LTE CPE（J912）User Manual

Index

1. About this Manual

The content of this User Manual has been made as accurate as possible. However, due to continual product improvements, specifications and other information are subject to change without notice.

2. Product Overview

This CPE supports LTE Band (Subject to the configuration of LTE module) and it supports popular operating systems like Windows, Linux and Mac.

Please refer to the Quick Start Guide that is part of the CPE supply. Once you have identified the place for CPE, insert USIM card supplied by your service provider at the appropriate place, plug in the adapter in the AC socket and DC in the power port of CPE. Switch on the power Off/On switch and after few minutes the CPE should attach itself to the LTE network. It is as simple as that. It is advised to read this manual at leisure to make best use of the CPE.

3. Configuring the CPE

The basic settings in WebGUI consist of four main parts named Home, Diagnostics, Settings, LTE. You can login to WebGUI as follows, and configure the settings according to your requirements.

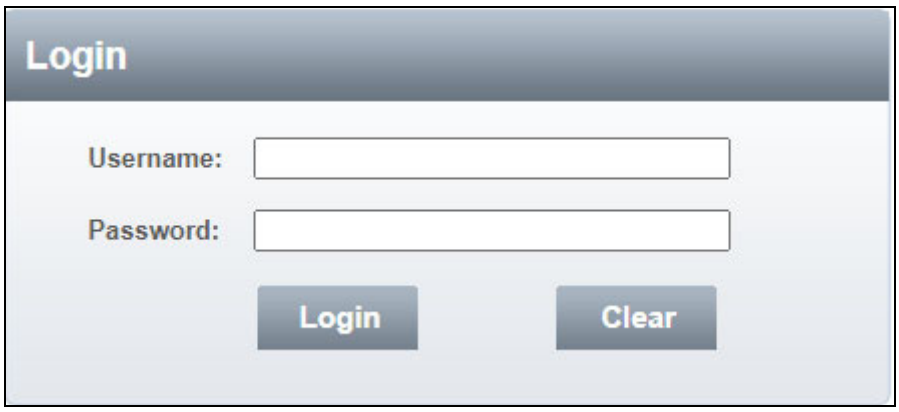
3.1 Login

Open your Web browser and enter 192.168.0.1 in the address bar;

Login window will popup;

When prompted for User name and password, enter the following username and password.

Username/Password: admin/admin

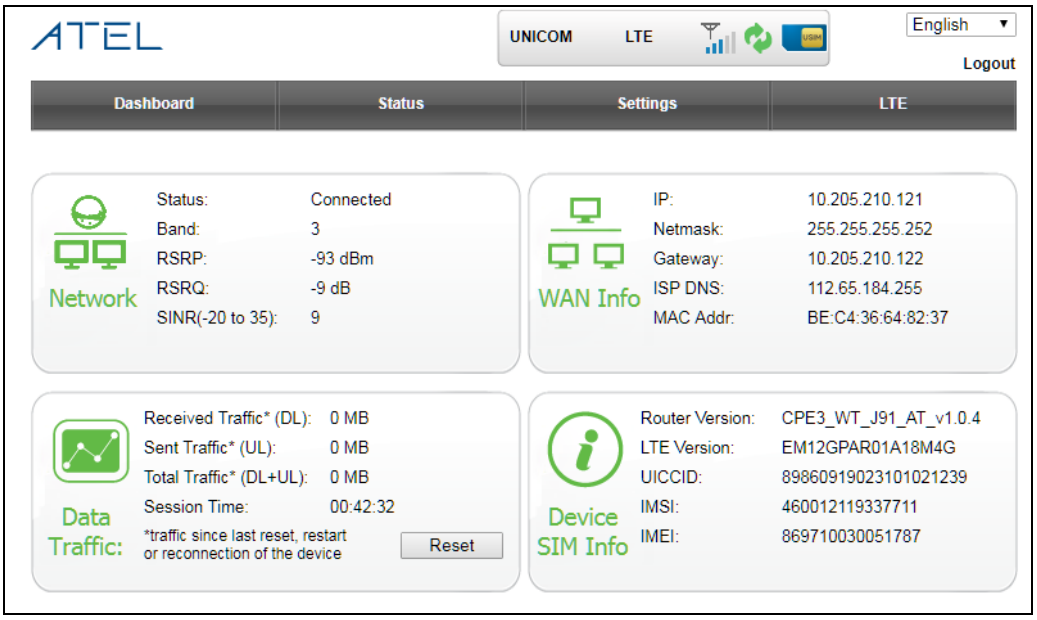


3.2Dashboard

After successful login, the following screen will appear and you will see four main menus on the top bar of the WebGUI.

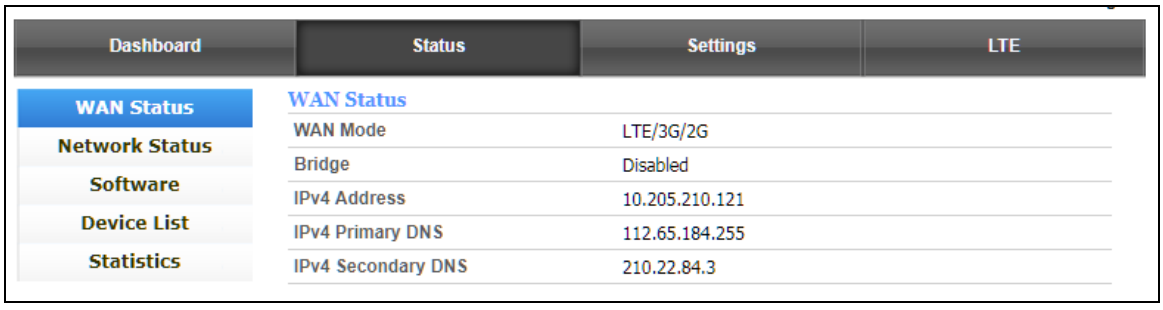
The bars in the middle indicate the received signal level and USIM icon displays the status of USIM. Click “Logout”, the screen will turn to login window.

From this page, you can also know the LTE network status and the LTE data transmission. Click “OK”, it will take you to the device settings page, then you can modify the password as you like (32 characters max). Login the system by the new password, you can see the home page.



3.3 Status

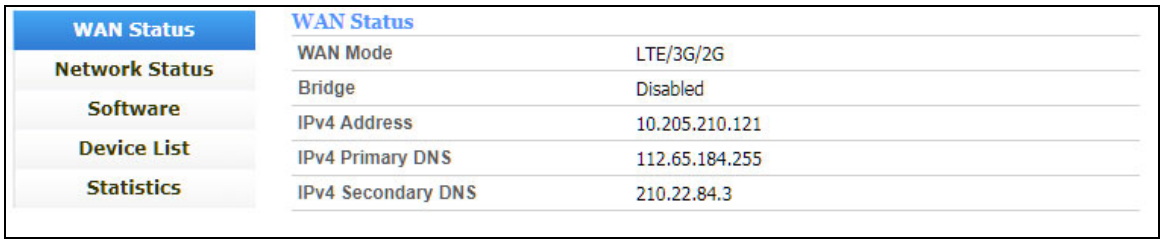
On this page, you can see WAN Status, Network Status, Software, Device List and Statistics.



3.3.1 WAN Status

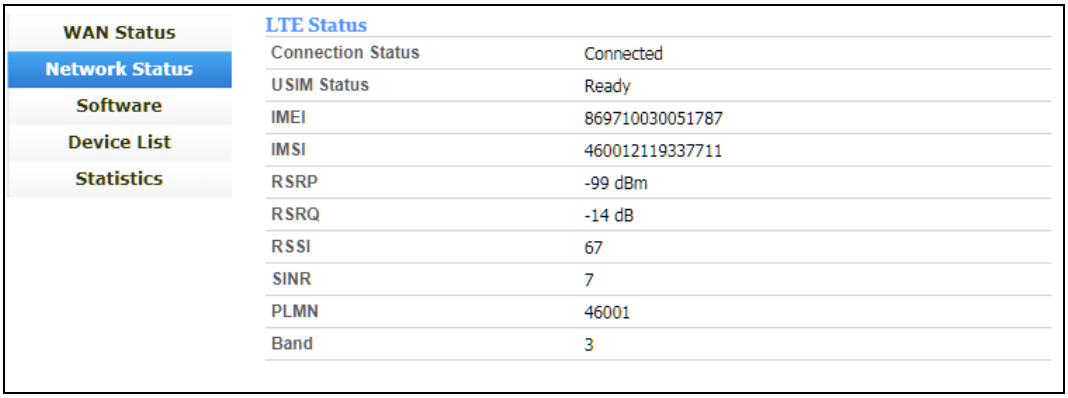
From the WAN Status, you can see WAN Mode,Bridge,IPv4 Address, WAN

Primary DNS and DNS information.



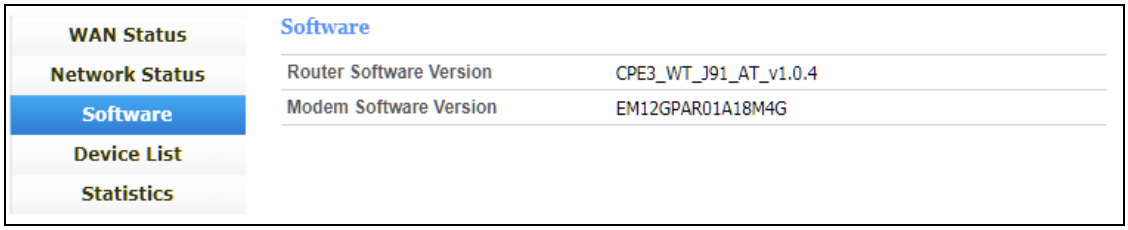
3.3.2 Network Status

Clicking on the "Network Status", you can see the LTE information i.e. Connection Status, USIM Status, IMEI, IMSI, RSRP, RSRQ, RSSI, SINR, PLMN and Band.



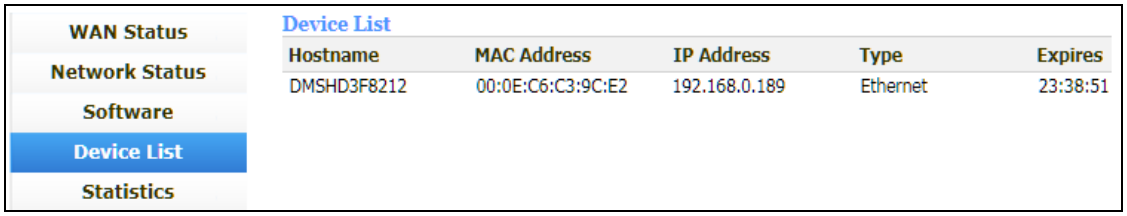
3.3.3 Software

Clicking on the "Software", you can see the Router Software version and Modem Software Version.



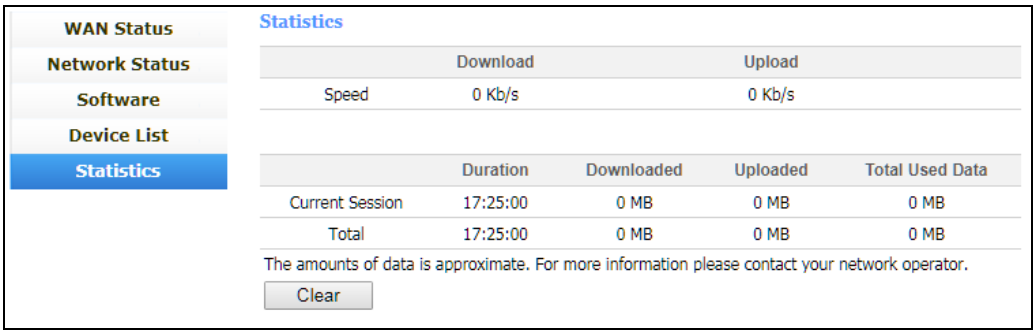
3.3.4 Device List

From the device list, you can know the users'hostname, MAC address, IP address ,Type and expires time.



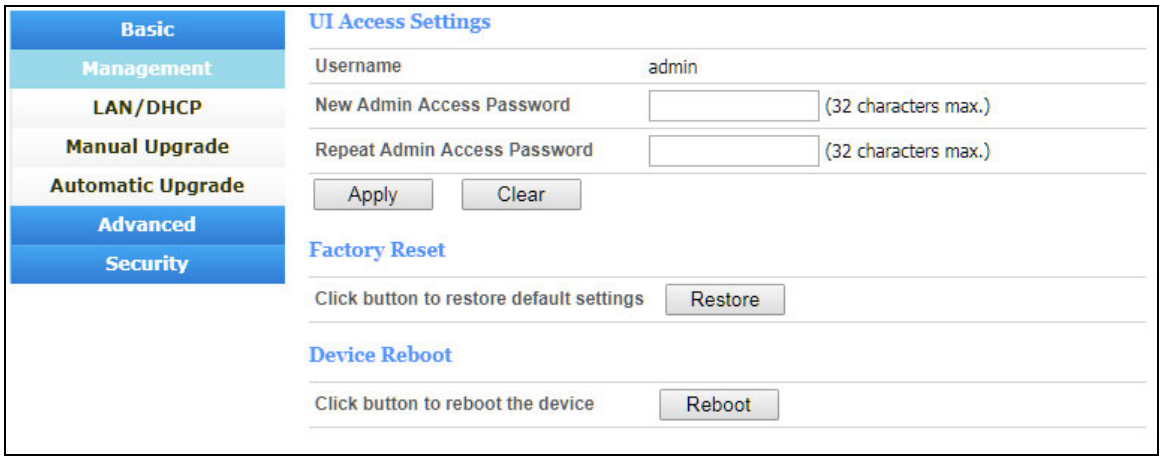
3.3.5 Statistics

From the device list, you can know the speed, Download, Upload and Total Used Data.



3.4 Settings

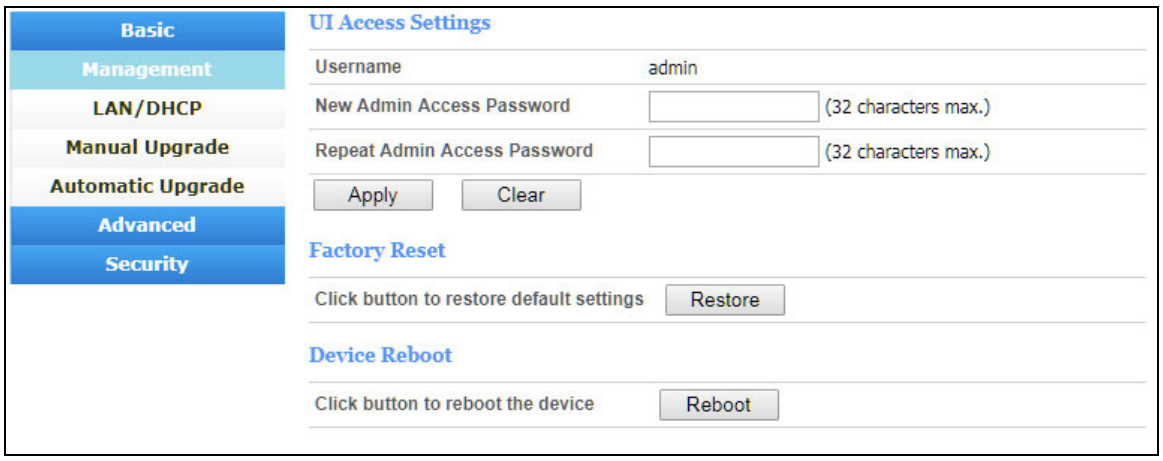
The settings menu consists of three main menus named Basic advanced and Security settings.



3.4.1 Basic

3.4.1.1 Management

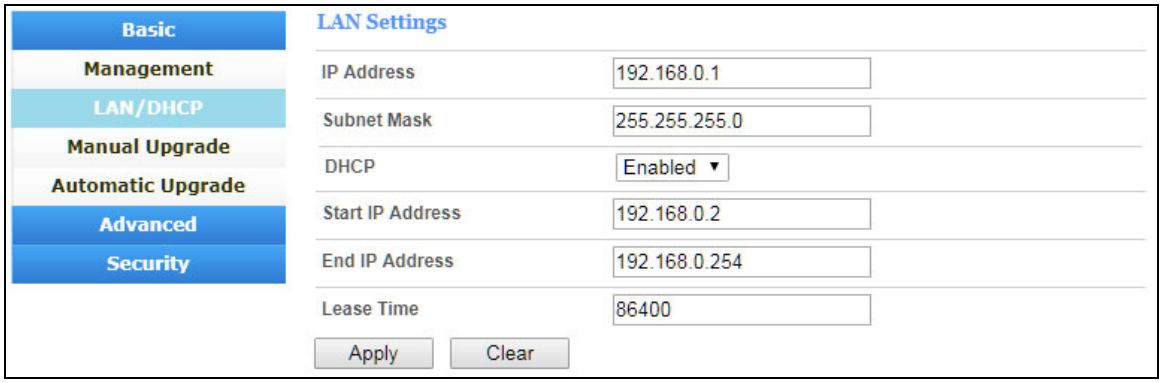
On this page, you can see UI Access Settings, Factory reset and device reboot.



- **UI Access Settings –**The default password is admin, you can enter 1~32 characters for 2 times as your new password. Then you would logout automatically and you should login to the system by the new password.
- **Factory Reset –**From this page, you can click the "Restore" button to load default to the factory setting.
- **Device Reboot–**From this page, you can click the "Reboot" button to restart the device.

3.4.1.2 LAN Settings

Clicking on the "LAN Settings" tab will take you to the "LAN Settings" header page. On this page, all settings for the internal LAN setup of the CPE router can be viewed and changed.



- **IP Address -** Enter the IP address of your router (factory default: 192.168.254.251).

- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **DHCP Type** - Enable or Disable the DHCP server. If you disable the Server, you must have another DHCP server within your network or else you must configure the address of your PC manually.
- **Start IP Address** - Specify an IP address for the DHCP server to start with when assigning IP address. The default start address is 192.168.254.2.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP address. The default end address is 192.168.254.200.
- **Lease Time** - The Lease Time is the amount of time a network user will be allowed connection to the router with their current dynamic IP address. Enter the amount of time in minutes and the user will be "leased" this dynamic IP address. After the time is up, the user will be assigned a new dynamic IP address automatically.

☞ **Note:**

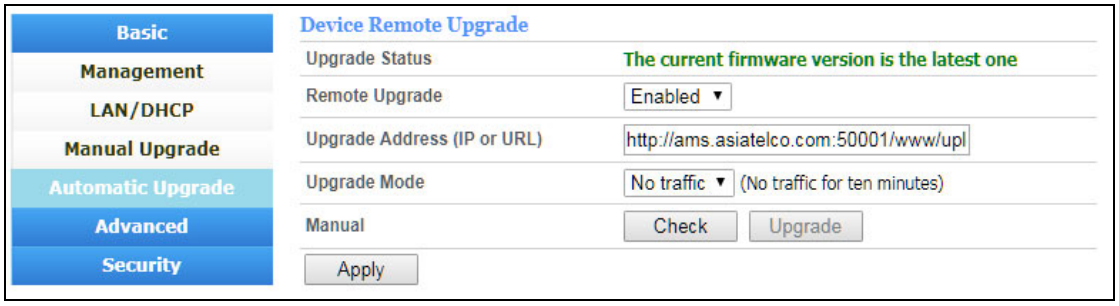
1. If you change the IP Address of LAN, you must use the new IP address to login to the CPE router.
2. If the new LAN IP address you set is not in the same subnet, the IP address pool of the DHCP server will change at the same time, while the Virtual Server and DMZ Host will not take effect until they are re-configured.

3.4.1.3 Device Software Upgrade

On this page, you can upgrade the current Router version from the local PC. 100s is needed to complete the whole upgrade process, and then the device will reboot automatically

3.4.1.4 Automatic Upgrade

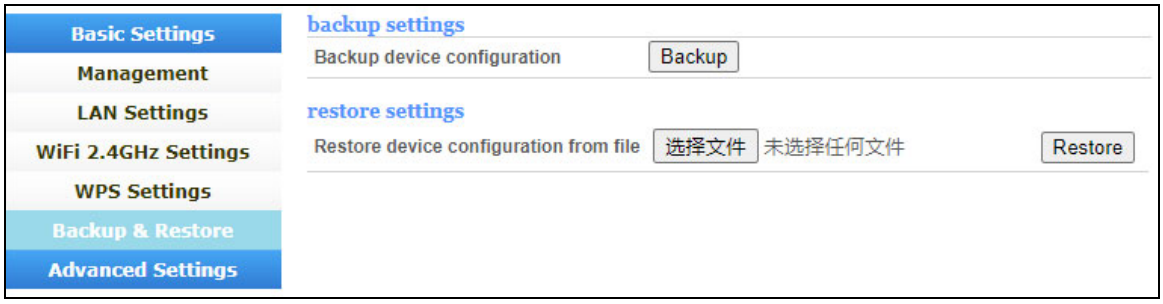
You should enable the Remote Upgrade before you use this function.



Backup &Restore

Clicking the “Backup” button, the current settings will be saved as a data file to the local PC. You can restore the device configuration from the files that you saved.

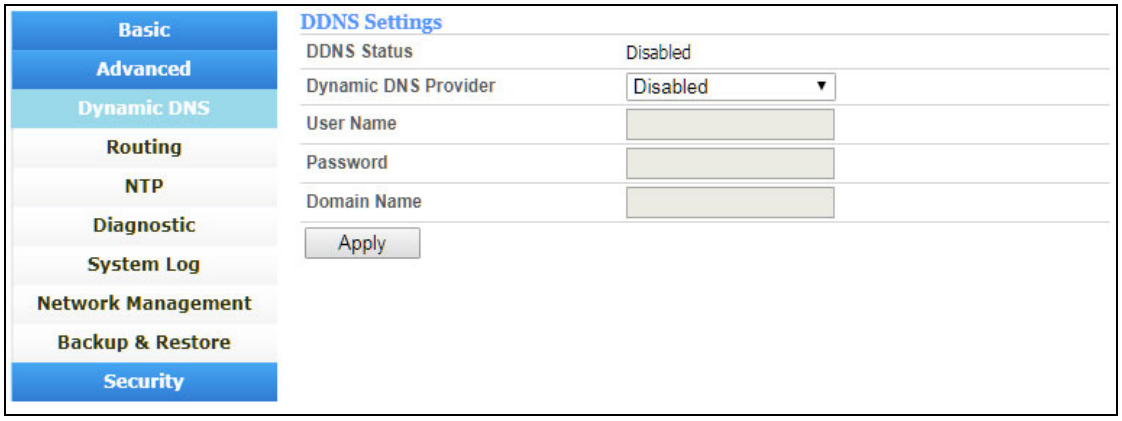
Click the “Restore” button to load default to the factory setting.



3.4.2 Advanced

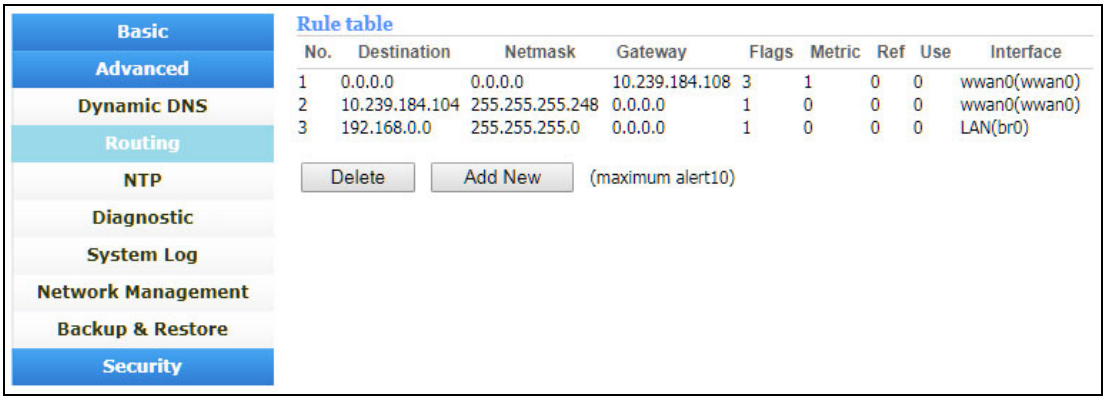
3.4.2.1 Dynamic DNS

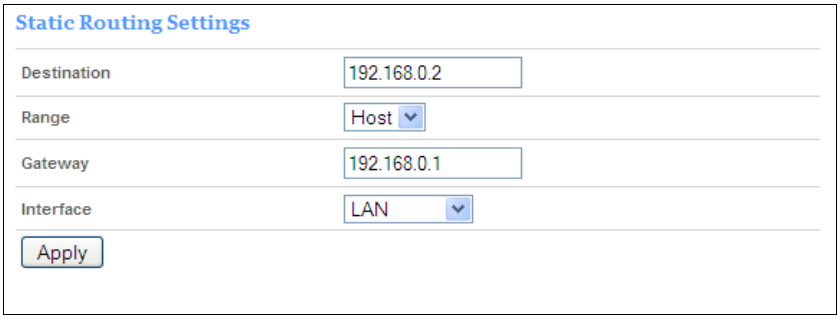
The dynamic DNS function is disabled in default, you can choose the dynamic DNS provider to configure the DDNS settings.



3.4.2.2 Routing

From the rule table, you can see the default route information. Clicking on the "Add New" button, you can configure the static routing setting. The new rules will be shown on the rule table, here you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 10.

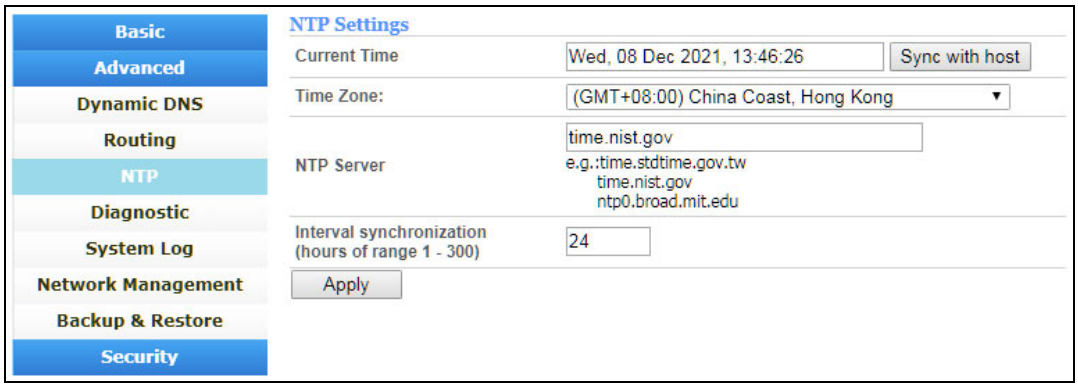




- **Destination:** The address of the network or host that assigned by the static route;
- **Range:** Host/Net;
- **Gateway :** This is the IP address of the gateway device that is used to contact between the router and the network or host;
- **Interface:** LAN/WAN/Custom;
- **RIP**: Enable the RIP, every 30 seconds, the system will update and learn the routing information nearby automatically.

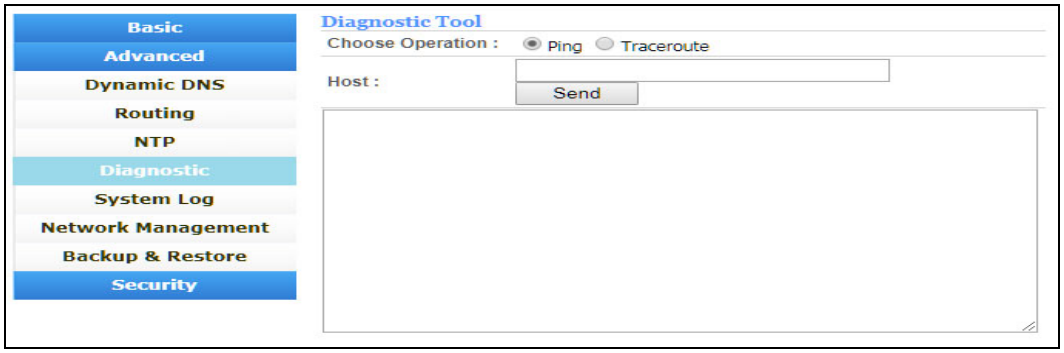
3.4.2.3 NTP

From this page, you can set the Current Time, Time Zone, NTP Server and NTP synchronization. When the device obtains the WAN IP, the current time will synchronize with the NTP server automatically.



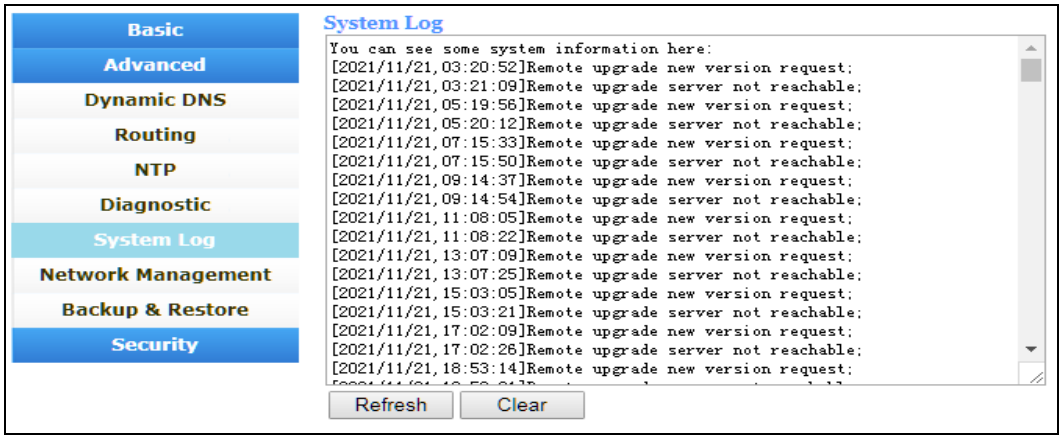
3.4.2.4 Diagnostic

From this page,you can ping and Traceroute IP.



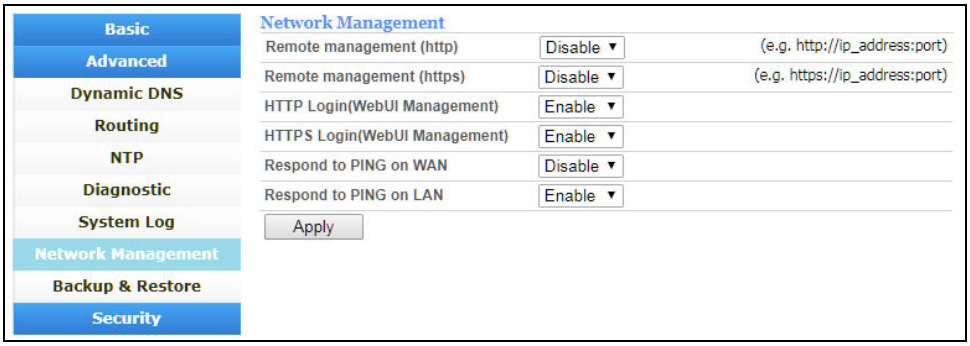
3.4.2.5 System Log

From this page,you can check System log.



3.4.2.6 Network Management

You can configure the system security settings to protect the device itself from the external attacking.



➢ **Remote management(http)**

You can access to the router via http IP address and achieve the remote control function when the remote management feature is enabled.

➢ **Remote management(https)**

You can access to the router via https IP address and achieve the remote control function when the remote management feature is enabled.

➢ **HTTP Web Login**

This function allows the users to login the system by the http protocol method.

➢ **HTTPS Web Login**

This function allows the users to login the system by the https protocol method.

➢ **Respond to PING on WAN**

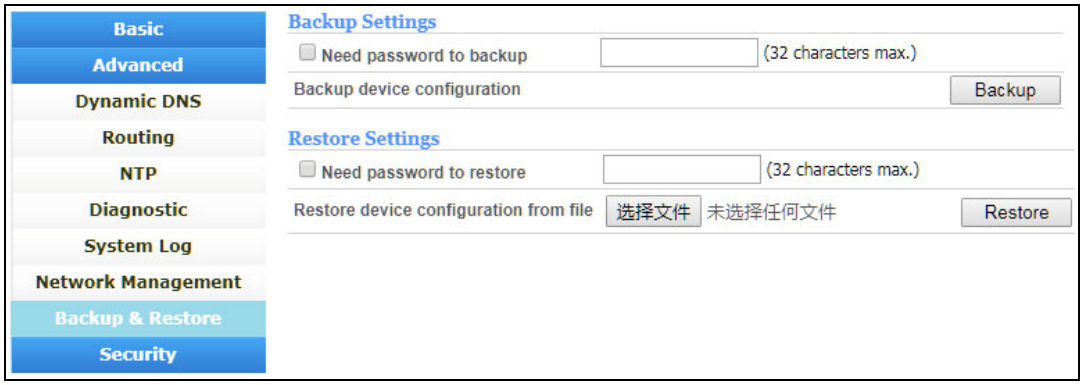
It is allowed to ping on WAN in default, you can disable it here.

➢ **Respond to PING on LAN**

It is allowed to ping on LAN in default, you can disable it here.

3.4.2.7 Backup&Restore

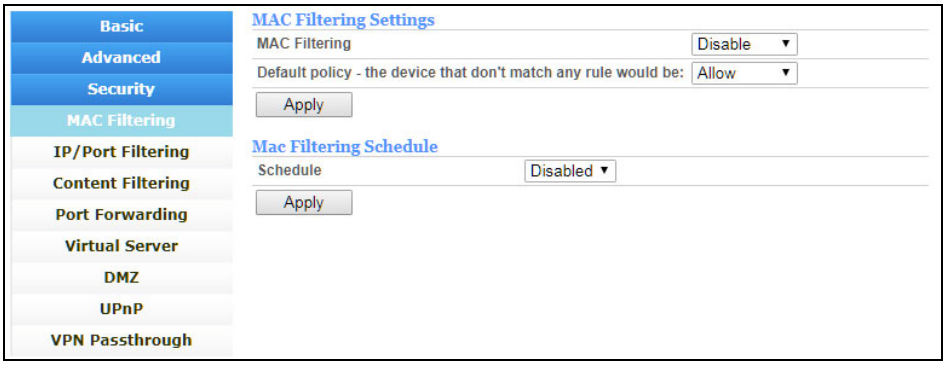
Clicking the “Backup” button, the current settings will be saved as a data file to the local PC. You can restore the device configuration from the files that you saved.



3.4.3 Security

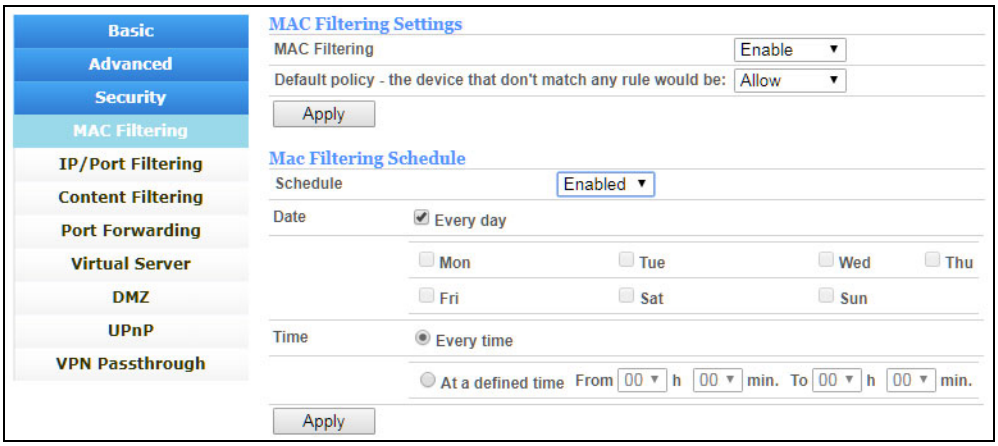
3.4.3.1 MAC Filtering

This function is a powerful security feature that allows you to specify which wireless client users are not allowed to surf the Internet.



The default MAC filtering setting is disabled, so you should enable it before you begin to configure the filter. Then click the "Add New" button, you can configure the rules you like.

Mac Filtering Schedule: MAC devices that do not comply with the Schedule would be "Allow/Deny".



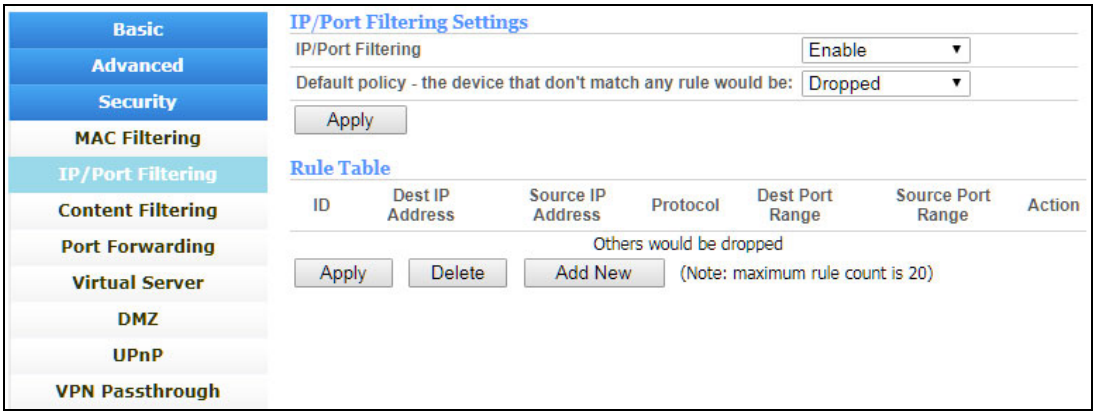
3.4.3.2 IP/Port Filtering

From this page, you can configure the IP/Port filter to forbid relevant users to login the router device.

The default IP/Port filter setting is disabled, so you should enable it before you begin to configure the filter. Then clicking the "Add New" button, you can configure the settings you like (Figure 3-4-2-2-3).

Default Policy: The packets that don't match with any rules would be "Dropped/Accepted". If you choose "Dropped" here, the action of the new rule

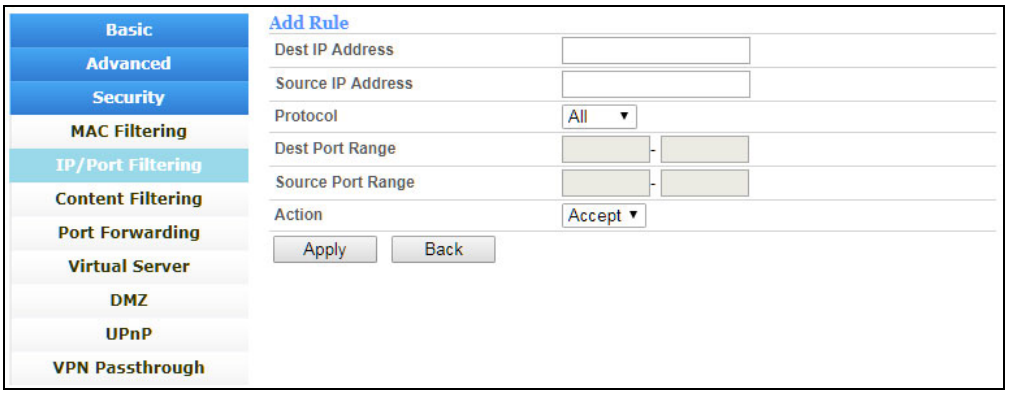
would be “Accept”. Otherwise, the action turns to be “Drop” and the packet that don’t match with any rules would be accepted.



Dest IP Address – The IP address of a website that you want to filter (Such as google 74.125.128.106).

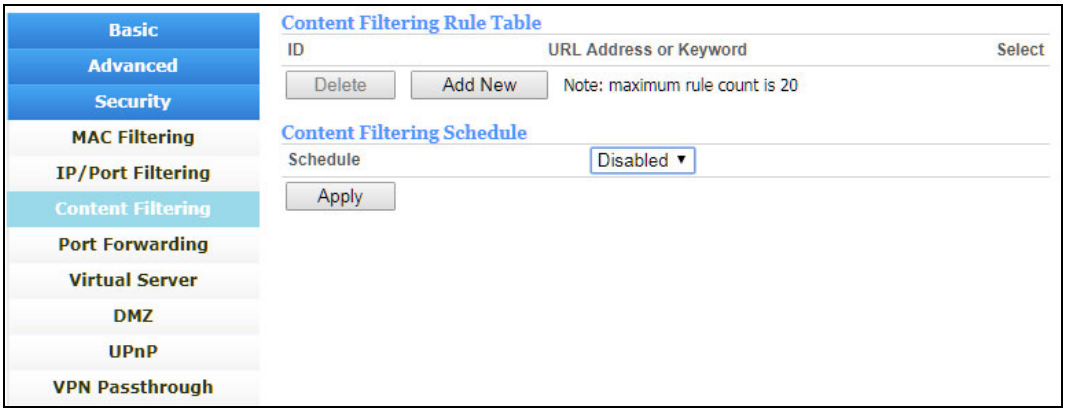
- **Source IP Address -** The IP address of PC. (Such as 192.168.0.2).
- **Protocol-** TCP, UDP, ICMP
- **Dest Port Range-** To restrict Internet access to the single user, you can set a fixed value, such as 21-21.
- **Source Port Range-** 1~65535
- **Action-** Accept, Drop

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially . The maximum rule count is 10.



3.4.2.3 Content Filtering

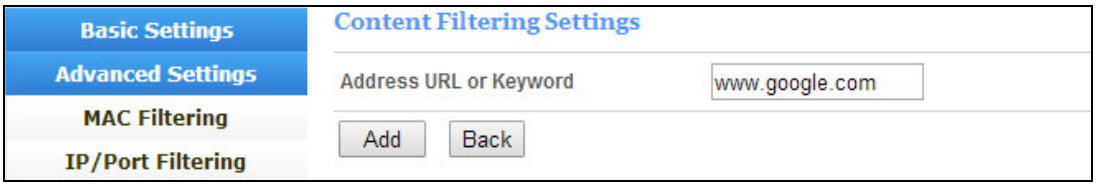
From this page, you can configure the URL filter and the content filtering schedule.



- **Content Filtering**

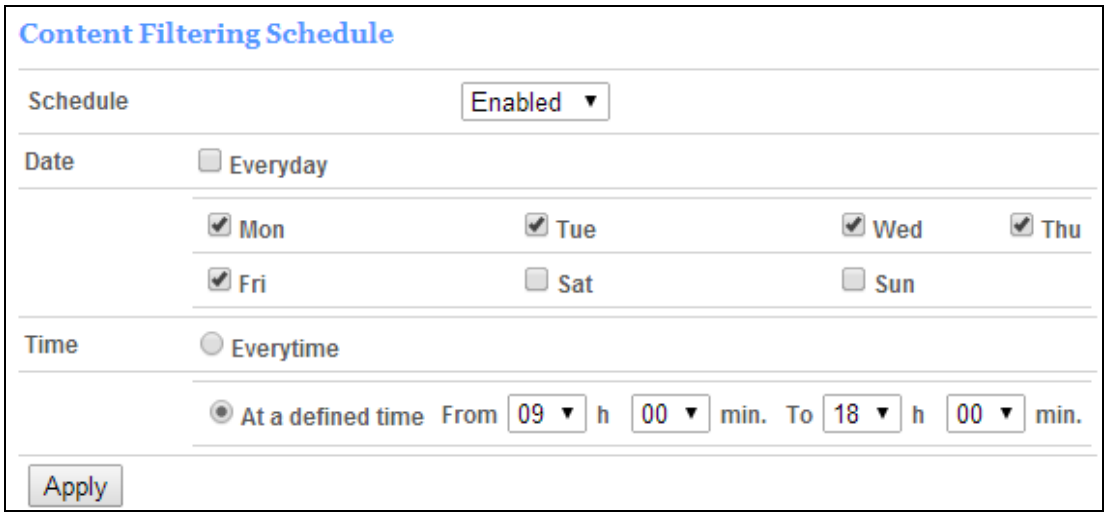
It is a function that forbids users to login the URL or keyword on the rule table. You can configure the settings you like by clicking the “Add New” button.

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially. The maximum rule count is 8.



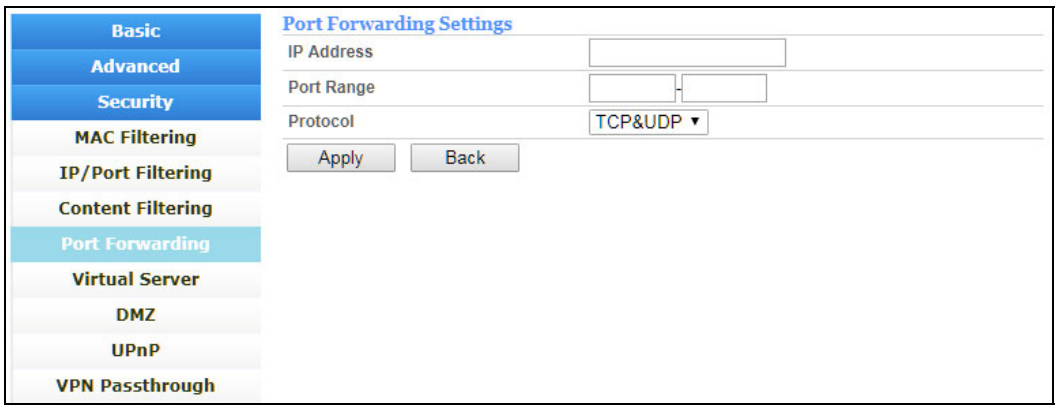
- **Content Filtering Schedule**

Here you can configure the schedule to define when the rules take effect. This feature is disabled in default, you should enable it first and then configure the date and time, such as working time. Click the “Apply” button, you can see the new rule on the content filtering page.



3.4.2.4 Port Forwarding

Clicking on the header of the "Port Forwarding" button will take you to the "Port Forwarding" header page. Clicking on the "Add New" button, you can configure IP address, port range to achieve the port forwarding purpose.

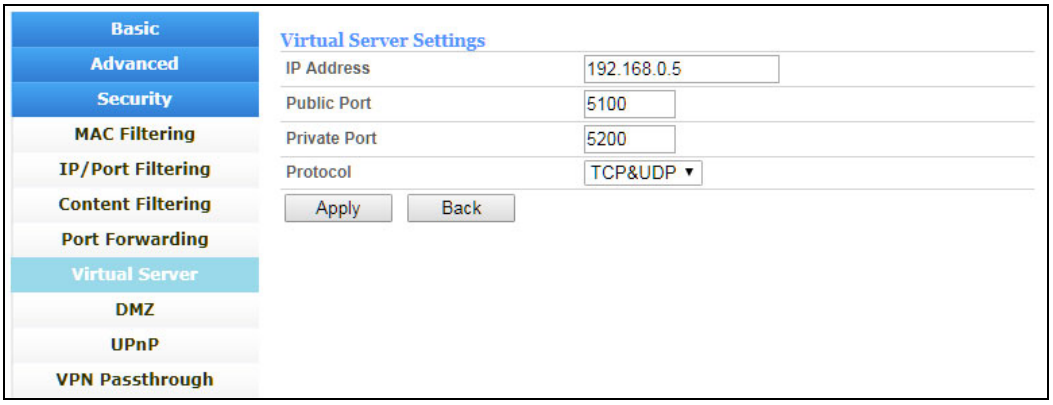


- **IP Address-** The IP address of the PC running the service application;
- **Port Range-** You can enter a range of service port or set a fixed value;
- **Protocol-** UDP, TCP, TCP&UDP.

The new rules will be shown on the rule table, you can delete the items that you have selected or add new rules by clicking the "Add New" button here. The maximum rule count is 20.

3.4.2.5 Virtual Server

Clicking on the header of the "Virtual Server" button will take you to the "Virtual Server" header page. It is a feature that similar to port forwarding, clicking on the "Add New" button, you can configure IP address, public port, private port and protocol to achieve the virtual server function.



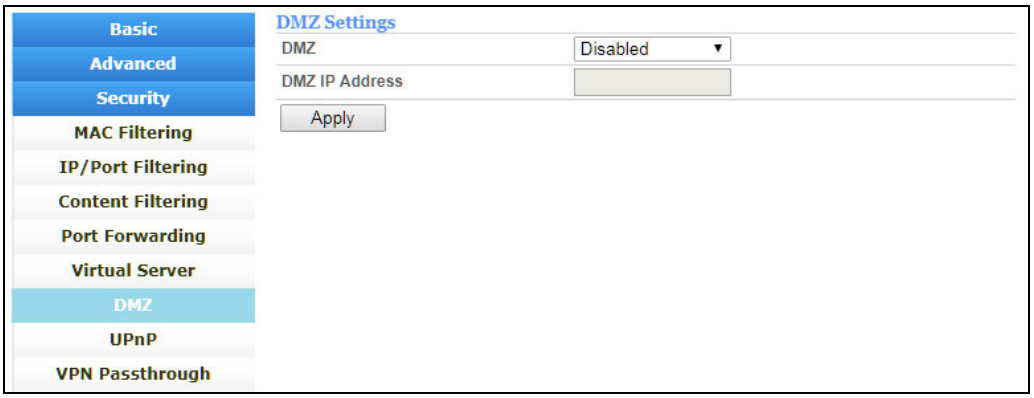
- **IP Address-** The IP address of the PC running the service application;
- **Public Port-** The port of server-side;
- **Private Port-** The port of client-side, it can be same with the public port;
- **Protocol-** UDP, TCP, TCP&UDP.

The new rules will be shown on the rule table, you can delete the items that you have selected or add new rules by clicking the "Add New" button here. The

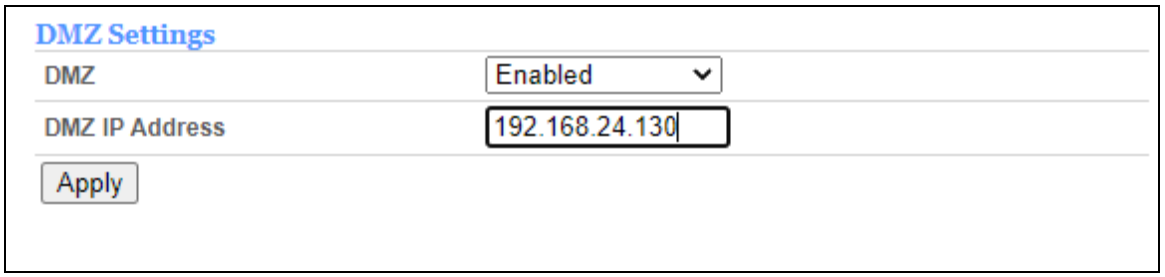
maximum rule count is 20.

3.4.2.6 Demilitarized Zone

From this page, you can configure a De-militarized Zone (DMZ) to separate internal network and Internet.

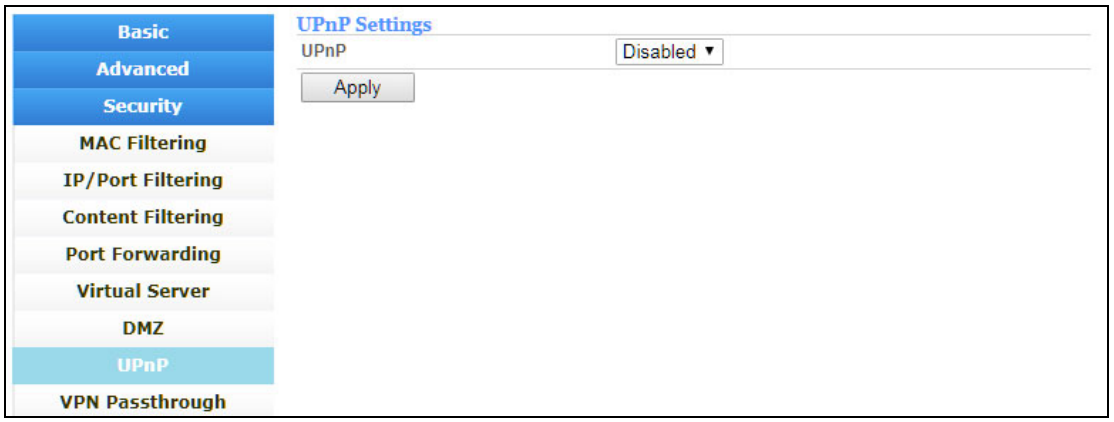


- **DMZ IP Address-** The IP address of your PC. (such as 192.168.254.130)



3.4.2.7 Upnp

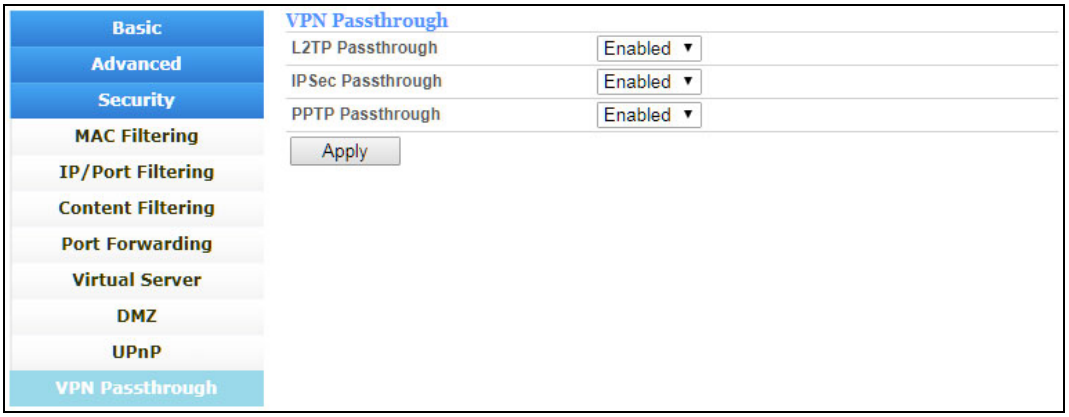
The UPnP function is Enabled in default, you should enable it on the system security page. before using it. The new rules that you added will be shown on this page.



3.4.2.8 VPN Passthrough

A virtual private network (VPN) is a point-to-point connection across a private or public network (Internet).

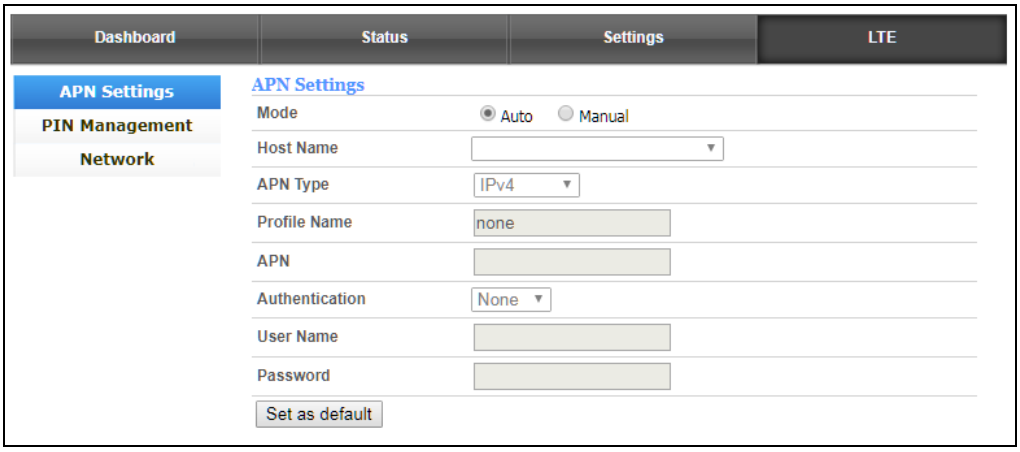
VPN Passthrough allows the VPN traffic to pass through the router. Thereby we can establish VPN connections to remote network. For example, VPNs allow you to securely access your company's intranet at home. There are three main kinds of the VPN tunneling protocol, PPTP, L2TP and IPSec.



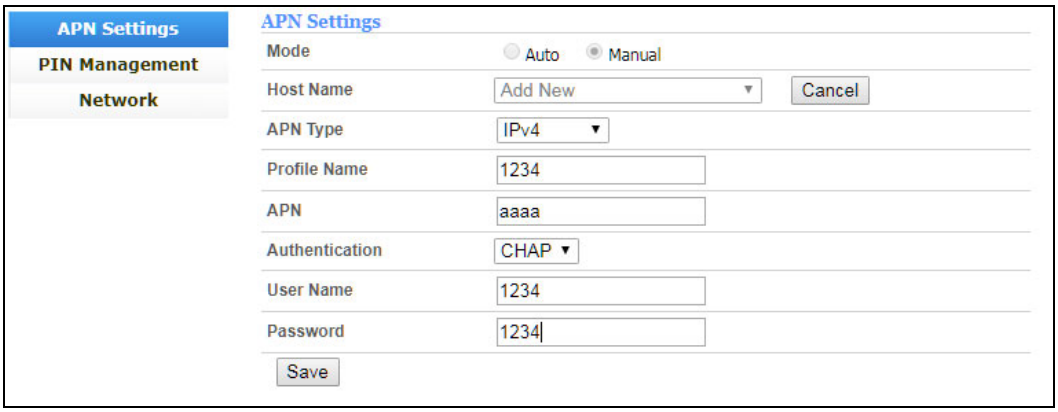
3.5 LTE

3.5.1 APN Settings

The default APN mode is automatic and APN is NULL, if you want to configure the LTE APN, you should choose the manual mode, then you can configure the APN settings by clicking on the “Add New” button.



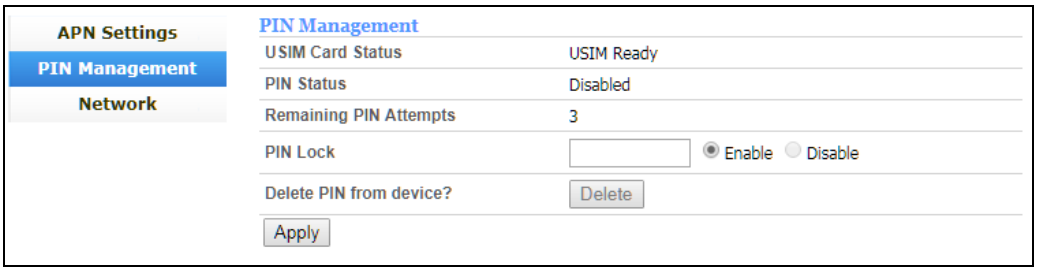
From the "Host Name" option, you can choose the APN that you had configured, then click "Set as default" to make it take effect.



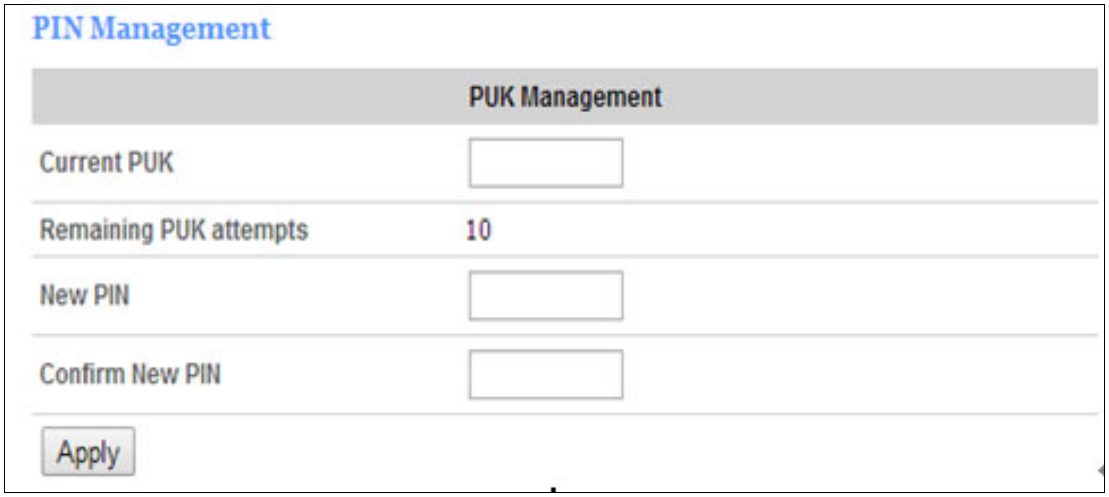
3.5.2 PIN Management

From this page, you can see the USIM card status and PIN status.

The default PIN status is disabled, you can input the correct PIN to enable the PIN function. The maximum PIN attempts are 3, otherwise you must enter PUK to reset the PIN code. The USIM will be invalid after the unsuccessful attempts for 10 times.



- **PIN Management**: Enter the correct PIN to enable or disable the PIN function, PIN code should be 4 to 8 digits;
- **Save PIN**: The system will remember the PIN code of the USIM and verify the USIM automatically if the save PIN function is enabled.
- **PIN change:** You can input the current PIN code 1 time and the new PIN code for 2 times to change the PIN code. PIN code should be 4 to 8 digits.
- **PUK Management**: Input the correct PUK code and the new PIN code for 2 times to reset the PIN code. The PIN code should be 4 to 8 digits.



4. Revision History

Author	Revision	Changes	Date
Jiawang	1.0	Create Draft	2021-12-08

FCC Regulations:

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

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

Changes or modifications not expressly approved by the manufacturer could void the user’s authority to operate the equipment.

FCC RF Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. To comply with FCC RF Exposure compliance requirements, this grant is applicable to only Mobile Configurations. The antennas used for the transmitter must be installed to provide a separation distance of at least 20cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.