APEX Outdoor CPE

User Manual

Model: AOL-J912

4G LTE Cat 12 Outdoor CPE

LTE Network Bands

B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20
B21/B25/B26/B28/B29/B30/B32/B38/B39B40/B41/B66

Version 1.9, July 21, 2022

User Manual - Subject to change and edits due to continual product improvements. Instructions, specifications and other information is confidential until product launch and subject to change without notice.

Contents

Package Contents

The following items can be found in your package:

- AOL-J912 4G LTE Outdoor CPE
- Power cord with POE Injector
- Mounting Accessories (mount brackets with screws for Pole and/or Wall mount)
- Quick Start Guide

Note: Make sure that the package contains the above items. If any of the listed items are damaged or missing, please contact ATEL distributor/Service Provider.

Conventions

Any occurrence of “Device”/”Router”/”ODU” or “J912” in this User Manual, refers to the AOL-J912 4G LTE Outdoor CPE.

Chapter 1 Introduction

This chapter introduces what the functions of AOL-J912 and reviews its appearance. This chapter contains the following sections:

- Device Overview
- Panel Layout

1.1 Device Overview

The AOL-J912 is designed to meet the needs of Small Office/Home Office (SOHO) networks for high-speed data services over 4G LTE/LTE-A networks. This device is specially designed to be installed outside (like on a roof). External walls receive better 4G LTE signals and feed them into the home or internal living space via an Ethernet cable using the POE feature. It is a great product for users who have poor network signals indoors but want higher data speeds.

The J-Series is a Category-12 LTE device, which can provide download and upload speeds up to 600Mbps and 75Mbps respectively. It is also simple and convenient to set up and configure this device via its intuitive Online Device Portal (WebGUI).

1.2 Main Features & Interface

- Supports 4G LTE/LTE-A Network Supported Bands

  B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20/B21/B25/B26/B28/B29/B30/B32/B38/B39B40/B41/B66

- LTE UE Category 12
- Supports High-Speed data download and upload up to 600Mbps and 75Mbps respectively.
- 1 x RJ45 Gigabit Ethernet Port with passive POE
- Built-in Antennas with 2x2 LTE MIMO support.
- 2FF standard SIM card support.
- Reset Button
- Easy-to-use web management interface (WebGUI).
- 4 x LED Indicators for better understanding of device status.
- POE Injector (AC input: 110V~240V and DC output: 48V-56V; 1.5-meter cable) with POE and Data Port.
- Wall/Pole Mount Supported
- IP67 Compliance

1.3 Panel Layout

1.3.1 Front Panel

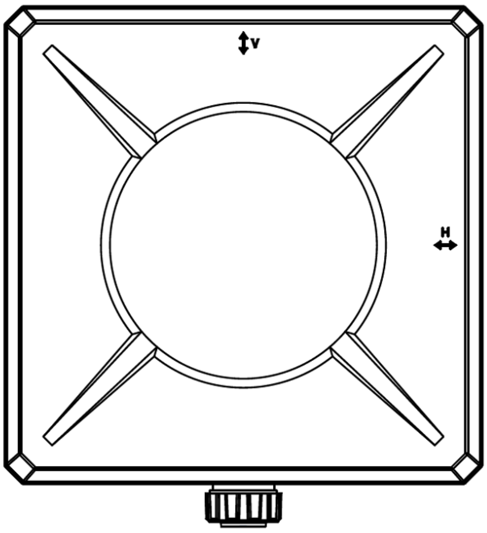


Figure 1. Front Panel Sketch (Dimensions are 265 x 265mm)

You can see Horizontal & Vertical indicators engraved on the housing surface for help during installation/mounting.

1.3.2 The Rear Panel

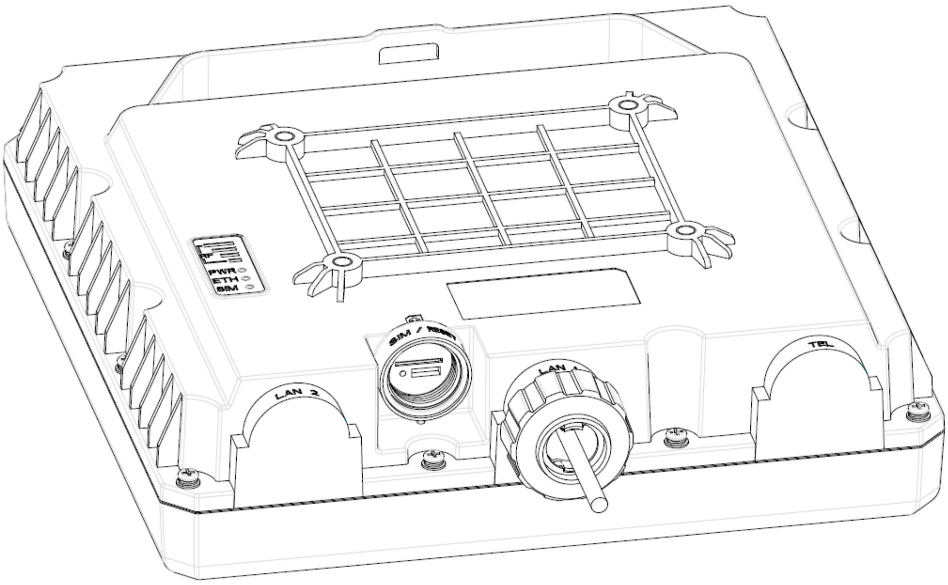


Figure 2. Rear Panel Sketch

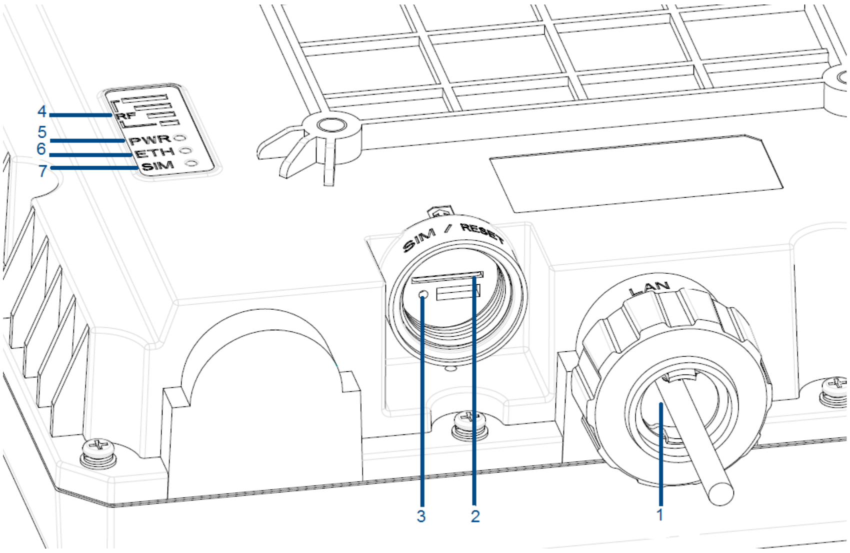


Figure 3. Interface & LEDs Location

The following parts are located on the rear panel (as marked with numbers):

1. **Ethernet Port**: indicates the location for the Ethernet Cable to connect.
2. **SIM Slot**: indicates the U-SIM card slot location.
3. **Reset Key:** indicates the location of the Reset key to perform factory resets.
4. **RF/Signals:** indicates the level of signal being received.
5. **PWR:** indicates the device power status.
6. **ETH:** indicates Ethernet/LAN status.
7. **SIM:** indicates U-SIM card status.

🔔 *You might see differences in the LED indicator behavior than what is described below due to continuous product development to meet customer requirements.*

LED	Status	Color	Description
RF/Signal	4-Bar	Green	Best receiving signals, SINR > 11dB
	3-Bar	Green	Good receiving signals, SINR 5 ~ 10dB
	2-Bar	Green	Normal receiving signals, SINR 1 ~4dB
	1-Bar	Green	Weak receiving signals, SINR - 2 ~ 0dB
	No Bar	-	No/Very Weak receiving signals, SINR < - 2dB
PWR	On	Green	Device is Powered On
	Off	-	Device is Powered Off
ETH	On	Green	Ethernet/LAN connection is established.
	Off	-	Ethernet/LAN connection is not established.
SIM	On	Green	SIM card is inserted/detected.
	Off	-	SIM card is not inserted/detected.

1.3.3 General Application of this Device

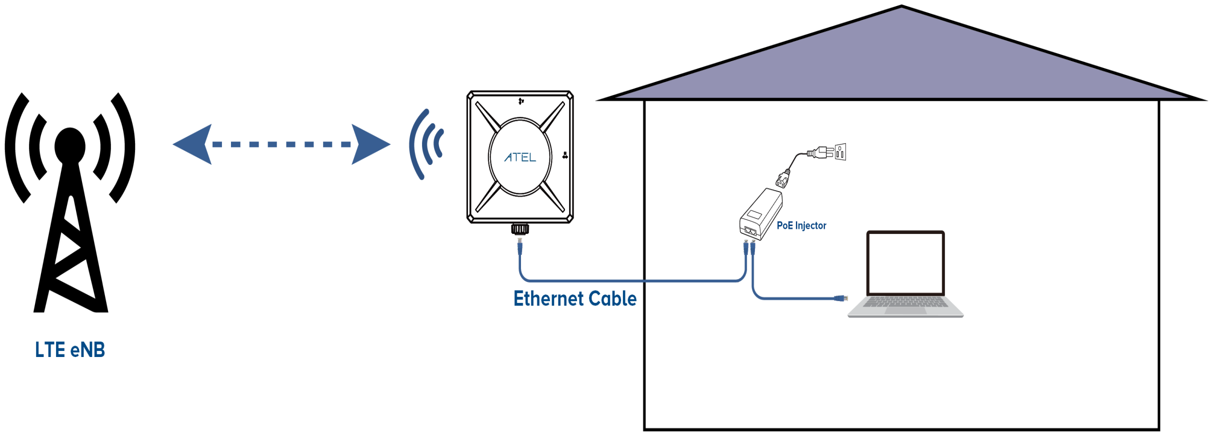


Figure 3. AOL-J912 connected to a PC directly via the POE Injector.

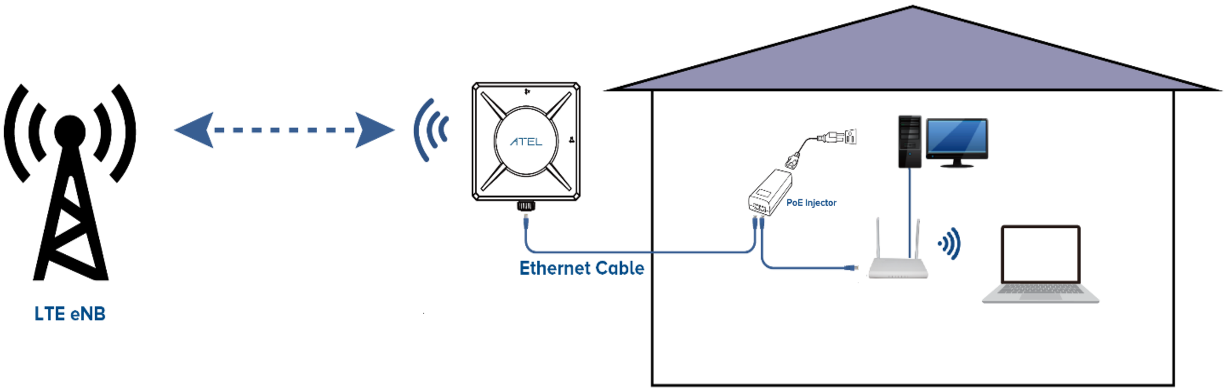


Figure 4. AOL-J912 connected to a Wi-Fi Router via the POE Injector.

Chapter 2 Quick Setup Guide

2.1 System Requirements

- Active SIM card with data enabled.
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors.
- Web browser, such as Microsoft Internet Explorer, Mozilla Firefox or Apple Safari.

2.2 Installation Environment Requirements

- The ODU should be placed outside and facing an open area towards an eNodeB/Cell Tower. Obstructions such as concrete walls, glass partitions or wooden walls can affect the transmission and reception of network signals.
- Keep the ODU away from household electrical appliances that produce strong electric or magnetic fields such as satellite dishes or antennas.
- Operating Temperature: -30℃~60℃
- Operating Humidity: 5%~95%

2.3 Setup the Device

The device supports high-speed data over 4G LTE networks. By default, the device will attempt to connect over available 4G networks, and the user can access to Internet on a connected computer/PC (note that an active SIM and data plan may be required).

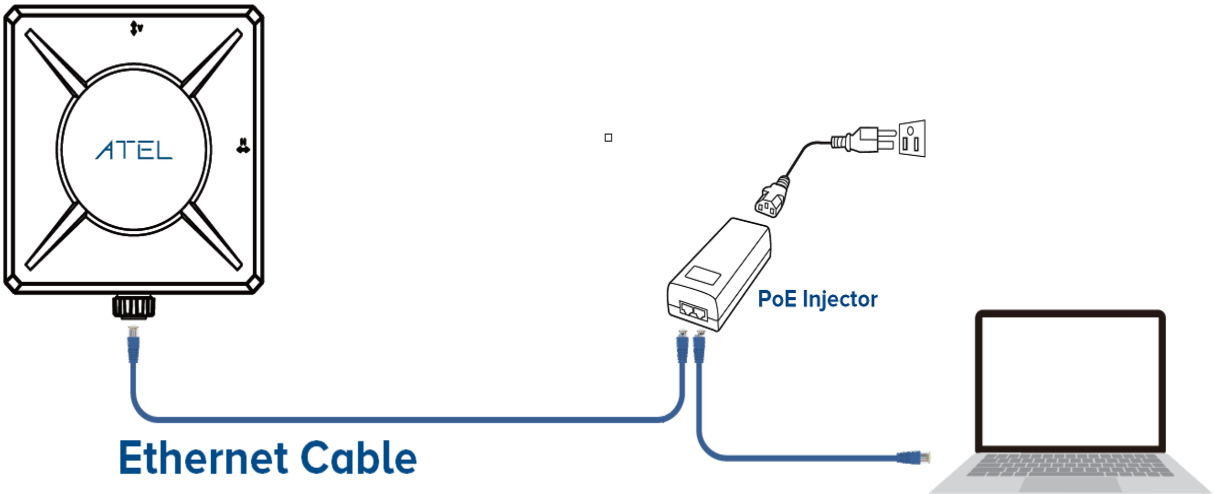


Figure 5. AOL-J912 connected to a PC via the POE injector.

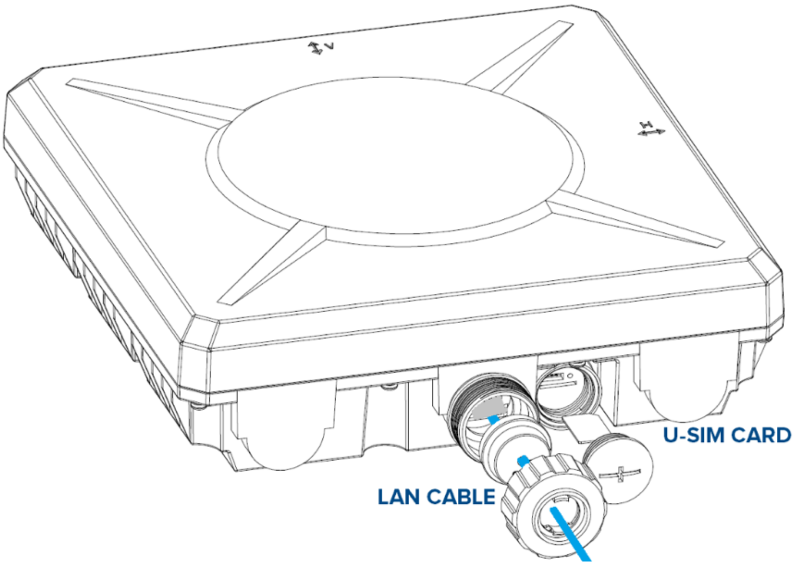
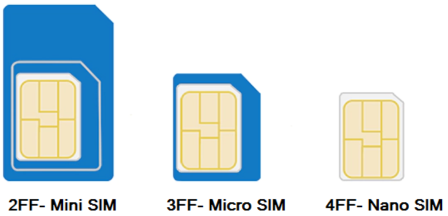


Figure 6. AOL-J912 SIM card & Ethernet cable connections.

1. Open the SIM Slot section (as shown in Figure 7) and insert the SIM card into the slot until you hear a click. Then close it.
   Note: Use a standard SIM card (2FF).



2. Open the Ethernet Port section and connect a LAN cable through the cap (the silicon shield to the RJ45 Port of the AOL-J912). Then close it.

3. Connect the Power cord to the POE injector and then make the remaining connections with an ethernet cable as outlined below:

   - **P+D/OUT Port:** The other end of the Ethernet/LAN cable connected with Outdoor CPE (AOL-J912) should be connected here. This helps supply Power to the ODU via ethernet using the Power over Ethernet feature). Use a 4 Pair standard Ethernet cable.
   - **Data/IN Port:** The other end of the Ethernet/LAN cable connected with your PC/Computer should be connected here.
   - **PWR LED:** The “On” state indicates that the POE injector is receiving power.
   - **PoE LED:** The “On” state indicates that the Connected Outdoor CPE is powered On.

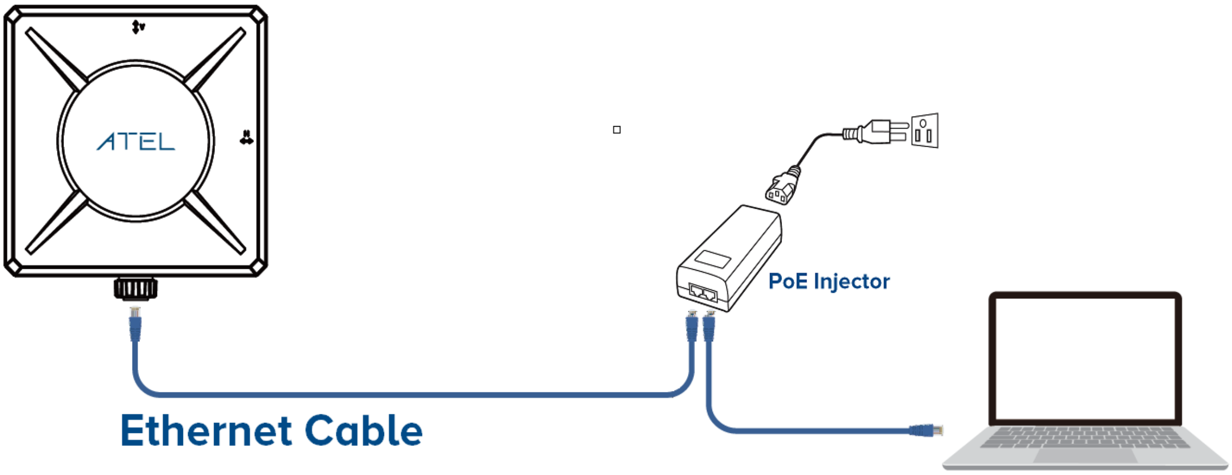


Figure 7. PoE Connection Setup

4. Once a connection is made as outlined above, you can find the outdoor CPE's PWR (Power) LED lit-up. That indicates that the CPE is powered On.

5. Verify the hardware connection by checking the LEDs' status. If the RF/Signal LED is on, your device found the signal and it is ready for use.

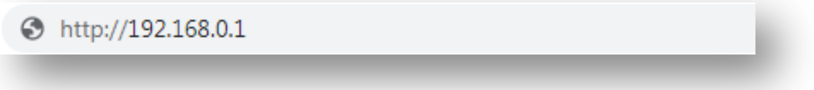
   Note: For better data speed, please make sure the Signal LED is lit with 3-4 bars. If not, change the location or direction of the device during installation for best available signals.

How to Access the Online Device Portal (WebGUI):

Please follow the steps below to access the device's online management portal (WebGUI) for the current configuration or to get network related information.

1. Once your Computer/PC is connected to the Outdoor CPE AOL-J912 over Ethernet, you can see the ETH (Ethernet) LED in the "On" state.

2. To access the configuration webpage, open a web-browser and type the default address, http://192.168.0.1 in the address field of the browser.



http://192.168.0.1

Figure 8. Login URL.

3. After a moment, a login window will appear. Enter **admin** for the Username and Password, both in all lower-case letters. Then click the Sign In button.

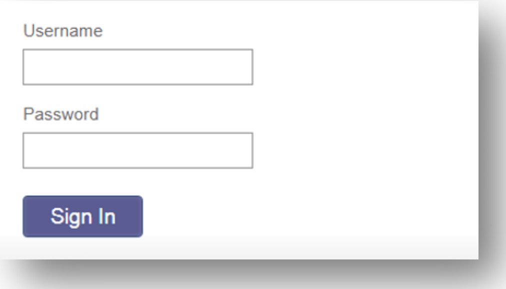
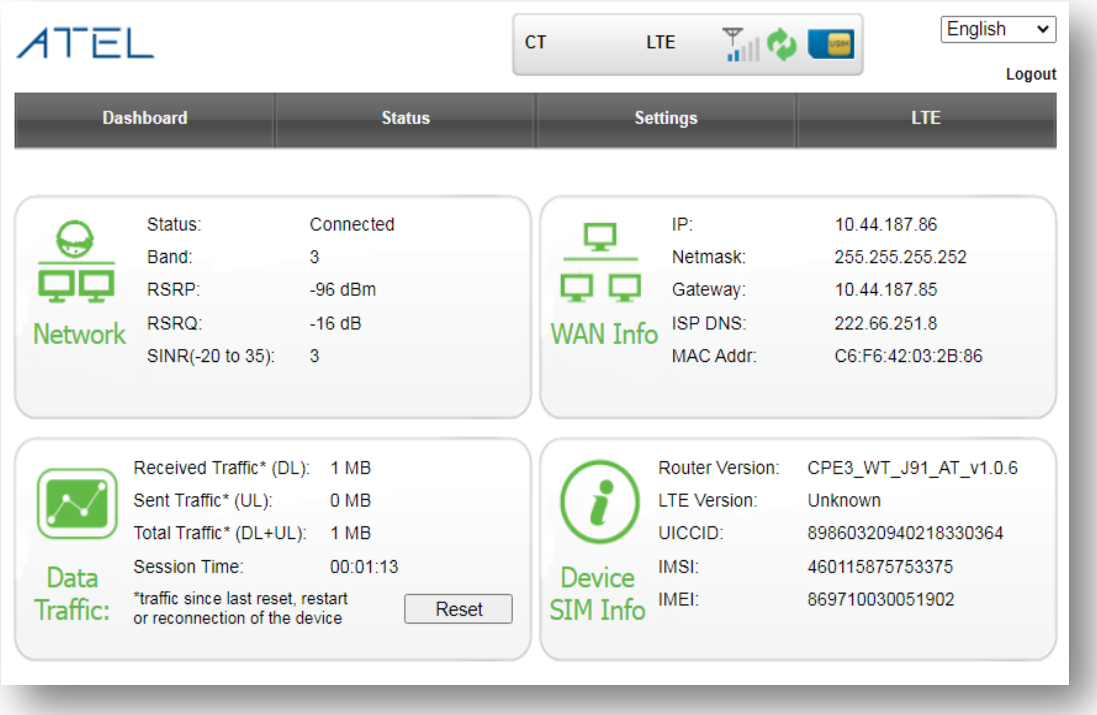


Figure 9. Login Window.

Note: If the above screen does not pop-up, try clearing your web browser cache memory. You can also try checking the connection with ping. Open the command prompt and input to **ping 192.168.0.1**. You should see the ping response if a LAN connection has been established.

4. Once you've successfully logged in, you will see a Dashboard page where all the basic configurations related to the device are presented for quick check (i.e. SIM status, Connection Status with Network and Network Parameters).



Network
Status: Connected
Band: 3
RSRP: -96 dBm
RSRQ: -16 dB
SINR(-20 to 35): 3

WAN Info
IP: 10.44.187.86
Netmask: 255.255.255.252
Gateway: 10.44.187.85
ISP DNS: 222.66.251.8
MAC Addr: C6:F6:42:03:2B:86

Data Traffic:
Received Traffic* (DL): 1 MB
Sent Traffic* (UL): 0 MB
Total Traffic* (DL+UL): 1 MB
Session Time: 00:01:13
*traffic since last reset, restart or reconnection of the device

Device SIM Info
Router Version: CPE3_WT_J91_AT_v1.0.6
LTE Version: Unknown
UICCID: 89860320940218330364
IMSI: 460115875753375
IMEI: 869710030051902

Figure 10. Dashboard Page

Your device is now ready for use.
For details about each form of installation, please refer here.

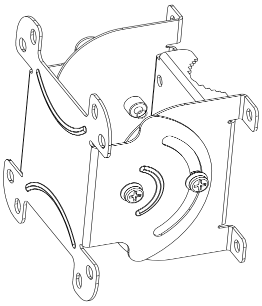
5. For an additional step, you can install the Outdoor CPE on a wall or Pole as per your needs for best signal reception/results. Refer to the installation guide (Chapter 3 of this User Manual).

Chapter 3 Installation Guide

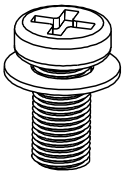
The AOL-J912 Outdoor CPE supports both Wall, as well as Pole mount installation.

3.1 Installation Kit

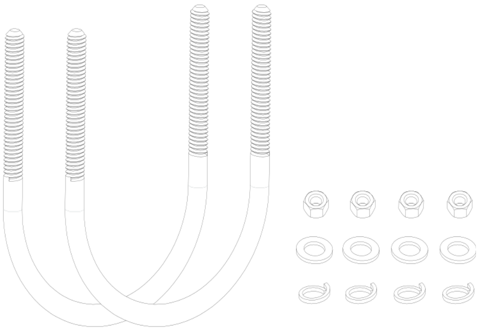
1. Mounting Bracket



2. #2 Phillips Head Screw x4



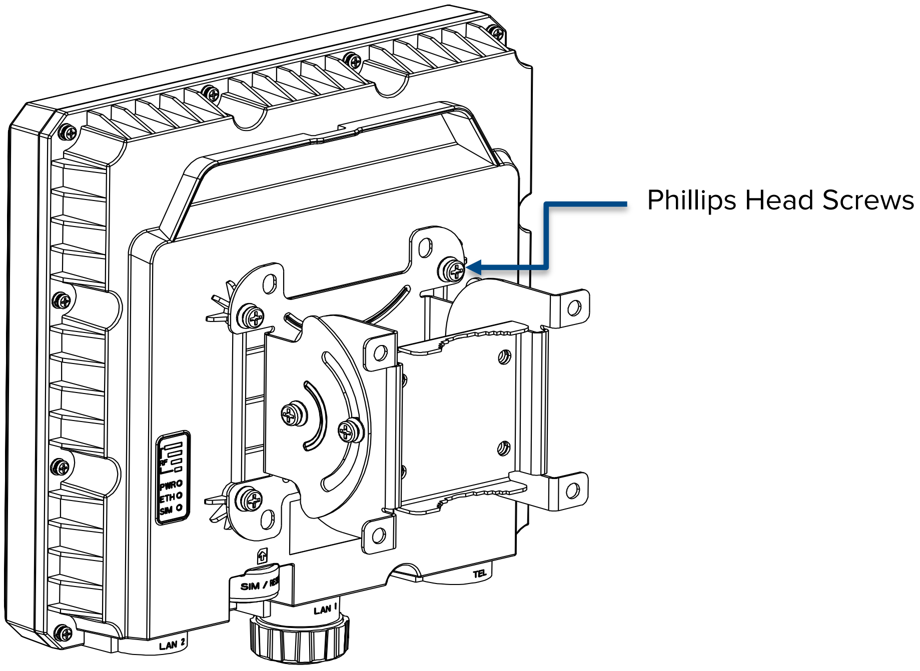
3. U-Bolt Clamp Set



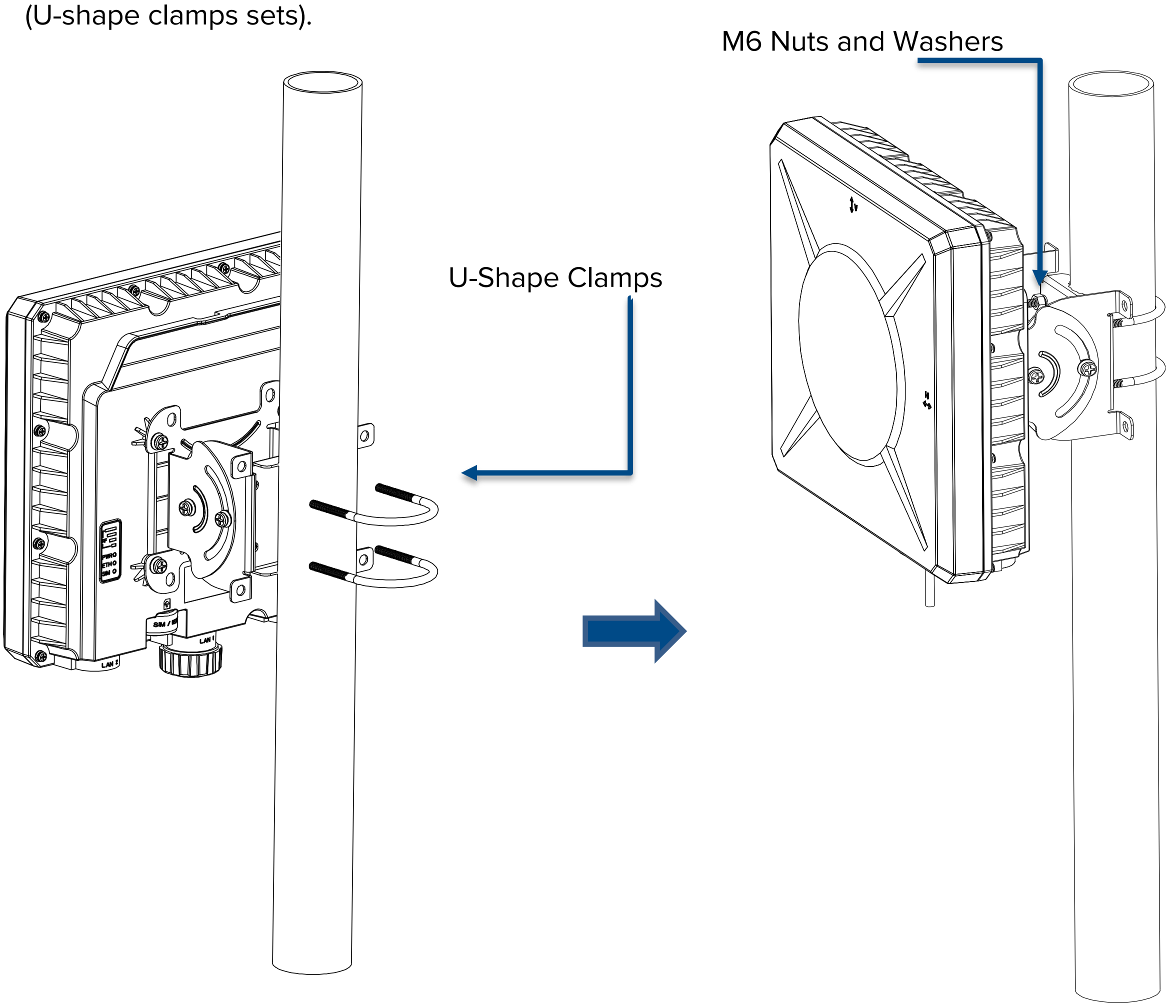
NOTE: Tools are not included in the installation kit. You will need a Phillips head screwdriver and M6 wrench to install (not included).

3.2 Pole Mount Installation Instructions

1. Attach the mounting bracket to the rear panel of the ODU using four #2 Phillips head screws.



2. Attach the other side of mounting bracket to the pole using the provided mounting ties (U-shape clamps sets).



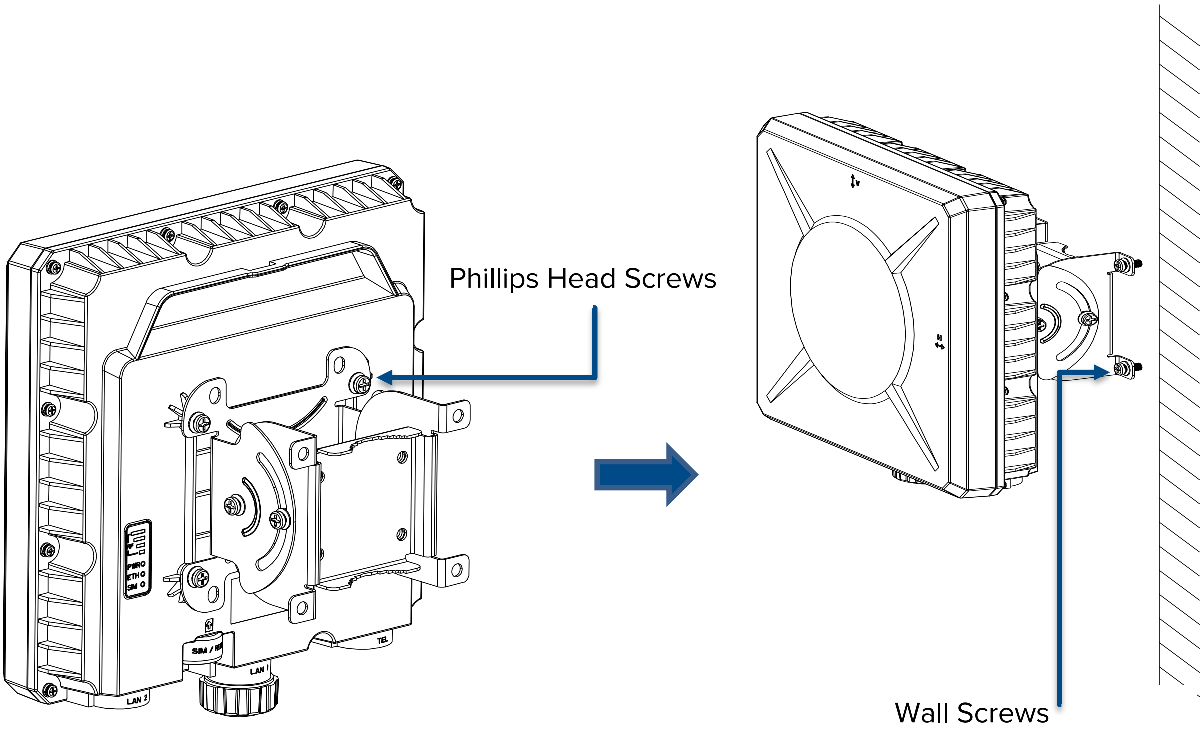
3.3 Wall Mount Installation Instructions

To Affix a mount bracket to the AOL-J912 rear panel:

1. Use four screws to attach the mounting bracket to the rear panel of the AOL-J912 CPE.
2. Place the mounting bracket fixed on the rear side of the AOL-J912 to the U-shaped bracket and use four screws to stack two mounting brackets together.
3. Position the AOL-J912 CPE at the desired angle and attach it with four screws.

To Affix a Mount bracket to a wall:

4. Place the mounting bracket against the wall in the desired position.
5. Use a 4mm drill bit to make four holes approximately 30mm deep, then insert four wall anchors into the holes.
6. Use four screws to attach the mounting bracket to the wall.



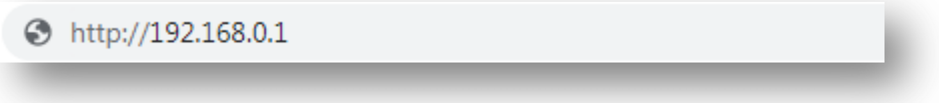
NOTE: Screws and installation tools for wall mounting are not included in the installation kit.

Chapter 4 Device Configurations

This chapter will cover each of the Online Device Portal's (WebGUI) key functions and the configuration procedure.

4.1 Login

1. To access the configuration utility, open a web-browser and type the default address **http://192.168.0.1** into the address field of the browser.



http://192.168.0.1

2. After a moment, a login window will appear. Enter "admin" for the Username and Password, both in lower case letters. Then click the **Login** button.

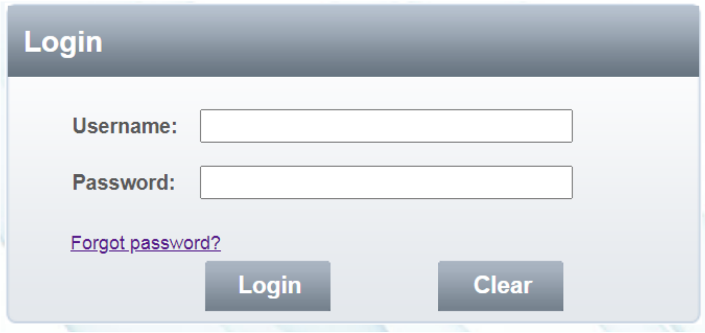


Figure 11. Web Login Window.

NOTE: Check device label for default password if you get any error with above credentials.

After your successful login, you will see the main menus on the top of the Web-based utility.

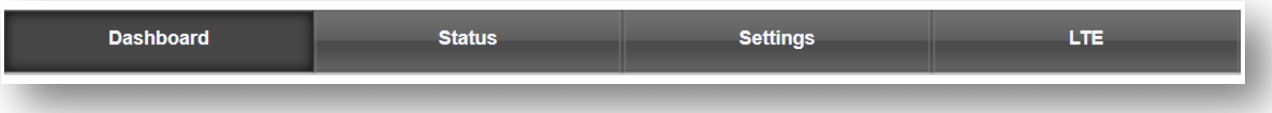
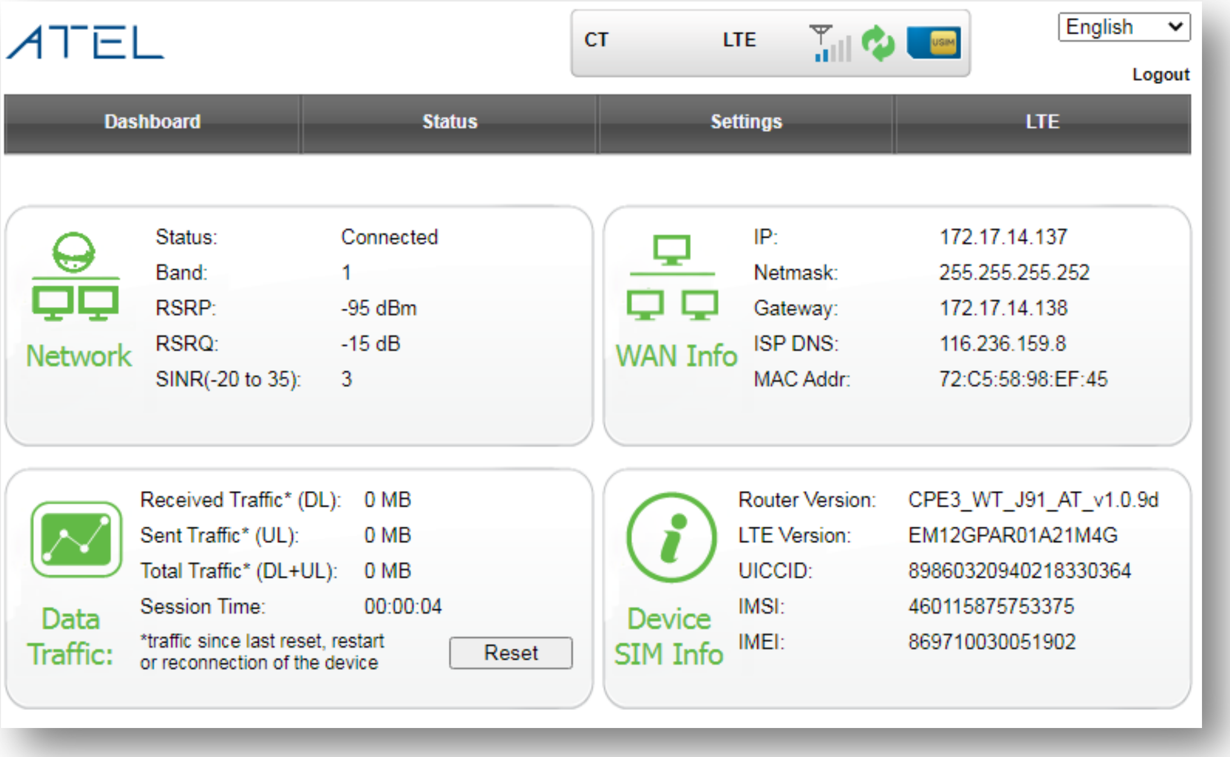


Figure 12. Main Menu Bar.

The menu interface includes Four sections/Submenus: **Dashboard**, **Status**, **Settings** and **LTE** You can access the device configuration through the menu page and modify the parameters according to your needs. The detailed explanations for each menu and their key functions are described below.

4.2 Dashboard

The dashboard menu page provides the current status of the device and important information about the device.



Status: Connected
Band: 1
RSRP: -95 dBm
RSRQ: -15 dB
SINR(-20 to 35): 3

IP: 172.17.14.137
Netmask: 255.255.255.252
Gateway: 172.17.14.138
ISP DNS: 116.236.159.8
MAC Addr: 72:C5:58:98:EF:45

Received Traffic* (DL): 0 MB
Sent Traffic* (UL): 0 MB
Total Traffic* (DL+UL): 0 MB
Session Time: 00:00:04
*traffic since last reset, restart or reconnection of the device

Router Version: CPE3_WT_J91_AT_v1.0.9d
LTE Version: EM12GPAR01A21M4G
UICCID: 89860320940218330364
IMSI: 460115875753375
IMEI: 869710030051902

Figure 13. Dashboard Menu.

This page has six sections that provide device information. It is very helpful for learning about your device's current status. Refer to the information below for more details.

- **Header**

  On the top/header section of the Online Portal page, some important details like connected Network Name, Signal Bars, Connection Status, SIM Card Status, Language Selection, and the logout button are displayed.

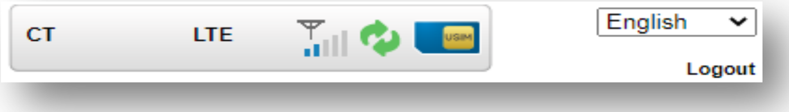


Figure 14. Device in Connected State with Network Example.

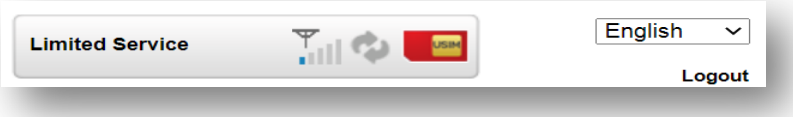


Figure 15. Device in Disconnected State with Network Example.

USIM Red Color indicates that the SIM card is either not inserted or failed to detect.

USIM Blue Color indicates that the SIM card is detected by the device.

🔄 Green Color indicates that the device is connected to an LTE network.

Logout Click on this button to log out from the Online Portal.

- **Network**

  Displays the current Connection Status, connected Band, Cell ID, and Network signal parameters (i.e. RSRP, RSRQ & SINR).

- **WAN Info**

  Displays the PDP/WAN configuration (i.e. WAN IP, Gateway IP & DNS IP) acquired if the device is attached to network.

- **Data Traffic**

  Displays the Data traffic statistics for Total, Sent, Received and Session Time. You can reset statistics by clicking the Reset Button.

- **Device/SIM Info**

  Displays the device Software version, IMEI, and SIM card details (i.e. UICCID, IMSI).

4.3 Status

In this menu, you will find the submenus: **WAN Status**, **Network Status**, Neighbor Cell, **Software**, **Device List** & **Statistics**.

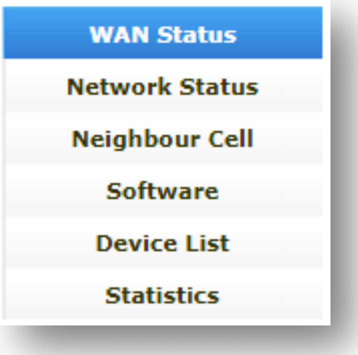
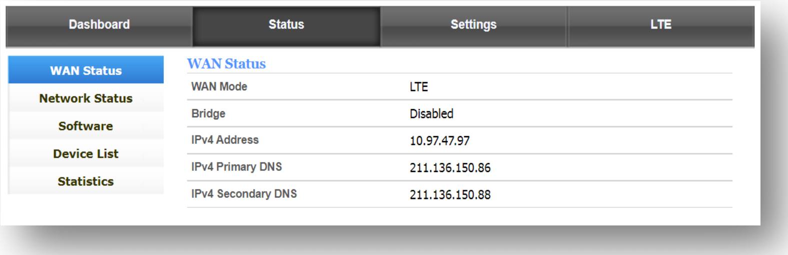


Figure 16. Submenu under Status Menu.

4.3.1 WAN Status

With this menu, you can view WAN information about the device if it is connected to a network. If not, no information will be available here.



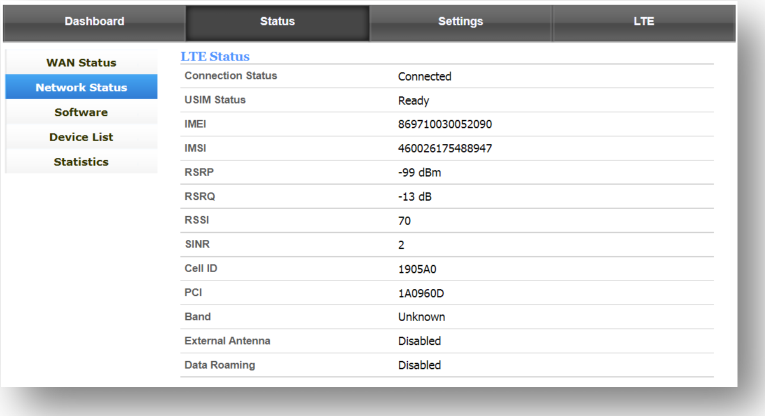
WAN Status

WAN Mode	LTE
Bridge	Disabled
IPv4 Address	10.97.47.97
IPv4 Primary DNS	211.136.150.86
IPv4 Secondary DNS	211.136.150.88

Figure 17. WAN Status.

4.3.2 Network Status

With this menu, you can view network and device related information such as, Device Connected State, Cell ID, Device IMEI, SIM Card Status, IMSI, and Network Parameters (i.e. RSRP, RSSI, RSRQ, SINR).



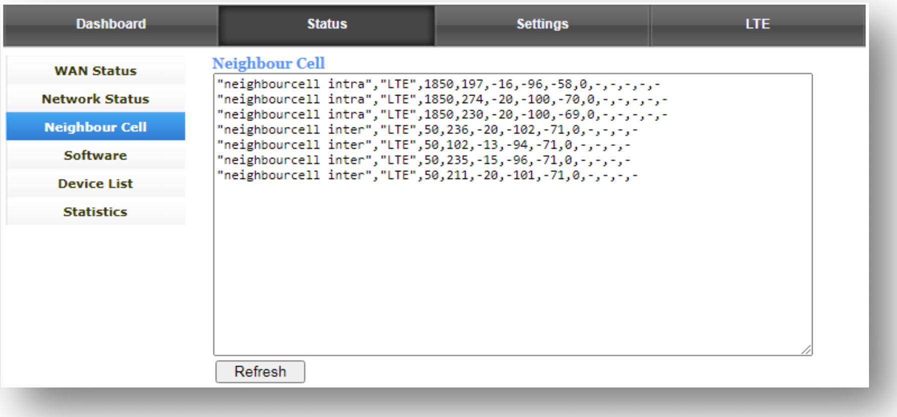
LTE Status

Connection Status	Connected
USIM Status	Ready
IMEI	869710030052090
IMSI	460026175488947
RSRP	-99 dBm
RSRQ	-13 dB
RSSI	70
SINR	2
Cell ID	1905A0
PCI	1A0960D
Band	Unknown
External Antenna	Disabled
Data Roaming	Disabled

Figure 18. Network Status.

4.3.3 Neighbor Cell

With this menu, you can view neighbor cell related information such as RAT Type State, Cell ID, EARFCN, and network parameter. This information is useful when you want to use PCI lock feature where device will lock to a specific Cell.



Neighbour Cell

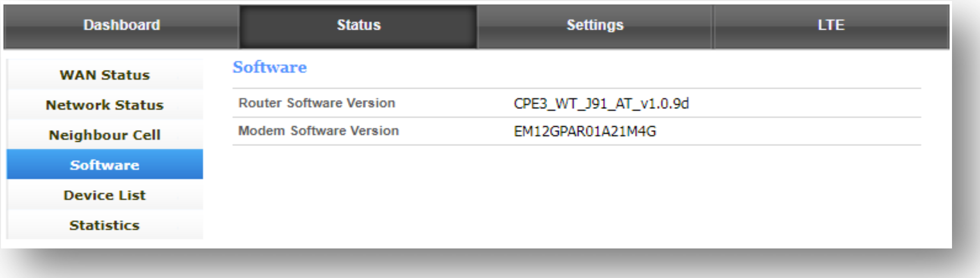
```
"neighbourcell intra","LTE",1850,197,-16,-96,-58,0,-,-,-,-,-
"neighbourcell intra","LTE",1850,274,-20,-100,-70,0,-,-,-,-,-
"neighbourcell intra","LTE",1850,230,-20,-100,-69,0,-,-,-,-,-
"neighbourcell inter","LTE",50,236,-20,-102,-71,0,-,-,-,-
"neighbourcell inter","LTE",50,102,-13,-94,-71,0,-,-,-,-
"neighbourcell inter","LTE",50,235,-15,-96,-71,0,-,-,-,-
"neighbourcell inter","LTE",50,211,-20,-101,-71,0,-,-,-,-
```

Figure 19. Neighbor Cell information.

Click on the Refresh button to refresh the values.

4.3.4 Software

With this menu, you can view the device’s current Software Version.



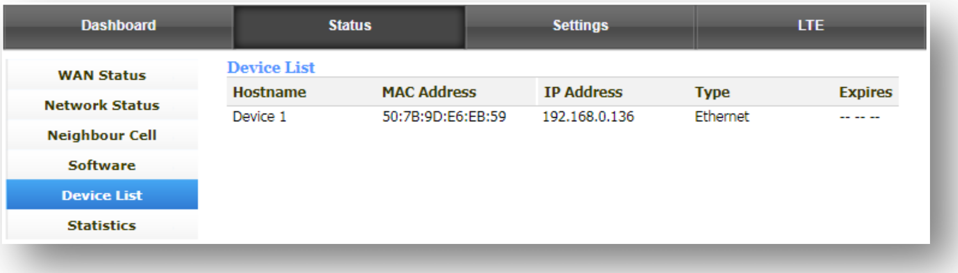
Software

Router Software Version	CPE3_WT_J91_AT_v1.0.9d
Modem Software Version	EM12GPAR01A21M4G

Figure 20. Device Software Information.

4.3.5 Device List

With this menu, you can view the connected device/PC details, such as, Hostname & MAC Address, IP Address allotted on local side, Connection interface/Type, Ethernet, and Expires time.



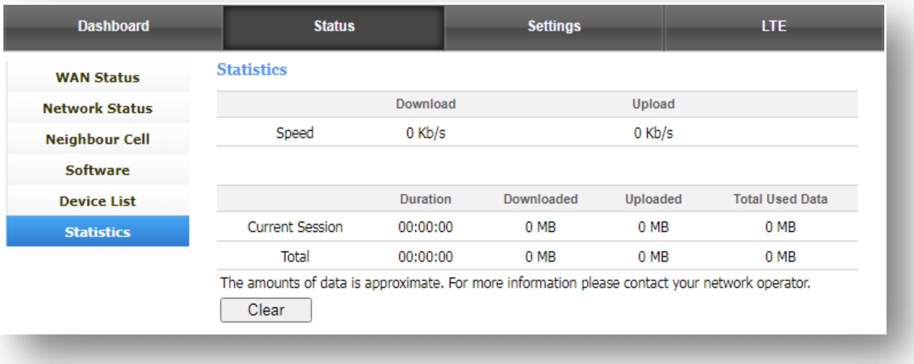
Device List

Hostname	MAC Address	IP Address	Type	Expires
Device 1	50:7B:9D:E6:EB:59	192.168.0.136	Ethernet	-- -- --

Figure 21. Connected Device List on LAN.

4.3.6 Statistics

With this menu, you can view the current data traffic statistics, as well as the total data sessions made by the device. You can also see real time download and upload speeds between the device and network in Kilobits (Kb/s) per second.



Statistics

	Download	Upload
Speed	0 Kb/s	0 Kb/s

	Duration	Downloaded	Uploaded	Total Used Data
Current Session	00:00:00	0 MB	0 MB	0 MB
Total	00:00:00	0 MB	0 MB	0 MB

The amounts of data is approximate. For more information please contact your network operator.

Figure 22. Data Statistics.

Click the **Clear** button to reset all data statistics.

4.4 Settings

With this menu, you can view the Submenus: **Basic**, **Advanced** and **Security**. These are important and useful features, which can help you to edit the current configuration of the device as per your needs and requirements.

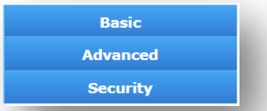


Figure 23. Submenus under Settings Menu.

Click any of the submenus and you will be able to configure the corresponding function. The detailed explanations for each submenu are provided below.

4.4.1 Basic

With this menu, you can view the following basic menus: **Management**, **LAN/DHCP** and **Manual Upgrade**. These menus will allow you to review features such as; Reboot & Reset, Configure LAN, and SW upgrade on the device.

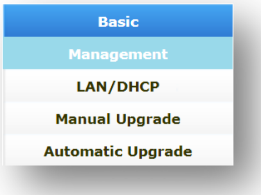
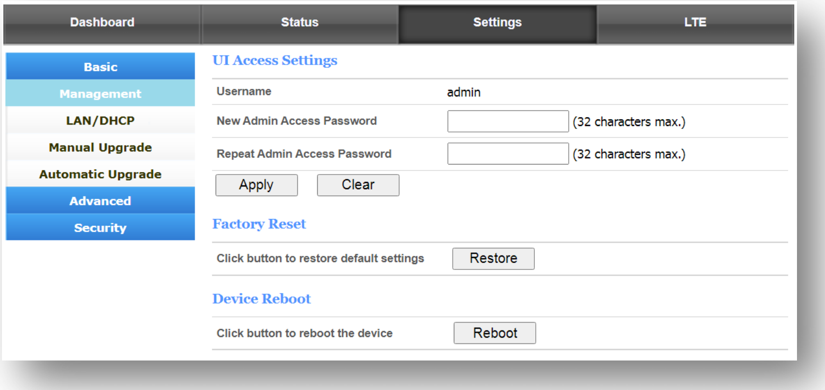


Figure 24. Submenu under “Basic”.

4.4.1.1 Management

With this menu, you can set a new password for the Online Portal (WebGUI) access, Reset, and reboot the device.



UI Access Settings

Username	admin
New Admin Access Password	(32 characters max.)
Repeat Admin Access Password	(32 characters max.)

Factory Reset

Click button to restore default settings

Device Reboot

Click button to reboot the device

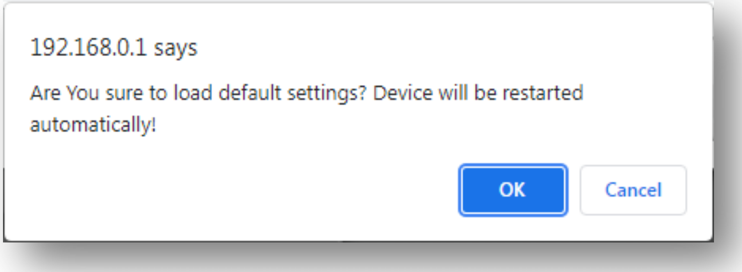
Figure 25. Management Menu.

- **UI Access Settings**
  Here you can set the new password for your Online Portal (WebGUI). Input the new password in the New Admin Access Password box and input it again in the Repeat Admin Access Password box and click on **Apply** to save the change. Click on **Clear** to cancel or ignore the changes.

Note: The default username and password are admin. We strongly recommend that you change the password when setting up your device to avoid any unwanted access.

- **Factory Reset**
  Here you can perform the factory reset, which will erase all configurations made on the device and revert them to factory default configurations. This feature can be useful during troubleshooting.

  To reset the device, click on the **Restore** button. You will get a prompt message to select **OK** to continue or **Cancel** to abort the reset function.



192.168.0.1 says

Are You sure to load default settings? Device will be restarted automatically!

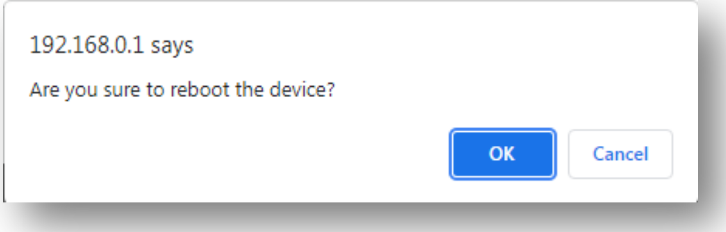
Figure 26. Message prompt for Reset.

Once you've clicked OK, the device will start the reset function and reboot itself with factory default configurations.

Note: All your changed configurations will be lost after reset and the device will revert to the factory default configurations. Make sure the device's power supply is uninterrupted during Reset.

- **Device Reboot**
  Here you can do the soft reboot, which will help to do power cycles to the device. This feature can be useful during troubleshooting.

  To reboot the device, click the **Reboot** button. You will get a prompt message to select **OK** to continue or **Cancel** to abort the reboot function.



192.168.0.1 says

Are you sure to reboot the device?

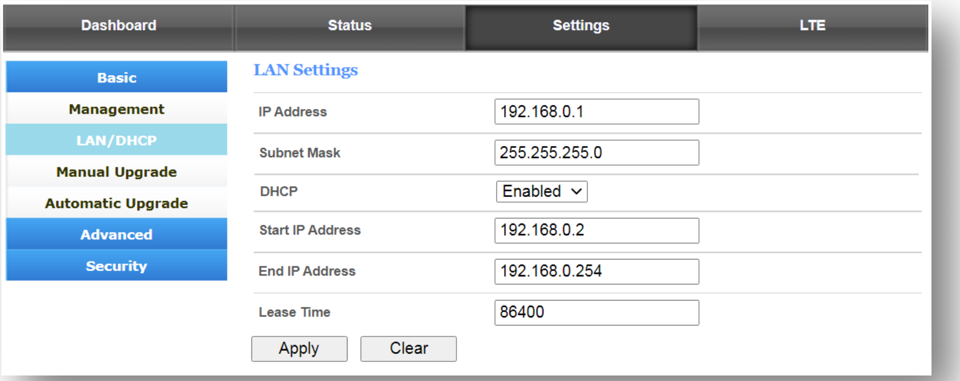
Figure 27. Message prompt for Reboot.

Once you've clicked OK, the device will reboot itself.

Note: Make sure the device's power supply is uninterrupted during reboot.

4.4.1.2 LAN/DHCP

With this menu, you can configure the Local area network (LAN) of the device from default values to your preferred configurations.



LAN Settings

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP	Enabled
Start IP Address	192.168.0.2
End IP Address	192.168.0.254
Lease Time	86400

Figure 28. LAN/DHCP Configuration.

- **IP address:**
  Define your desired IP address. Default IP is 192.168.0.1.

- **Subnet Mask:**
  Define your desired Subnet mask. Default Mask 255.255.255.0.

- **DHCP:**
  Select your preference for DHCP Server. Default selection is Enabled:
  Disabled, DHCP server's function will not work.
  Enabled, DHCP server's function will work.

- **Start IP Address/End IP Address:**
  Define your desired start/end IP address.

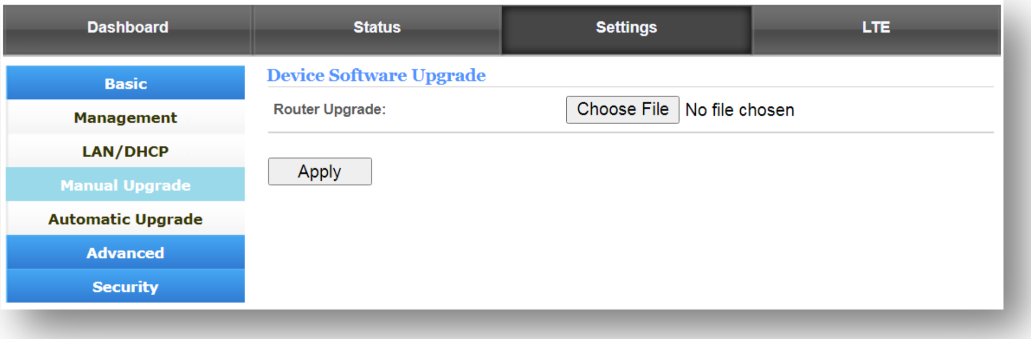
- **Lease Time:**
  Define the lease time. How long clients can hold the IP address.
  Default value is 86400 Seconds.

Once you've made your selections, click the **Apply** button to save the changes. You can also click the **Clear** button to ignore/cancel the changes.

4.4.1.3 Manual Upgrade

With this menu, you can update the device Software if you have an authentic, authorized file on your Computer/PC.

Establish a LAN connection with the device from your PC, click on the "Choose File" button, browse and select the desired file which you want to use for the Software upgrade.
Click **Apply** to start the download process.



Device Software Upgrade

Router Upgrade: No file chosen

Figure 29. Manual Software Upgrade.

The device will reboot itself after a successful SW upgrade.

Note: The firmware version must correspond to the hardware. The upgrade process takes a few moments, and this device restarts automatically when the upgrade is complete. It is important to keep power applied during the entire process. Loss of power during the upgrade could damage the device.

4.4.2 Advanced

On this menu, you can view the submenus: Dynamic DNS, Routing, NTP, Diagnostic, System Log, Network Management and Backup & Restore.

The detailed explanations for each submenu are provided below.

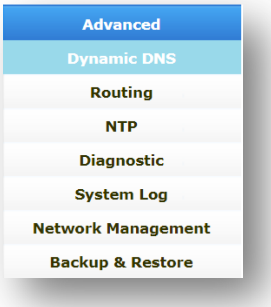
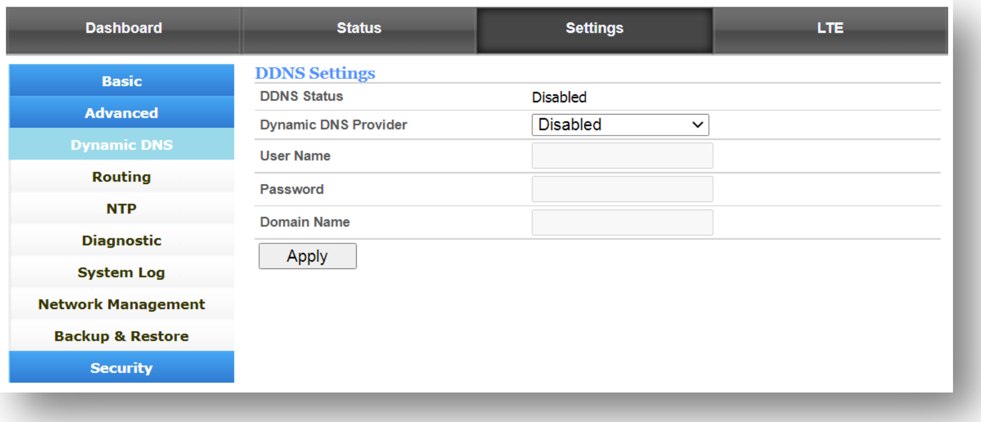


Figure 30. Submenus under Advanced.

4.4.2.1 Dynamic DNS

On this menu, you can define the DDNS provider of your preference.



DDNS Settings

DDNS Status	Disabled
Dynamic DNS Provider	Disabled
User Name	
Password	
Domain Name	

Figure 31. DDNS.

DDNS Status
Displays the current status of DDNS. By default, it is Disabled.

Dynamic DNS Provider
Disabled: Select this if you don’t want to use this feature.
DDNS Provider List: Select one as per your preference. You need to input credentials to use services from these DDNS providers.

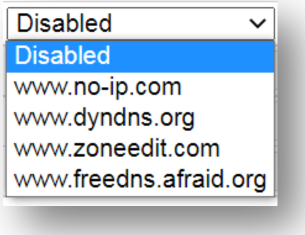
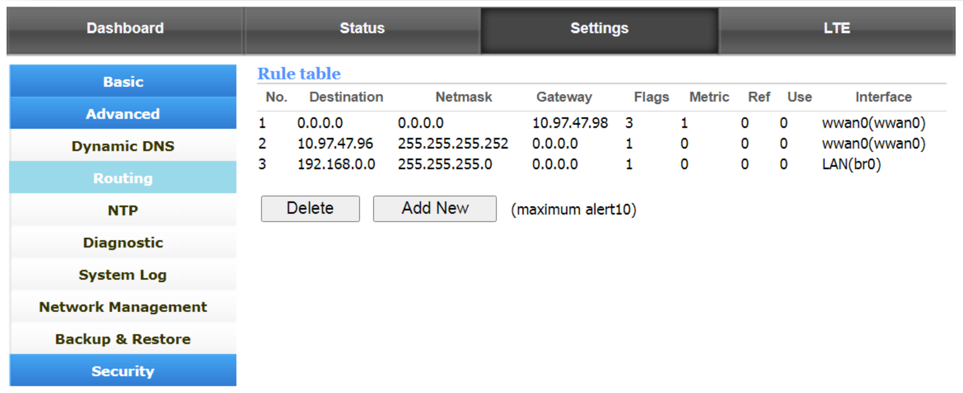


Figure 32. DDNS Provider list.

Username, Password & Domain Name: input these credentials to make this feature work.

4.4.2.2 Routing

On this menu, you can view the existing routings working on device. You can add a new route as per your needs and edit/delete added routes.



Rule table

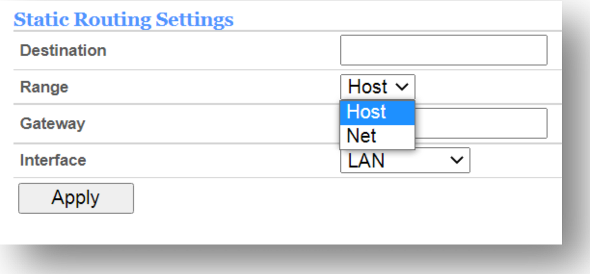
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface
1	0.0.0.0	0.0.0.0	10.97.47.98	3	1	0	0	wwan0(wwan0)
2	10.97.47.96	255.255.255.252	0.0.0.0	1	0	0	0	wwan0(wwan0)
3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)

(maximum alert10)

Figure 33. Route Table.

Click the **Add New** button to add a new router. You will get the options below:

- **Destination** Input your required destination IP address for your route.
- **Range** Select between Host or Net:
  - Select Host if the destination IP/network belongs on a Local area network/host side.
  - Select Net if the destination IP/network belongs to a network side.

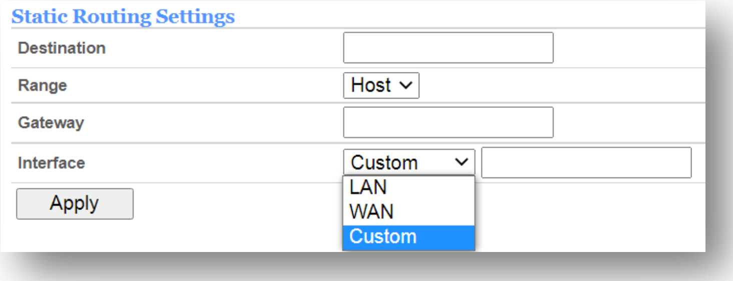


Static Routing Settings

Destination	
Range	Host
Gateway	
Interface	LAN

Figure 34. Add New Route (Example 1).

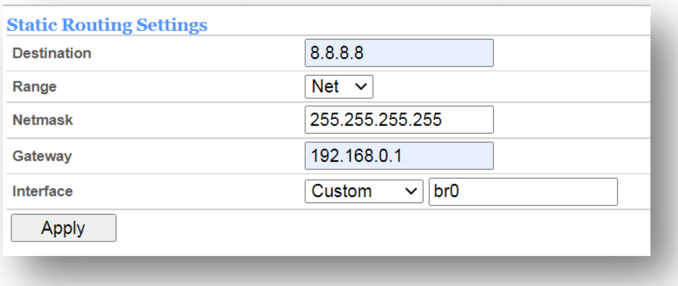
- **Gateway** Define your gateway IP address.
- **Interface** Select your interface between LAN/WAN/Custom.



Static Routing Settings

Destination	
Range	Host
Gateway	
Interface	Custom

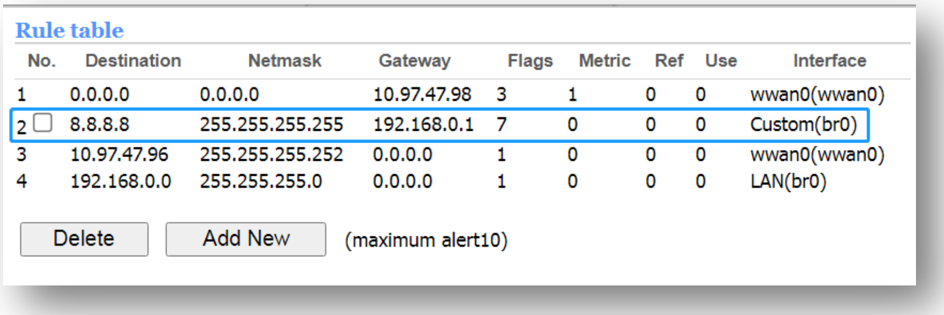
Figure 35. Add New Route (Example 2).



Static Routing Settings

Destination	8.8.8.8
Range	Net
Netmask	255.255.255.255
Gateway	192.168.0.1
Interface	Custom br0

Figure 36. Add New Route (Completed Example).



Rule table

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface
1	0.0.0.0	0.0.0.0	10.97.47.98	3	1	0	0	wwan0(wwan0)
2 □	8.8.8.8	255.255.255.255	192.168.0.1	7	0	0	0	Custom(br0)
3	10.97.47.96	255.255.255.252	0.0.0.0	1	0	0	0	wwan0(wwan0)
4	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)

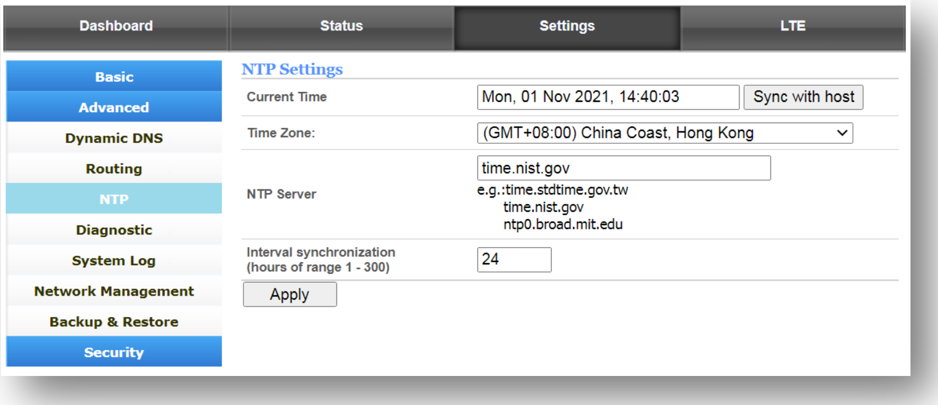
(maximum alert10)

Figure 37. Route table with an added route.

Click the **Delete** button to manually delete the added route or click the **Add New** button to add more routes manually.

4.4.2.3 NTP

On this menu, you can select your preferred time settings.
You can get the current time by clicking the button **Sync with host.** You can also select your desired NTP server.



NTP Settings

Current Time	Mon, 01 Nov 2021, 14:40:03
Time Zone:	(GMT+08:00) China Coast, Hong Kong
NTP Server	time.nist.gov e.g.:time.stdtime.gov.tw time.nist.gov ntp0.broad.mit.edu
Interval synchronization (hours of range 1 - 300)	24

Figure 38. NTP.

Current Time
Displays the current time.

Time Zone
Select your desired time zone.

NTP Server
Select your preferred server from the available options.

Interval Synchronization
Select your preferred time interval (in hours).

Click the **Apply** Button to save your changes.

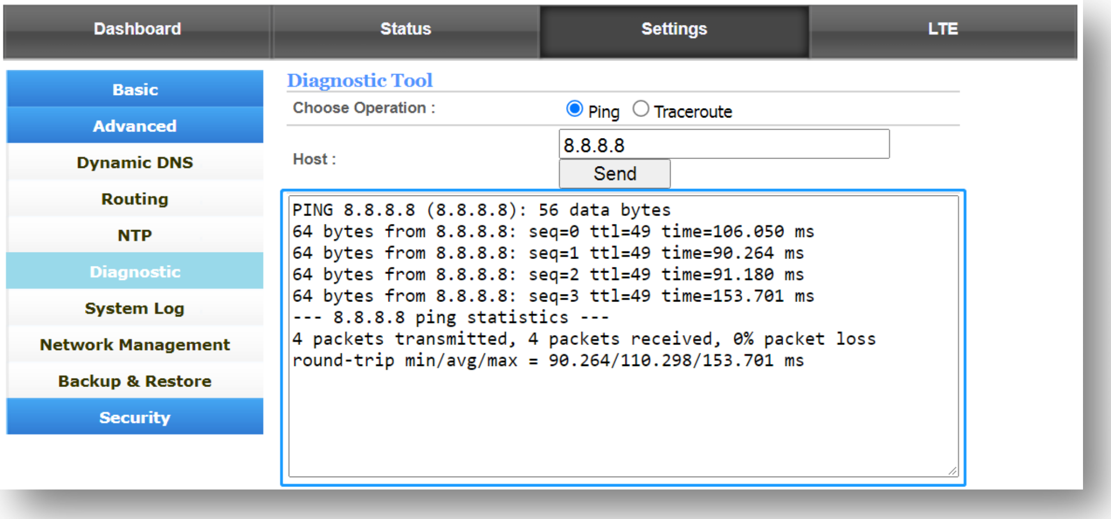
4.4.2.4 Diagnostic

With this menu, you can do your own troubleshooting if you need to perform a ping test or trace a route to check network connectivity.

Choose Operation
Select from Ping or Traceroute.

Host
Input your testing IP address or Host name.

Click the **Send** button to start the test and results will appear in window (as shown below).



Choose Operation : ● Ping ○ Traceroute

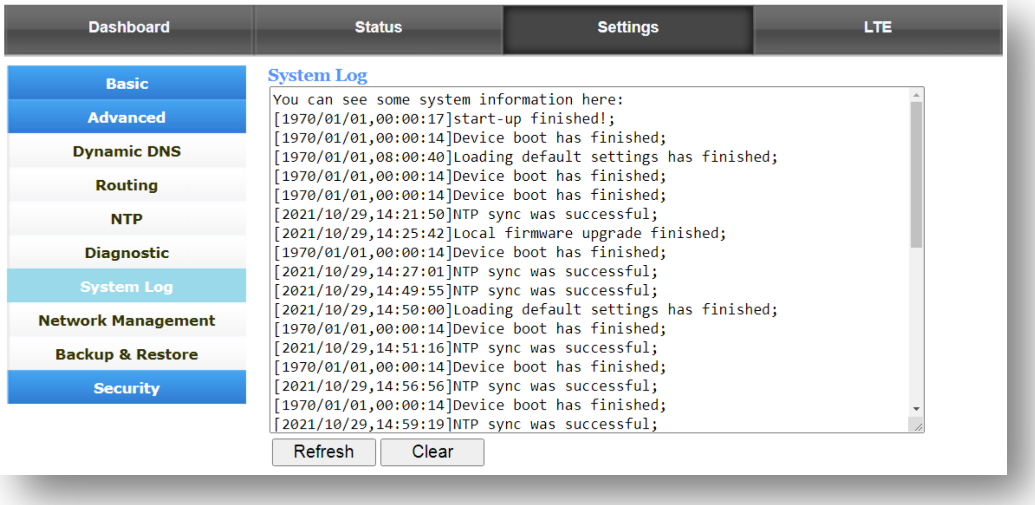
Host : 8.8.8.8

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: seq=0 ttl=49 time=106.050 ms
64 bytes from 8.8.8.8: seq=1 ttl=49 time=90.264 ms
64 bytes from 8.8.8.8: seq=2 ttl=49 time=91.180 ms
64 bytes from 8.8.8.8: seq=3 ttl=49 time=153.701 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 90.264/110.298/153.701 ms
```

Figure 39. Diagnostic.

4.4.2.5 System Log

With this menu, you can view the device/system logs. These are required by the device support team to analyze or troubleshoot for customer support.



System Log

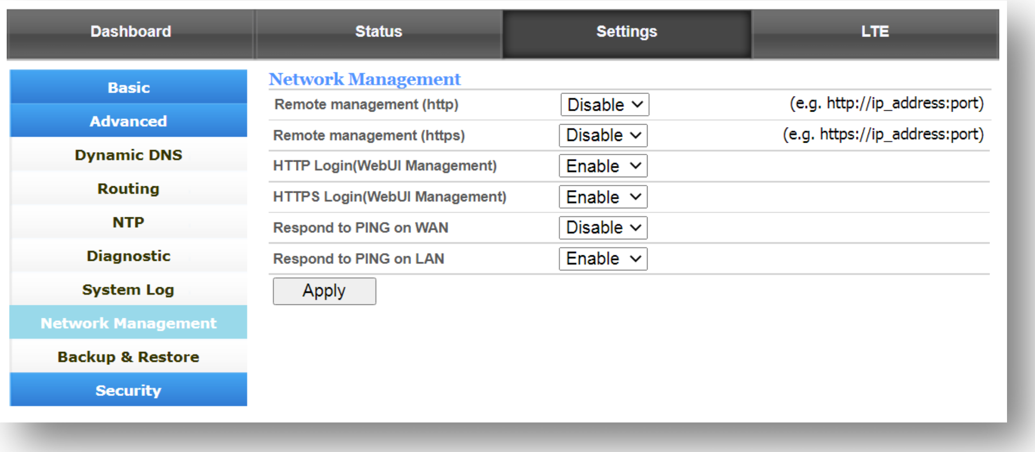
```
You can see some system information here:
[1970/01/01,00:00:17]start-up finished!;
[1970/01/01,00:00:14]Device boot has finished;
[1970/01/01,08:00:40]Loading default settings has finished;
[1970/01/01,00:00:14]Device boot has finished;
[1970/01/01,00:00:14]Device boot has finished;
[2021/10/29,14:21:50]NTP sync was successful;
[2021/10/29,14:25:42]Local firmware upgrade finished;
[1970/01/01,00:00:14]Device boot has finished;
[2021/10/29,14:27:01]NTP sync was successful;
[2021/10/29,14:49:55]NTP sync was successful;
[2021/10/29,14:50:00]Loading default settings has finished;
[1970/01/01,00:00:14]Device boot has finished;
[2021/10/29,14:51:16]NTP sync was successful;
[1970/01/01,00:00:14]Device boot has finished;
[2021/10/29,14:56:56]NTP sync was successful;
[1970/01/01,00:00:14]Device boot has finished;
[2021/10/29,14:59:19]NTP sync was successful;
```

Figure 40. System Logs.

Click the **Refresh** button to refresh the logs and the **Clear** button to clear the logs appearing in the log window.

4.4.2.6 Network Management

With this menu, you can view useful information, which can help to define device behavior with network communications. This is a very simple kind of firewall which is easy to setup and quite useful.



Network Management

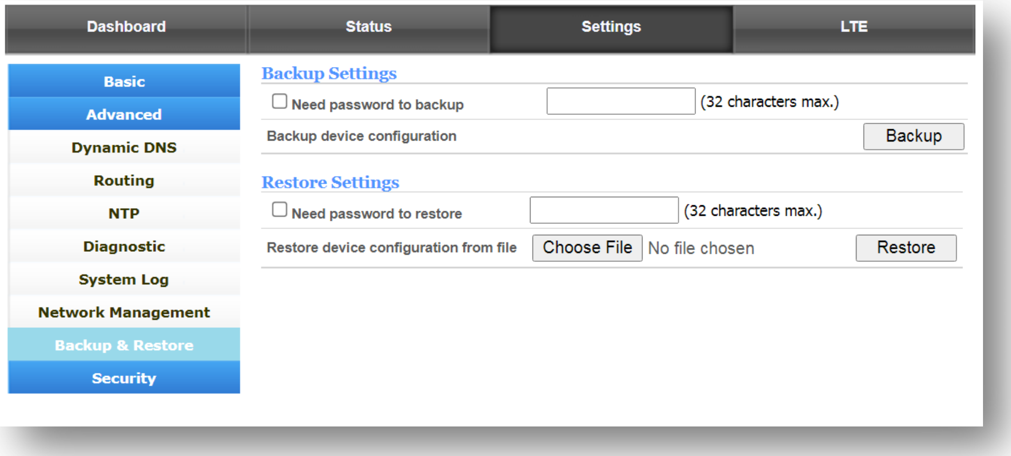
Remote management (http)	Disable	(e.g. http://ip_address:port)
Remote management (https)	Disable	(e.g. https://ip_address:port)
HTTP Login(WebUI Management)	Enable	
HTTPS Login(WebUI Management)	Enable	
Respond to PING on WAN	Disable	
Respond to PING on LAN	Enable	

Figure 41. Network Management.

Click the **Apply** Button to save your changes.

4.4.2.7 Backup & Restore

With this menu, you can back up the device configuration and restore it to the device whenever required. This is a useful feature when you must set multiple devices to the same configuration or when you want to keep your configurations as a backup to use in the future if you've lost your current configuration due to a SW update or reset.



Backup Settings

□ Need password to backup (32 characters max.)

Backup device configuration [Backup]

Restore Settings

□ Need password to restore (32 characters max.)

Restore device configuration from file [Choose File] No file chosen [Restore]

Figure 42. Backup & Restore.

- Click the **Backup** button to save device configurations to your connected computer/PC.

- Click the **Choose File** button and then browse for the configuration file on your connected PC. Select it and then click the **Restore** button to load the configuration to the connected device.

4.4.3 Security

With this menu, you can find some special security related feature such as; MAC Filter, IP/Port Filtering, Content Filtering, Port Forwarding, Virtual Server, DMZ, UPnP, VPN Passthrough and Parent Control. Back up the device configuration and restore it to device whenever required. This is very useful feature when you have multiple devices to set with same configuration or when you want to keep your configurations as a backup to use in the future if you've lost your current configuration due to SW update or reset accidently.

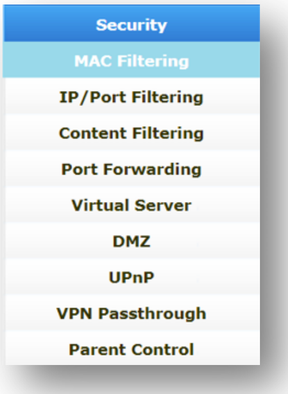


Figure 43. Submenus under Security Menu.

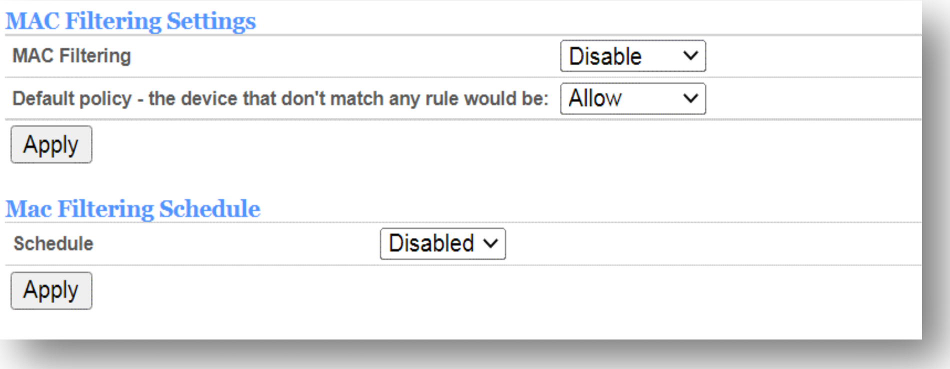
Note: Do not try to setup any rules if you are not sure about the changes with these available features. It might cause abnormal device behavior. Kindly contact to your service provider for any help or support if required.

With this menu, you can block or allow specific users to connect with device for ISP services like access to internet or some other services using their MAC address.

4.4.3.1 MAC Filtering Settings

MAC Filtering By default, this feature is disabled. You need to enable it using the drop-down menu if want to use this feature.

Default Policy select Allow or Block options for Default Policy.



MAC Filtering Settings

MAC Filtering	Disable
Default policy - the device that don't match any rule would be:	Allow

Apply

Mac Filtering Schedule

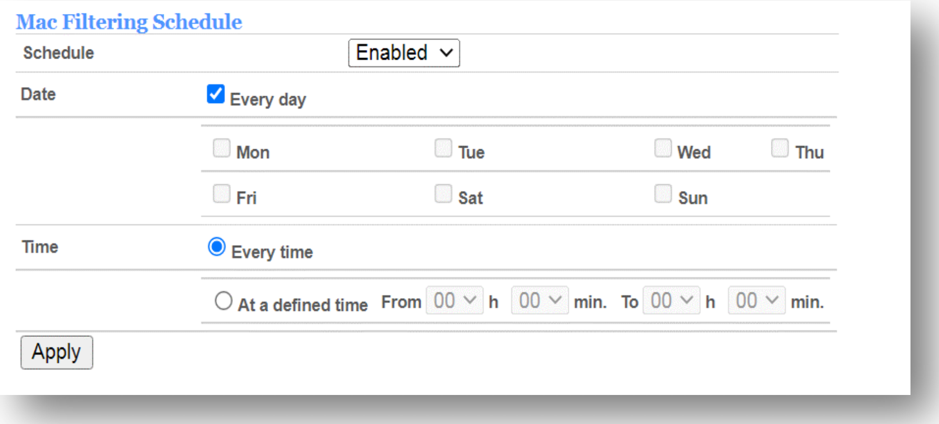
Schedule	Disabled

Apply

Figure 44. MAC Filter.

MAC Filtering Schedule

- **Schedule:** By default, this feature is disabled. You need to enable it using the drop-down menu if want to use this feature.
- **Date:** Choose your preferred option from the available options.
- **Time:** Choose your preferred option from the available options.



Mac Filtering Schedule

Schedule	Enabled			
Date	☑ Every day			
	□ Mon	□ Tue	□ Wed	□ Thu
	□ Fri	□ Sat	□ Sun	
Time	● Every time			
	○ At a defined time From 00 h 00 min. To 00 h 00 min.			

Apply

Figure 45. MAC Filter Rules.

Click on **Apply** Button to save your changes.

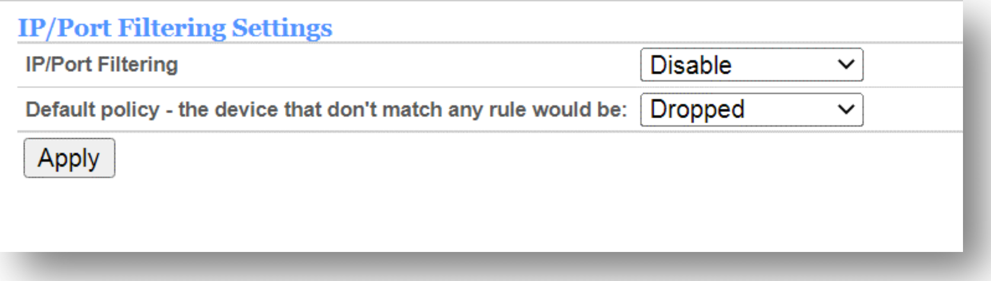
4.4.3.2 IP/Port Filtering

With this menu, you can use the IP/Port Filtering feature, where you can allow or drop any connection using source, destination IP address to specific port address and traffic type.

IP/Port Filtering: By default this feature is disabled. You need to enable it using the drop down menu if want to use this feature.

Default Policy

- **Dropped:** Connection will be blocked if created rule matches.
- **Allow:** Connection will be allowed if created rule matches.



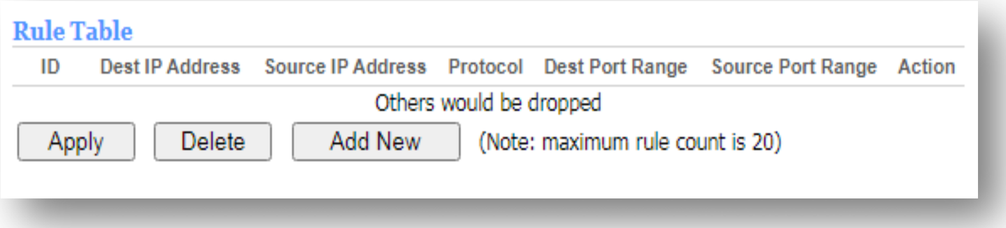
IP/Port Filtering Settings

IP/Port Filtering: Disable

Default policy - the device that don't match any rule would be: Dropped

Figure 46. IP/Port Filter.

When this feature is enabled. You will find rule table where you can see existing rules, create rules, delete rules and apply them using the checkbox under ID column. You can define maximum rules up to 20.

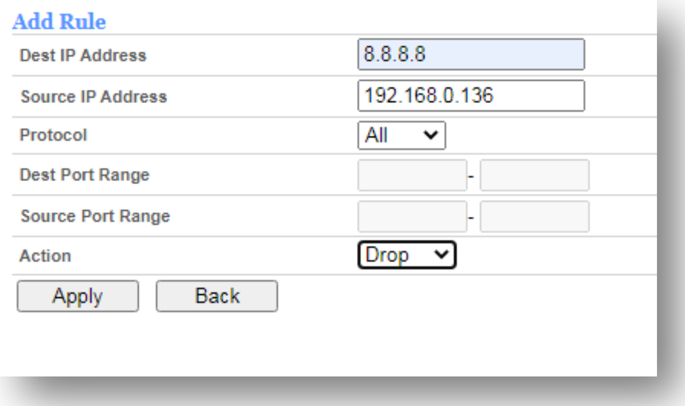


Rule Table

ID	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action
Others would be dropped						

(Note: maximum rule count is 20)

Figure 47. IP/Port Filter Rules.

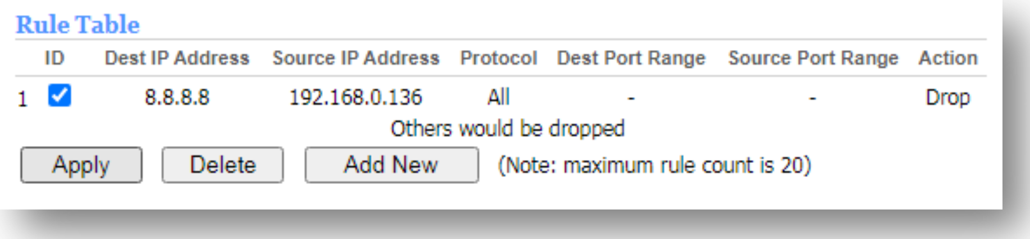


Add Rule

Dest IP Address	8.8.8.8
Source IP Address	192.168.0.136
Protocol	All
Dest Port Range	-
Source Port Range	-
Action	Drop

Figure 48. IP/Port Filter- Add Rule.

- **Dest IP Address:** Define the destination IP address for the rule.
- **Source IP Address:** Define the source IP address for the rule.
- **Protocol:** Select any one from; All, TCP, UDP, ICMP.
- **Dest Port Range:** Define the port range.
- **Source Port Range:** Define the port range.
- **Action:** Select "Drop" to block the connection or "Accept" to allow the connection.



Rule Table

ID		Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action
1	☑	8.8.8.8	192.168.0.136	All	-	-	Drop

Others would be dropped

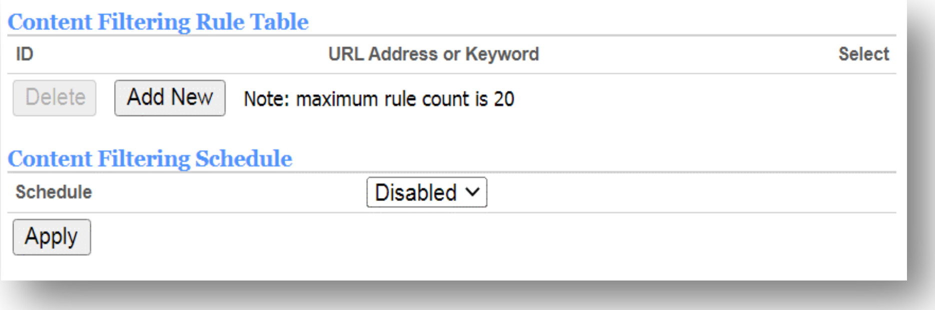
(Note: maximum rule count is 20)

Figure 49. IP/Port Filter- Example.

Click on **Apply** Button to save your changes.

4.4.3.3 Content Filtering

With this menu, you can use the Content Filtering feature. It allows you to control the content access by the connected users while connected with the device. You can define the URL, IP Address or Keyword (for e.g. games), to block or allow it with scheduling, if required.


Content Filtering Rule Table

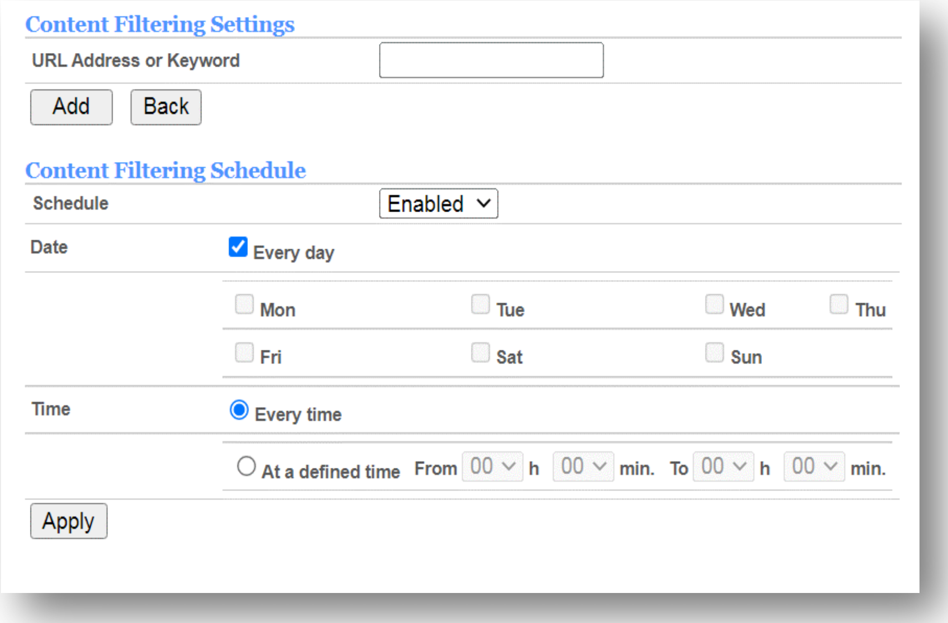
ID	URL Address or Keyword	Select

Note: maximum rule count is 20

Content Filtering Schedule

Schedule: Disabled

Figure 50. Content Filter.


Content Filtering Settings

URL Address or Keyword: □

Content Filtering Schedule

Schedule: Enabled

Date: ☑ Every day

□ Mon □ Tue □ Wed □ Thu

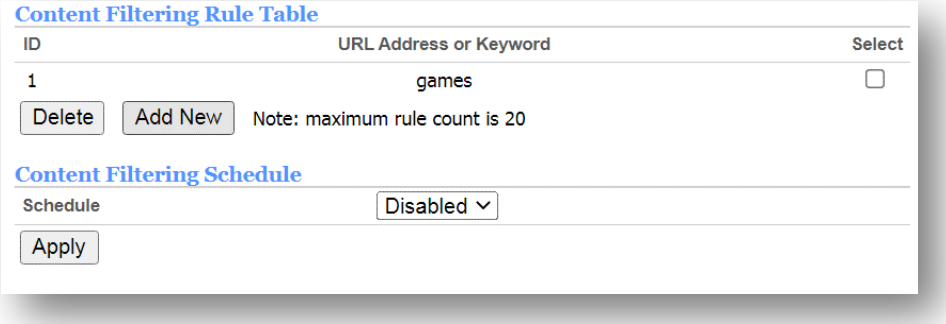
□ Fri □ Sat □ Sun

Time: ● Every time

○ At a defined time From 00 h 00 min. To 00 h 00 min.

Figure 51. Content Filter Schedule.

Click on the **Add New** button to define the Content Filtering parameters required, see the below image:


Content Filtering Rule Table

ID	URL Address or Keyword	Select
1	games	□

Note: maximum rule count is 20

Content Filtering Schedule

Schedule: Disabled

Figure *52*. Content Filter Rule Table.

You can define maximum rules up to 20.

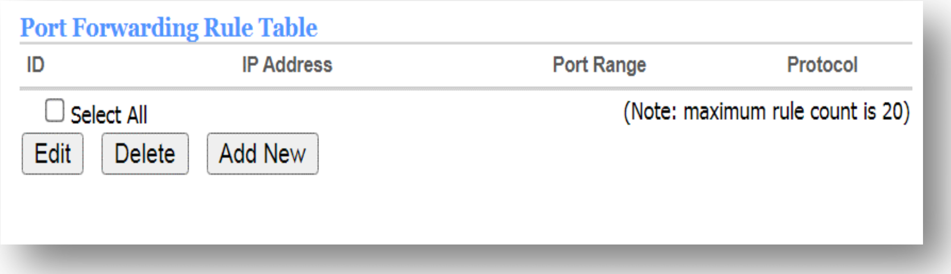
Select the check box in the ID column for a specific rule or the **Select All** check box to select all of the added rules.

Click the **Delete** button to delete the selected rule(s).

Click on the **Apply** Button to save your changes.

4.4.3.4 Port Forwarding

With this menu, you can use the Port Forwarding feature, where you can define the host IP Address, allowed Port Range and type of Protocol for your application.



Port Forwarding Rule Table

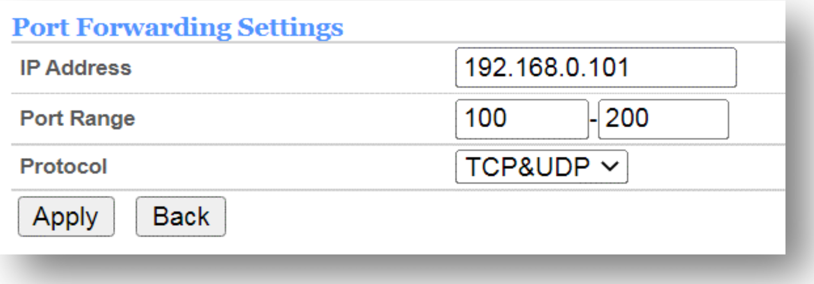
ID	IP Address	Port Range	Protocol

□ Select All

(Note: maximum rule count is 20)

Figure 53. Port Forwarding Rule Table.

Click on the **Add New** button to define the Port Filtering parameters required as shown below:



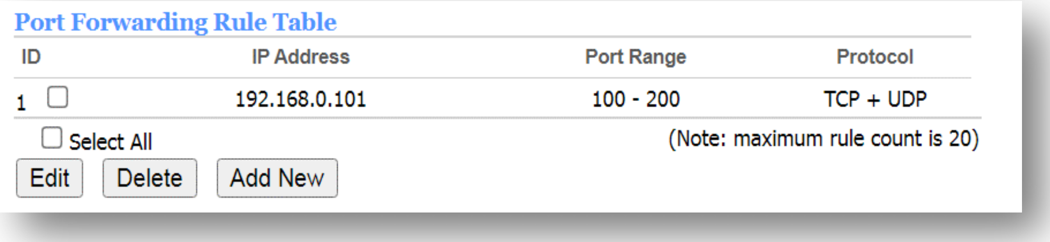
Port Forwarding Settings

IP Address	192.168.0.101
Port Range	100 - 200
Protocol	TCP&UDP

Figure 54. Port Forwarding Rules.

- **IP Address:** Define your required IP address.
- **Port Range:** Define your port range (1~65535).
- **Protocol:** Select any one type from the available options:
    - TCP
    - UDP
    - TCP/UDP

Click on the **Apply** Button to save your changes.



Port Forwarding Rule Table

ID	IP Address	Port Range	Protocol
1 □	192.168.0.101	100 - 200	TCP + UDP

□ Select All (Note: maximum rule count is 20)

Figure 55. Port Forwarding Example.

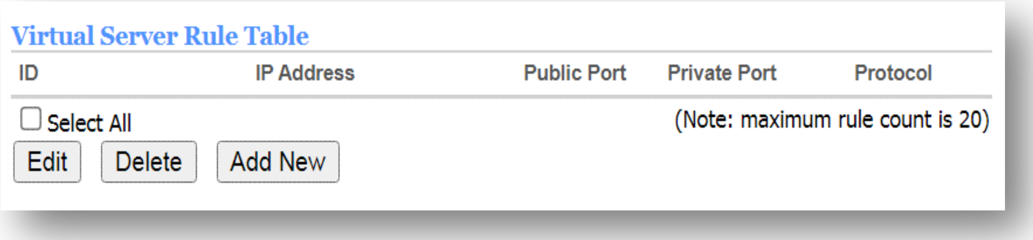
You can define maximum rules up to 20.

Click the check box in the ID column for a specific rule or **Select All** check box to select all the added rules.

Click the **Delete** button to delete and the **Edit** button to edit the selected added rule(s).

4.4.3.5 Virtual Server

With this menu, you use the Virtual Server feature. Click on the **Add New** button to define your required configuration for virtual servers.



Virtual Server Rule Table

ID	IP Address	Public Port	Private Port	Protocol

□ Select All (Note: maximum rule count is 20)

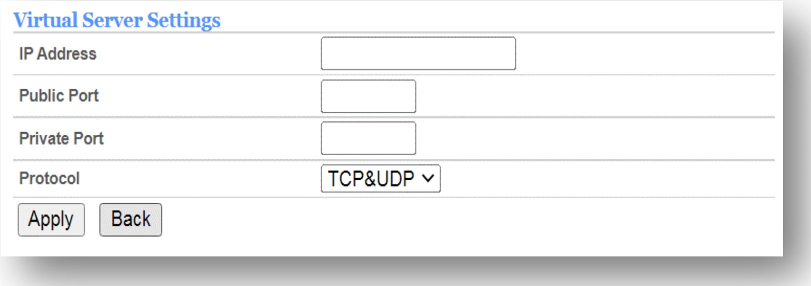
Figure *56*. Virtual Server.

You can define maximum rules up to 20.

Click the check box in the ID column for a specific rule or the **Select All** check box to select all the added rules.

Click the **Delete** button to use delete and the **Edit** button to edit the selected added rule(s).

- **IP Address:** Define your required IP address.
- **Public Port:** Define the port number (1~65535).
- **Private Port:** Define the port number (1~65535).
- **Protocol:** Select any one type from the available options:
  - TCP
  - UDP
  - TCP/UDP



Virtual Server Settings

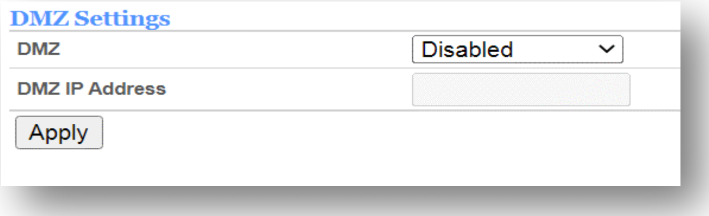
IP Address	
Public Port	
Private Port	
Protocol	TCP&UDP

Figure 57. Virtual Server Rules.

Click on the **Apply** Button to save your changes.

4.4.3.6 DMZ

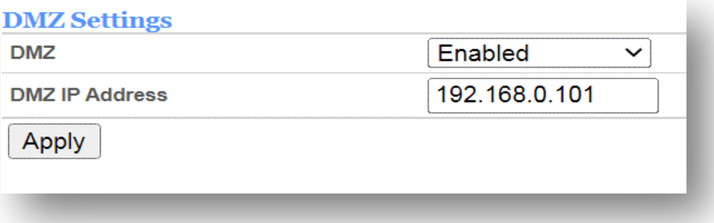
With this menu, you can configure and use the DMZ feature.
The DMZ feature allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or video conferencing. The router forwards packets of all services to the DMZ host. Any PC that is set to be a DMZ host must have its DHCP client function disabled and should have a static IP address assigned to it because its IP Address may change after a reboot due to DHCP function.



DMZ Settings

DMZ	Disabled
DMZ IP Address	

Figure 58. DMZ.



DMZ Settings

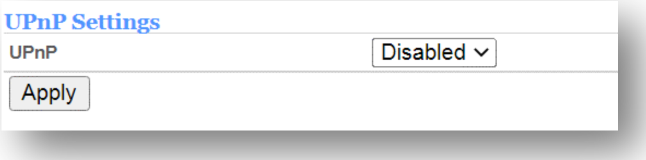
DMZ	Enabled
DMZ IP Address	192.168.0.101

Figure 59. DMZ Rules.

Click on the **Apply** Button to save your changes.

4.4.3.7 UPnP (Universal Plug and Play)

With this menu, you can see the current status for the UPnP feature. Using the dropdown menu, this feature can be enabled or disabled.



UPnP Settings

UPnP: Disabled

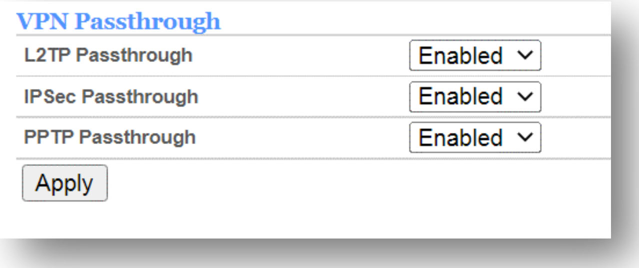
Figure 60. UPnP Feature.

Click on **Apply** Button to save your changes.

4.4.3.8 VPN Passthrough

With this menu, you see the current status for the VPN Passthrough feature. This is very useful when connected users, either on LAN or WiFi, require access to or the use of VPN services. This feature helps for such communication to work with ease.

By default, L2TP/IPsec/PPTP Passthrough is enabled. You can simply use the dropdown menu to disable or enable any or all of them based on your requirements.



VPN Passthrough

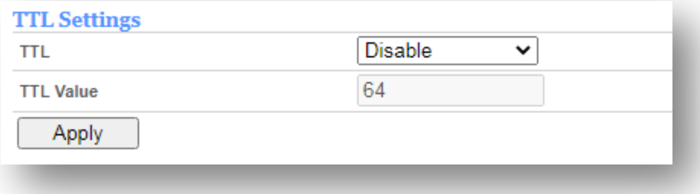
L2TP Passthrough	Enabled
IPSec Passthrough	Enabled
PPTP Passthrough	Enabled

Figure 61. VPN Passthrough.

Click on the **Apply** button to save your changes.

4.4.3.9 TTL

With this menu, you can set the TTL (Time to Live) value for the Data packets going to your ISP/Internet. Kindly confirm any change with your ISP as it might cause issues with Internet reachability.



TTL Settings

TTL	Disable
TTL Value	64

Figure 62. TTL Settings.

Click on the **Apply** button to save your changes.

4.5 LTE

With this menu, you can view six submenus: APN Settings, PIN Management, Bridge, Network, PCI Lock & MTU.

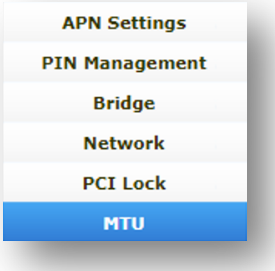
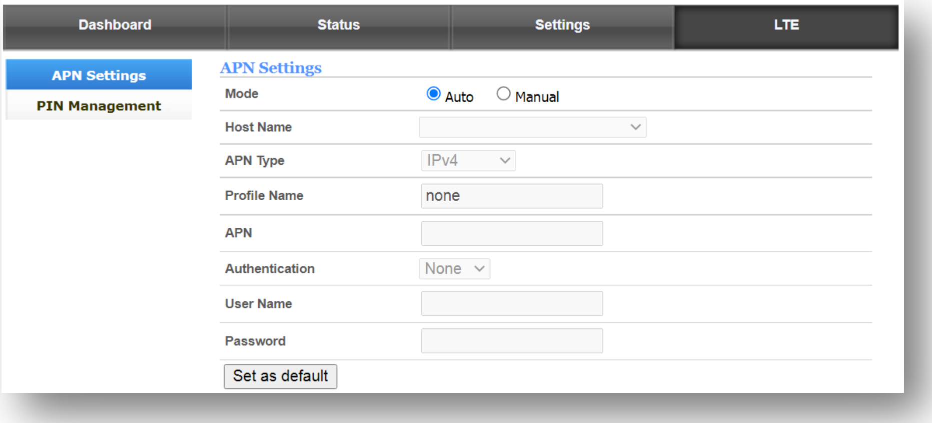


Figure 63. Submenus under LTE Menu.

4.5.1 APN Settings

With this menu, you can set manual APNs if you don't want the device to use the auto APN method.

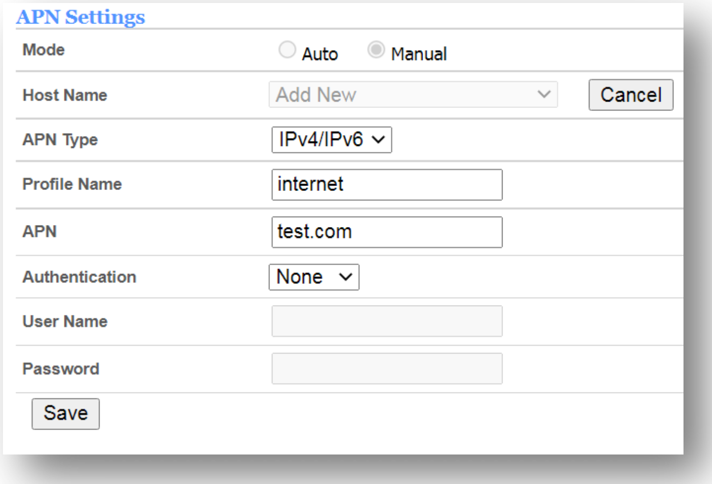


APN Settings

Mode	● Auto ○ Manual
Host Name	
APN Type	IPv4
Profile Name	none
APN	
Authentication	None
User Name	
Password	

Figure 64. APN.

Mode Displays the current APN mode. Default APN mode is Auto. Select the Manual option by checking the box to add/use manual APN. When you do so, you will get the window as shown below:



APN Settings

Mode	○ Auto ● Manual	
Host Name	Add New	Cancel
APN Type	IPv4/IPv6	
Profile Name	internet	
APN	test.com	
Authentication	None	
User Name		
Password		

Figure 65. Manual APN.

APN Type
Choose from the available options: IPv4, IPv6, and IPv4/IPv6.

Profile Name
Define a profile name.

APN
Define the APN name you want the device to use while connected with the network.

Authentication
Choose from the available options: None, CHAP & PAP.

Username
Input the username if PAP or CHAP is selected for Authentication.

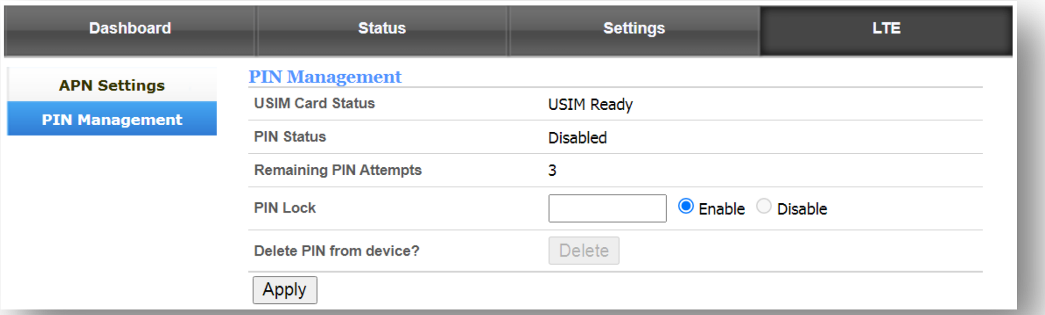
Password
Input the password if PAP or CHAP is selected for Authentication.

Note: Manually added APNs should be allowed/accepted by the network to attach. Device will disconnect and connect/attach with the network once you add APNs and select them as Default.

4.5.2 PIN Management

With this menu, you can lock the SIM card using its PIN (Personal Identification Number) feature. This is a useful and secure way to keep your SIM card safe from any unwanted access to data.

Once you enable the SIM PIN, the device will ask to enter the PIN (security number) to connect to the network.



PIN Management

USIM Card Status	USIM Ready
PIN Status	Disabled
Remaining PIN Attempts	3
PIN Lock	● Enable ○ Disable
Delete PIN from device?	Delete

Figure 66. PIN Management.

USIM Card Status: Displays the current SIM card status.

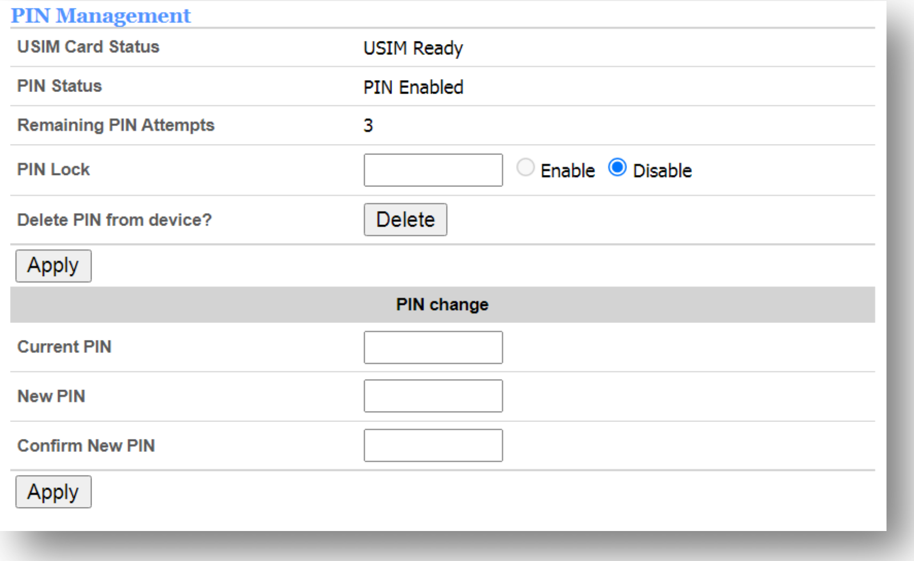
- USIM Ready
- USIM Locked
- USIM PIN Enabled

PIN Status: Displays the current PIN status.

- Enabled
- Disabled

Remaining PIN Attempts: Displays the remaining attempts for PIN Lock enable/disable.

PIN Lock Input: Correct PIN to enable or disable the SIM card PIN.



PIN Management

USIM Card Status	USIM Ready
PIN Status	PIN Enabled
Remaining PIN Attempts	3
PIN Lock	○ Enable ● Disable
Delete PIN from device?	Delete

PIN change

Current PIN	
New PIN	
Confirm New PIN	

Figure 67. PIN Management Example.

You can also change the default PIN, but please remember your SIM card PIN. If you attempt to use the wrong credentials, the SIM card might be locked, and you will need to contact your service provider to unlock your SIM card.

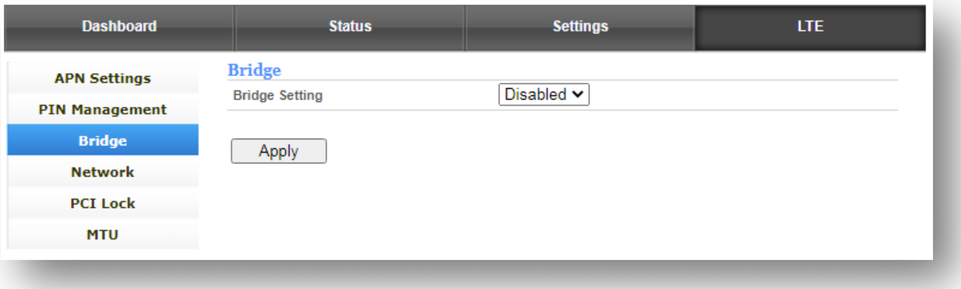
Click the **Apply** button to save your changes.

4.5.3 Bridge

With this menu, you can get Public/WAN IP address from your ISP to the connected device on LAN when this feature is enabled.

Bridge Setting: Displays the current Bridge setting status.

- Disabled
- Enabled



Bridge

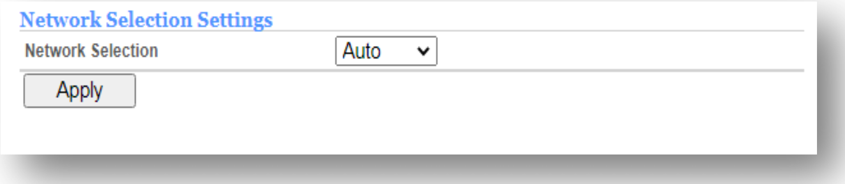
Bridge Setting: Disabled

Figure 68. Bridge Settings.

Click the **Apply** button to save your changes.

4.5.4 Network

With this menu, you can lock the device with your desired frequency band.



Network Selection Settings

Network Selection: Auto

Figure 69. Network Settings.

Network Selection Settings: Select your desired option:

- Auto - Device will select the best suitable band automatically.
- 4G Only - Device will connect to selected bands only.

When 4G Only is selected, you will find the option to select the desired frequency band from the available bands.

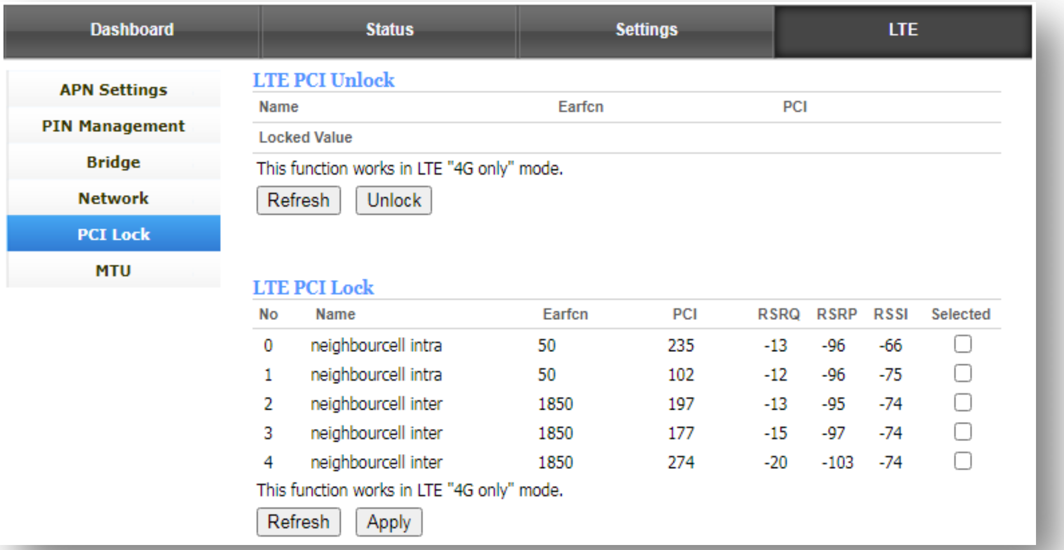
LTE Band: Displays current LTE band selection:

- Checked
- Unchecked

Click the **Apply** button to save your changes.

4.5.5 PCI Lock

With this menu, you can lock the device to your desired cell ID/Cell Tower.



LTE PCI Unlock

Name	Earfcn	PCI
Locked Value		

This function works in LTE "4G only" mode.

Refresh Unlock

LTE PCI Lock

No	Name	Earfcn	PCI	RSRQ	RSRP	RSSI	Selected
0	neighbourcell intra	50	235	-13	-96	-66	□
1	neighbourcell intra	50	102	-12	-96	-75	□
2	neighbourcell inter	1850	197	-13	-95	-74	□
3	neighbourcell inter	1850	177	-15	-97	-74	□
4	neighbourcell inter	1850	274	-20	-103	-74	□

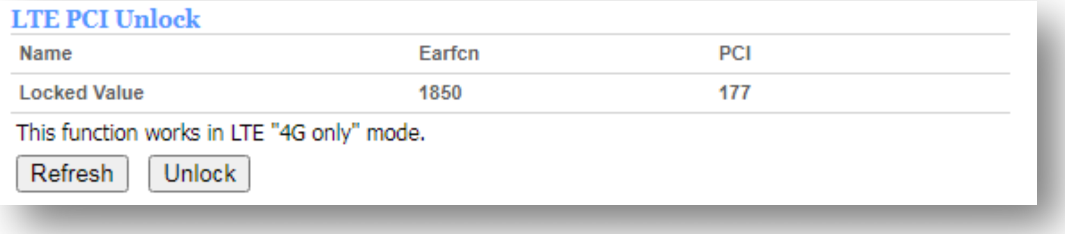
This function works in LTE "4G only" mode.

Refresh Apply

Figure 70. PCI Lock.

LTE PCI Unlock: Displays the locked PCI, if any:

- Earfcn - Displays Earfcn value.
- PCI - Displays the PCI value.



LTE PCI Unlock

Name	Earfcn	PCI
Locked Value	1850	177

This function works in LTE "4G only" mode.

Refresh Unlock

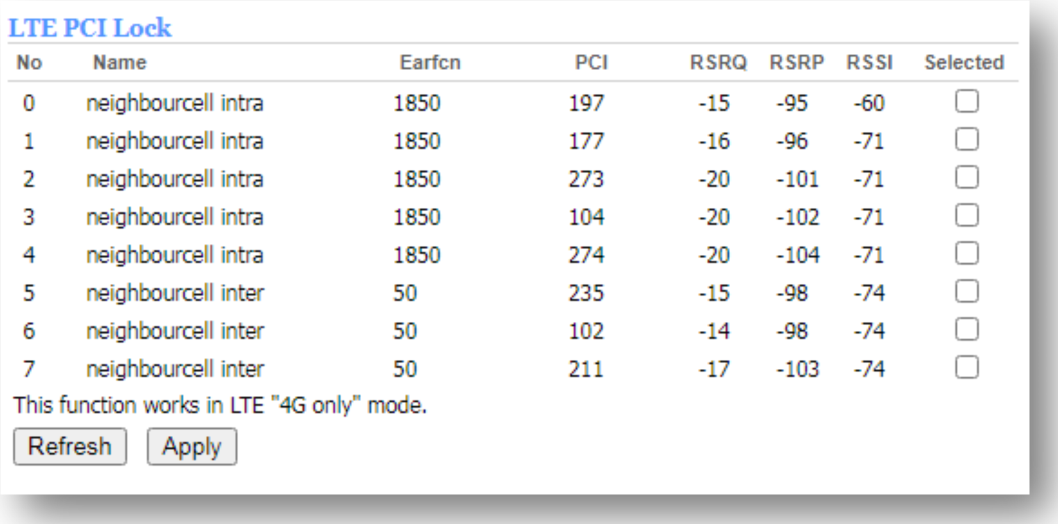
Figure 71. PCI Lock Cell.

Click on the **Refresh** button to refresh the information.
Click on the **Unlock** button to disable the PCI Lock.

LTE PCI Lock: Displays the available Cell:

- Name - Displays the cell information (i.e. Intra/Inter) for cell in the list.
- Earfcn - Displays the Earfcn value for the cell in list.
- PCI - Displays the PCI value for the listed cell.
- RSRQ - Display the RSRQ value for the listed cell.
- RSRP - Displays the RSRP value for the listed cell.

- RSSI - Displays the RSSI value for the listed cell.
- Selected - Displays the checkbox to check/uncheck for your selection of PCI.



LTE PCI Lock

No	Name	Earfcn	PCI	RSRQ	RSRP	RSSI	Selected
0	neighbourcell intra	1850	197	-15	-95	-60	☐
1	neighbourcell intra	1850	177	-16	-96	-71	☐
2	neighbourcell intra	1850	273	-20	-101	-71	☐
3	neighbourcell intra	1850	104	-20	-102	-71	☐
4	neighbourcell intra	1850	274	-20	-104	-71	☐
5	neighbourcell inter	50	235	-15	-98	-74	☐
6	neighbourcell inter	50	102	-14	-98	-74	☐
7	neighbourcell inter	50	211	-17	-103	-74	☐

This function works in LTE "4G only" mode.

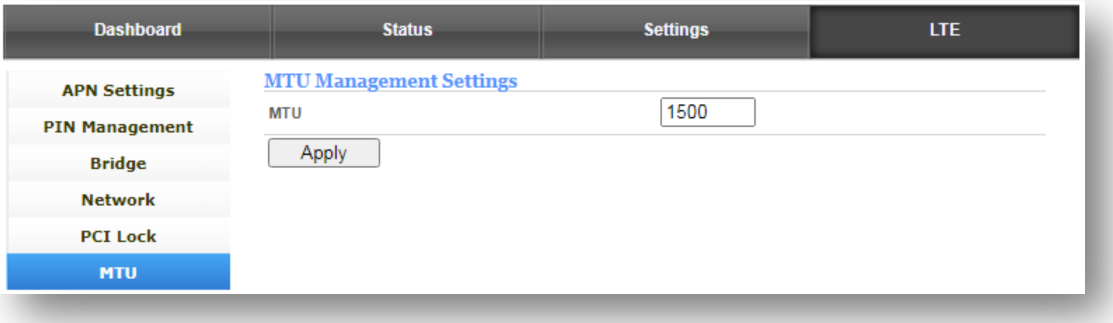
Figure 72. PCI Lock List.

Click on the **Refresh** button to refresh the information.
Click on the **Unlock** button to disable the PCI Lock.

Click the **Apply** Button to save your changes.

4.5.6 MTU

With this menu, you can define the MTU Size. (Allowed value from 1300 to 1500.) Kindly confirm any change with your ISP as it might cause issue(s) with Internet reachability.



MTU Management Settings

MTU 1500

Figure 73. MTU Settings.

Click the **Apply** Button to save your changes.

Appendix A: Troubleshooting & FAQ

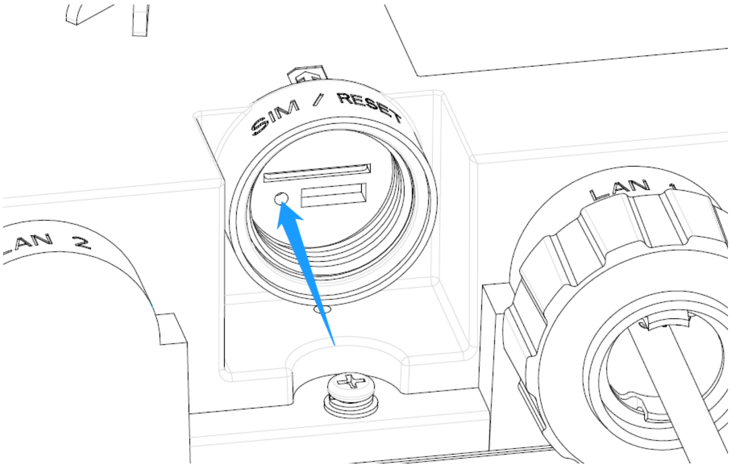
1. **What can I do if the login page does not appear?**
   - Verify that the computer is set to obtain an IP address automatically from the Device.
   - Test with http://192.168.0.1 (if default IP address not changed).
   - If your ccomputer failed to obtain IP addresses from the device, you can try to set IP addresses manually.
   - Verify that `http://192.168.0.1` is correctly entered into the web browser and click Login.
   - Use another web browser and try again or try to clear your browser history or cache memory.
   - Reboot your device and try again.
   - Disable and enable the active network adapter and try again.
   - Try Resetting the device, refer to Troubleshooting and FAQ Q3.
   - If the issue persists, kindly contact to your service provider.

2. **What can I do if I cannot connect to Internet?**
   - Check Signal LED status for receiving signal quality, refer to the LED definitions for details.
   - Verify that your SIM card is installed properly and activated.
   - Verify that your SIM card has sufficient credit and/or a data plan has been set up with your ISP (service provider).
   - Verify that your SIM card and device is in your ISP's service area.
   - Verify that your device is connected to the network. You can login to the Online Portal (WebGUI) and check your network status on the dashboard. Refer to Chapter 3 for more details.
   - Try the diagnostic page. Login to the Online Portal (WebGUI) and perform a ping test to a known IP and web URL, such as, 8.8.8.8 or www.google.com.
   - Try Resetting the device, refer to Troubleshooting and FAQ Q3.
   - If the issue persists, kindly contact to your service provider.

3. **How do I restore the device to its factory default settings?**

   There are two ways to perform a Reset to Factory defaults of the Device:

Option 1) With the device powered on, press and hold down the **RESET** button on the bottom panel of the device for about 10 seconds, then release it. The device will restore and reboot automatically.



Option 2) Login to the web management page (WebGUI) of the device and go to Settings > Basic > Management > Restore, click the Restore button and wait until the reset process completes.

Note: During the Reset process, make sure the power adaptor is connected to the device to ensure an uninterrupted power supply.

4. **What can I do if I forget my web management page password?**

   - Refer to Troubleshooting and FAQ > Q3 to restore the device to its factory default settings and then use the default Username and Password, “admin” to login.

Appendix B: Specifications

Model J912	
Supported Bands	LTE Bands B1/B2/B3/B4/B5/B7/B8/B9/B12/B13/B14/B17/B18/B19/B20 B21/B25/B26/B28/B29/B30/B32/B38/B39B40/B41/B66 UMTS Bands B1/B2/B3/B4/B5/B8/B9/B19
Data Speeds	Upload: up to 75Mbps Download: up to 600Mbps
Network Type	LTE/LTE-A
LTE MIMO	4x2
LTE Antenna Gain	For lower bands: 2dBi For higher bands: 12dBi
Antenna Configuration	Ant 0: Tx/Rx Ant 1: Rx Diversity only
Interface definition	
LAN Port	1x RJ45 Gigabit
USIM interface	1x 2FF SIM card Slot
Reset	Button to perform Reset/factory default function
LEDs	4 LEDs RF/Signal, ETH, SIM, Power
Electrical and Environmental Specifications	
Operating Temperature	-30°C~60°C
Operating Humidity	5%~95%
PoE Injector Input Voltage	AC 100-240V
PoE Injector Supported Frequency	50~60HZ
PoE Injector Output Voltage	DC 48~56V
IP Rating	IP67
RF Performance	
Receiver sensitivity	<-99.3dBm@BW=5MHz <-96.3dBm@BW=10MHz <-94.5dBm@BW=15MHz <-93.3dBm@BW=20MHz
Output power	Maximum output power: 23dBm Minimum output power: < -39dBm
Physical Details	
Dimensions	265 x 265 x 90mm
Weight	5.07lbs / 2.3kg (with Mount Fixture)

Appendix C: Glossary

- **WebGUI** (**Web**/browser **G**raphical **U**ser **I**nterface) **-** Simple and easy to use device management portal based on browser/web pages, which helps users to change/modify device configurations.

- **LTE/LTE-A -** LTE (Fourth generation of cellular communications)/LTE-A Fourth generation of cellular communications-Advanced).

- **4G LTE Outdoor CPE -** Device that supports 4G LTE frequency bands and helps to provide high-speed data over connected device(s). It is required to install outside of the customer's premises. It uses PoE terminology, data and power supply to reach the ODU through Ethernet cable and PoE injector. The Outdoor CPE device is an outdoor access point (AP) or router to provide a **long-distance wireless network solution.**

- **CPE** (**C**ustomer **P**remises **E**quipment) **-** Telecommunication hardware located near the customer's home or office.

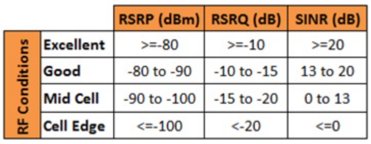
- **PCI- P**hysical **C**ell **I**d (PCI) is the identifier of a cell in the physical layer of the LTE network, which is used for separation of different transmitters. Due to the construction of PCIs, the number of PCIs are limited to 504 (0 to 503).

- **RSSI -** In telecommunications, **R**eceived **S**ignal **S**trength **I**ndicator (RSSI) is a measurement of the power present in a received radio signal.

- **RSRP - R**eceived **S**ignal **R**eceived **P**ower (RSRP) is an estimated measurement by a device for received signals from an available network.

- **RSRQ - R**eference **S**ignals **R**eceived **Q**uality, A measurement of the received quality (SNR) and SNR is defined as the ratio of signal power to the noise power.

- **SINR - S**ignal to **i**nterference **N**oise **R**atio. A measurement is represented in dB; the greater the value, the better the signal quality.



		RSRP (dBm)	RSRQ (dB)	SINR (dB)
RF Conditions	Excellent	>=-80	>=-10	>=20
	Good	-80 to -90	-10 to -15	13 to 20
	Mid Cell	-90 to -100	-15 to -20	0 to 13
	Cell Edge	<=-100	<-20	<=0

- ODU – **O**ut**d**oor **U**nit. It represents the type of device and characterizes it as an outdoor unit.

- **PIN - P**ersonal **I**dentification **N**umber. It represents an access code made up of four digits. When you buy a SIM card, you also receive a PIN for it. You need this four-digit code to enable the SIM card and access your operator's network once you have inserted it into your device.

- **IP67 - IP** Code or **I**ngress **P**rotection Code is defined in IEC 60529 which classifies and provides a guideline to the degree of protection provided by mechanical casings and electrical enclosures against intrusion, dust, accidental contact, and water.

  6-Totally protected against dust

  7- Protected against the effects of temporary immersion between 15cm and 1m. Duration of test 30 minutes

Regulatory Statements

FCC Equipment Authorization ID: XYO-J912

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

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

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

FCC CAUTION: Any changes or modification not expressly approved by ATEL, the party responsible for compliance could void the user's authority to operate this equipment.
This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

RF Exposure Warning Statements:
The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons during the normal operations.

NOTE: The Radio Frequency (RF) emitter installed in your modem must not be located or operated in conjunction with any other antenna or transmitter, unless specifically authorized by ATEL.

Safety Hazards

Follow Safety Guidelines
Always follow the applicable rules and regulations in the area in which you are using your device. Turn your device off in areas where its use is not allowed or when its use may cause interference or other problems. Note that this type of device should be placed at least 10 ft from work area(s).

Electronic Devices
Most modern electronic equipment is shielded from radio frequency (RF) signals. However, inadequately shielded electronic equipment may be affected by the RF signals generated by your device.

Medical and Life Support Equipment
Do not use your device in healthcare facilities or where medical life support equipment is located as such equipment could be affected by your device's external RF signals.

Pacemakers

- It is recommended to maintain a minimum separation of six inches between a RF device and a pacemaker in order to avoid potential interference with the pacemaker.
- Persons with pacemakers should always follow these guidelines:
- Always keep the device at least six inches away from a pacemaker when the device is turned on.
- Place your device on the opposite side of your body where your pacemaker is implanted in order to add extra distance between the pacemaker and your device.
- Avoid placing a device that is on next to a pacemaker (e.g., do not carry your device in a shirt or jacket pocket that is located directly over the pacemaker).
- If you are concerned or suspect for any reason that interference is taking place with your pacemaker, turn your device OFF immediately.

Hearing Devices

When some wireless devices are used with certain hearing devices (including hearing aids and cochlear implants) users may detect a noise which may interfere with the effectiveness of the hearing device.

Use of Your Device while Operating a Vehicle

Please consult the manufacturer of any electronic equipment that has been installed in your vehicle as RF signals may affect electronic systems in motor vehicles.
Please do not operate your device while driving a vehicle. This may cause a severe distraction, and, in some areas, it is against the law.

Use of Your Device on an Aircraft

Don’t use your device during flight, it may violate FAA regulations. Because your device may interfere with onboard electronic equipment, always follow the instructions of the airline personnel and turn your device OFF.

Blasting Areas

In order to avoid interfering with blasting operations, your device should be turned OFF when in a blasting area or in an area with posted signs indicating that people in the area must turn off two-way radios. Please obey all signs and instructions when you are in and around a blasting area.

Proper Battery & Adapter Use and Disposal

- Do not disassemble or open, crush, bend or deform, puncture or shred.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, expose to fire, explosion or another hazard.
- Only use the battery for the system for which it is specified.
- Do not short circuit a battery or allow metallic conductive objects to contact battery terminals.
- Replace the battery only with another battery that has been qualified with the system per this standard. Use of an unqualified battery may present a risk of fire, explosion, leakage or another hazard. Only authorized service providers shall replace the battery.
- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.
- Avoid dropping the battery. If the battery is dropped, especially on a hard surface, and the user suspects damage, take it to a service center for inspection.
- Improper battery use may result in a fire, explosion or another hazard.

Disclaimer

Certain variations may be present between the device and user manual description depending on software release or specific network services. ATEL shall not be held legally responsible for such deviations, if any, nor for their potential consequences.

Limited Warranty

The full ATEL USA Warranty Policy can be found at www.atel-usa.com/warranty. On this page you can “Start a Warranty Claim”, “Check on an Existing Claim” and read our Warranty Policy by clicking on “ATEL’s Warranty Policy”. Please follow all warranty instructions available and if you have any questions contact us at support@atel-usa.com.

Trademark