M4D-UC User Manual

Note:

Operating temperature: -30°C to 65°C (-22°F to 149°F).

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

M4D-UC is HPUE CPE.

3. Configuring the CPE

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

Connect the PC to CPE using the Ethernet cable. Use any one of the four Ethernet ports on the CPE. Power on the device and waiting for about one minutes until the device finished initializing. Please ensure that USIM card has been inserted into USIM slot in CPE.

You can also connect the PC to CPE by WiFi, choose the correct WiFi SSID and input the accurate password as the label shows. The default WiFi SSID is ice.net-XXXXXX, XXXXXX denotes the last six digits of the CPE's MAC address.

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/ FBB0662C

3.2 Dashboard

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

The bars at the top right corner indicate the received signal level, connection status and USIM icon displays the status of USIM., Click “Logout”, the screen will turn to login window.

From this page, you can also know 4G status, Wi-Fi status, WAN Info, LAN Info, Data Traffic and Device&SIM Info.

3.3Status

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

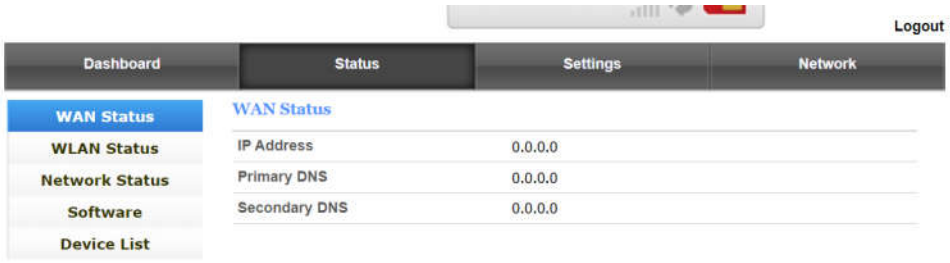

Figure 3-3-1 Status

3.3.1 WAN Status

From the WAN Status, WAN IP Address, WAN Primary DNS and WAN Secondary DNS information can be displayed

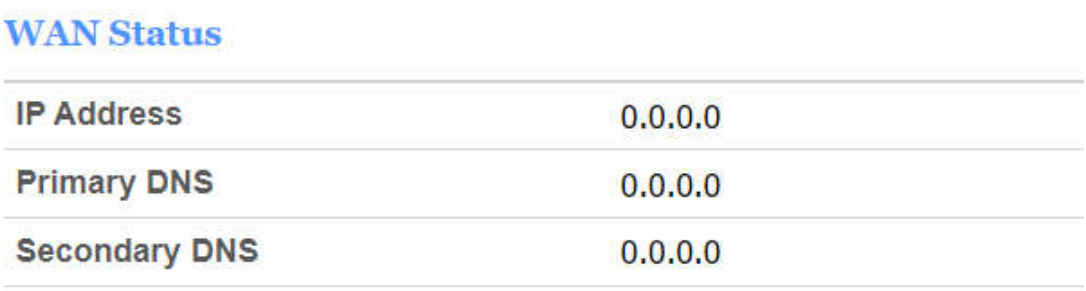

Figure 3-3-1-1 WAN Status

3.3.2 WLAN Status

From this page, you can know the WLAN Status such as SSID, Channel, Security, Key, LAN IP and DHCP Server.

3.3.3 Network Status

Clicking on the “network Status”, you can see the LTE information such as Connection Status, USIM Status, IMEI, IMSI, RSRP, RSRQ, RSSI, SINR, Localization and Frequency.

3.3.4 Software

This page is used to display Router software version, Modem software version.

Figure 3-3-4-1 Software

3.3.5 Device List

All clients connect to CPE can be displayed. You can see the users’ information, include hostname, MAC address, IP address and expires time.

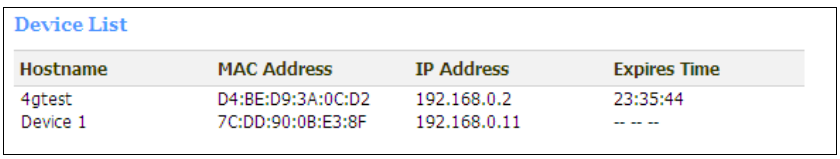

Figure 3-3-5-1 Device List

3.4 Settings

The setting menu consists of three main menus named Basic Settings, Advanced Settings.

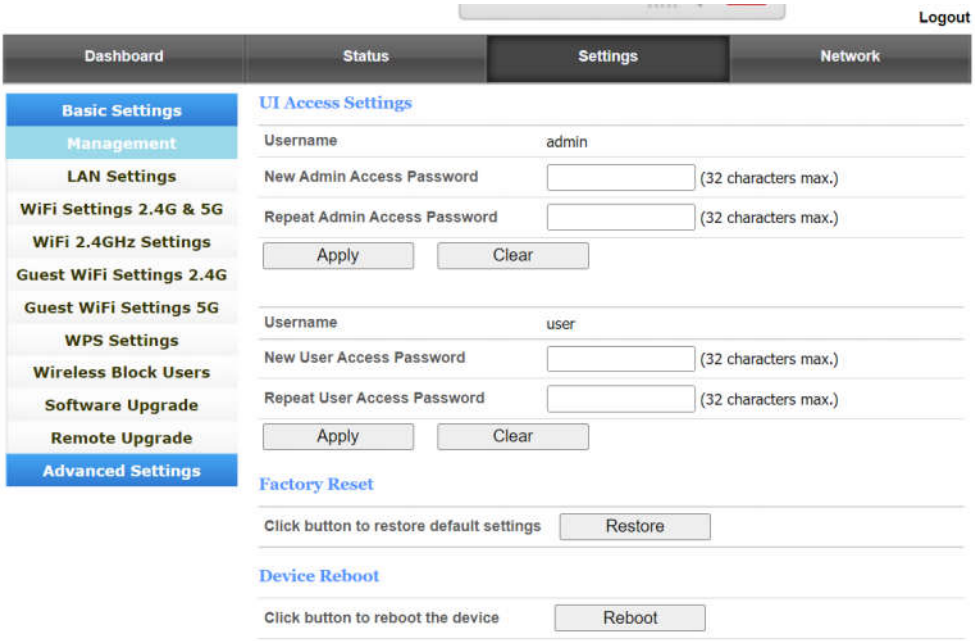

Figure 3-4-1 Settings

3.4.1 Management

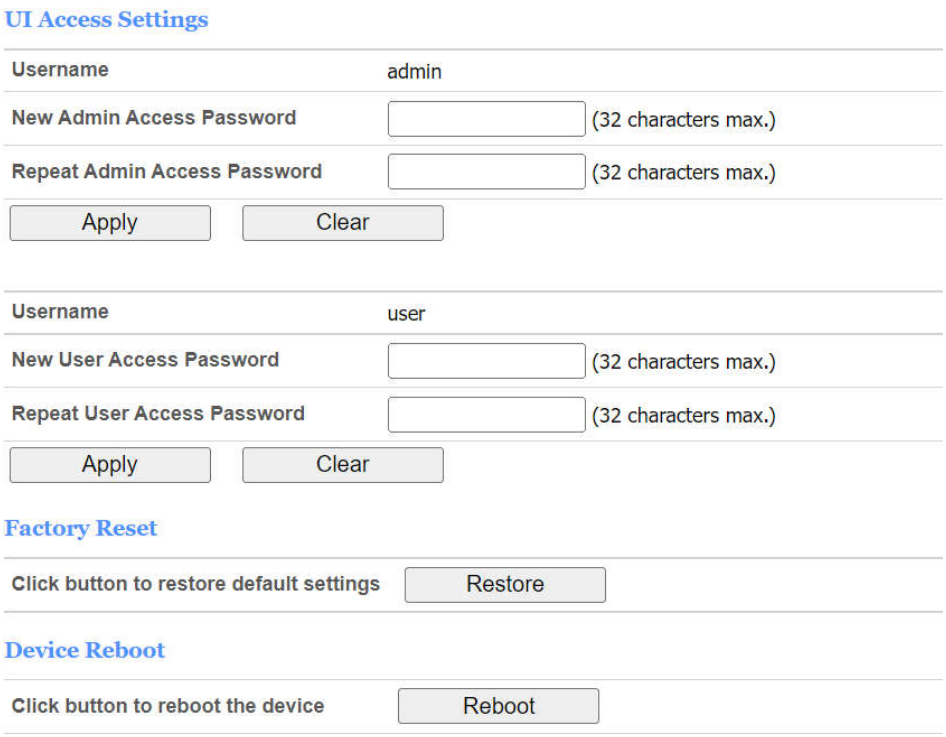

Figure 3-4-1-1 Management

3.4.1.1 UI Access Settings

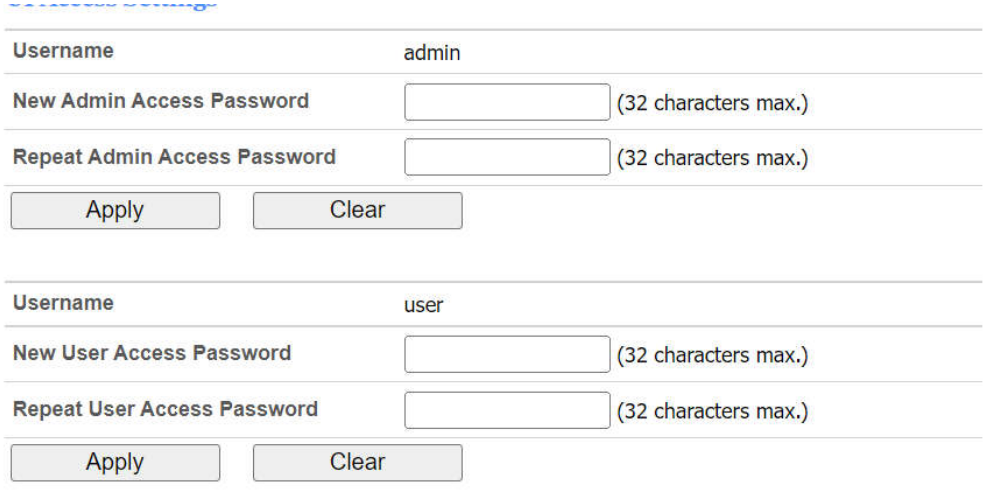

Figure 3-4-1-1 UI access settings

3.4.1.2 Reset&Reboot

From this page, you can click the “Restore” button to load default to the factory setting and click the “Reboot” button to reboot the device.

Figure 3-4-1-2 Reset&Reboot

3.4.2 Basic Settings

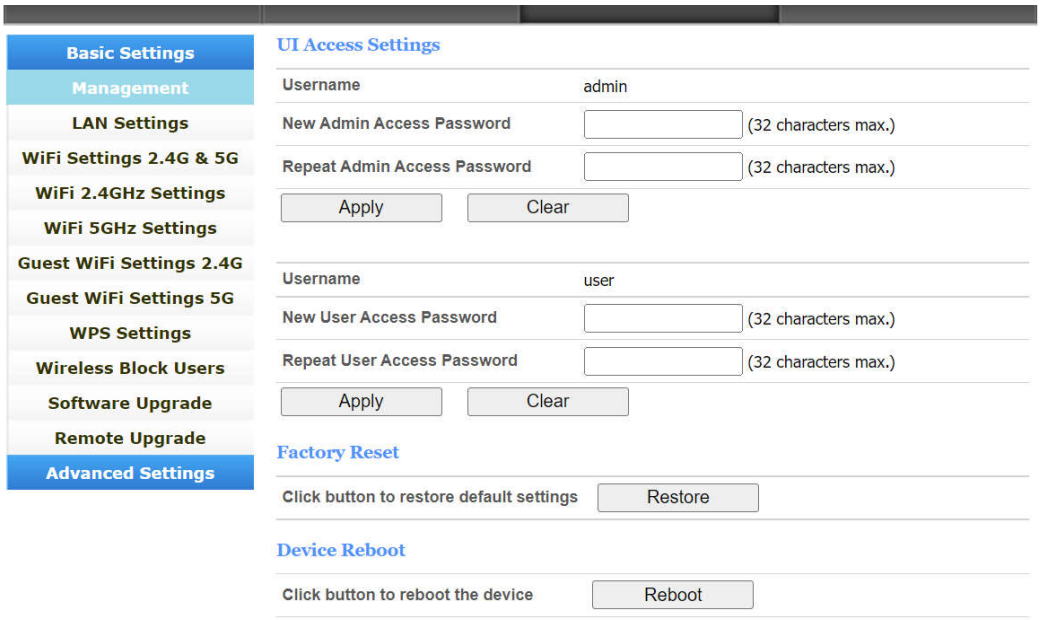

Figure 3-4-2-1 Basic Settings

3.4.2.1 LAN Setting

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.

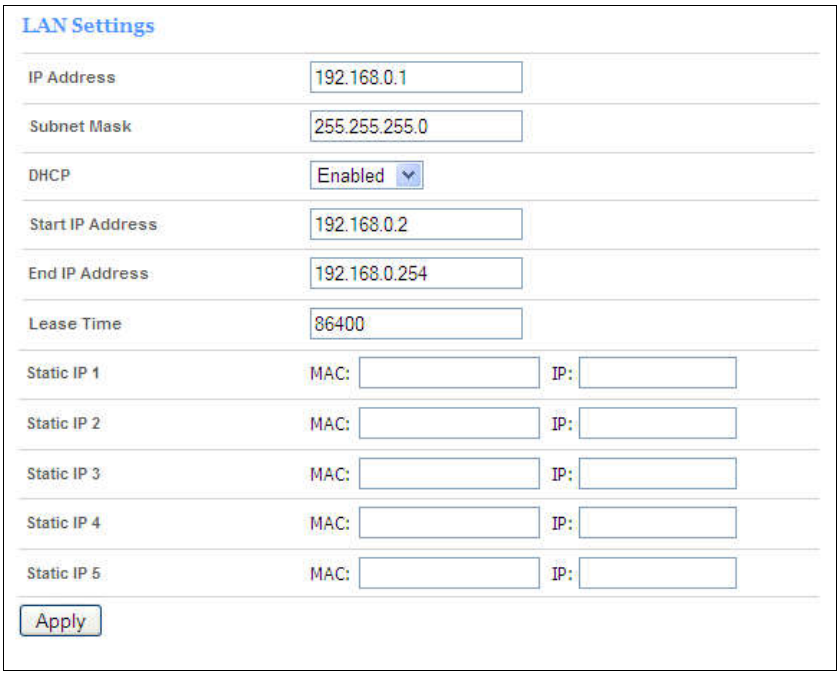

Figure 3-4-2-1-1 LAN Settings

- **IP Address -** Enter the IP address of your router (factory default: 192.168.0.1).
- **Subnet Mask** - An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
- **DHCP** - Enable or Disable the DHCP. If you disable the DHCP function, Client cannot get valid IP address from CPE automatically. But you can configure the address of your PC manually to connect CPE.
- **Start IP Address** - Specify an IP address for the DHCP server to start with when assigning IP address. The default start address is 192.168.0.2.
- **End IP Address** - Specify an IP address for the DHCP Server to end with when assigning IP address. The default end address is 192.168.0.254.
- **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.
- **Static IP** - IP/MAC binding function, the system will assign a fixed IP address to the MAC according to the rules.

☞ **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.

3.4.2.2 WiFi Settings

Clicking on "WiFi Settings" will take you to the following header and on this page you can configure the WiFi settings and WiFi security.

- **WiFi Settings**

You can set the WiFi status, configure the WiFi standard, configure the network name and select the WiFi channel from 1 to 11.

➢ **WiFi Status:** Enabled(default)/Disabled

The WiFi status is enabled in default; you can only connect to the device by CAT-5 Ethernet cable if it is disabled.

➢ **WiFi Standard:**

The router can be operated in five different wireless modes: "11b only", "11g only", "11n only", "11b/g mixed mode" and"11b/g/n mixed mode".

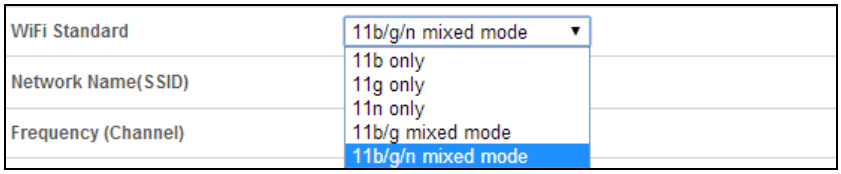

Figure 3-4-2-2-2 WiFi standard

➢ **Network Name(SSID)**

To identify your wireless network, a name called the SSID (Service Set Identifier) is used. You can set it to anything you like and you should make sure that your SSID is unique if there are other wireless networks operating in your area.

➢ **Frequency (Channel)**

This field determines which operating frequency will be used for WiFi. It is not necessary to change the wireless channel unless you noticed the interference problems with other access points nearby.

➢ **Broadcast SSID:** Enabled(default)/Disabled

When wireless clients search the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disabled this feature, the WiFi of the router is invisible.

➢ **AP Isolation:** Enabled/Disabled(default)

This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the router but not with each other.

- **Channel Bandwidth:** 20MHz, 20/40MHz

- **WiFi Security**

Setting the wireless security and encryption to prevent the router from unauthorized access and monitoring. Default security mode is WPA2-PSK and the default password is unique (Figure 3-4-1-2-1), you can modify the security mode and password you like from this page.

- **Security Mode:** Disabled, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK

WPA Security Mode

- **Security Mode:** WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK
- **WPA Algorithms**: TKIP, AES, TKIPAES
- **Keywords:** 8 ~ 63 ASCII characters
- **Key Renewal Interval:** 0~4194303s

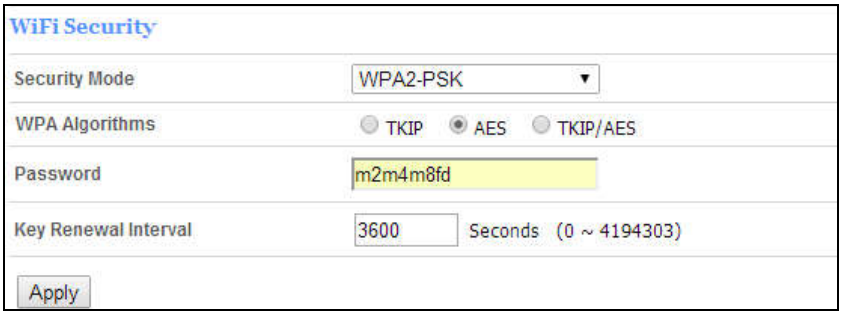

Figure 3-4-2-2-6 Default WiFi Security

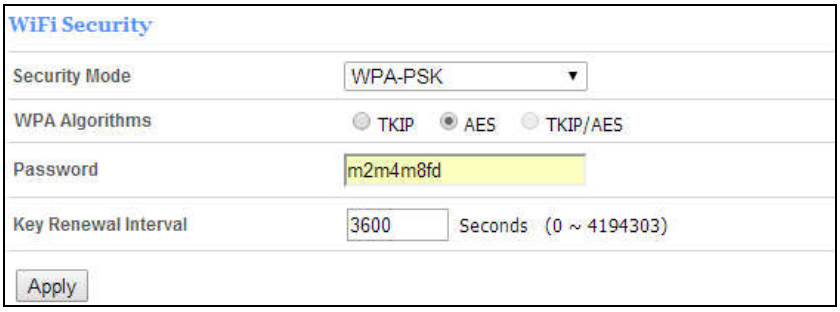

Figure 3-4-2-2-7 WPA-PSK

Figure 3-4-2-2-8 WPA-PSK/WPA2-PSK

3.4.2.3 Multiple SSID

From this page, you can add the multiple SSID of the router, the maximum rule count is 5. Click on the "Add New" button, you can configure the SSID information.

Figure 3-4-2-3-1 Multiple SSID page

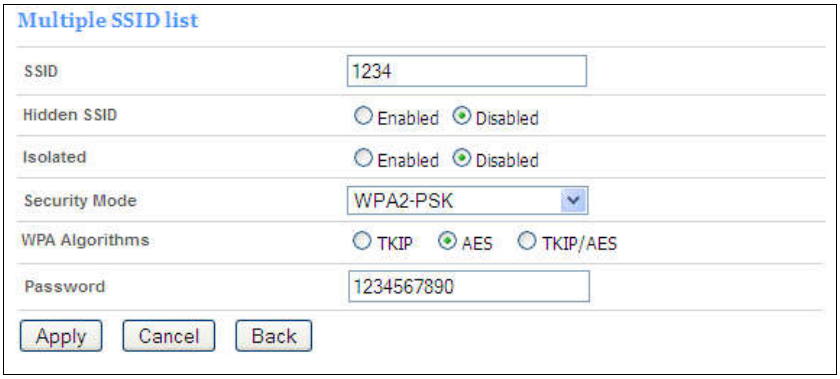

Figure 3-4-1-3-2 Add New Rule

The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially (Figure 3-4-1-3-3). Connect any WiFi SSID by the correct password on the rule table, you would be able to access to the router.

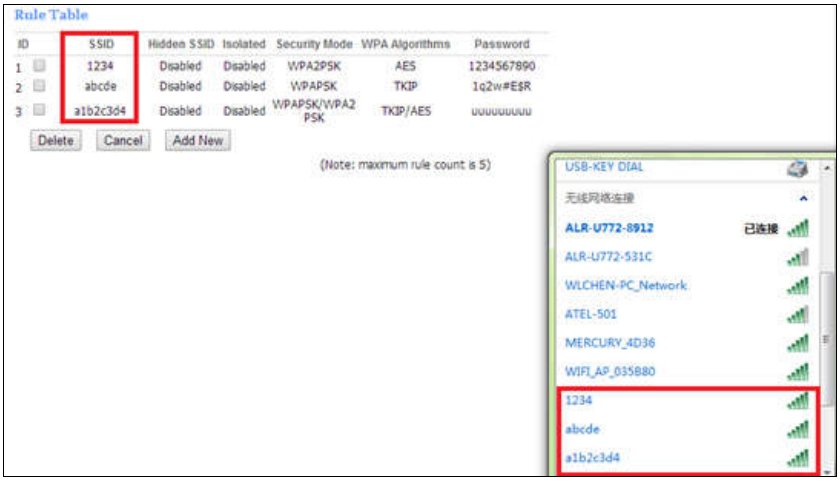

Figure 3-4-2-3-3 Rule Table

3.4.3 Advanced Settings

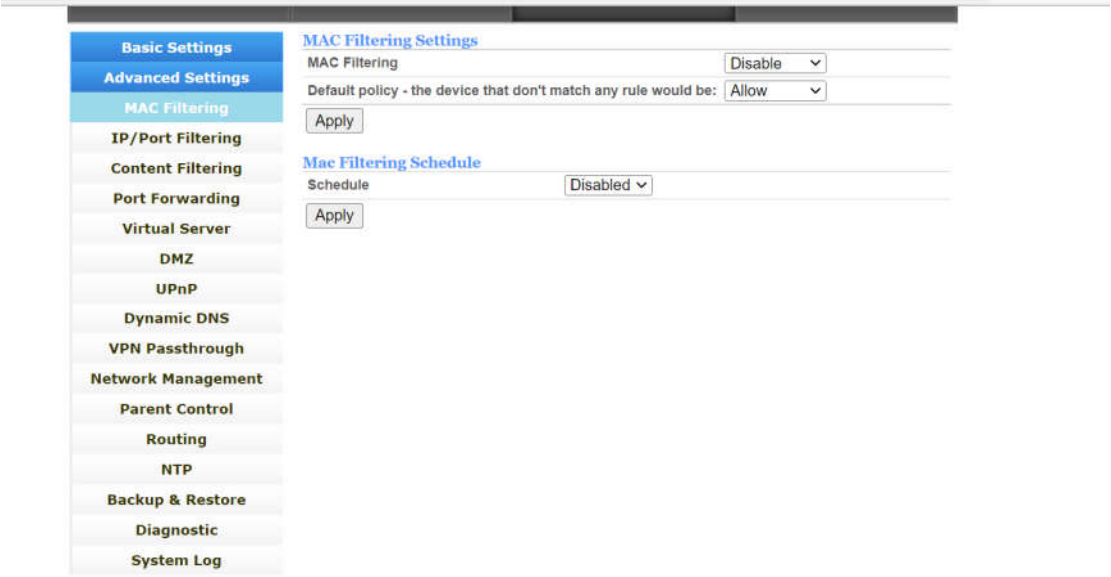

Figure 3-4-3-1 Advanced Settings

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.

Figure 3-4-3-1-1 MAC Filtering page

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 (Figure 3-4-3-1-3).

Default Policy: The packets that don't match with any rules would be "Allow/Deny". If you choose the "Allow" button here, the MAC address that you add would be dropped. Otherwise, only the MAC addresses on the rule table can be accepted.

The new rules will be shown on the rule table, here you can delete the rules that you have selected and add new rules sequentially. The maximum rule count is 10. (Figure 3-4-3-1-4)

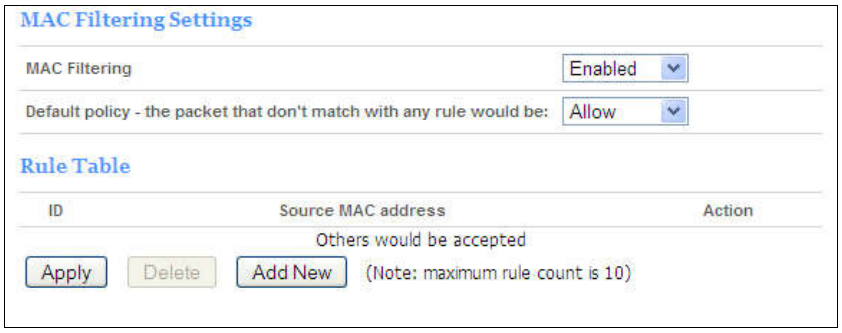

Figure 3-4-3-1-2 Enable MAC Filtering function

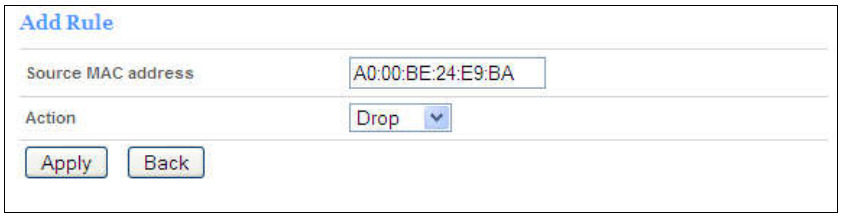

Figure 3-4-3-1-3 Add Rule

Figure 3-4-3-1-4 Rule Table

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.

Figure 3-4-3-2-1 IP/Port filtering page

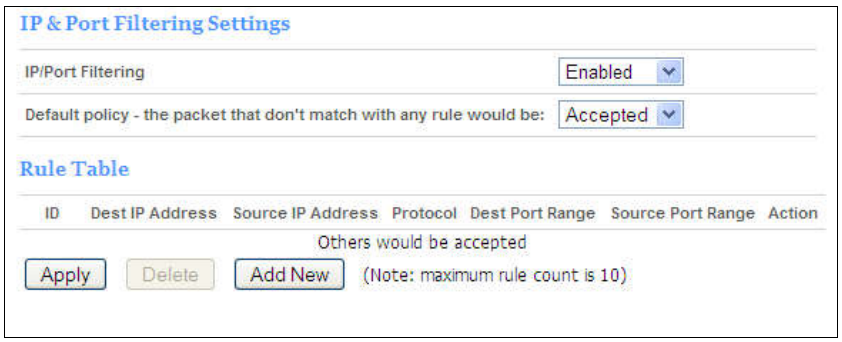

Figure 3-4-3-2-2 Enable IP/Port Filtering function

- **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 (Figure 3-4-2-2-4). The maximum rule count is 10.

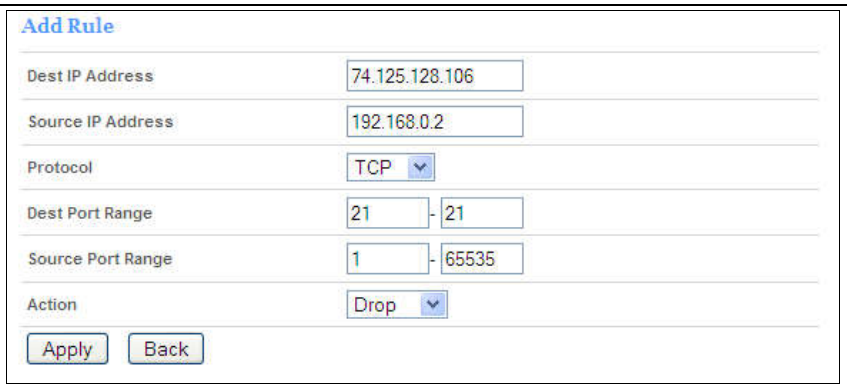

Figure 3-4-3-2-3 Add New Rule

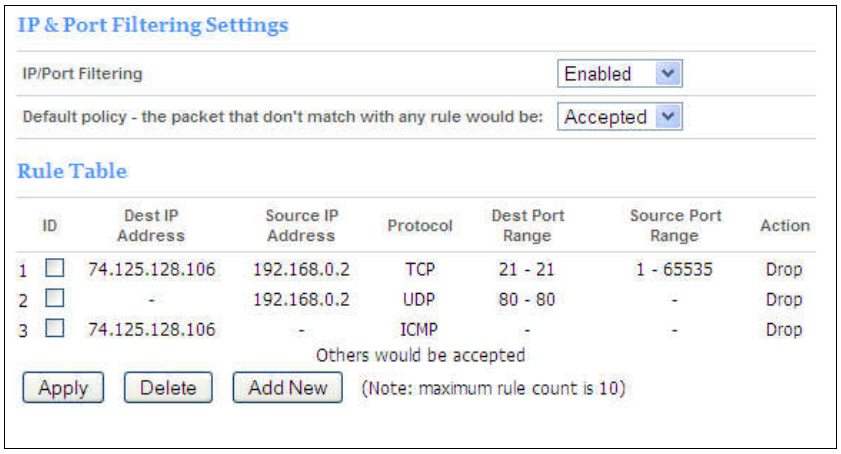

Figure 3-4-3-2-4 Rule Table

3.4.3.3 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 (Figure 3-4-2-3-4). The maximum rule count is 8.

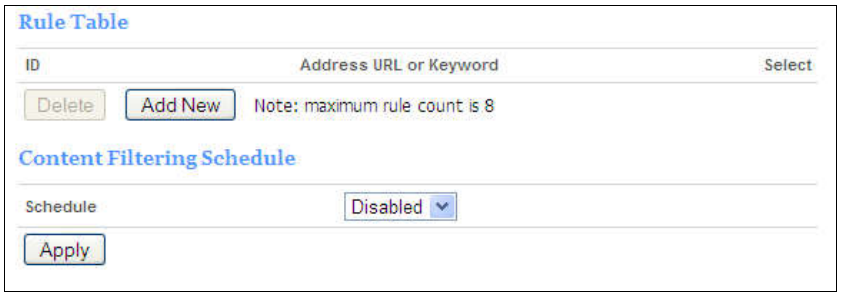

Figure 3-4-3-3-1 Content Filtering page

Figure 3-4-3-3-2 Add New Rule

- **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.

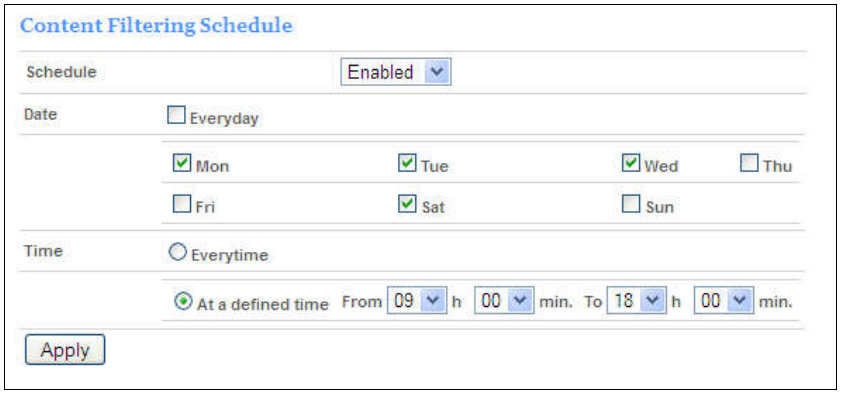

Figure 3-4-3-3-3 Configure Filtering Schedule

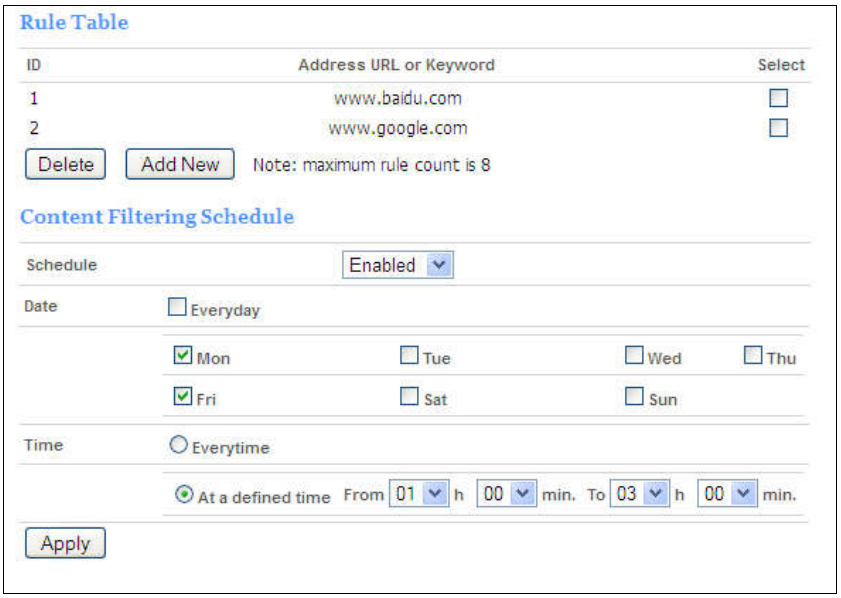

Figure 3-4-3-3-4 Content Filtering Rules

3.4.3.4 Port Forwarding

Clicking on the header of the "Port Forwarding" button will take you to the "Port Forwarding" header page (Figure 3-4-3-4-1). Clicking on the "Add New"

button, you can configure IP address, port range to achieve the port forwarding purpose.

Figure 3-4-3-4-1 Port Forwarding page

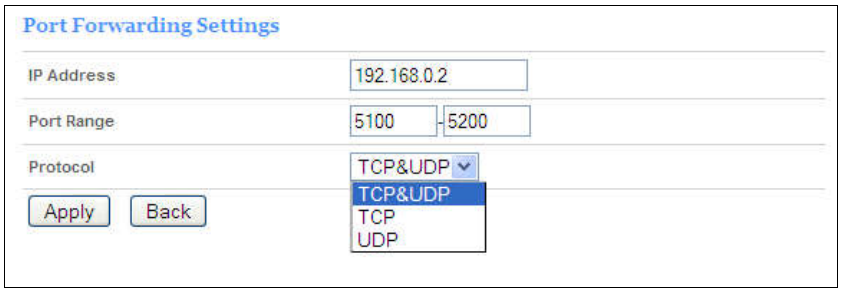

Figure 3-4-3-4-2 Port Forwarding Setting

- **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.

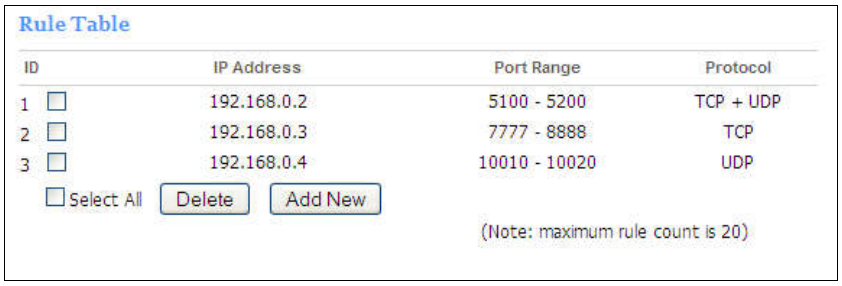

Figure 3-4-3-4-3 Rule Table

3.4.3.5 Virtual Server

Clicking on the header of the "Virtual Server" button will take you to the "Virtual Server" header page (Figure 3-4-2-5-1). 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.

Figure 3-4-3-5-1 Virtual Server page

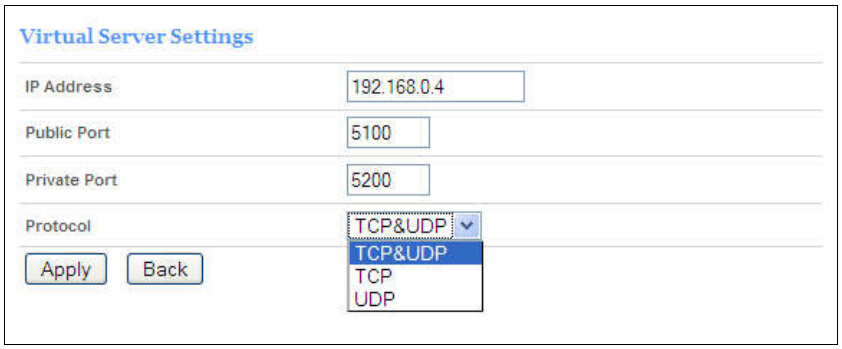

Figure 3-4-3-5-2 Virtual Server Setting

- **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.

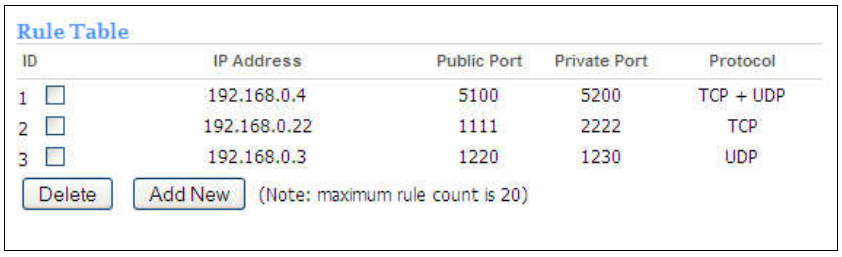

Figure 3-4-3-5-3 Rule Table

3.4.3.6 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.

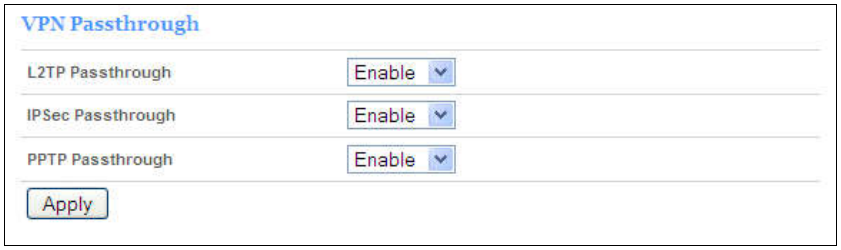

Figure 3-4-3-6-1 VPN Passthrough

Note: VPN Passthrough does not mean the router can create a VPN endpoint. VPN Passthrough is a feature that allows VPN traffic created by other endpoints to "pass through" the router.

3.4.3.7 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 192.168.0.3)

Figure 3-4-3-7-1 DMZ page

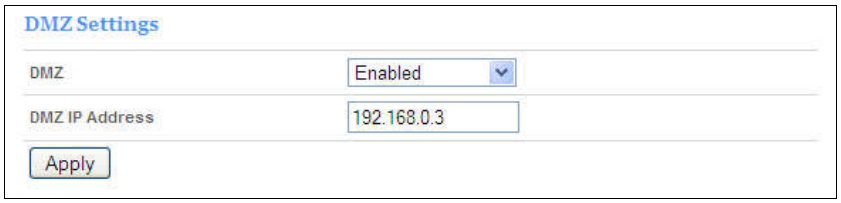

Figure 3-4-3-7-2 DMZ Setting

3.4.3.8 Dynamic DNS

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

Figure 3-4-3-8-1 Dynamic DNS setting

3.4.3.9 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. (Figure 3-4-2-9-3)

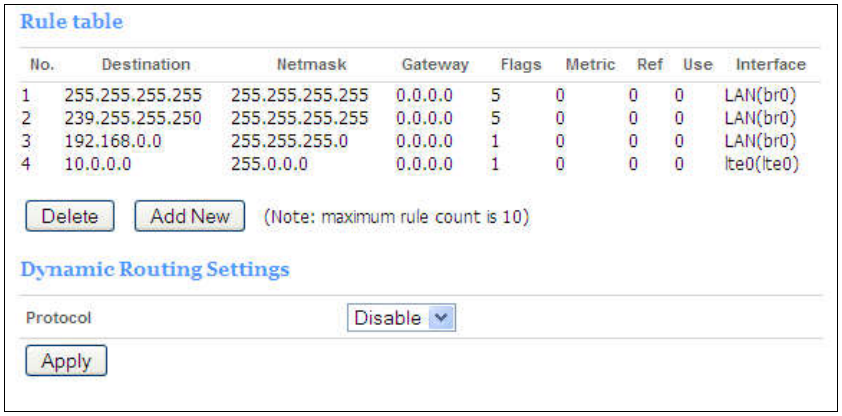

Figure 3-4-3-9-1 Rule Table

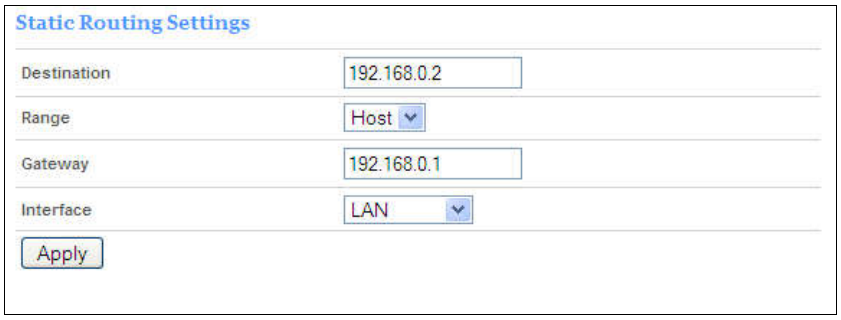

Figure 3-4-3-9-2 Configure the static routing settings

- **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.

Figure 3-4-3-9-3 New rule table

3.4.3.10 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.

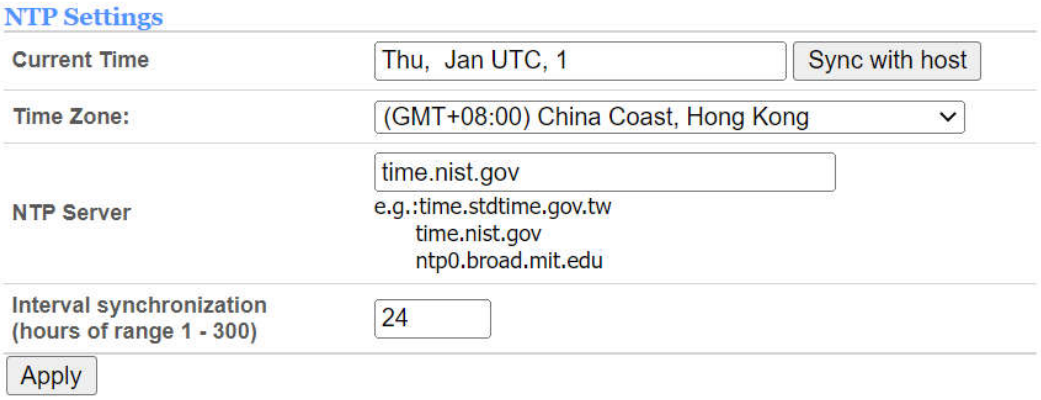

Figure 3-4-3-10-3 New rule table

3.4.3.11 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.

Figure 3-4-3-11-1 Backup&restore

3.4.3.12 Bridge Mode

The default LTE Bridge mode is disabled. You can enable and change the device to bridge mode.

Figure 3-4-3-12-1 LTE Bridge Setting page

Figure 3-4-3-12-2 Enable bridge mode

3.4.3.13 Diagnostic

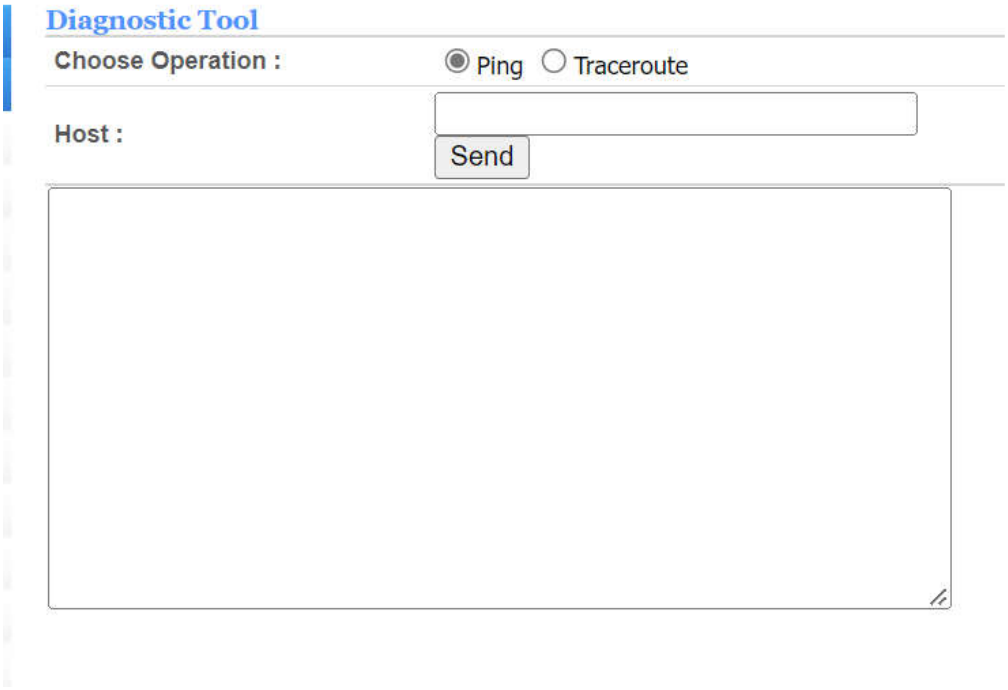

Figure 3-4-3-13-1 Diagnostic

3.4.3.14 System log

This function is used to display system information. Click “Refresh” key, system log can be refreshed. Clear key can clear all information.

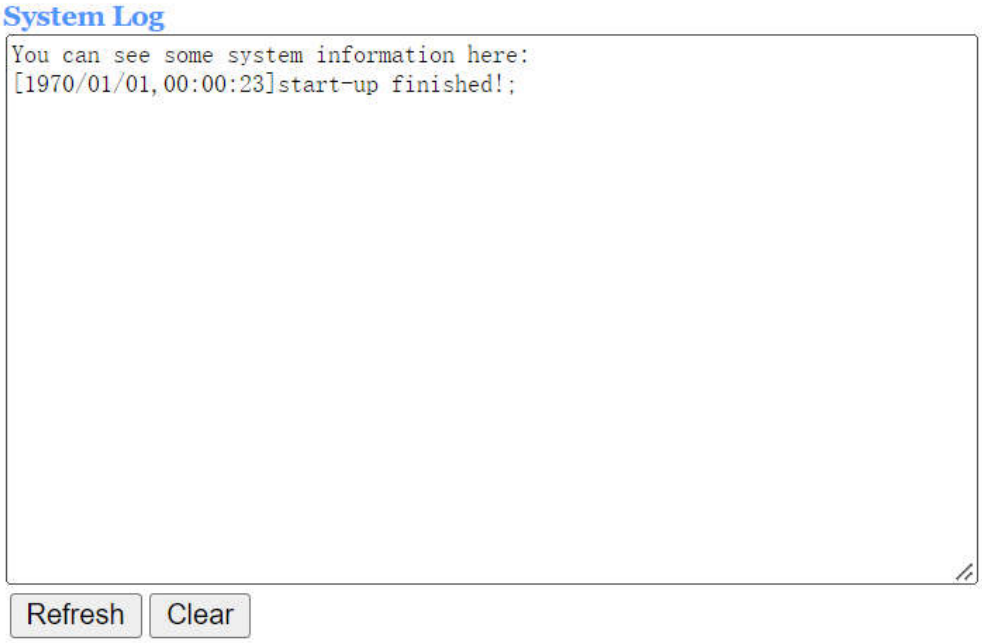

Figure 3-4-3-14-1 System Log

Figure 3-4-4-8-1 System Log

3.5 Network

Click on the “network” button, you can see four parts as below: APN Settings, PIN management, Band selection and Antenna.

Figure 3-5-1 network

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, and then you can configure the APN settings by clicking on the “Add New” button (Figure 3-5-1-2).

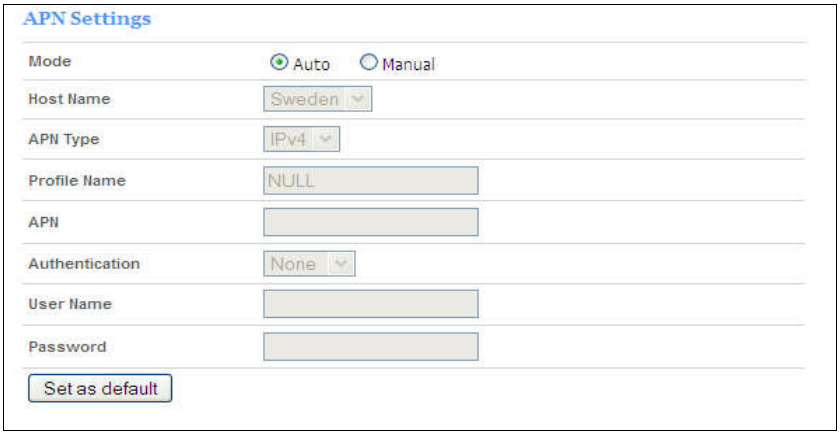

Figure 3-5-1-1 LTE APN page

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

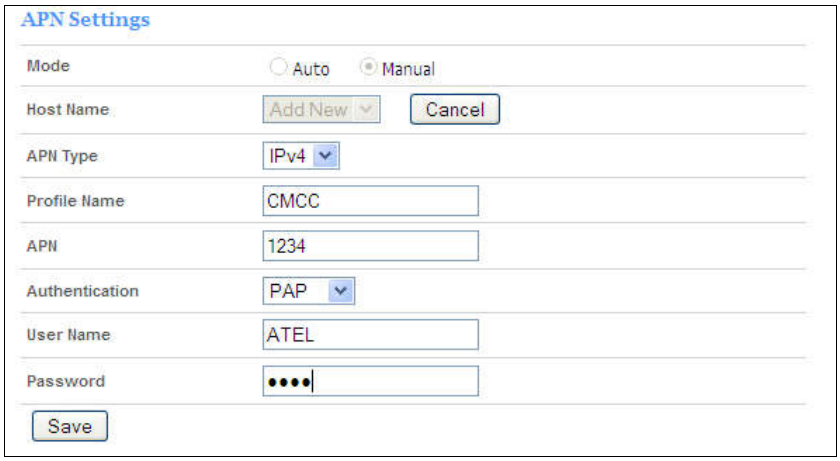

Figure 3-5-1-2 APN Configuration

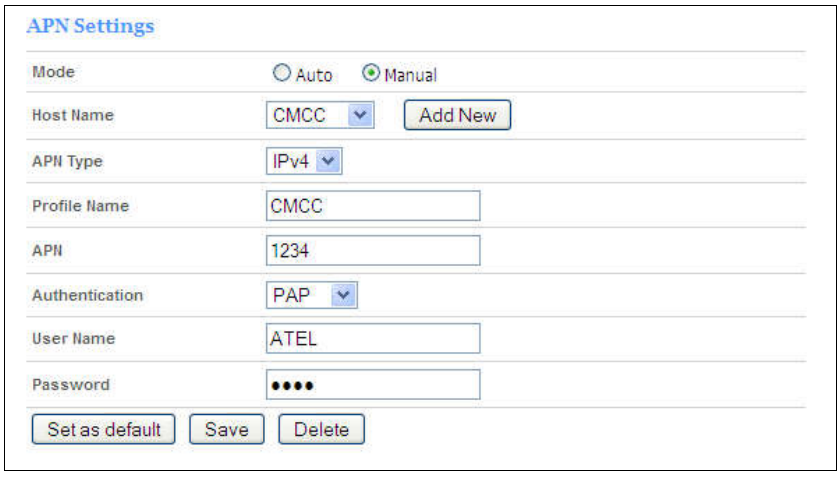

Figure 3-6-1-3 Choose the user-defined APN

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;
- **Remember 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.

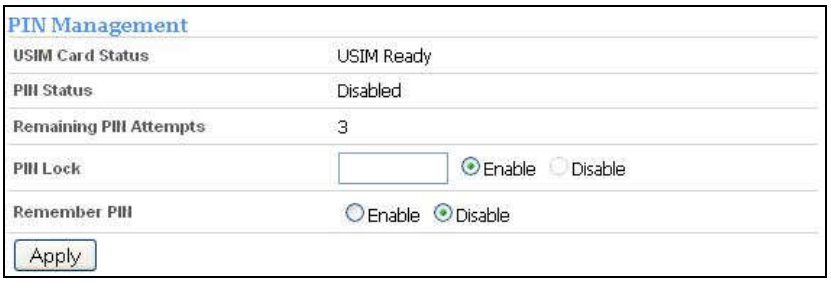

Figure 3-5-2-1 PIN Management page

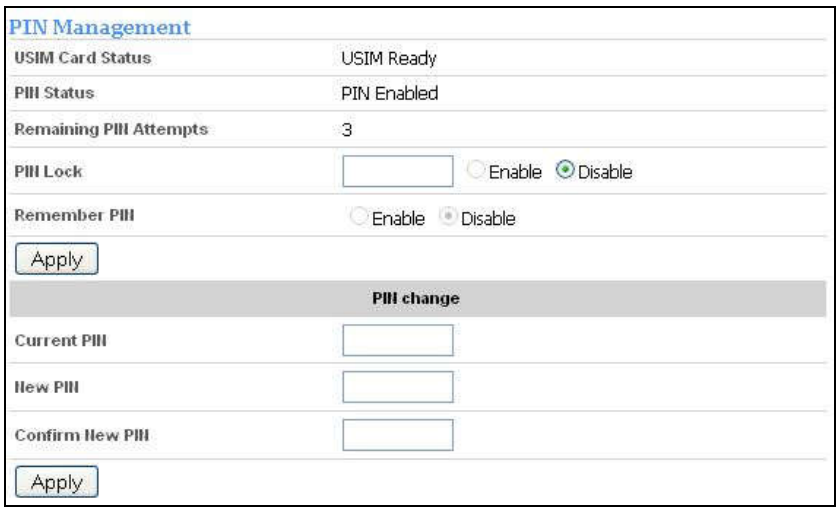

Figure 3-5-2-2 Enable the PIN

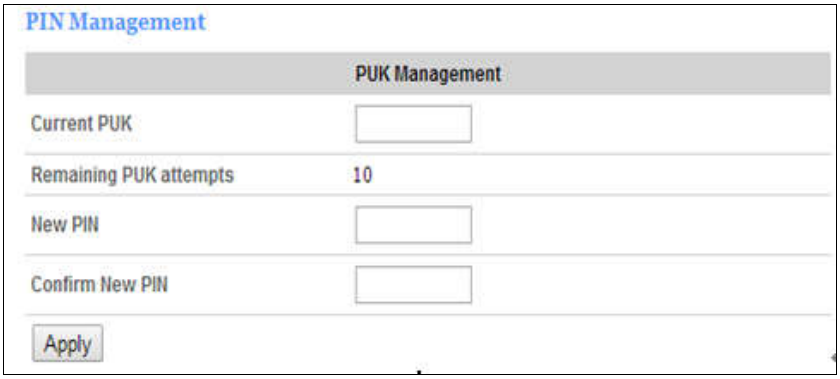

Figure 3-5-2-3 PUK Management page

FCC Regulations:

This mobile router 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 mobile router 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 radiated 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.
FCC Note:
Caution: Changes or modifications not expressly approved by the party responsible for compliance could void the user‘s authority to operate the
equipment.

RF Exposure Information

This device meets the government’s requirements for exposure to radio waves.
This device is designed and manufactured not to exceed the emission limits for exposure to radio frequency (RF) energy set by the Federal Communications Commission of the U.S. Government.

This device complies with FCC radiation exposure limits set forth for an uncontrolled

environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 30cm during normal operation.