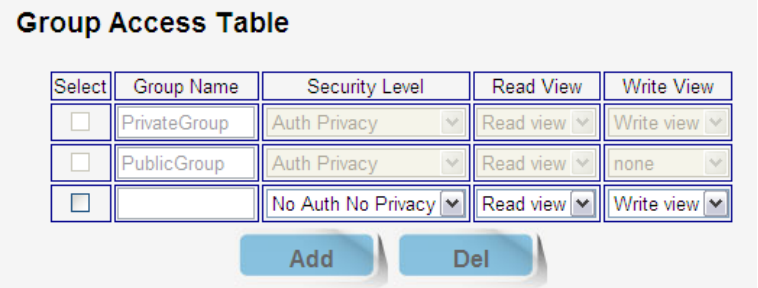
- **SNMP Server:** The type of the server. It includes SNMPv2c, SNMPv3.
- **SNMP MIBS Version:** 1.4.2
- **SNMP Read-Only Community (SNMPv2 only):** The "SNMP Community string" is like a user id or password that allows access to a router's or other device's statistics. If the community string is correct, 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.

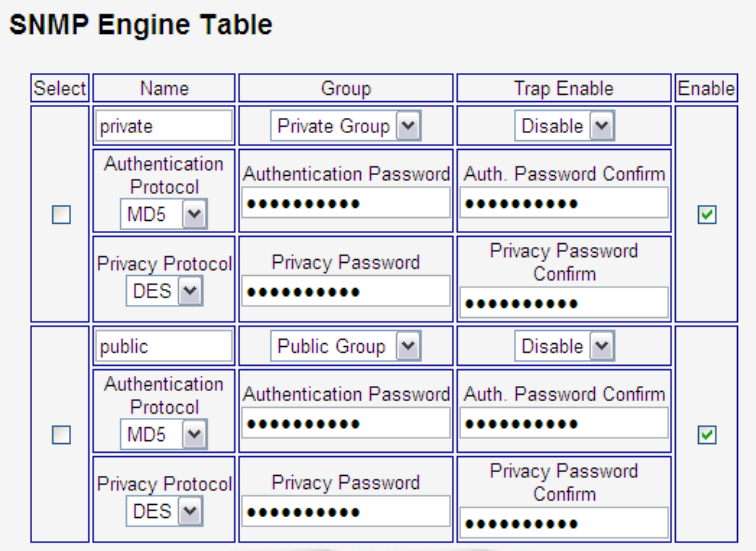
- **SNMP Trap Server IP Address:** As titled.
- **SNMP Trap Server Port:** As titled.
- **Contact:** The name or organization responsible for the switch.
- **System Name:** The name that identifies the SNMP agent.
- **Location:** A location for the SNMP Agent.
- **Latitude:** A part of geo-location attributes.
- **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 snmpEngineID was last configured.
- **SNMP Engine Time (SNMPv3 only):** The number of seconds since the snmpEngineBoots counter was last incremented
- **Trap Receiver Table (SNMPv3 only):**



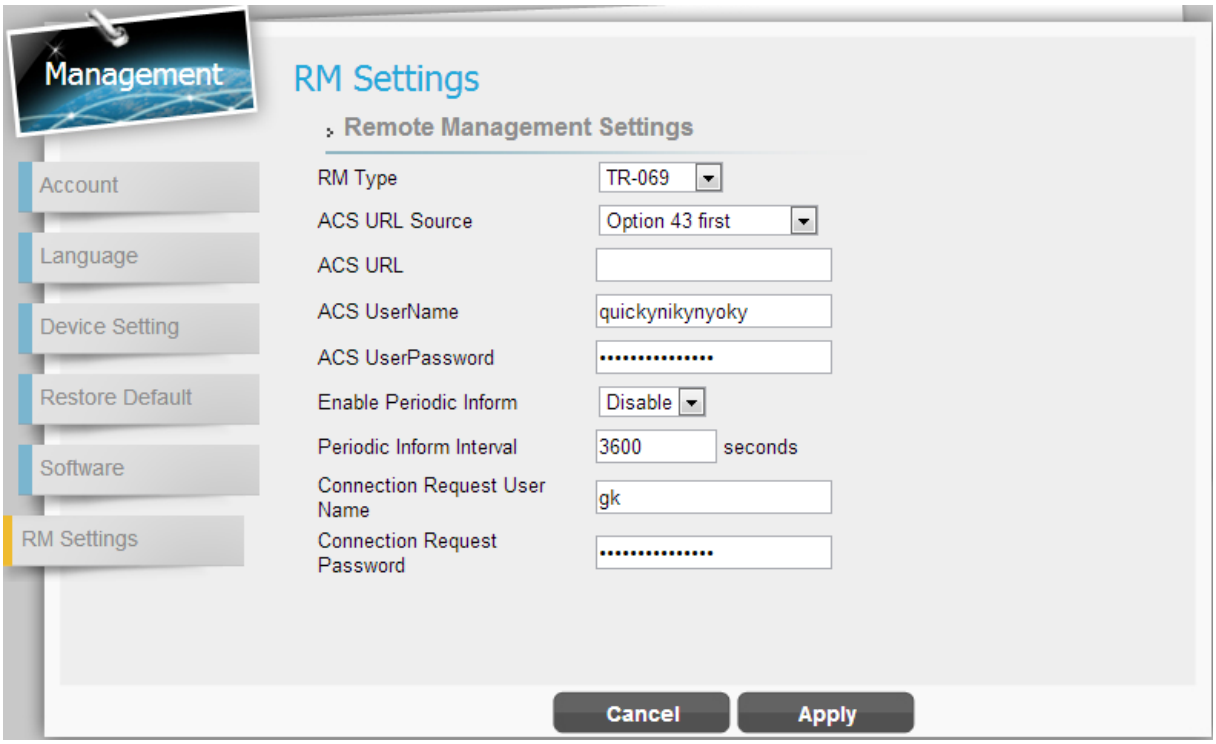
- **Group Access Table (SNMPv3 only):**



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



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



Management > RM Settings(TR-069)

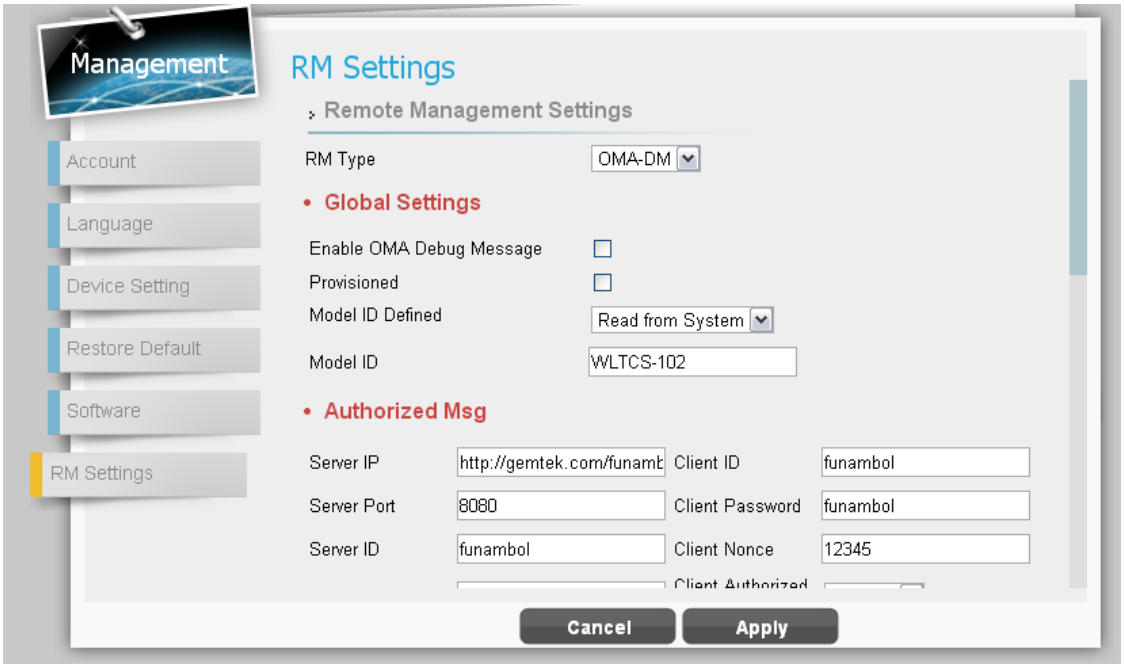
TR-069 is a technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. In the following, the word ACS stands for Auto Configuration Server.

- **ACS URL Source:** It includes "**Options 43 first**" and "**Only from WEB GUI**". If users select "Options 43 first" and CPE would get the ACS URL from the DHCP server if possible. Otherwise, CPE would take the URL provided by the users.
- **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 Password:** The password for authentication when CPE connects to ACS. (20 alphanumeric characters allowed)

- **Enable Periodical Inform:** Enable/Disable CPE to ask ACS periodically for configuration update.
- **Periodical Inform Interval:** The period to update the configuration if the "**Enable Periodical Inform**" is enabled.
- **Connection Request Username:** When ACS connects to CPE, CPE also needs to challenge ACS for authentication. ACS has to provide the username which matches this field. (20 alphanumeric characters allowed)
- **Connection Request Password:** When ACS connects to CPE, CPE also needs to challenge ACS for authentication. ACS has to send the password which matches this field. (20 alphanumeric characters allowed)

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

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



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 Msg:** Enable it, and then the debug message is printed in the console.
  - **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.

➢ **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**

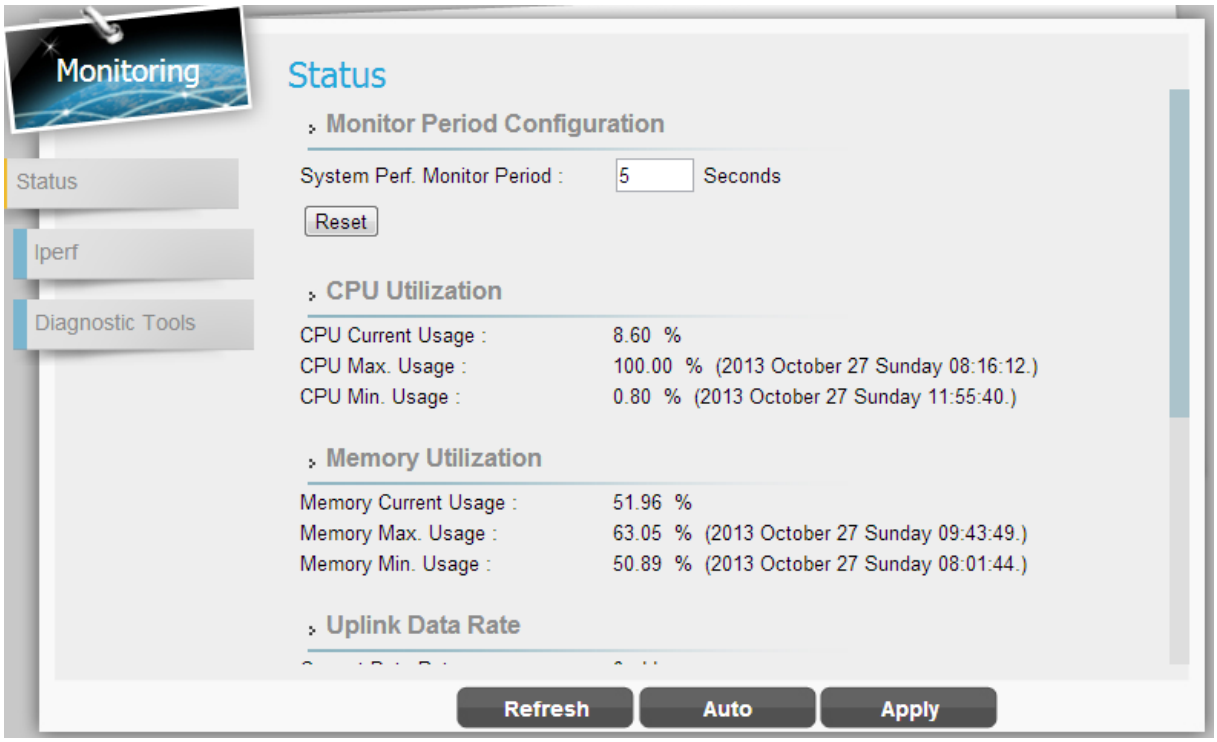
- **Client Initial Session:** If you press this button, the client would ask the server for

tasks to do immediately.

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

Monitoring

Monitoring | Status



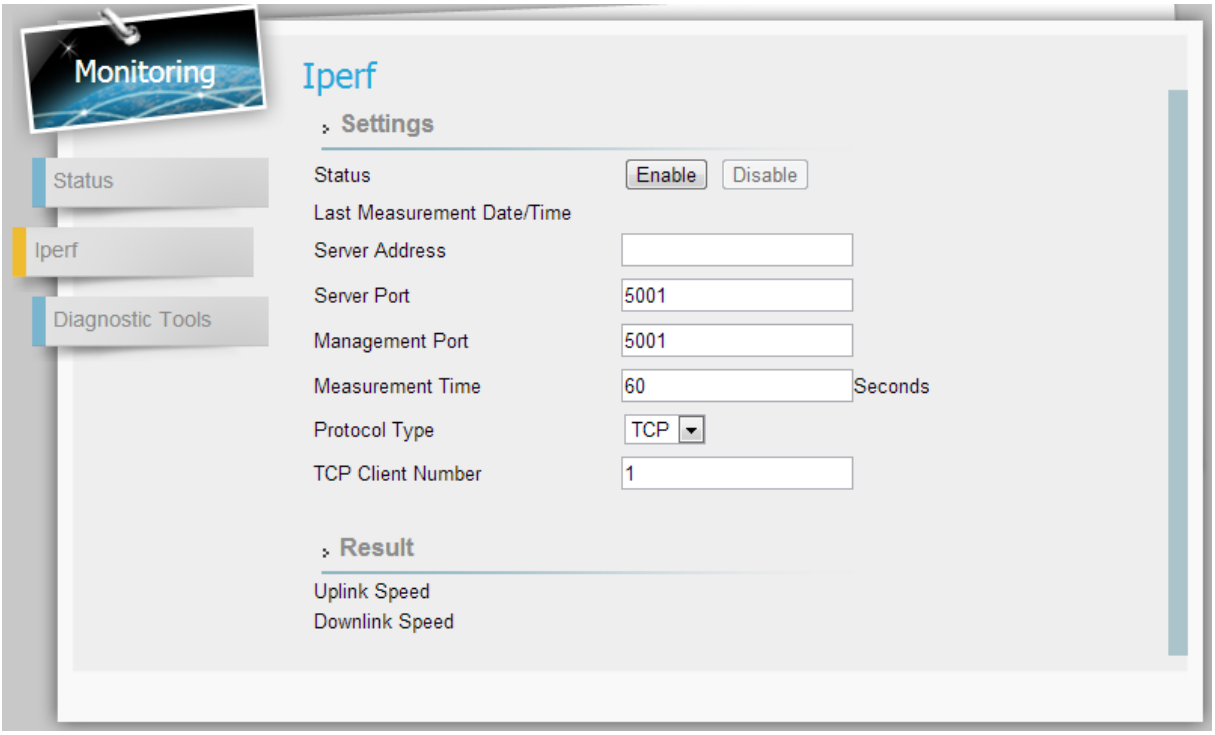
Monitor > Status

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

- Memory Min Usage:

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

Monitoring | Iperf



Monitor > Iperf

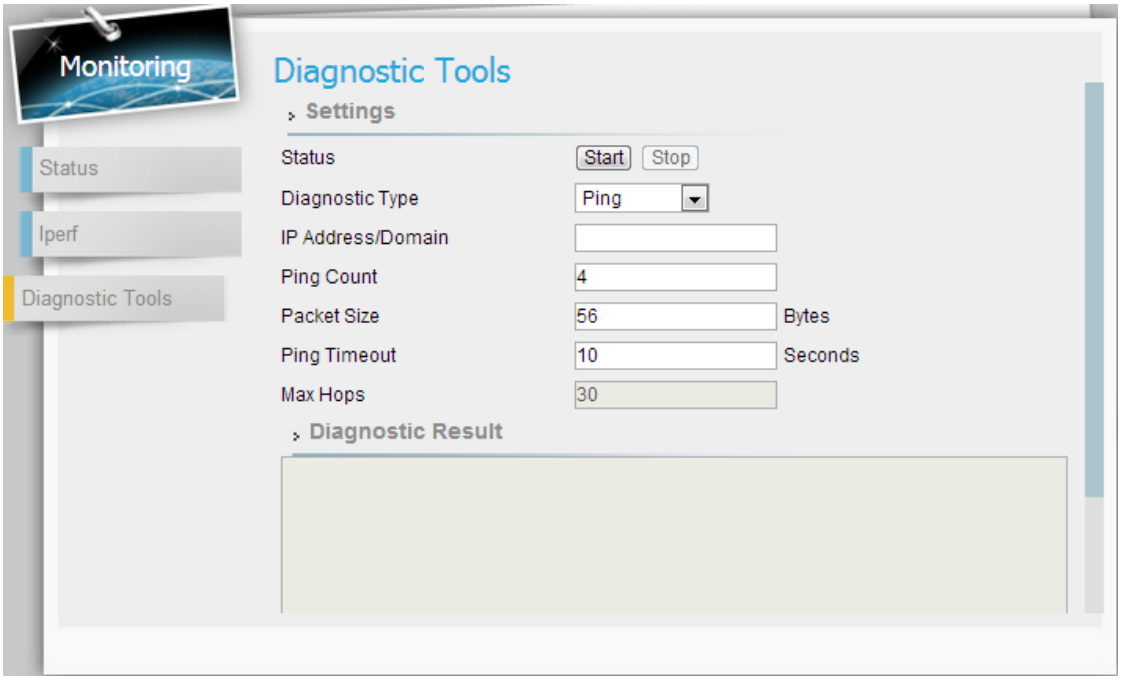
Iperf is a tool to measure network environment such as throughput, packet loss and delay jitter. Typically, to use Iperf, there should be a client and a server. The server opens a port and waits for clients to build the connection. Iperf in CPE only plays as a client.

- **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.
- **Monitor Period Configuration:** The result
  - Uplink Latency (only UDP)
  - Downlink Latency (only UDP)
  - Uplink Speed.
  - Downlink Speed.

Monitoring| Diagnostic Tools



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”.

Both ping and traceroute are using management interface only (not on data path).

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

About

About| Status

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.
- **Hardware Version:** As titled.
- **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 boot loader.
- **Bootrom Creation Date:** As titled.
- **WiMAX Frequency Range:** The supported WiMAX frequency range.
- **LTE Support Band:** The supported LTE band.