LTE CPE（ALR-U series）User Manual

Index

1. About this Manual..3

2. Product Overview..3

3. Configuring the CPE..3

3.1 Login 3
3.2 Dashboard.. 4
3.3 Status 5
3.3.1 WAN Status.. 5
3.3.2 WiFi&LAN Status.. 5
3.3.3 4G Status 6
3.3.4 Software 6
3.3.5 Device List.. 6
3.3.6 UPnP 7
3.4 Settings 7
3.4.1 Basic Settings.. 8
3.4.2 Advanced Settings 15
3.4.3 System Settings.. 26
3.5 4G 31
3.5.1 APN Settings.. 31
3.5.2 PIN Management.. 33

Note:

Operating temperature: -30℃—60℃.

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 3/7/20/31 (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 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 three 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.

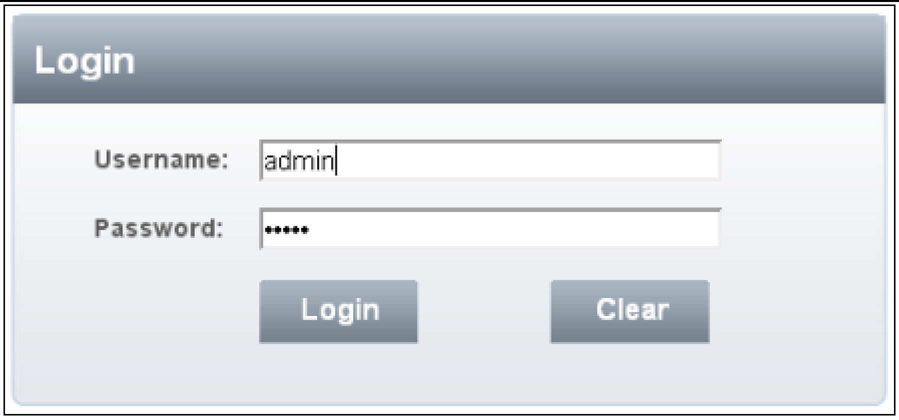
3.1 Login

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/admin



Login

Username: admin

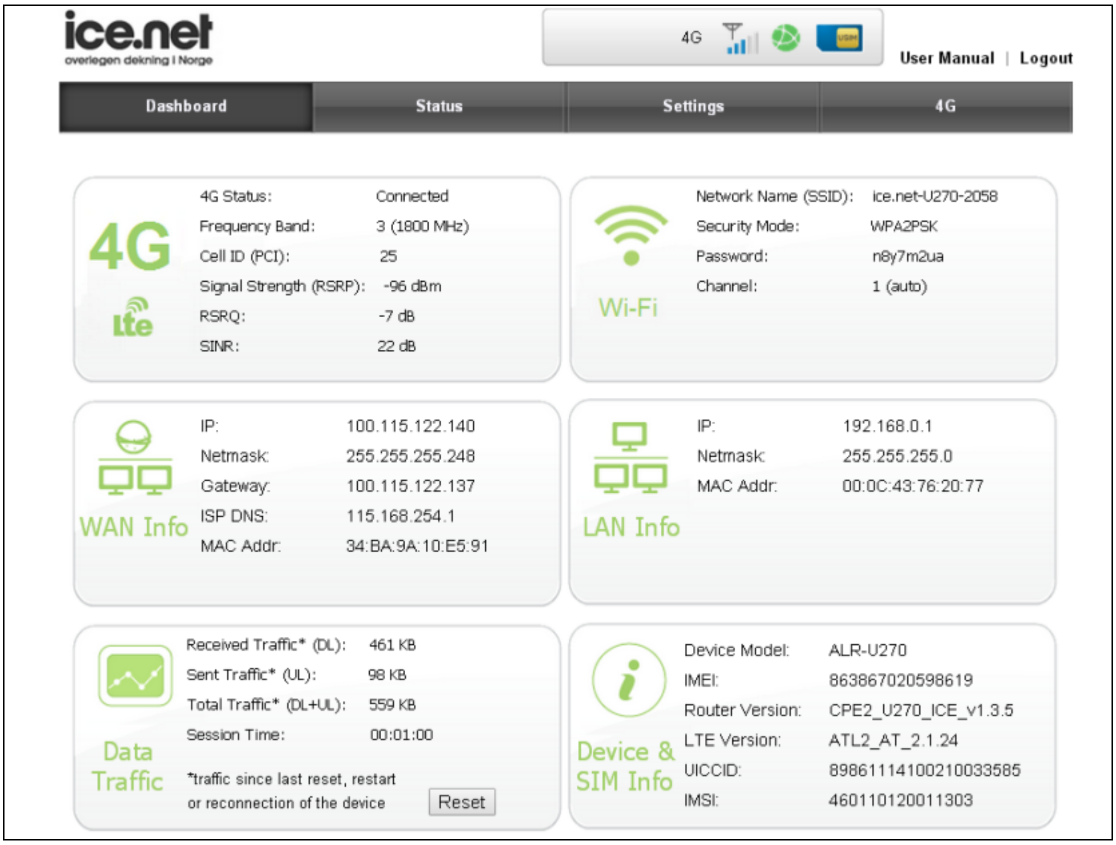
Password: •••••

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. You can see the dashboard page as figure 3-2-1.



4G Status: Connected
Frequency Band: 3 (1800 MHz)
Cell ID (PCI): 25
Signal Strength (RSRP): -96 dBm
RSRQ: -7 dB
SINR: 22 dB

Network Name (SSID): ice.net-U270-2058
Security Mode: WPA2PSK
Password: n8y7m2ua
Channel: 1 (auto)

IP: 100.115.122.140
Netmask: 255.255.255.248
Gateway: 100.115.122.137
ISP DNS: 115.168.254.1
MAC Addr: 34:BA:9A:10:E5:91

IP: 192.168.0.1
Netmask: 255.255.255.0
MAC Addr: 00:0C:43:76:20:77

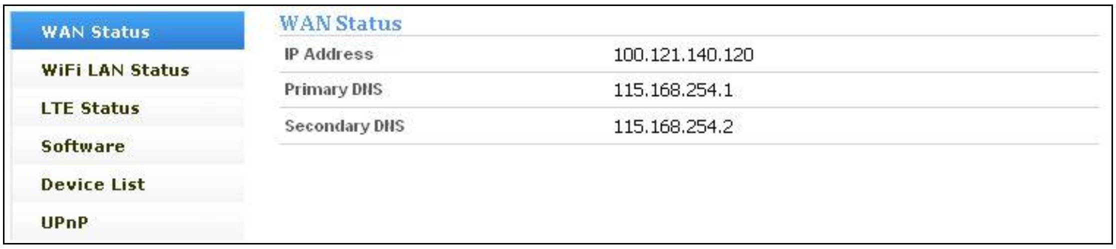
Received Traffic* (DL): 461 KB
Sent Traffic* (UL): 98 KB
Total Traffic* (DL+UL): 559 KB
Session Time: 00:01:00
*traffic since last reset, restart or reconnection of the device

Device Model: ALR-U270
IMEI: 863867020598619
Router Version: CPE2_U270_ICE_v1.3.5
LTE Version: ATL2_AT_2.1.24
UICCID: 89861114100210033585
IMSI: 460110120011303

Figure 3-2-1 Dashboard Page

3.3 Status

On this page, you can see WAN Status, WiFi&LAN Status, 4G Status, Software, Device List and UPnP.



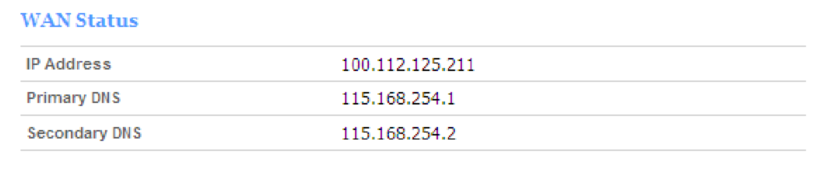
WAN Status

IP Address	100.121.140.120
Primary DNS	115.168.254.1
Secondary DNS	115.168.254.2

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



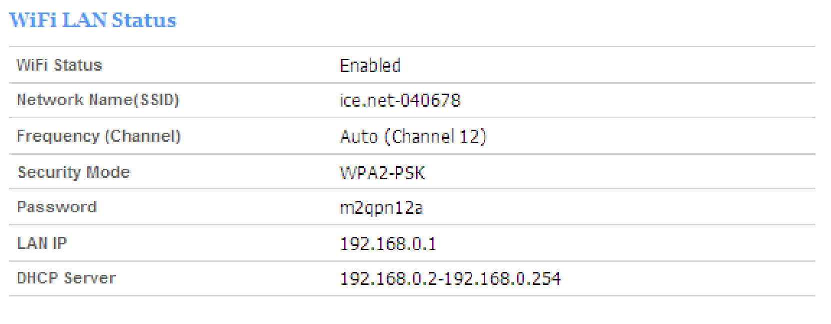
WAN Status

IP Address	100.112.125.211
Primary DNS	115.168.254.1
Secondary DNS	115.168.254.2

Figure 3-3-1-1 WAN Status

3.3.2 WiFi&LAN Status

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



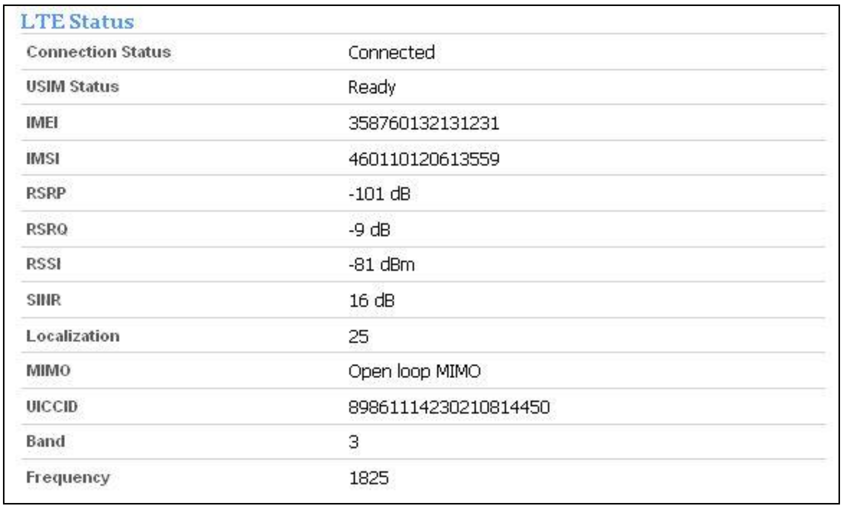
WiFi LAN Status

WiFi Status	Enabled
Network Name(SSID)	ice.net-040678
Frequency (Channel)	Auto (Channel 12)
Security Mode	WPA2-PSK
Password	m2qpn12a
LAN IP	192.168.0.1
DHCP Server	192.168.0.2-192.168.0.254

Figure 3-3-2-1 WiFi LAN Status

3.3.3 4G Status

Clicking on the “4G Status”, you can see the LTE information such as Connection Status, USIM Status, IMEI, IMSI, RSRP, RSRQ, RSSI, SINR, Localization and Frequency.



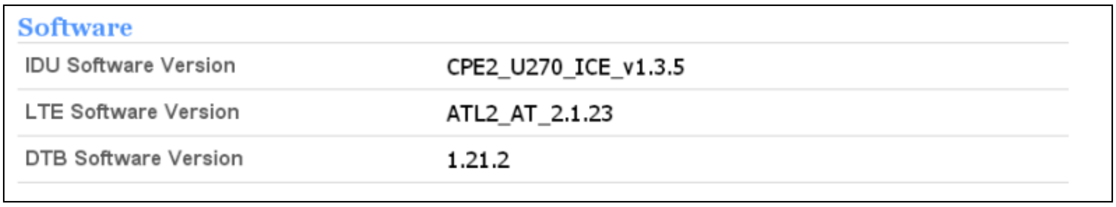
LTE Status

Connection Status	Connected
USIM Status	Ready
IMEI	358760132131231
IMSI	460110120613559
RSRP	-101 dB
RSRQ	-9 dB
RSSI	-81 dBm
SINR	16 dB
Localization	25
MIMO	Open loop MIMO
UICCID	89861114230210814450
Band	3
Frequency	1825

Figure 3-3-3-1 LTE Status

3.3.4 Software

This page is used to display IDU software version ,LTE software version and DTB version.



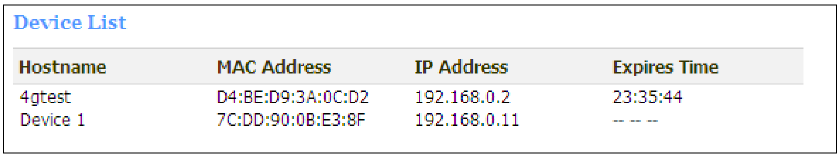
Software

IDU Software Version	CPE2_U270_ICE_v1.3.5
LTE Software Version	ATL2_AT_2.1.23
DTB Software Version	1.21.2

Figure 3-3-4-1 Software

3.3.5 Device List

All clients connect to U270 can be displayed. You can see the users’ information, include hostname, MAC address, IP address and expires time.



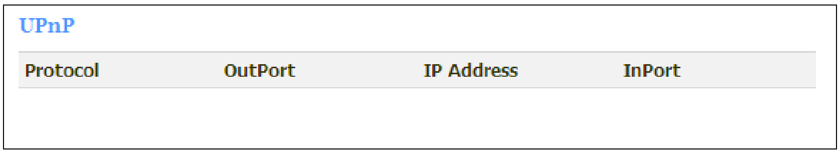
Device List

Hostname	MAC Address	IP Address	Expires Time
4gtest	D4:BE:D9:3A:0C:D2	192.168.0.2	23:35:44
Device 1	7C:DD:90:0B:E3:8F	192.168.0.11	-- -- --

Figure 3-3-5-1 Device List

3.3.6 UPnP

The UPnP function is disabled in default; you should enable it on the system security page (3.4.3.2) before using it. The new rules that you added will be shown on this page.



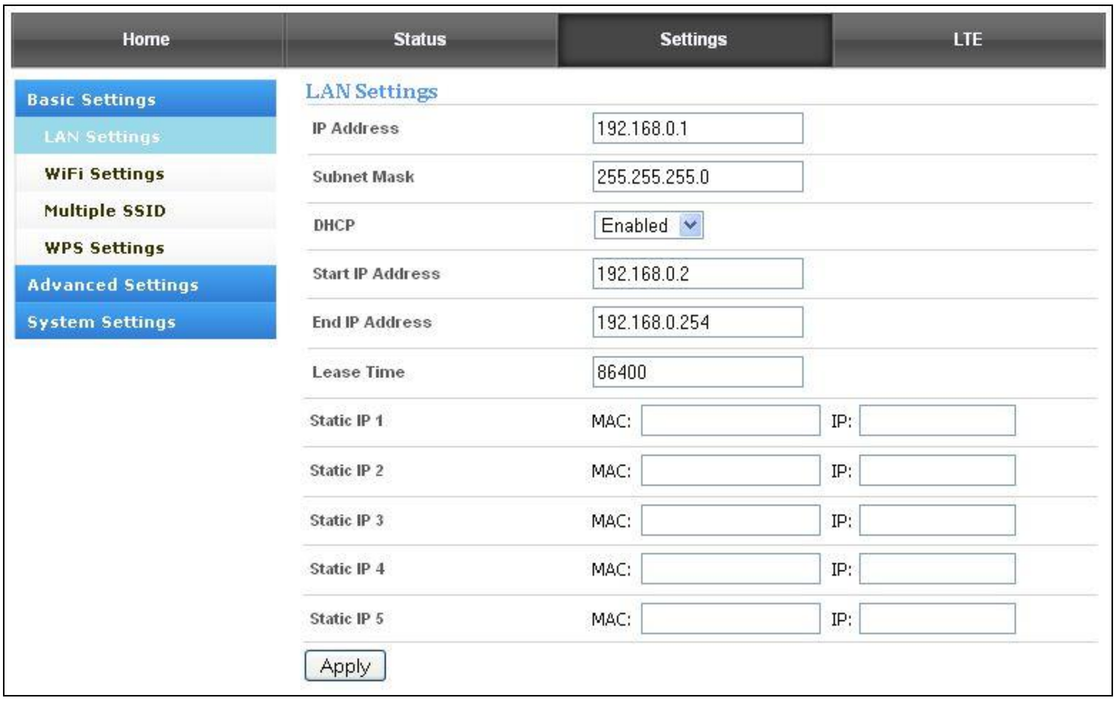
UPnP

Protocol	OutPort	IP Address	InPort

Figure 3-3-6-1 UPnP

3.4 Settings

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



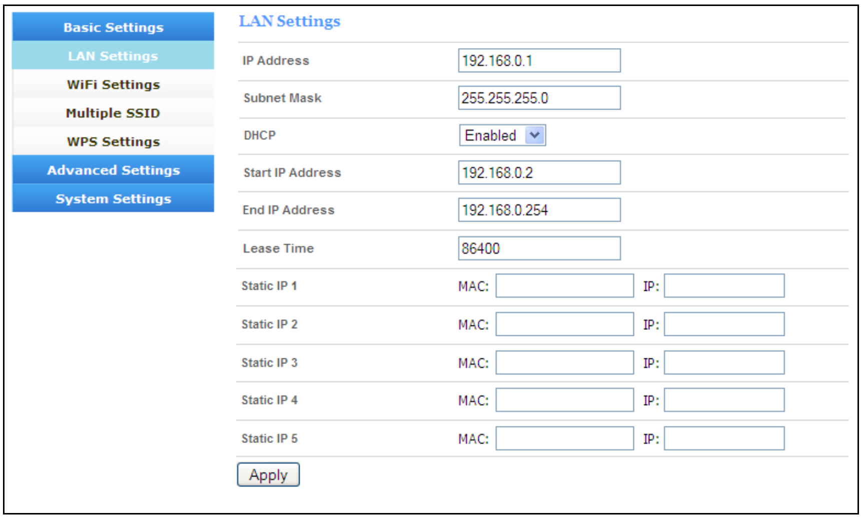
LAN Settings

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		
Static IP 1	MAC:	IP:	
Static IP 2	MAC:	IP:	
Static IP 3	MAC:	IP:	
Static IP 4	MAC:	IP:	
Static IP 5	MAC:	IP:	

Apply

Figure 3-4-1 Settings

3.4.1 Basic Settings



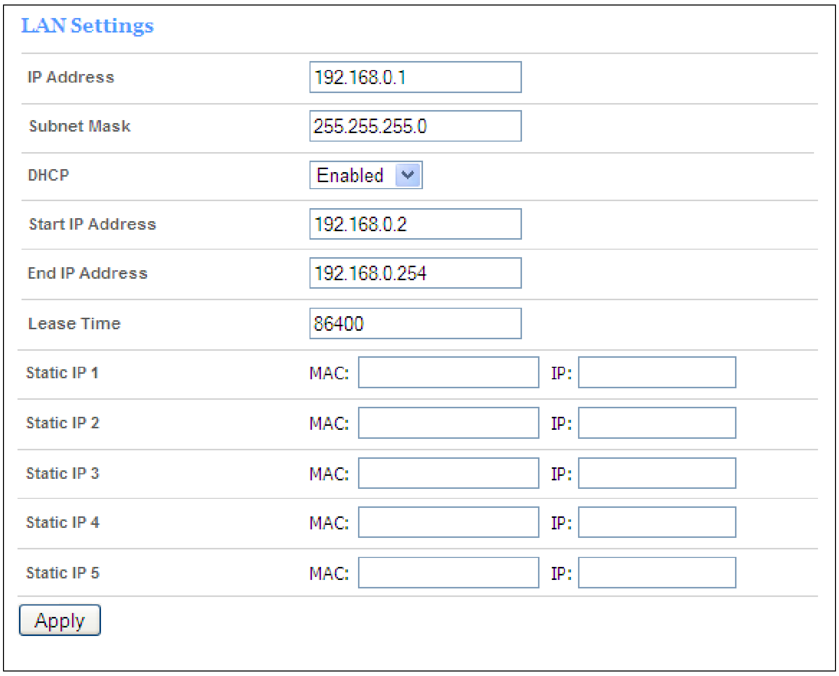
LAN Settings

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			
Static IP 1	MAC:		IP:	
Static IP 2	MAC:		IP:	
Static IP 3	MAC:		IP:	
Static IP 4	MAC:		IP:	
Static IP 5	MAC:		IP:	

Figure 3-4-1-1 Basic Settings

3.4.1.1 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.



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			
Static IP 1	MAC:		IP:	
Static IP 2	MAC:		IP:	
Static IP 3	MAC:		IP:	
Static IP 4	MAC:		IP:	
Static IP 5	MAC:		IP:	

Figure 3-4-1-1-1 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:**

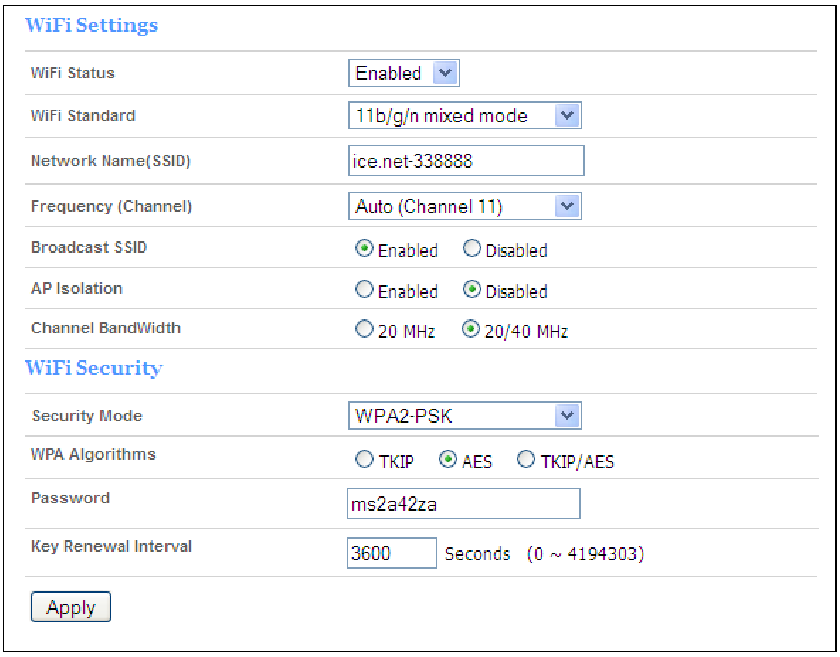
1. If you change the IP Address of LAN, you must use the new IP address to login to the CPE router.
2. If the new LAN IP address you set is not in the same subnet, the IP address pool of the DHCP server will change at the same time, while the Virtual Server and DMZ Host will not take effect until they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

3.4.1.2 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 13.



WiFi Settings

WiFi Status: Enabled

WiFi Standard: 11b/g/n mixed mode

Network Name(SSID): ice.net-338888

Frequency (Channel): Auto (Channel 11)

Broadcast SSID: ● Enabled ○ Disabled

AP Isolation: ○ Enabled ● Disabled

Channel BandWidth: ○ 20 MHz ● 20/40 MHz

WiFi Security

Security Mode: WPA2-PSK

WPA Algorithms: ○ TKIP ● AES ○ TKIP/AES

Password: ms2a42za

Key Renewal Interval: 3600 Seconds (0 ~ 4194303)

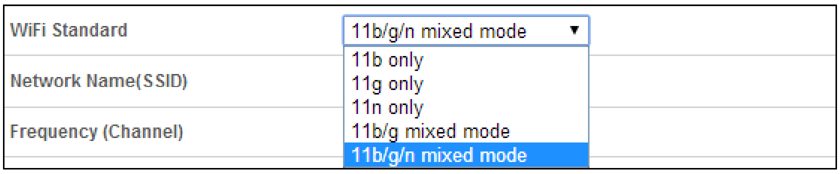
Figure 3-4-1-2-1 WiFi Settings

- **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/g mixed mode", "11b only", "11g only", "11n only", "11b/g mixed mode","11b/g/n mixed mode".



WiFi Standard: 11b/g/n mixed mode

Network Name(SSID)

Frequency (Channel)

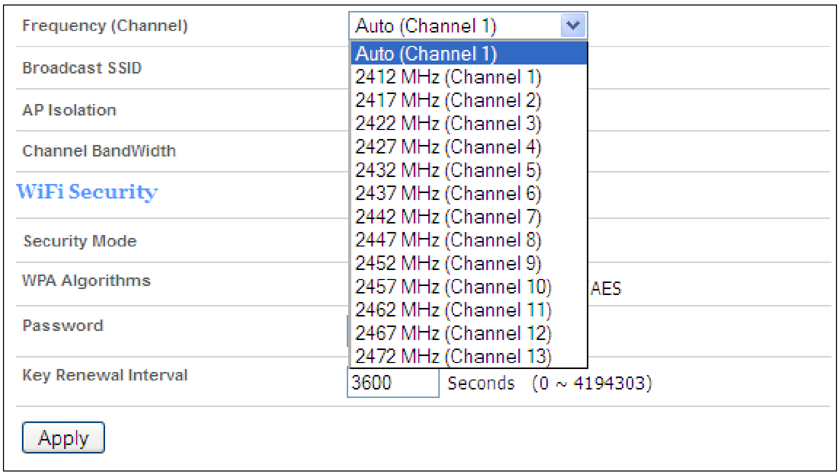
Figure 3-4-1-2-2 WiFi standard

- **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.



Frequency (Channel) Auto (Channel 1)

Broadcast SSID

AP Isolation

Channel BandWidth

WiFi Security

Security Mode

WPA Algorithms AES

Password

Key Renewal Interval 3600 Seconds (0 ~ 4194303)

Figure 3-4-1-2-3 Frequency (Channel)

- **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

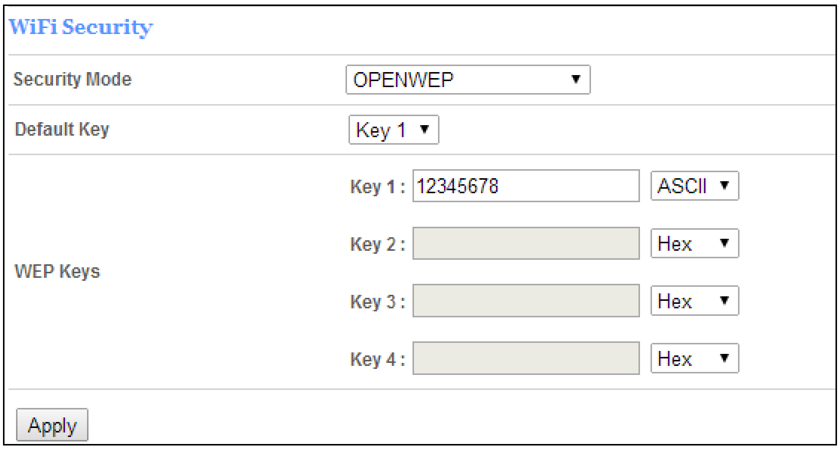
- **WiFi Security**

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, OPENWEP, SHAREDWEP, WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK

a) WEP Security Mode

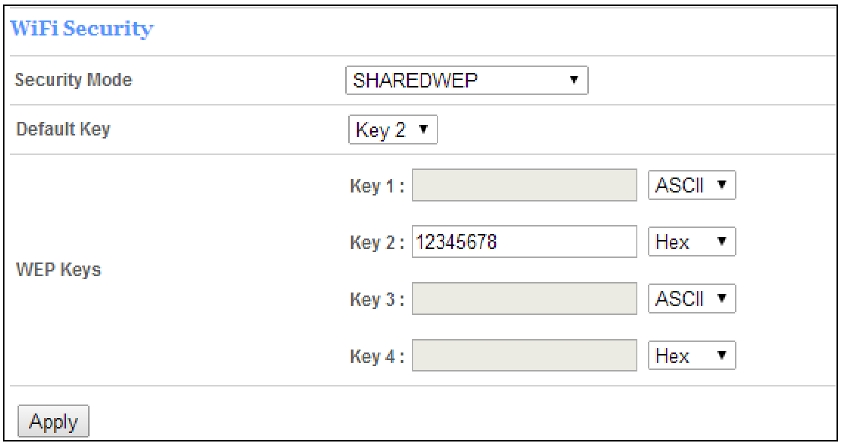
- **Security Mode:** OPEN, SHARED
- **Key Format:** Hexadecimal and ASCII formats are provided. Hexadecimal format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length. ASCII format stands for any combination of keyboard characters in the specified length.
- **Default Key:** Anyone of Key 1, Key 2, Key 3 and Key4 with 2 kinds of key format.



WiFi Security

Security Mode	OPENWEP ▾
Default Key	Key 1 ▾
WEP Keys	Key 1 : 12345678 ASCII ▾ Key 2 : Hex ▾ Key 3 : Hex ▾ Key 4 : Hex ▾

Figure 3-4-1-2-4 OPENWEP



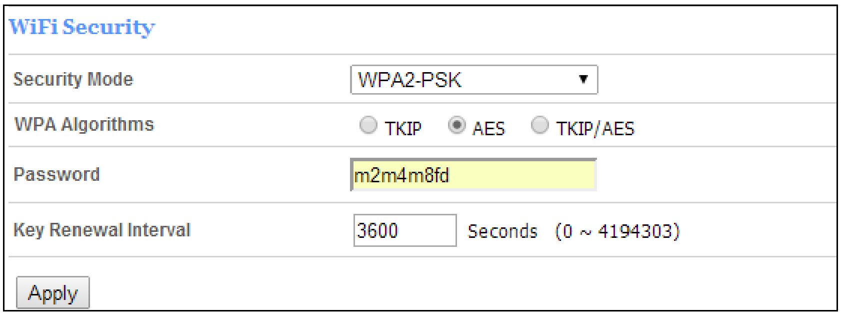
WiFi Security

Security Mode	SHAREDWEP ▾
Default Key	Key 2 ▾
WEP Keys	Key 1 : ASCII ▾ Key 2 : 12345678 Hex ▾ Key 3 : ASCII ▾ Key 4 : Hex ▾

Figure 3-4-1-2-5 SHAREDWEP

b) WPA Security Mode

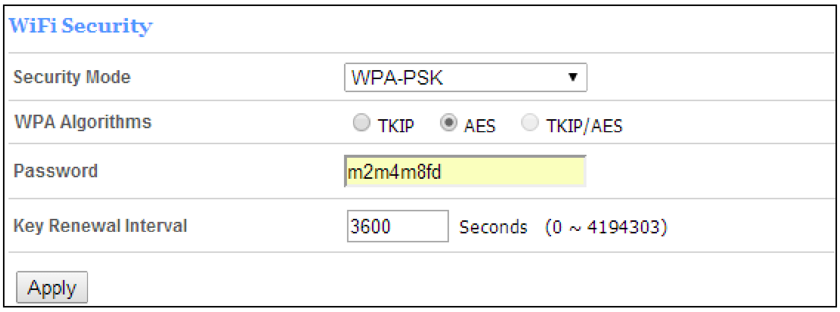
- **Security Mode:** WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK
- **WPA Algorithms**: TKIP, AES, TKIPAES
- **Keywords:** 8 ~ 63 ASCII characters
- **Key Renewal Interval:** 0~4194303s



WiFi Security

Security Mode	WPA2-PSK ▾
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	m2m4m8fd
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

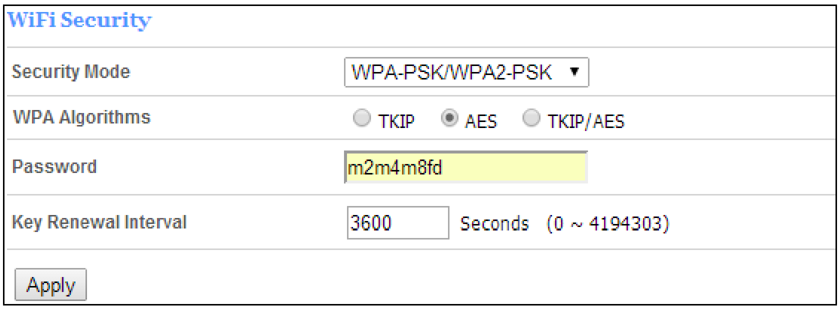
Figure 3-4-1-2-6 Default WiFi Security



WiFi Security

Security Mode	WPA-PSK ▾
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	m2m4m8fd
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

Figure 3-4-1-2-7 WPA-PSK



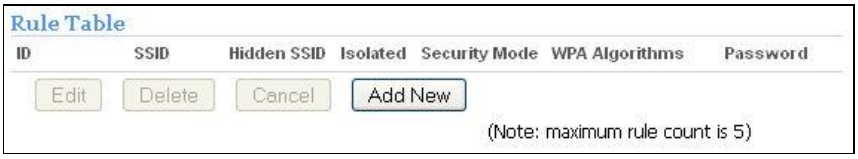
WiFi Security

Security Mode	WPA-PSK/WPA2-PSK ▾
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	m2m4m8fd
Key Renewal Interval	3600 Seconds (0 ~ 4194303)

Figure 3-4-1-2-8 WPA-PSK/WPA2-PSK

3.4.1.3 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.

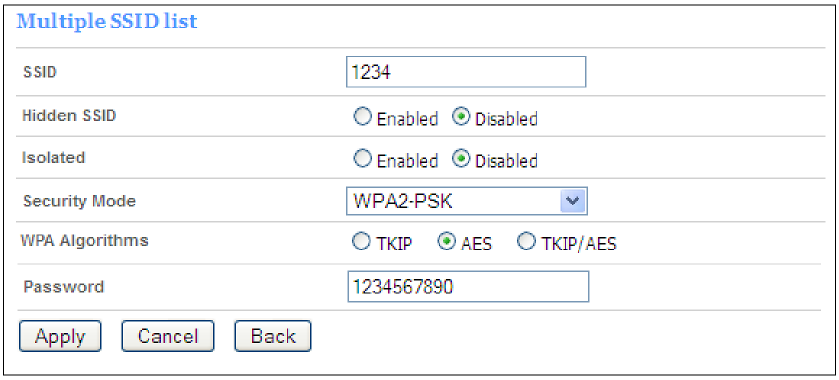


Rule Table

ID	SSID	Hidden SSID	Isolated	Security Mode	WPA Algorithms	Password

(Note: maximum rule count is 5)

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

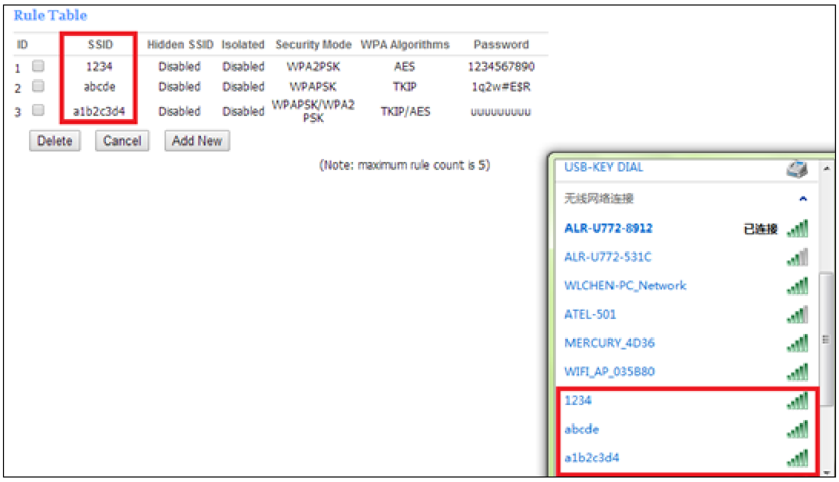


Multiple SSID list

SSID	1234
Hidden SSID	○ Enabled ● Disabled
Isolated	○ Enabled ● Disabled
Security Mode	WPA2-PSK ▾
WPA Algorithms	○ TKIP ● AES ○ TKIP/AES
Password	1234567890

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.



Rule Table

ID		SSID	Hidden SSID	Isolated	Security Mode	WPA Algorithms	Password
1	□	1234	Disabled	Disabled	WPA2PSK	AES	1234567890
2	□	abcde	Disabled	Disabled	WPAPSK	TKIP	1q2w#E$R
3	□	a1b2c3d4	Disabled	Disabled	WPAPSK/WPA2 PSK	TKIP/AES	uuuuuuuuu

(Note: maximum rule count is 5)

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

3.4.1.4 WPS Settings

You can setup security easily by choosing PIN or PBC method to do WiFi Protected Setup. On this page, you can modify WPS settings. This feature can make your wireless client within a few minutes automatically synchronized with the AP devices and establish the connection via WiFi.

- **WPS method-** Push the button (default), Enter the PIN of client device, Use the PIN of the device.
- **WPS Status-** The real-time information of WPS processing while the wireless client tries to communicate with WiFi each other.
- **PBC Mode**

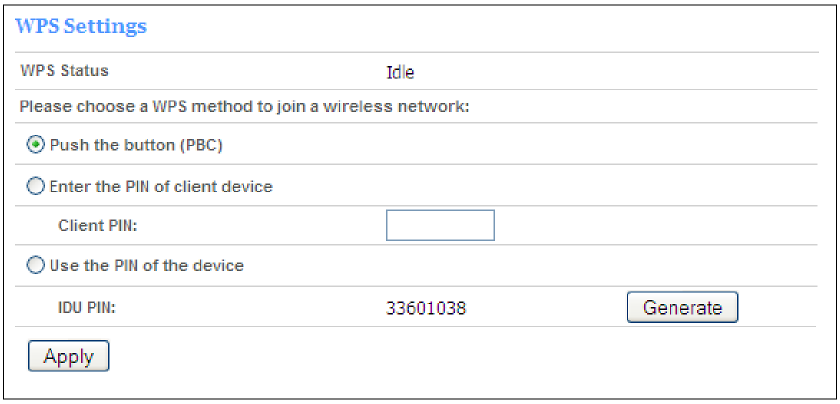
(1) Press the WPS button of the CPE directly;
(2) Then CPE and wireless client will automatically complete the interaction and connect via WiFi if these two devices can match with each other.

- **Enter the PIN of client device**

(1) Wireless clients choose enrollee mode, the wireless client software will randomly generate a PIN code. Then click on the tool interface "PIN" button.
(2) Input the PIN code which got from the wireless client and click the “Apply” button on this “WPS” configuration page.

- **Use the PIN of the device**

(1) Create the random PIN by clicking the “Generate” button, and share this PIN to wireless client.
(2) In the wireless client choice registrar model, and the input device of the PIN code.



WPS Settings

WPS Status Idle

Please choose a WPS method to join a wireless network:

● Push the button (PBC)

○ Enter the PIN of client device

Client PIN:

○ Use the PIN of the device

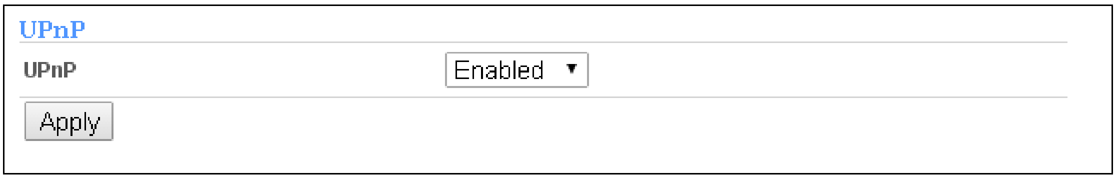
IDU PIN: 33601038 Generate

Apply

Figure 3-4-1-4-1 WPS page

3.4.1.5 UPNP

You should enable the UPnP feature firstly before you use this function.



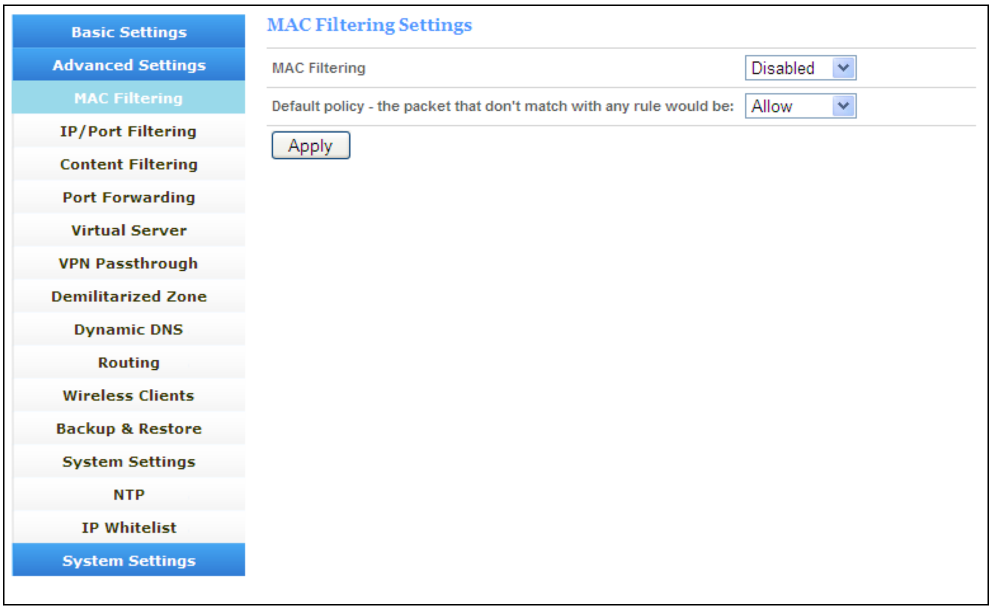
UPnP

UPnP Enabled

Apply

Figure 3-4-1-5-1 UPNP page

3.4.2 Advanced Settings



MAC Filtering Settings

MAC Filtering Disabled

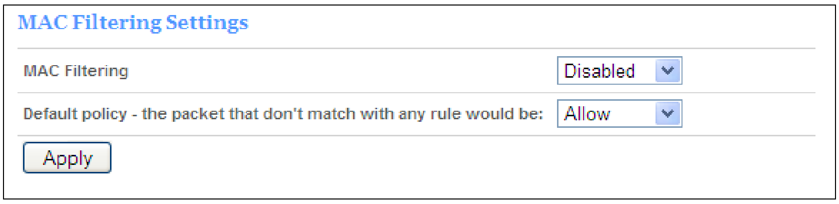
Default policy - the packet that don't match with any rule would be: Allow

Apply

Figure 3-4-2-1 Advanced Settings

3.4.2.1 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.



MAC Filtering Settings

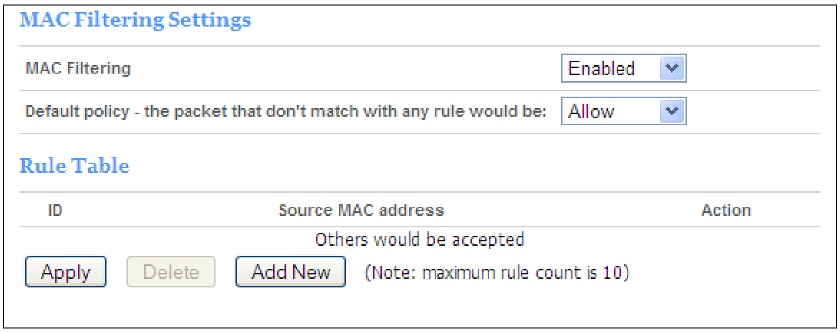
MAC Filtering	Disabled
Default policy - the packet that don't match with any rule would be:	Allow

Figure 3-4-2-1-1 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 3-4-2-1-3).

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 3-4-2-1-4)



MAC Filtering Settings

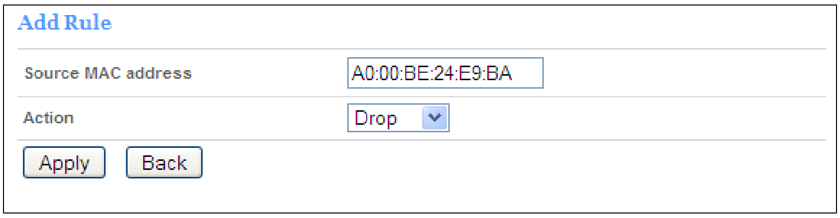
MAC Filtering	Enabled
Default policy - the packet that don't match with any rule would be:	Allow

Rule Table

ID	Source MAC address	Action
	Others would be accepted	

(Note: maximum rule count is 10)

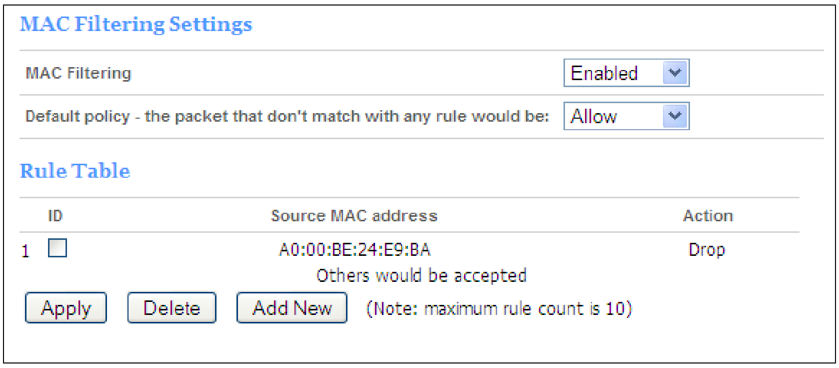
Figure 3-4-2-1-2 Enable MAC Filtering function



Add Rule

Source MAC address	A0:00:BE:24:E9:BA
Action	Drop

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



MAC Filtering Settings

MAC Filtering: Enabled

Default policy - the packet that don't match with any rule would be: Allow

Rule Table

ID		Source MAC address	Action
1	☐	A0:00:BE:24:E9:BA	Drop

Others would be accepted

(Note: maximum rule count is 10)

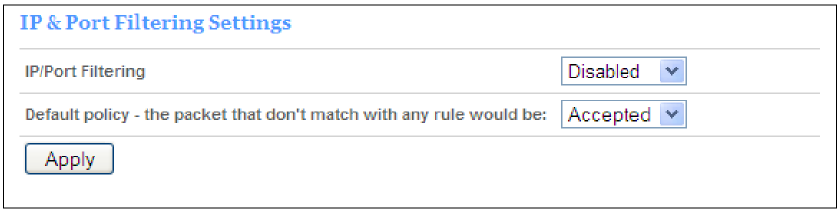
Figure 3-4-2-1-4 Rule Table

3.4.2.2 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.

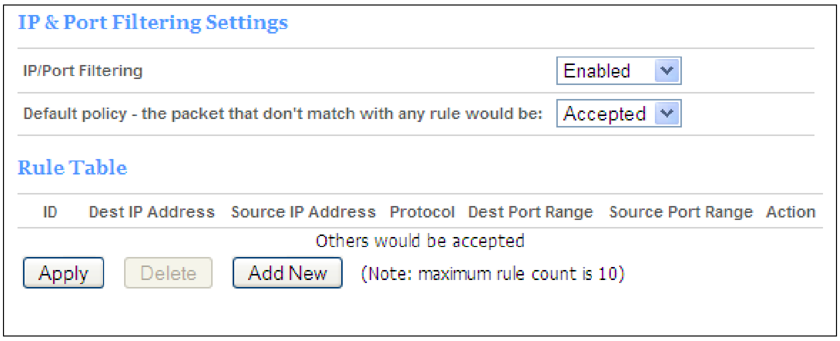


IP & Port Filtering Settings

IP/Port Filtering: Disabled

Default policy - the packet that don't match with any rule would be: Accepted

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



IP & Port Filtering Settings

IP/Port Filtering: Enabled

Default policy - the packet that don't match with any rule would be: Accepted

Rule Table

ID	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action

Others would be accepted

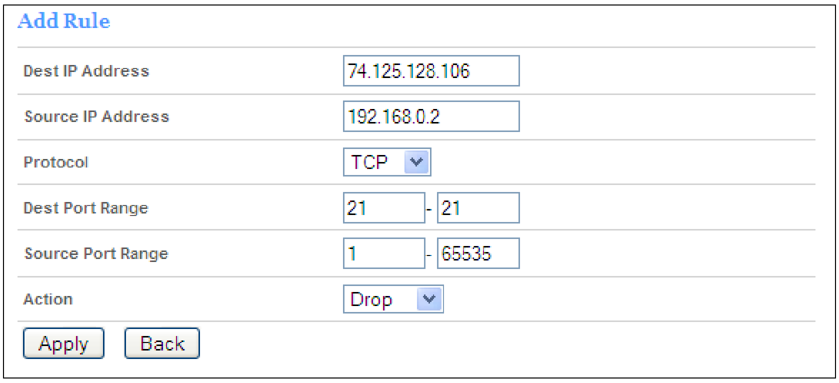
(Note: maximum rule count is 10)

Figure 3-4-2-2-2 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

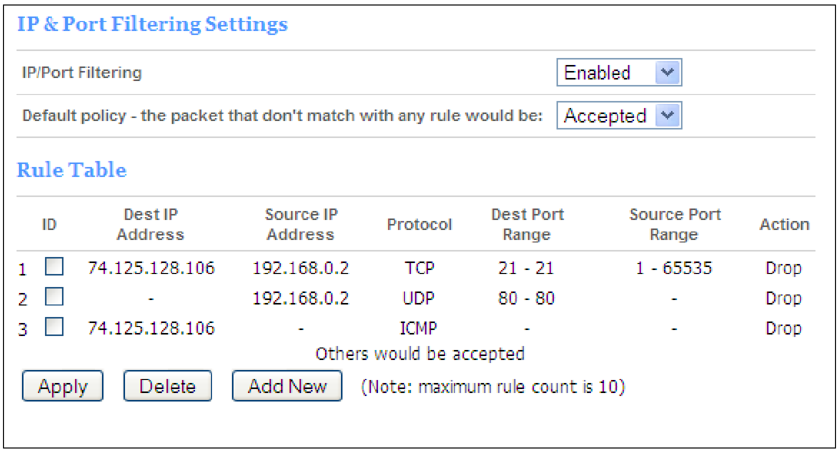
The new rules will be shown on the rule table, you can delete the rules that you have selected or add new rules sequentially (Figure 3-4-2-2-4). The maximum rule count is 10.



Add Rule

Dest IP Address	74.125.128.106
Source IP Address	192.168.0.2
Protocol	TCP
Dest Port Range	21 - 21
Source Port Range	1 - 65535
Action	Drop

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



IP & Port Filtering Settings

IP/Port Filtering	Enabled
Default policy - the packet that don't match with any rule would be:	Accepted

Rule Table

ID		Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action
1	□	74.125.128.106	192.168.0.2	TCP	21 - 21	1 - 65535	Drop
2	□	-	192.168.0.2	UDP	80 - 80	-	Drop
3	□	74.125.128.106	-	ICMP	-	-	Drop

Others would be accepted

(Note: maximum rule count is 10)

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

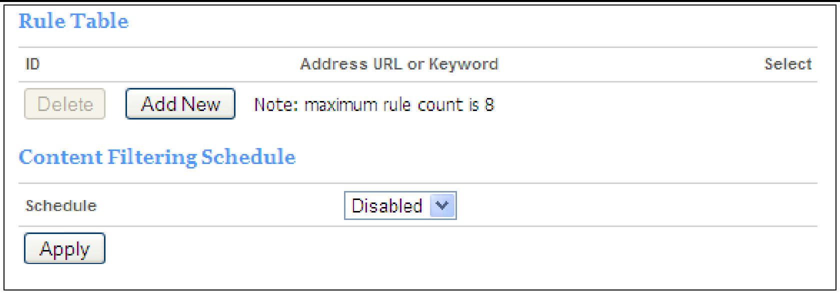
3.4.2.3 Content Filtering

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



Rule Table

ID	Address URL or Keyword	Select

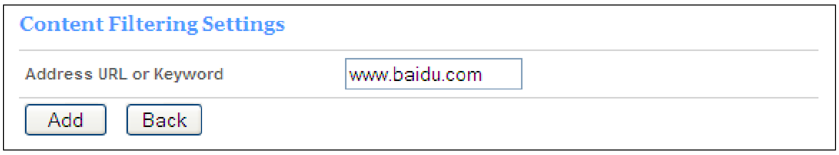
Delete　Add New　Note: maximum rule count is 8

Content Filtering Schedule

Schedule: Disabled

Apply

Figure 3-4-2-3-1 Content Filtering page



Content Filtering Settings

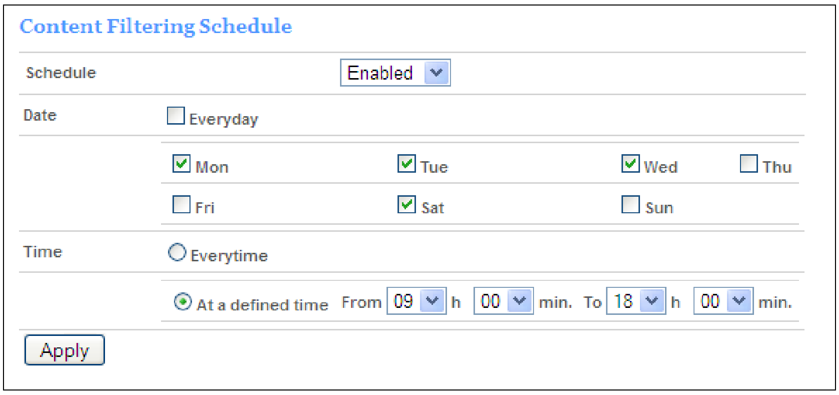
Address URL or Keyword: www.baidu.com

Add　Back

Figure 3-4-2-3-2 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.



Content Filtering Schedule

Schedule: Enabled

Date: □ Everyday

☑ Mon　☑ Tue　☑ Wed　□ Thu

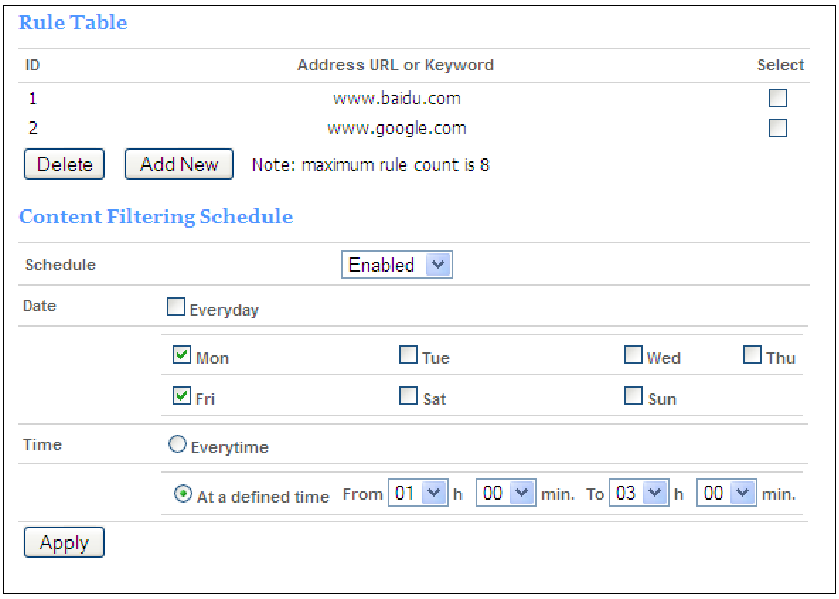
□ Fri　☑ Sat　□ Sun

Time: ○ Everytime

● At a defined time　From 09 h 00 min. To 18 h 00 min.

Apply

Figure 3-4-2-3-3 Configure Filtering Schedule



Rule Table

ID	Address URL or Keyword	Select
1	www.baidu.com	□
2	www.google.com	□

Note: maximum rule count is 8

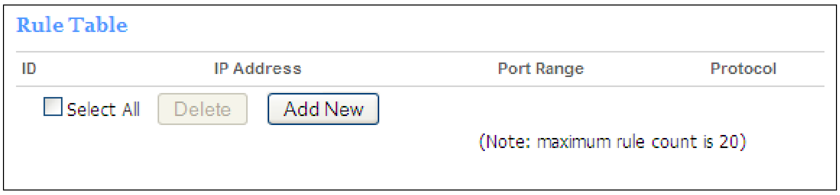
Content Filtering Schedule

Schedule	Enabled			
Date	□ Everyday			
	☑ Mon	□ Tue	□ Wed	□ Thu
	☑ Fri	□ Sat	□ Sun	
Time	○ Everytime			
	● At a defined time From 01 h 00 min. To 03 h 00 min.			

Figure 3-4-2-3-4 Content Filtering Rules

3.4.2.4 Port Forwarding

Clicking on the header of the “Port Forwarding” button will take you to the “Port Forwarding” header page (Figure 3-4-2-4-1). Clicking on the “Add New” button, you can configure IP address, port range to achieve the port forwarding purpose.

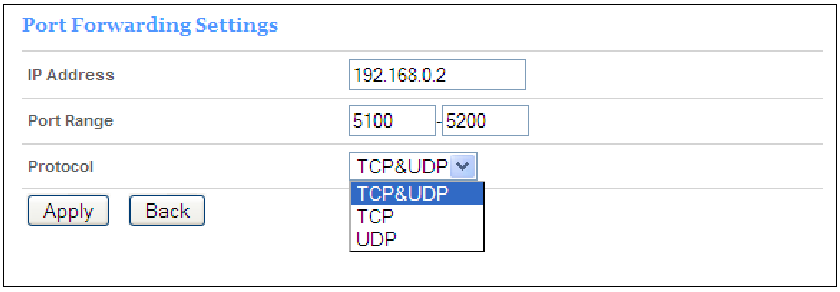


Rule Table

ID	IP Address	Port Range	Protocol

(Note: maximum rule count is 20)

Figure 3-4-2-4-1 Port Forwarding page



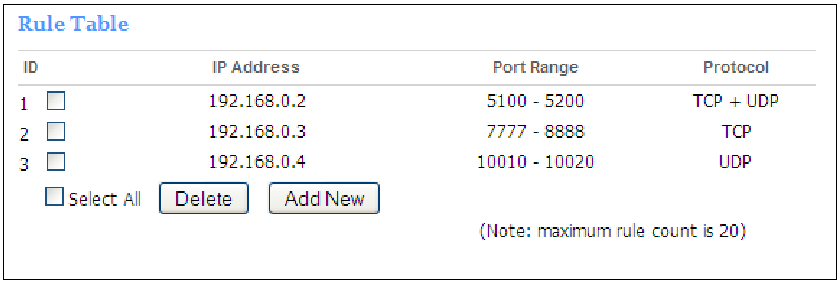
Port Forwarding Settings

IP Address	192.168.0.2
Port Range	5100 - 5200
Protocol	TCP&UDP

Figure 3-4-2-4-2 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.



Rule Table

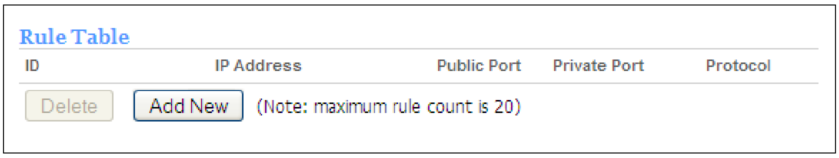
ID	IP Address	Port Range	Protocol
1 □	192.168.0.2	5100 - 5200	TCP + UDP
2 □	192.168.0.3	7777 - 8888	TCP
3 □	192.168.0.4	10010 - 10020	UDP

(Note: maximum rule count is 20)

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

3.4.2.5 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.

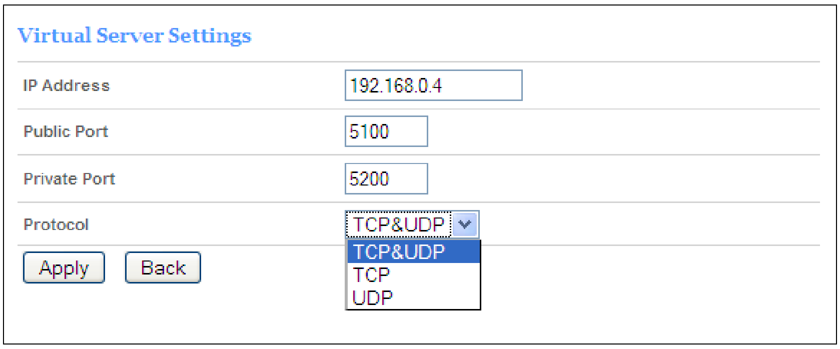


Rule Table

ID	IP Address	Public Port	Private Port	Protocol

(Note: maximum rule count is 20)

Figure 3-4-2-5-1 Virtual Server page



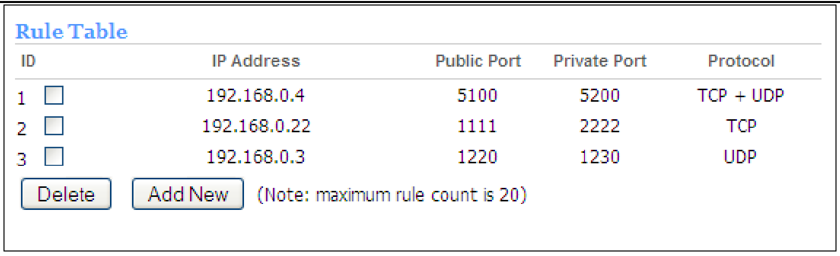
Virtual Server Settings

IP Address	192.168.0.4
Public Port	5100
Private Port	5200
Protocol	TCP&UDP

Figure 3-4-2-5-2 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.



Rule Table

ID		IP Address	Public Port	Private Port	Protocol
1	□	192.168.0.4	5100	5200	TCP + UDP
2	□	192.168.0.22	1111	2222	TCP
3	□	192.168.0.3	1220	1230	UDP

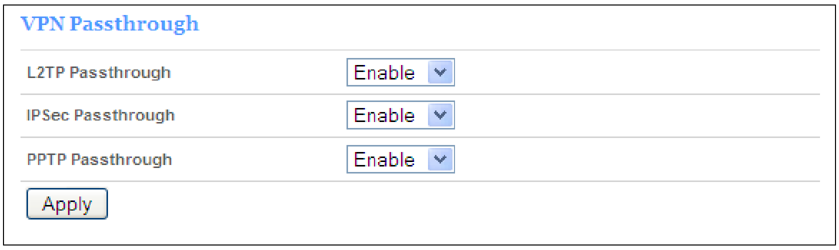
(Note: maximum rule count is 20)

Figure 3-4-2-5-3 Rule Table

3.4.2.6 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.



VPN Passthrough

L2TP Passthrough: Enable

IPSec Passthrough: Enable

PPTP Passthrough: Enable

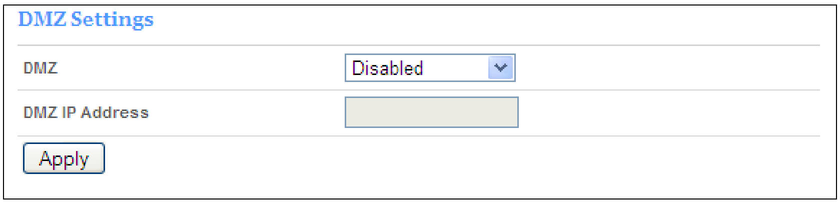
Figure 3-4-2-6-1 VPN Passthrough

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.

3.4.2.7 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)

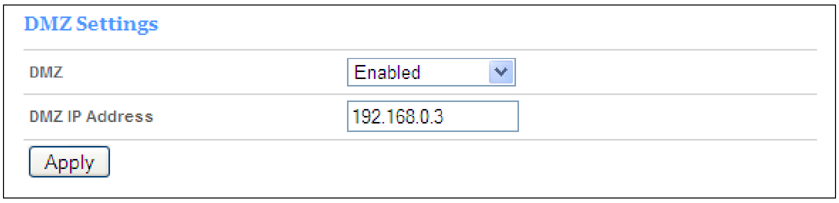


DMZ Settings

DMZ: Disabled

DMZ IP Address:

Figure 3-4-2-7-1 DMZ page



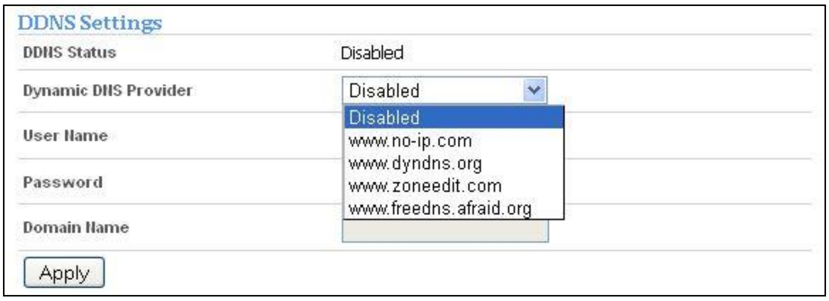
DMZ Settings

DMZ	Enabled
DMZ IP Address	192.168.0.3

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

3.4.2.8 Dynamic DNS

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



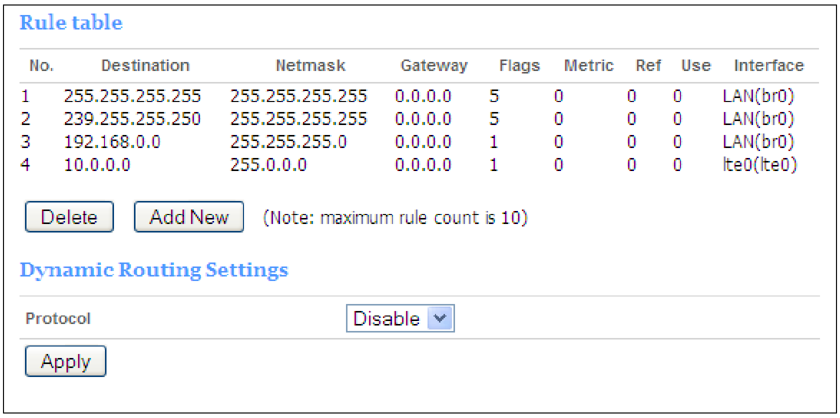
DDNS Settings

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

Figure 3-4-2-8-1 Dynamic DNS setting

3.4.2.9 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)



Rule table

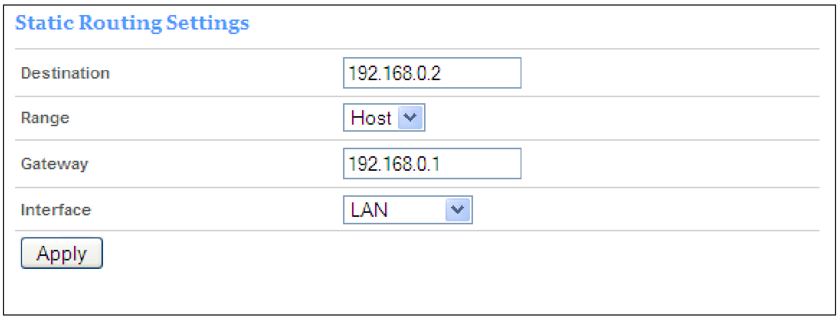
No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)
4	10.0.0.0	255.0.0.0	0.0.0.0	1	0	0	0	lte0(lte0)

(Note: maximum rule count is 10)

Dynamic Routing Settings

Protocol	Disable

Figure 3-4-2-9-1 Rule Table

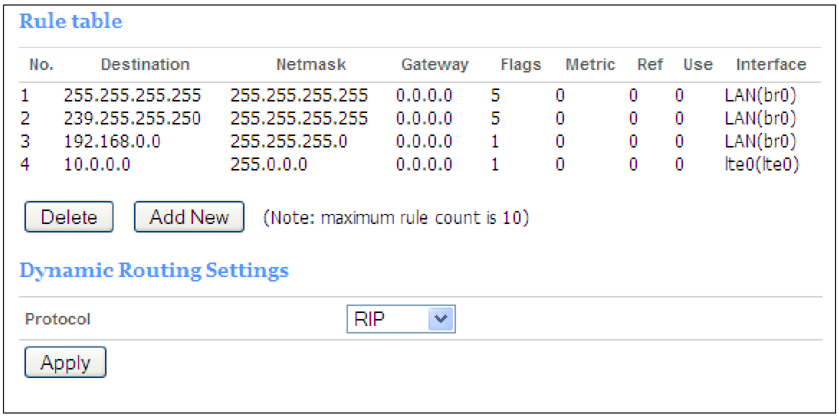


Static Routing Settings

Destination	192.168.0.2
Range	Host
Gateway	192.168.0.1
Interface	LAN

Figure 3-4-2-9-2 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.



Rule table

No.	Destination	Netmask	Gateway	Flags	Metric	Ref	Use	Interface
1	255.255.255.255	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
2	239.255.255.250	255.255.255.255	0.0.0.0	5	0	0	0	LAN(br0)
3	192.168.0.0	255.255.255.0	0.0.0.0	1	0	0	0	LAN(br0)
4	10.0.0.0	255.0.0.0	0.0.0.0	1	0	0	0	lte0(lte0)

(Note: maximum rule count is 10)

Dynamic Routing Settings

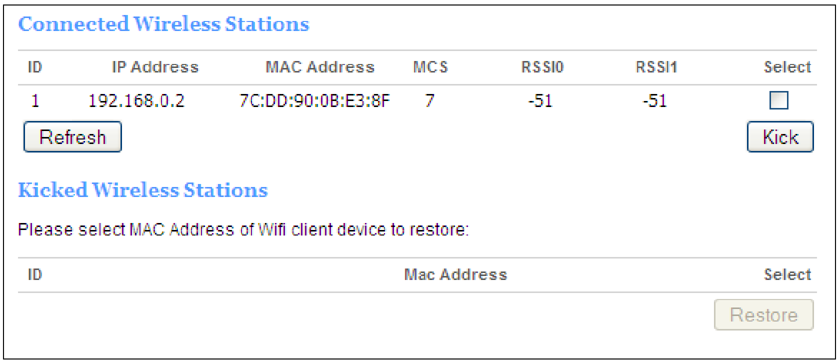
Protocol	RIP

Figure 3-4-2-9-3 New rule table

3.4.2.10 Wireless Clients

From the “Wireless Clients” page, you can see the detail information of the connected wireless devices, such as IP address, MAC address, MCS, RSSI and so on. You can also kick the selected users by clicking the “Kick” button, then the connection between the wireless clients and the router will be disconnect immediately.

The users that you kicked will be shown on the kicked wireless stations, you can restore them if you need.



Connected Wireless Stations

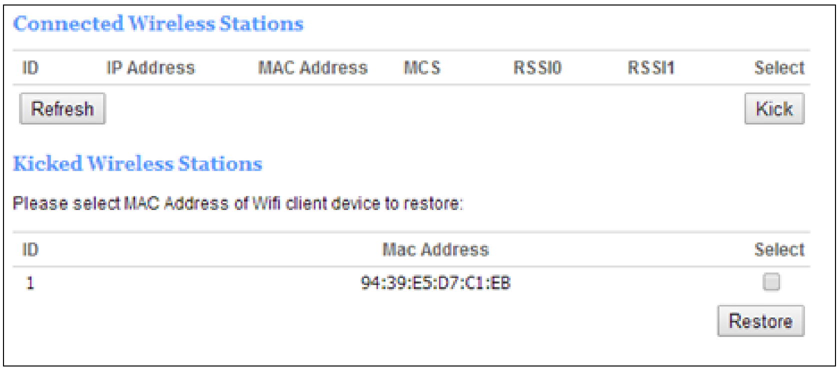
ID	IP Address	MAC Address	MCS	RSSI0	RSSI1	Select
1	192.168.0.2	7C:DD:90:0B:E3:8F	7	-51	-51	□

Kicked Wireless Stations

Please select MAC Address of Wifi client device to restore:

ID	Mac Address	Select

Figure 3-4-2-10-1 Connected Wireless Stations



Connected Wireless Stations

ID	IP Address	MAC Address	MCS	RSSI0	RSSI1	Select

Kicked Wireless Stations

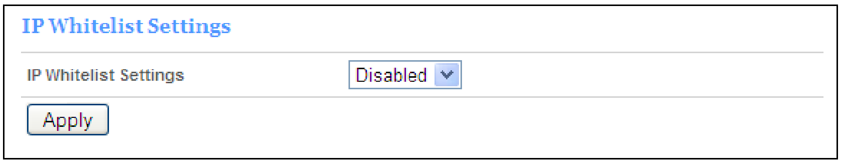
Please select MAC Address of Wifi client device to restore:

ID	Mac Address	Select
1	94:39:E5:D7:C1:EB	□

Figure 3-4-2-10-2 Kicked Wireless Stations

3.4.2.11 IP Whitelist

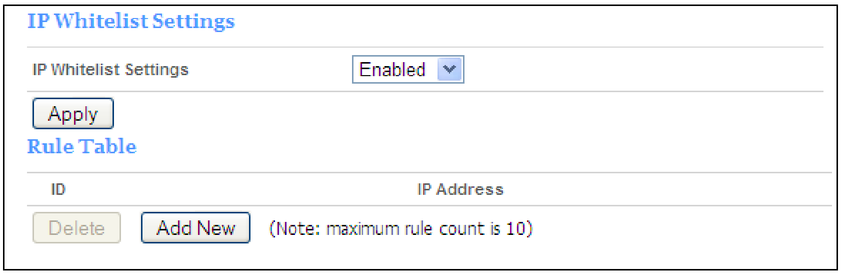
From this page, you can set the IP Whitelist. When IP whitelist is active the device shall only access the websites that have been whitelisted specifically through configuration.



IP Whitelist Settings

IP Whitelist Settings: Disabled

Figure 3-4-2-11-1 IP Whitelist page



IP Whitelist Settings

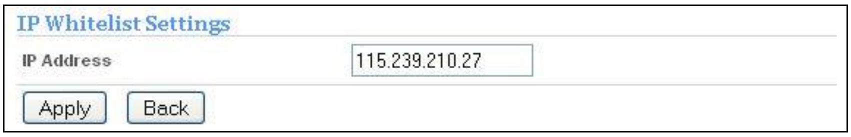
IP Whitelist Settings: Enabled

Rule Table

ID	IP Address

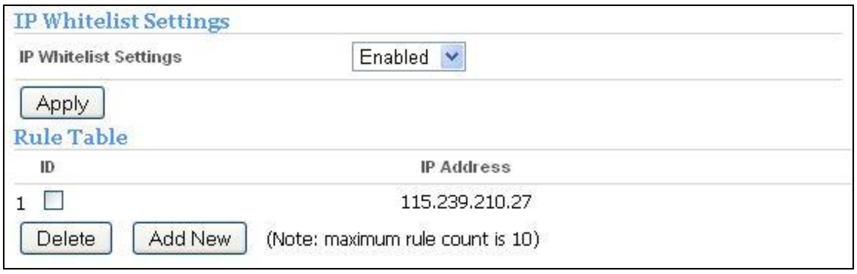
(Note: maximum rule count is 10)

Figure 3-4-2-11-2 Enable IP whitelist function


IP Whitelist Settings

IP Address: 115.239.210.27

Figure 3-4-2-11-3 Add new rule


IP Whitelist Settings

IP Whitelist Settings: Enabled

Rule Table

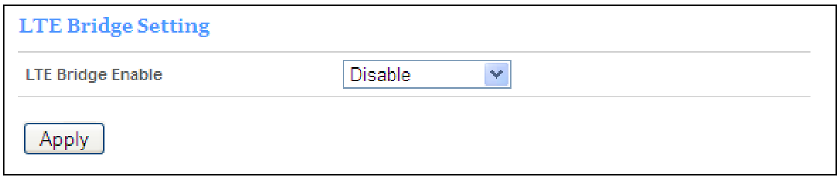
ID	IP Address
1 □	115.239.210.27

(Note: maximum rule count is 10)

Figure 3-4-2-11-4 Rule Table

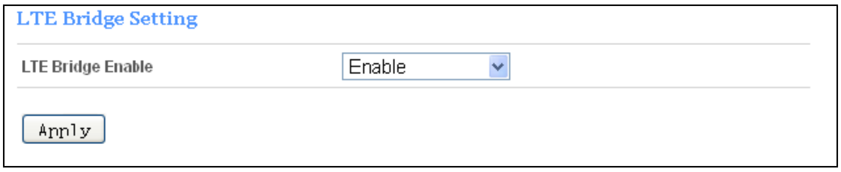
3.4.2.12 Bridge Mode

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


LTE Bridge Setting

LTE Bridge Enable: Disable

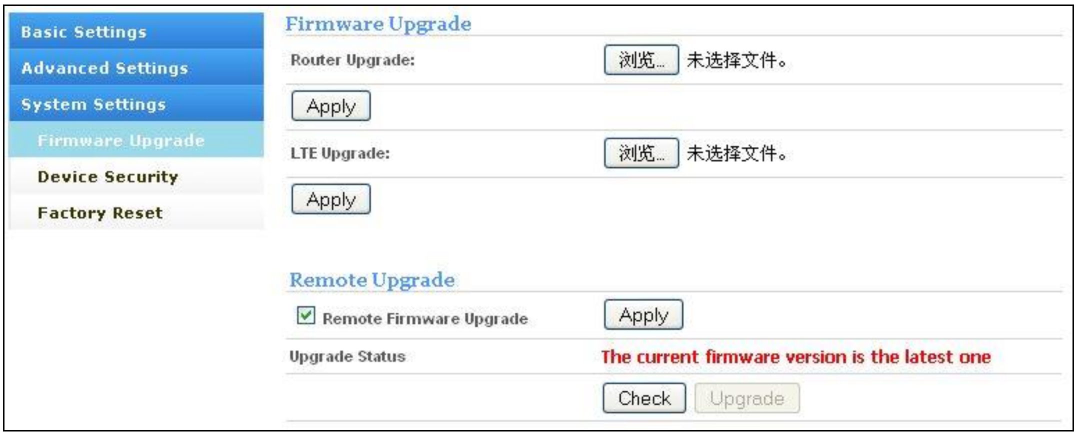
Figure 3-4-2-12-1 LTE Bridge Setting page


LTE Bridge Setting

LTE Bridge Enable: Enable

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

3.4.3 System Settings



Firmware Upgrade

Router Upgrade: 浏览... 未选择文件。

LTE Upgrade: 浏览... 未选择文件。

Remote Upgrade

☑ Remote Firmware Upgrade

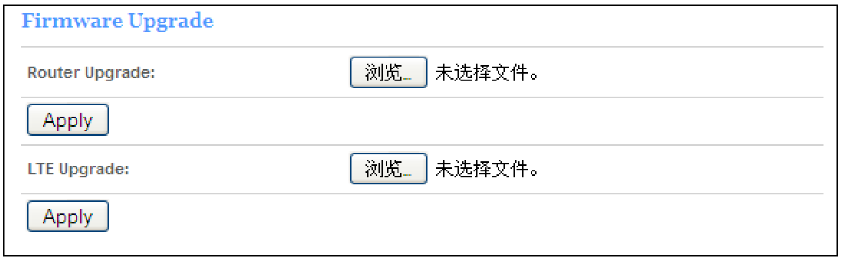
Upgrade Status: The current firmware version is the latest one

Figure 3-4-3-1 System Settings

3.4.3.1 Firmware Upgrade

➢ **Local Upgrade**

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



Firmware Upgrade

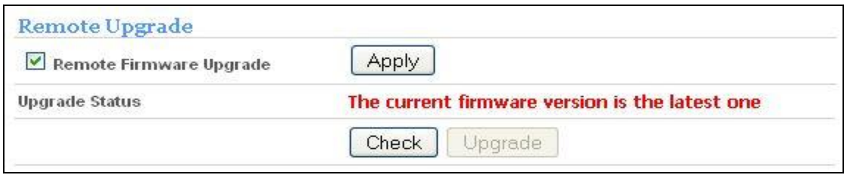
Router Upgrade: 浏览... 未选择文件。

LTE Upgrade: 浏览... 未选择文件。

Figure 3-4-3-1-1 Firmware Upgrade

➢ **Remote Upgrade**

After the device detects the new router and LTE version from Web server, the device will upgrade the new version automatically, or the device will upgrade the new version after you click the “Upgrade” button.



Remote Upgrade

☑ Remote Firmware Upgrade

Upgrade Status: The current firmware version is the latest one

Figure 3-4-3-1-2 Remote Upgrade

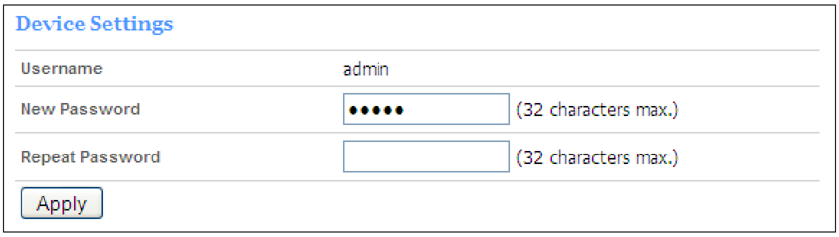
Note:

1) The firmware version must be suitable for the corresponding hardware;
2) Please make sure the adequate and stable power supply while upgrading.

3.4.3.2 Device Security

- Device Password:

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.



Device Settings

Username: admin

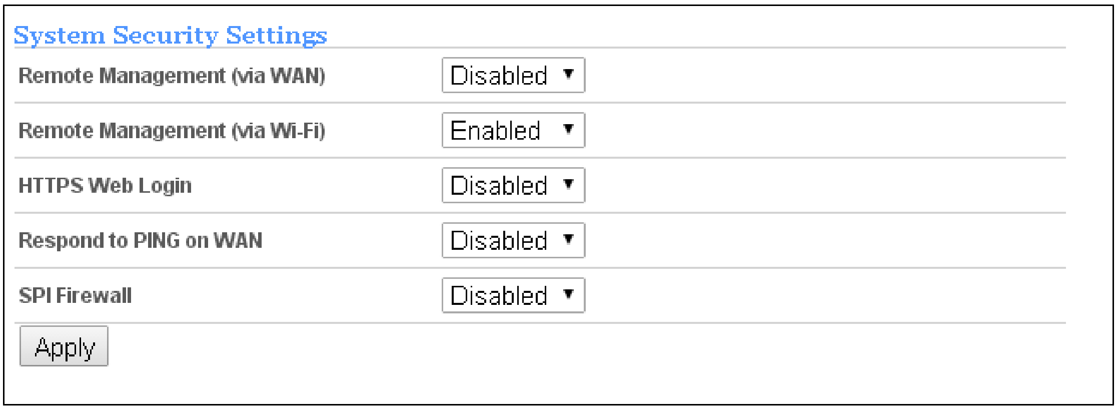
New Password: ●●●●● (32 characters max.)

Repeat Password: (32 characters max.)

Figure 3-4-3-2-1 Device Settings

- System Security Settings

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



System Security Settings

Remote Management (via WAN)	Disabled ▼
Remote Management (via Wi-Fi)	Enabled ▼
HTTPS Web Login	Disabled ▼
Respond to PING on WAN	Disabled ▼
SPI Firewall	Disabled ▼

Figure 3-4-3-2-2 System Security Settings page

➢ **Remote management(via WAN)**

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

➢ **Remote management(via Wi-Fi)**

The users on the wireless client are able to manage the WebGUI in default; you can disable this feature here.

➢ **Respond to PING on WAN**

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

➢ **SPI Firmware**

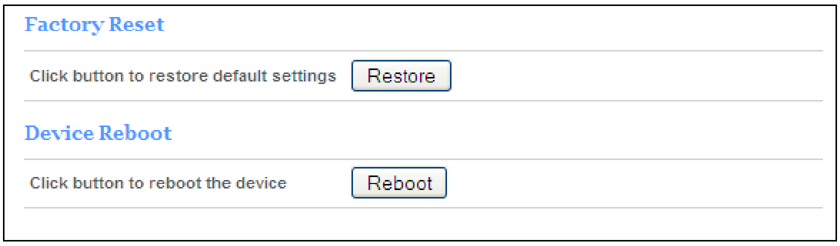
Enable this feature to enhance protection to all the wired and wireless PCs against intruders and most known Internet attacks.

➢ **HTTPS Web Login**

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

3.4.3.3 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.



Factory Reset

Click button to restore default settings

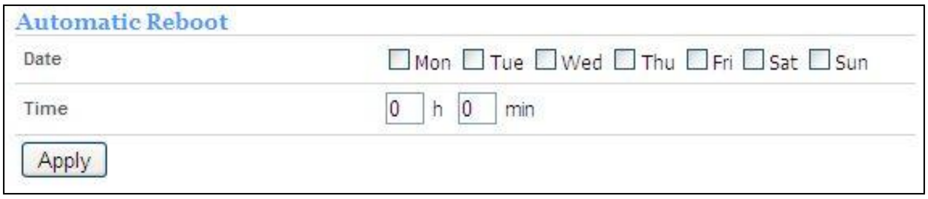
Device Reboot

Click button to reboot the device

Figure 3-4-3-3-1 Factory Reset

3.4.3.4 Scheduled Reboot

Clicking on the header of the “Scheduled Reboot” tab will take you to the “Scheduled Reboot” page. From this page, you can configure the time that the device reboots.



Automatic Reboot

Date	□Mon □Tue □Wed □Thu □Fri □Sat □Sun
Time	0 h 0 min

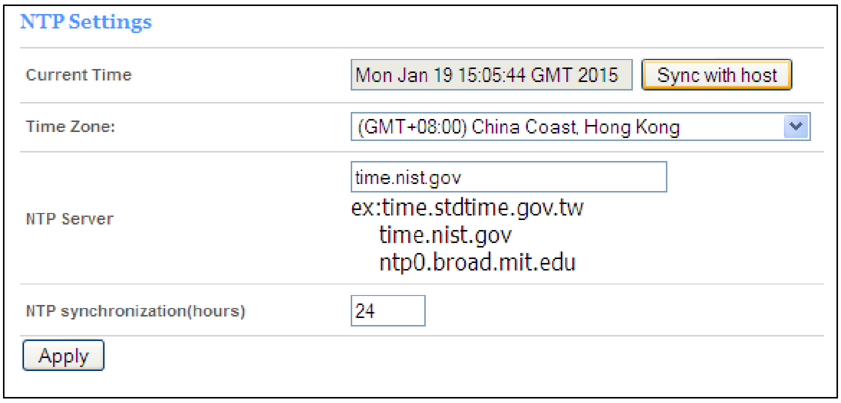
Apply

Figure 3-4-3-4-1 Scheduled Reboot

For example, choose “Mon” for “Date” and set 14h30min for “Time”, the device will reboot automatically at the 14:30 on Monday.

3.4.3.5 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.



NTP Settings

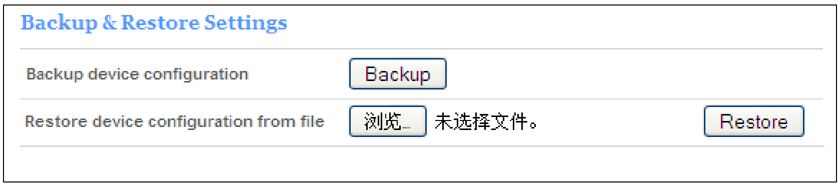
Current Time	Mon Jan 19 15:05:44 GMT 2015 Sync with host
Time Zone:	(GMT+08:00) China Coast, Hong Kong
NTP Server	time.nist.gov ex:time.stdtime.gov.tw time.nist.gov ntp0.broad.mit.edu
NTP synchronization(hours)	24

Apply

Figure 3-4-3-5-1 NTP Setting

3.4.3.6 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.



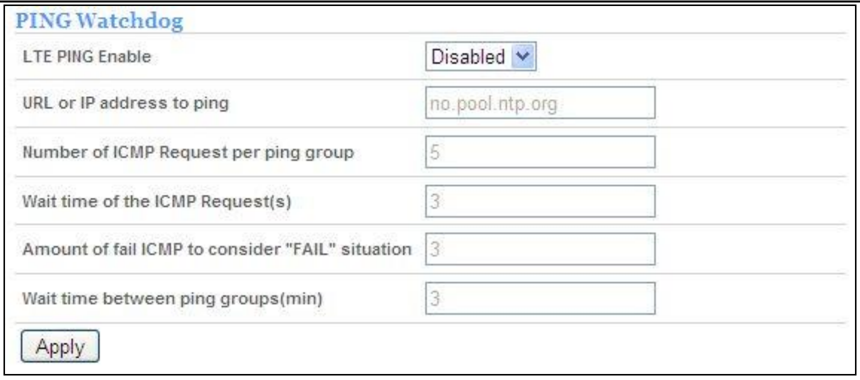
Backup & Restore Settings

Backup device configuration	Backup
Restore device configuration from file	浏览... 未选择文件。 Restore

Figure 3-4-3-6-1 Backup & Restore

3.4.3.7 Watchdog

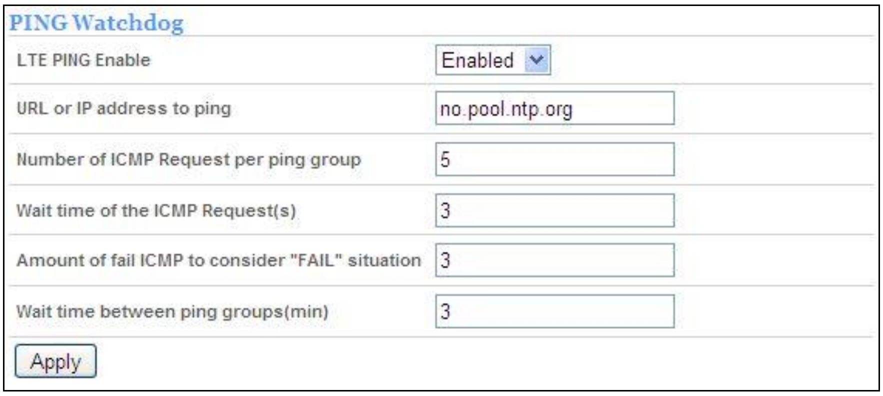
Clicking on the header of the “Ping Watchdog” tab will take you to the “Ping Watchdog” page. From this page, you can configure “Ping Watchdog” feature.



PING Watchdog

LTE PING Enable	Disabled
URL or IP address to ping	no.pool.ntp.org
Number of ICMP Request per ping group	5
Wait time of the ICMP Request(s)	3
Amount of fail ICMP to consider "FAIL" situation	3
Wait time between ping groups(min)	3

Figure 3-4-3-7-1 Ping Watchdog page



PING Watchdog

LTE PING Enable	Enabled
URL or IP address to ping	no.pool.ntp.org
Number of ICMP Request per ping group	5
Wait time of the ICMP Request(s)	3
Amount of fail ICMP to consider "FAIL" situation	3
Wait time between ping groups(min)	3

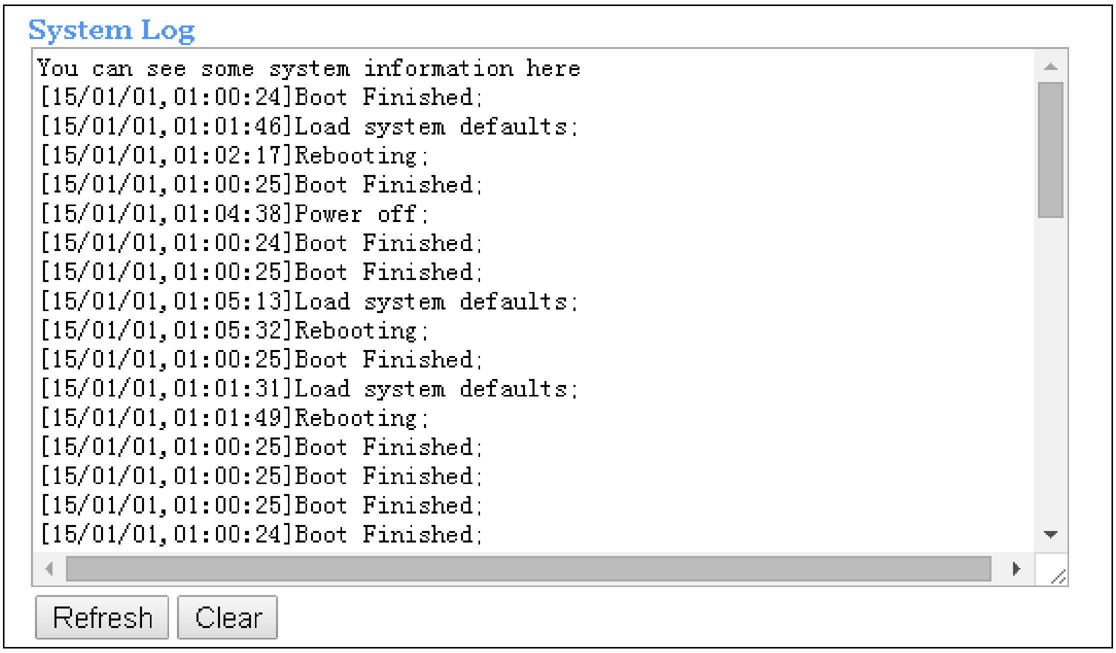
Figure 3-4-3-7-2 Enable Ping Watchdog

- **URL or IP address to ping:** the default URL is “no.pool.ntp.org”, you can also change it to other URL what you want to ping;
- **Number of ICMP Request per ping group:** the default value is 5, you can also change it to other values, the maximum value is 9;
- **Wait time of the ICMP Request(s):** the default value is 3, you can also change it to other values;
- **Amount of fail ICMP to consider “FAIL” situation:** the default value is 3, you can also change it to other values;
- **Wait time between ping groups(min):** the default value is 3, you can also change it to other values, the minimum value is 3.

According to the default status, it means ping URL “no.pool.ntp.org”, the number of ICMP Request per ping group is 5, wait time of the ICMP Request(s) is 3 seconds, wait time between ping groups(min) is 3 minutes, if amount of fail ICMP is 3 or more than 3, the LTE module will reboot automatically.

3.4.3.8 System Log

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



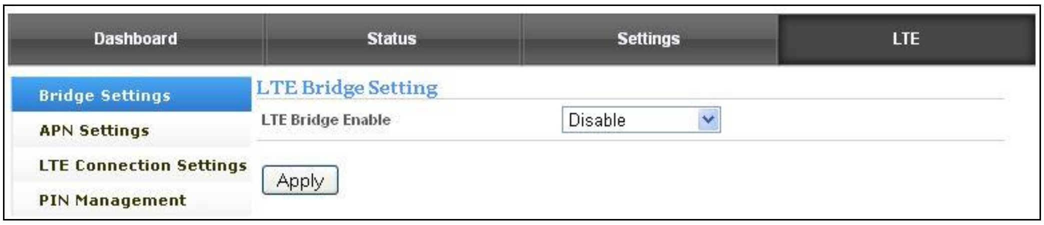
System Log

```
You can see some system information here
[15/01/01,01:00:24]Boot Finished;
[15/01/01,01:01:46]Load system defaults;
[15/01/01,01:02:17]Rebooting;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:04:38]Power off;
[15/01/01,01:00:24]Boot Finished;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:05:13]Load system defaults;
[15/01/01,01:05:32]Rebooting;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:01:31]Load system defaults;
[15/01/01,01:01:49]Rebooting;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:00:25]Boot Finished;
[15/01/01,01:00:24]Boot Finished;
```

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

3.5 4G

Click on the “4G” button, you can see four parts as below: Bridge Settings, APN Settings, LTE Connection Settings and PIN Management.

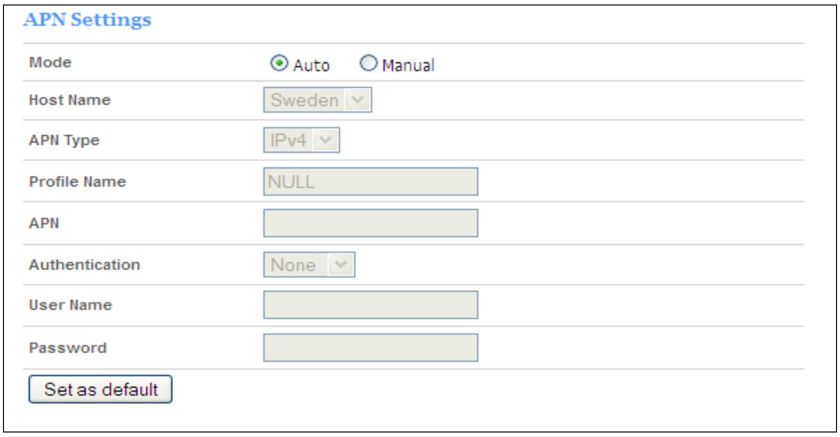


LTE Bridge Enable: Disable

Figure 3-5-1 4G

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).

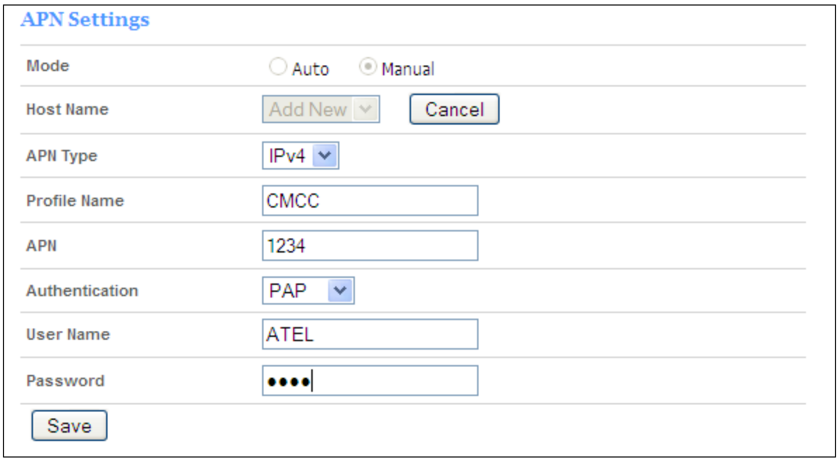


APN Settings

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

Figure 3-5-1-1 LTE APN page

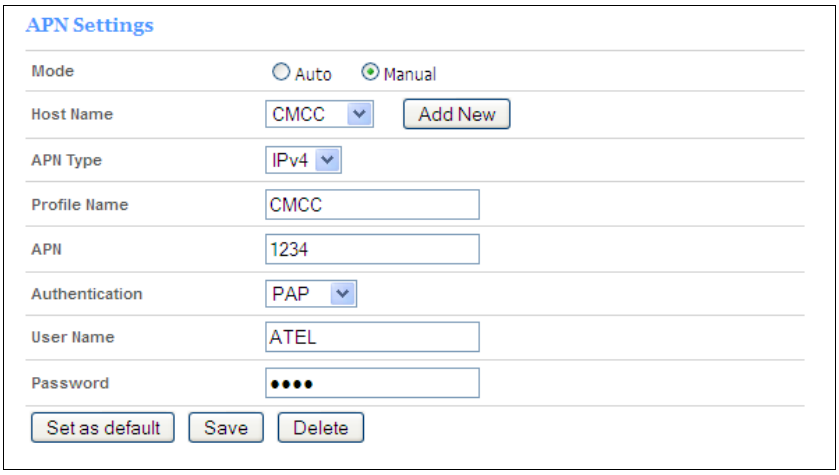
From the "Host Name" option, you can choose the APN that you had configured, then click "Set as default" to make it take effect.



APN Settings

Mode	○ Auto ● Manual
Host Name	Add New
APN Type	IPv4
Profile Name	CMCC
APN	1234
Authentication	PAP
User Name	ATEL
Password	••••

Figure 3-5-1-2 APN Configuration



APN Settings

Mode	○ Auto ● Manual
Host Name	CMCC
APN Type	IPv4
Profile Name	CMCC
APN	1234
Authentication	PAP
User Name	ATEL
Password	••••

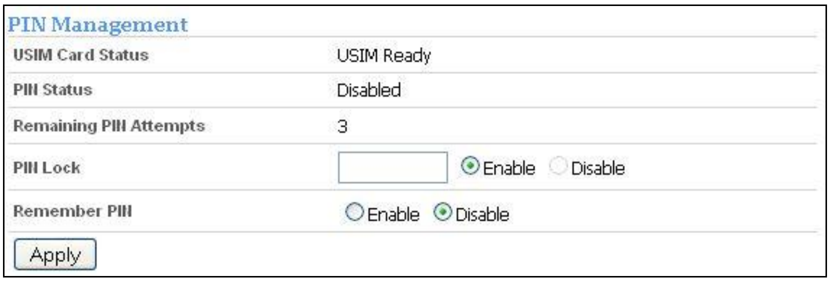
Figure 3-5-1-3 Choose the user-defined APN

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.

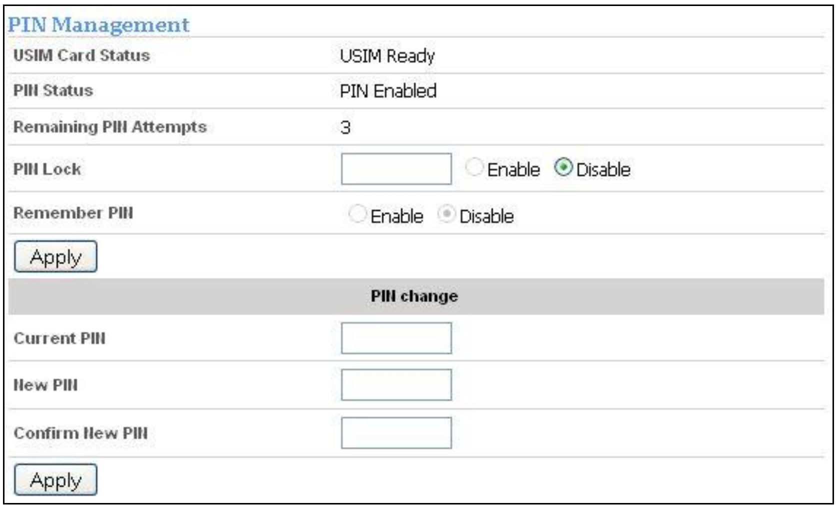
- **PIN Management**: Enter the correct PIN to enable or disable the PIN function, PIN code should be 4 to 8 digits;
- **Remember PIN**: The system will remember the PIN code of the USIM and verify the USIM automatically if the save PIN function is enabled.
- **PIN change:** You can input the current 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.



PIN Management

USIM Card Status	USIM Ready
PIN Status	Disabled
Remaining PIN Attempts	3
PIN Lock	● Enable ○ Disable
Remember PIN	○ Enable ● Disable

Figure 3-5-2-1 PIN Management page



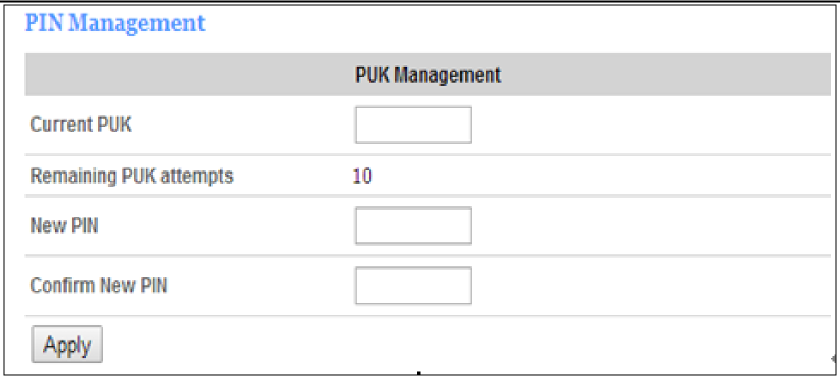
PIN Management

USIM Card Status	USIM Ready
PIN Status	PIN Enabled
Remaining PIN Attempts	3
PIN Lock	○ Enable ● Disable
Remember PIN	○ Enable ● Disable

PIN change

Current PIN	
New PIN	
Confirm New PIN	

Figure 3-5-2-2 Enable the PIN



PIN Management

PUK Management	
Current PUK	
Remaining PUK attempts	10
New PIN	
Confirm New PIN	

Figure 3-5-2-3 PUK Management page