

TN500 User Manual

Index

1.	About this Manual.....	5
2.	Product Overview.....	5
3.	Knowing your Modem.....	5
	3.1 Package Contents	5
	3.2 ROUTER Interfaces	5
4.	Configuring the ROUTER	6
	4.1 Login	6
	4.2 Dashboard	6
	4.3 Status	7
	4.3.1 WAN Status.....	7
	4.3.2 Wi-Fi LAN Status.....	8
	4.3.3 LTE Status.....	8
	4.3.4 Software Status	8
	4.3.5 Device List	9
	4.3.6 UPnP Status	9
	4.3.7 VoIP.....	9
	4.4 Settings.....	10
	4.4.1 Basic Settings	10
	4.4.2 Advanced Settings	18
	4.4.3 System Settings	30
	4.5 4G.....	31
	4.5.1 APN Settings.....	31
	4.5.2 PIN Management.....	32

Note:

Operating temperature: -10°C—45°C.

Safety Precautions

Do not operate the ROUTER:

- In areas where blasting is in progress
- Where explosive atmospheres may be present
- Near medical equipment
- ROUTER complies with RF specifications when ROUTER used at 20 cm from your body
- Near life support equipment or any equipment that may be susceptible to any form of radio interference. In such areas, the ROUTER MUST BE POWERED OFF. The ROUTER can transmit signals that could interfere with this equipment.

Do not operate the ROUTER in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the ROUTER MUST BE POWERED OFF. When operating, the ROUTER can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. The ROUTER may be used at this time.

The driver or operator of any vehicle should not operate the ROUTER while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offense.

FCC Statement

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.

Note: 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 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 party responsible for compliance could void the user's authority to operate the equipment.

RF Expoure Warning Statement:

The antenna(s) used for this device must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other transmitter.

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 ROUTER supports LTE Band4 and it supports popular operating systems like Windows, Linux and Mac.

Once you have identified the place for ROUTER, 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 ROUTER. Switch on the power Off/On switch and after few minutes the ROUTER 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 ROUTER.

3. Knowing your Modem

3.1 Package Contents

- ROUTER
- 2x Antenna
- User Manual
- Power Supply and Battery

3.2 ROUTER Interfaces

The ROUTER has been designed to be placed on a desktop. All of the cables exit from the front of the ROUTER for better organization and utility. The LED indicators are easily visible on the top of the ROUTER to provide you with information about network activity and status:

- **LED:**

● Items	Description	
Power	On(Yellow)	Only charger plug or Full charged
	Blinking(Yellow)	Charger plug in and charge for battery
	Blinking (Red)	Battery in and no charger plug in the battery is in low status,
WI-FI	On(Yellow)	WI-FI has turned on

4G LTE Router User Manual

	Blinking(Yellow)	Active data passed through Wi-Fi
	OFF	WI-FI has turned off
WPS	Blinking(Yellow)	WPS is activated. WPS led is off after one minutes
	Off	WPS is Off
Connect	On(Yellow)	LTE data connection has established
	Blinking(Yellow)	The device is trying to establish connection
	Off	No data connection
Signal	On(Yellow)	There has Service or Connected
	Off	No USIM or Limited Service

● Power

Connect the included 12V DC power supply to this jack

Note:

Adapter shall be installed near the equipment and shall be easily accessible.

4. Configuring the ROUTER

The basic settings in WebGUI consist of four main parts named Dashboard, Status, Settings and 4G. You can login to WebGUI as follows, and configure the settings according to your requirements.

Connect the PC to ROUTER using the CAT-5 Ethernet cable. Use any one of the three Ethernet ports on the ROUTER. Power on the device and waiting for about 40 seconds until the device finished initializing. Please ensure that USIM card has been inserted into USIM slot in ROUTER.

You can also connect the PC to ROUTER by Wi-Fi, choose the correct Wi-Fi SSID and input the accurate password as the label shows. The default Wi-Fi SSID is CLARO-XXXX, XXXX denotes the last 4 digits of the ROUTER's MAC address.

4.1 Login

Open your Web browser and enter 192.168.1.1 in the address bar;

Login window will popup;

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

Username/Password: 1admin0/ltecl4r0

4.2 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 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 4G status, Wi-Fi status, WAN Info, LAN Info, Data Traffic and Device&SIM Info. You can see the dashboard page as figure

4-2-1.

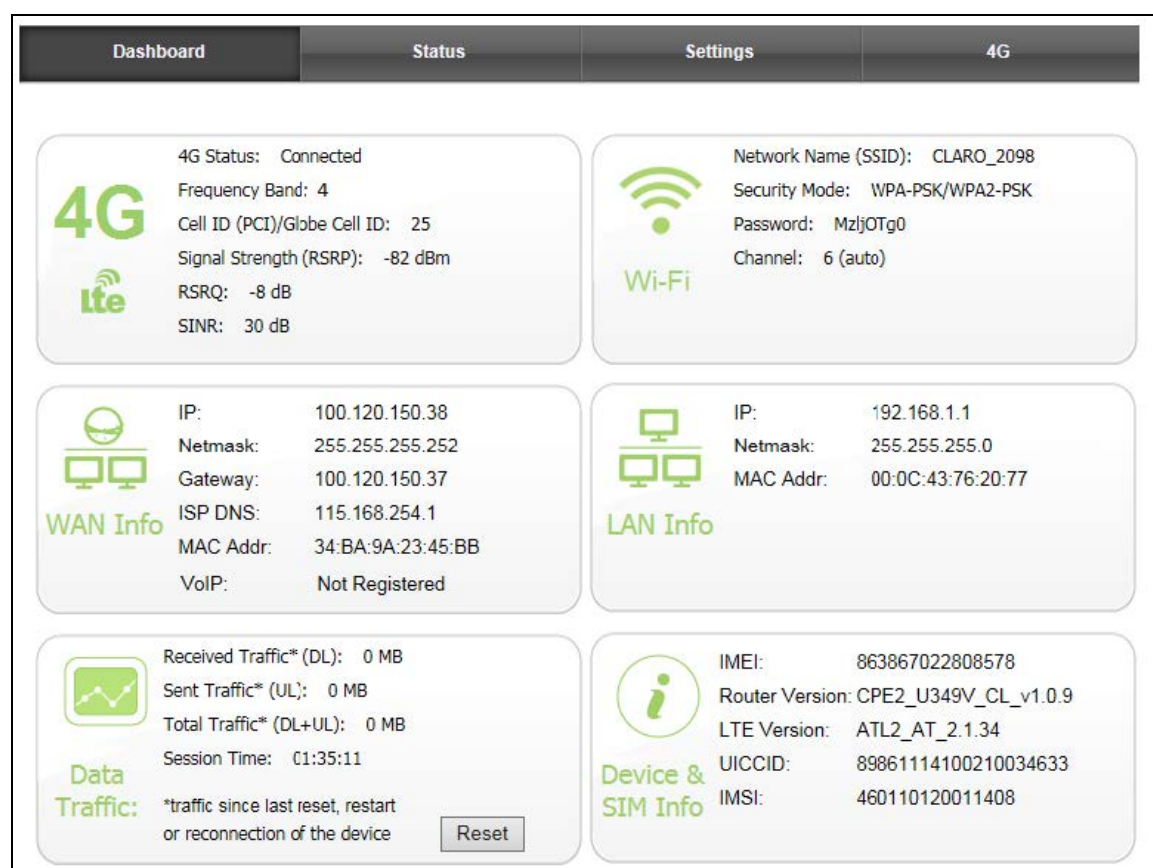


Figure 4-2-1 Dashboard Page

4.3 Status

On this page, you can see WAN Status, Wi-Fi&LAN Status, LTE Status, Software Status, Device List, UPnP Status and VoIP.

WAN Status	WAN Status
WiFi & LAN Status	IP Address 100.114.229.43
LTE Status	Primary DNS 115.168.254.1
Software Status	Secondary DNS 115.168.254.2
Device List	
UPnP Status	
VoIP	

Figure 4-3-1 Status

4.3.1 WAN Status

From the WAN Status, you can see WAN IP Address, WAN Primary DNS and WAN Secondary DNS information.

WAN Status	
IP Address	100.114.229.43
Primary DNS	115.168.254.1
Secondary DNS	115.168.254.2

Figure4-3-1-1 WAN Status

4.3.2 Wi-Fi LAN Status

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

WiFi LAN Status	
WiFi Status	Enabled
Network Name (SSID)	CLARO_0B99E9
Frequency (Channel)	Auto (Channel 8)
Security Mode	WPA2-PSK
Password	NjRIZWMz
LAN IP	192.168.1.1
DHCP Server	192.168.1.2-192.168.1.11

Figure 4-3-2-1 Wi-Fi LAN Status

4.3.3 LTE Status

Clicking on the “LTE Status”, you can see the LTE information i.e. Connection Status, USIM Status, IMEI, IMSI, RSRP, RSRQ, RSSI, SINR and Localization.

LTE Status	
Connection Status	Connected
USIM Status	Ready
IMEI	863867022510042
IMSI	460110120080191
RSRP	-108 dBm
RSRQ	-12 dB
RSSI	-92 dBm
SINR	8 dB
Localization	25

Figure 4-3-3-1 LTE Status

4.3.4 Software Status

From this page, you can know the IDU software version and the DTB software version.

Software	
IDU Software Version	CPE2_U349V_CL_v1.0.9
DTB Software Version	1.21.4

Figure 4-3-4-1 Software Status

4.3.5 Device List

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

Device List				
Hostname	MAC Address	IP Address	Type	Expires
jwhu-PC	98:90:96:BE:CB:38	192.168.1.2	Ethernet	23:54:35

Figure 4-3-5-1 Device List

4.3.6 UPnP Status

The UPnP function is disabled in default; you should enable it on the system security page (4.4.2.12) before using it. The new rules that you added will be shown on this page.

UPnP			
Protocol	OutPort	IP Address	InPort

Figure 4-3-6-1 UPnP Status

4.3.7 VoIP

You need an active VoIP subscription to use the VoIP feature. This page displays Registration status and APN. you can setting it in Settings→Advance Settings→VoIP page (4.4.2.14) before using it. The status will be shown on this page.

VoIP Status	
Registration status	Registered
VoIP APN	voip.claro.pe

Figure 4-3-7-1 VoIP

4.4 Settings

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

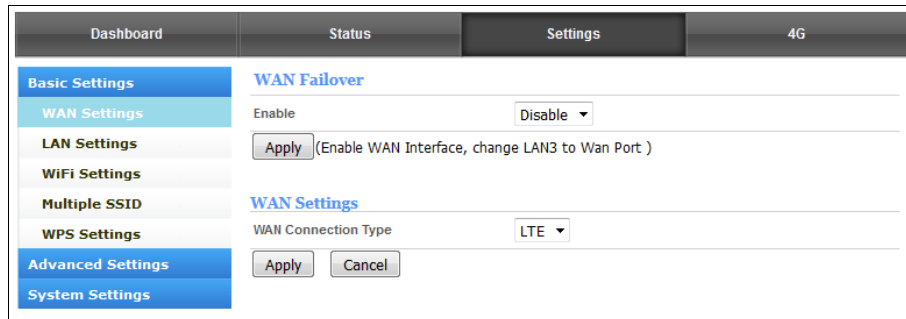


Figure4-4-1 Settings

4.4.1 Basic Settings

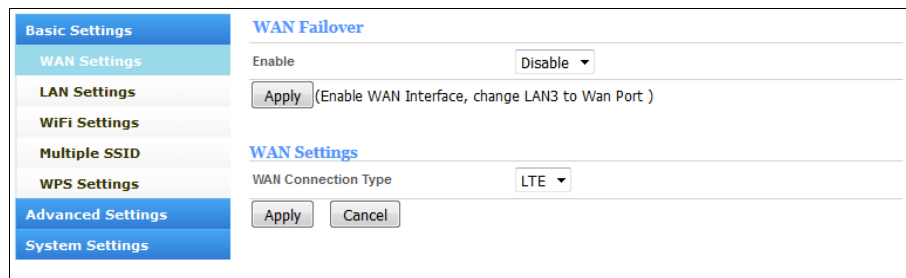


Figure4-4-1-1 Basic Settings

4.4.1.1 WAN Settings

Clicking on the “WAN Settings” tab will take you to the “WAN Settings” header page. On this page, you can choose which Internet to use after you Enable WAN Failover, the default status is Disable.

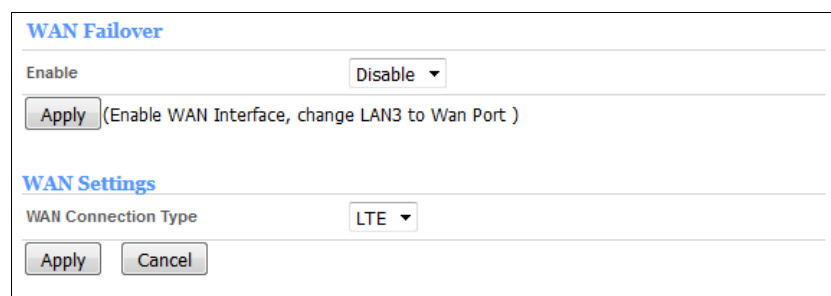


Figure 4-4-1-1-1 LAN Settings

- **WAN Failover**

You can Enable Wan Failover, the device will change LAN3 to Wan port.

WAN Failover

Enable Enable ▾

Apply (Enable WAN Interface, change LAN3 to Wan Port)

Figure 4-4-1-1-2 Enable Wan_Failover

● WAN Settings

You can choose four type, include STATIC, DHCP, PPPoE and LTE.

WAN Failover

Enable Enable ▾

Apply (Enable WAN Interface, change LAN3 to Wan Port)

WAN Settings

WAN Connection Type LTE ▾

Apply Cancel

STATIC (fixed IP)
DHCP (Auto config)
PPPoE (ADSL)
LTE

Figure 4-4-1-1-3 Enable Wan_Failover

- **STATIC (fixed IP)** - The static IP address is a regular address which is permanently assigned to a computer contactable over the Internet.

WAN Settings

WAN Connection Type STATIC (fixed IP) ▾

Static Mode

IP Address

Subnet Mask

Default Gateway

Primary DNS Server

Secondary DNS Server

Apply Cancel

Figure 4-4-1-1-4 STATIC(fixed IP)

- **DHCP (Auto config)** - If you choose the Server, you can got WAN IP parameters assigned dynamically by your ISP

WAN Settings

WAN Connection Type DHCP (Auto config) ▾

DHCP Mode

Hostname

Apply Cancel

Figure 4-4-1-1-5 DHCP(Auto config)

- **PPPoE (ADSL)** - If you choose PPPoE, you will use PPPoE to connect the Internet

The screenshot shows the 'WAN Settings' page with 'WAN Connection Type' set to 'PPPoE (ADSL)'. Under the 'PPPoE Mode' section, the 'User Name' is 'pppoe_user', and both 'Password' and 'Verify Password' fields are masked with dots. The 'Keep Alive' dropdown is set to 'Keep Alive'. Under 'Operation Mode', 'Keep Alive Mode: Redial Period' is set to 60 seconds, and 'On demand Mode: Idle Time' is set to 5 minutes. 'Apply' and 'Cancel' buttons are at the bottom.

Figure 4-4-1-1-6 PPPoE(ADSL)

- **LTE** - If you choose LTE, you connect the Internet will use the USIM card for 4G

The screenshot shows the 'WAN Settings' page with 'WAN Connection Type' set to 'LTE'. 'Apply' and 'Cancel' buttons are visible at the bottom.

Figure 4-4-1-1-7 LTE

4.4.1.2 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 ROUTER router can be viewed and changed.

The screenshot shows the 'LAN Settings' page. Fields include: 'IP Address' (192.168.1.1), 'Subnet Mask' (255.255.255.0), 'DHCP' (Enabled), 'Start IP Address' (192.168.1.2), 'End IP Address' (192.168.1.254), and 'Lease Time' (86400). There are five rows for 'Static IP' (1-5), each with 'MAC' and 'IP' input fields. An 'Apply' button is at the bottom.

Figure 4-4-1-2-1 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 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 192.168.0.2.
- **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 ROUTER 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.

4.4.1.3 Wi-Fi Settings

Clicking on “Wi-Fi Settings” will take you to the following header and on this page you can configure the Wi-Fi settings and Wi-Fi security.

- **Wi-Fi Settings**

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

WiFi Settings	
WiFi Status	Enabled ▼
WiFi Standard	11b/g/n mixed mode ▼
Network Name (SSID)	CLARO_2098
Frequency (Channel)	Auto (Channel 2) ▼
Broadcast SSID	☒ Enabled ☐ Disabled
AP Isolation	☐ Enabled ☒ Disabled
Channel BandWidth	☒ 20 MHz ☐ 20/40 MHz
WiFi Security	
Security Mode	WPA-PSK/WPA2-PSK ▼
WPA Algorithms	☐ TKIP ☒ AES ☐ TKIP/AES
Password	MzljOTg0
Key Renewal Interval	3600 Seconds (0 ~ 4194303)
Apply	

Figure 4-4-1-3-1 Wi-Fi Settings

➤ **Wi-Fi Status:** Enabled(default)/Disabled

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

➤ **Wi-Fi Standard:**

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

WiFi Standard	11b/g/n mixed mode ▼
Network Name(SSID)	11b only
	11g only
	11n only
Frequency (Channel)	11b/g mixed mode
	11b/g/n mixed mode

Figure 4-4-1-3-2 Wi-Fi 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 Wi-Fi. It is not necessary to change the wireless channel unless you noticed the interference problems with other access points nearby.

Frequency (Channel)	Auto (Channel 2) ▼	
Broadcast SSID	Auto (Channel 2)	
AP Isolation	2412 MHz (Channel 1)	
Channel BandWidth	2417 MHz (Channel 2)	
WiFi Security	2422 MHz (Channel 3)	
Security Mode	2427 MHz (Channel 4)	
WPA Algorithms	2432 MHz (Channel 5)	
Password	2437 MHz (Channel 6)	
	2442 MHz (Channel 7)	
	2447 MHz (Channel 8)	
	2452 MHz (Channel 9)	
	2457 MHz (Channel 10)	
	2462 MHz (Channel 11)	
Key Renewal Interval	3600	Seconds (0 ~ 4194303)
Apply		

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

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

When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast of the router. If you disabled this feature, the Wi-Fi 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

20 MHz channel bandwidth support up to 150 Mbit/s connections.

40 MHz channel bandwidth support up to 300 Mbit/s connections.

● **Wi-Fi Security**

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

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

a) **WPA Security Mode**

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

➤ **WPA Algorithms:** TKIP, AES, TKIP/AES

➤ **Keywords:** 1~32 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)
Apply	

Figure 4-4-1-3-4 Default Wi-Fi Security

WiFi Security	
Security Mode	WPA-PSK
WPA Algorithms	☐ TKIP ☒ AES ☐ TKIP/AES
Password	m2m4m8fd
Key Renewal Interval	3600 Seconds (0 ~ 4194303)
Apply	

Figure 4-4-1-3-5 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)
Apply	

Figure 4-4-1-3-6 WPA-PSK/WPA2-PSK

4.4.1.4 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.

ID	SSID	Hidden SSID	Isolated	Security Mode	WPA Algorithms	Password
Edit Delete Cancel Add New (Note: maximum rule count is 5)						

Figure 4-4-1-4-1 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 3-4-1-4-2 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 4-4-1-4-3). Connect any Wi-Fi 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	WPA2PSK	TKIP	1q2w#E\$R
3	a1b2c3d4	Disabled	Disabled	WPA2PSK/WPA2 PSK	TKIP/AES	uuuuuuuu

(Note: maximum rule count is 5)

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

4.4.1.5 WPS Settings

You can setup security easily by choosing PIN or PBC method to do Wi-Fi 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 Wi-Fi.

- **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 Wi-Fi each other.
- **PBC Mode**
 - (1) Press the WPS button of the ROUTER directly;
 - (2) Then ROUTER and wireless client will automatically complete the interaction and connect via Wi-Fi 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.

Figure 4-4-1-5-1 WPS page

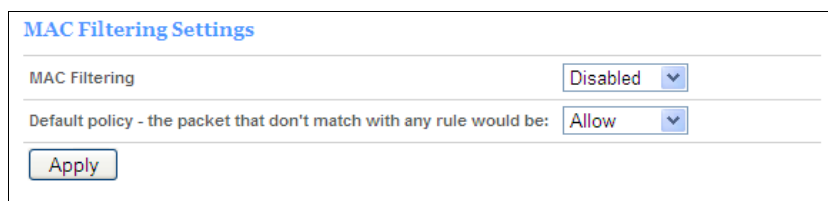
4.4.2 Advanced Settings

Figure 4-4-2-1 Advanced Settings

4.4.2.1 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.



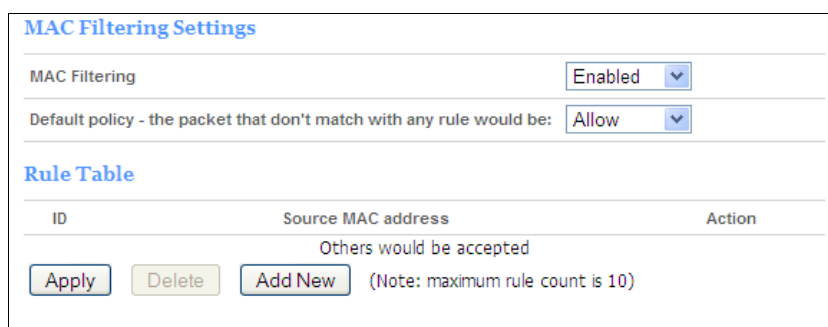
The screenshot shows the 'MAC Filtering Settings' page. At the top, the title 'MAC Filtering Settings' is in blue. Below it, there are two settings: 'MAC Filtering' set to 'Disabled' and 'Default policy - the packet that don't match with any rule would be:' set to 'Allow'. Both are dropdown menus. At the bottom, there is an 'Apply' button.

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

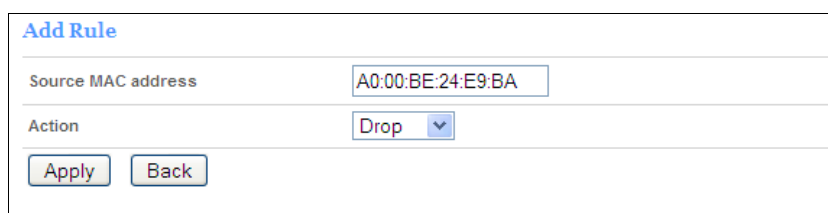
Default Policy: The packets that don't match with any rules would be “Allow/Deny”. If you choose the “Allow” button here, the MAC address that you add would be dropped. Otherwise, only the MAC addresses on the rule table can be accepted.

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 4-4-2-1-4)



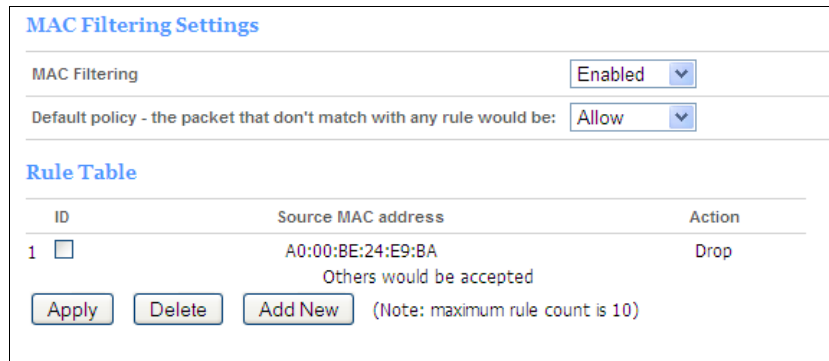
The screenshot shows the 'MAC Filtering Settings' page with the 'MAC Filtering' setting now set to 'Enabled'. Below this, there is a 'Rule Table' section. It contains a table with columns 'ID', 'Source MAC address', and 'Action'. Below the table, there are buttons for 'Apply', 'Delete', and 'Add New'. A note states: '(Note: maximum rule count is 10)'. The text 'Others would be accepted' is also visible.

Figure4-4-2-1-2 Enable MAC Filtering function



The screenshot shows the 'Add Rule' page. It has two input fields: 'Source MAC address' with the value 'A0:00:BE:24:E9:BA' and 'Action' set to 'Drop'. At the bottom, there are 'Apply' and 'Back' buttons.

Figure4-4-2-1-3 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

Apply Delete Add New (Note: maximum rule count is 10)

Figure4-4-2-1-4 Rule Table

4.4.2.2 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 4-4-2-2-3).

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.



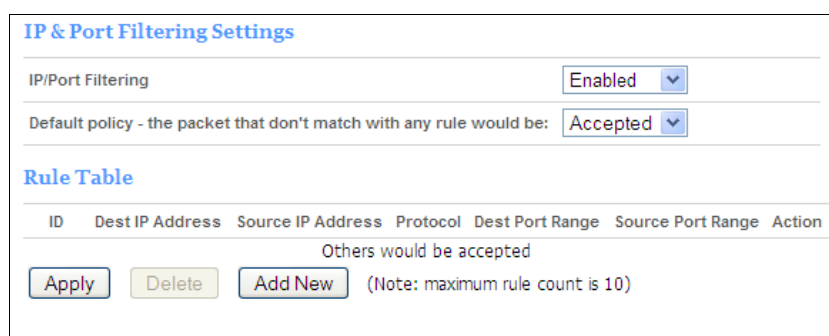
IP & Port Filtering Settings

IP/Port Filtering: Disabled

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

Apply

Figure 4-4-2-2-1 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						

Apply Delete Add New (Note: maximum rule count is 10)

Figure4-4-2-2-2 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 4-4-2-2-4). 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

Buttons: Apply, Back

Figure 4-4-2-2-3 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

Buttons: Apply, Delete, Add New

(Note: maximum rule count is 10)

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

4.4.2.3 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 4-4-2-3-4). The maximum rule count is 8.

The screenshot shows the 'Content Filtering' page. At the top is the 'Rule Table' section with a table header containing 'ID', 'Address URL or Keyword', and 'Select'. Below the header are 'Delete' and 'Add New' buttons, and a note stating 'Note: maximum rule count is 8'. Below this is the 'Content Filtering Schedule' section, which includes a 'Schedule' dropdown menu set to 'Disabled' and an 'Apply' button.

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

The screenshot shows the 'Add New Rule' dialog box. It has a title 'Content Filtering Settings'. Below the title is a text input field labeled 'Address URL or Keyword' containing the text 'www.baidu.com'. At the bottom are 'Add' and 'Back' buttons.

Figure 4-4-2-3-2 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.

The screenshot shows the 'Content Filtering Schedule' configuration page. The 'Schedule' dropdown is set to 'Enabled'. Under the 'Date' section, there are checkboxes for 'Everyday', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', and 'Sun'. 'Mon', 'Tue', 'Wed', and 'Sat' are checked. Under the 'Time' section, there are radio buttons for 'Everytime' and 'At a defined time'. 'At a defined time' is selected. Below this, there are time pickers for 'From' (09 h 00 min) and 'To' (18 h 00 min). An 'Apply' button is at the bottom.

Figure 4-4-2-3-3 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

Date ☐ Everyday

☒ Mon
 ☐ Tue
 ☐ Wed
 ☐ Thu

☒ Fri
 ☐ Sat
 ☐ Sun

Time ☐ Everytime

☒ At a defined time From h min. To h min.

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

4.4.2.4 Port Forwarding

Clicking on the header of the “Port Forwarding” button will take you to the “Port Forwarding” header page (Figure 4-4-2-4-1). 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
☐ Select All Delete Add New			

(Note: maximum rule count is 20)

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

Port Forwarding Settings

IP Address

Port Range -

Protocol

Figure 4-4-2-4-2 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
☐ Select All Delete Add New			
(Note: maximum rule count is 20)			

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

4.4.2.5 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 ▼
Apply	

Figure 4-4-2-5-1 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.

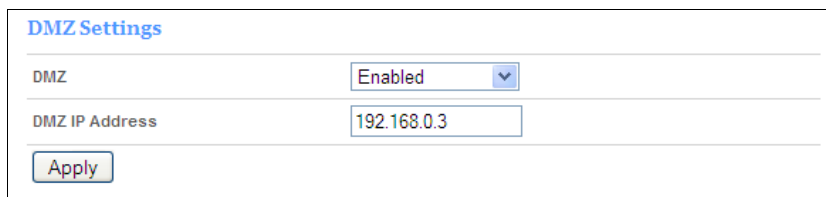
4.4.2.6 Demilitarized Zone

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 192.168.0.3)

DMZ Settings	
DMZ	Disabled ▼
DMZ IP Address	
Apply	

Figure 4-4-2-6-1 DMZ page



DMZ Settings

DMZ: Enabled

DMZ IP Address: 192.168.0.3

Apply

Figure 4-4-2-6-2 DMZ Setting

4.4.2.7 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: Disabled

Password: Disabled

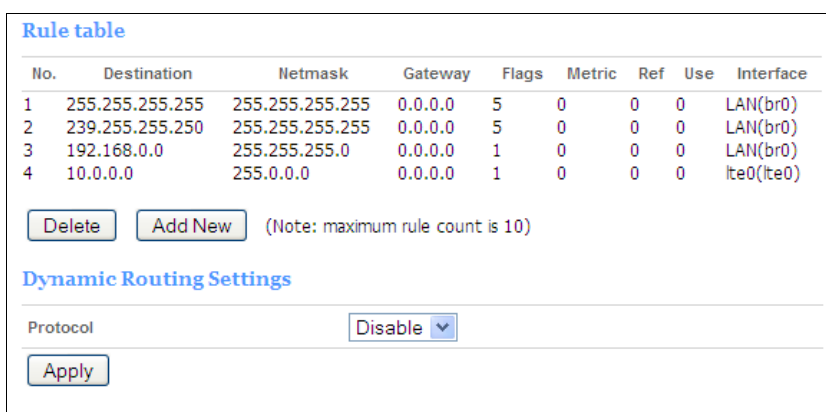
Domain Name: Disabled

Apply

Figure 4-4-2-7-1 Dynamic DNS setting

4.4.2.8 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)

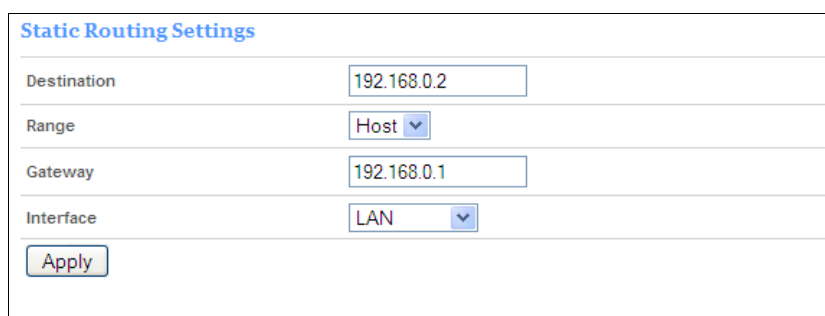
Delete Add New (Note: maximum rule count is 10)

Dynamic Routing Settings

Protocol: Disable

Apply

Figure4-4-2-8-1 Rule Table



Static Routing Settings

Destination: 192.168.0.2

Range: Host

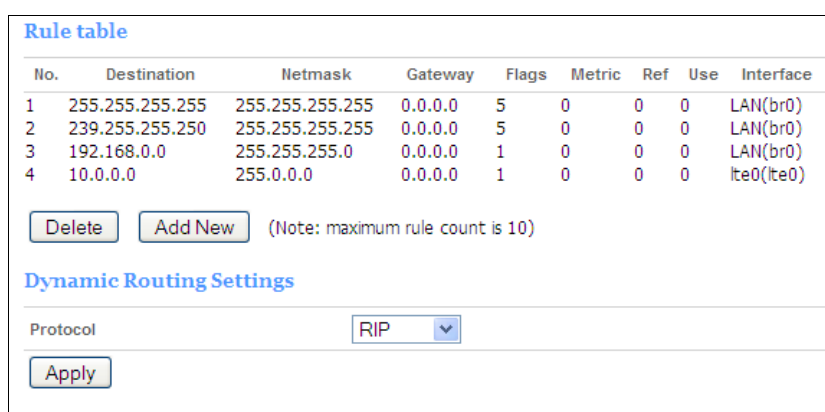
Gateway: 192.168.0.1

Interface: LAN

Apply

Figure 4-4-2-8-2 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)

Delete Add New (Note: maximum rule count is 10)

Dynamic Routing Settings

Protocol: RIP

Apply

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

4.4.2.9 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.

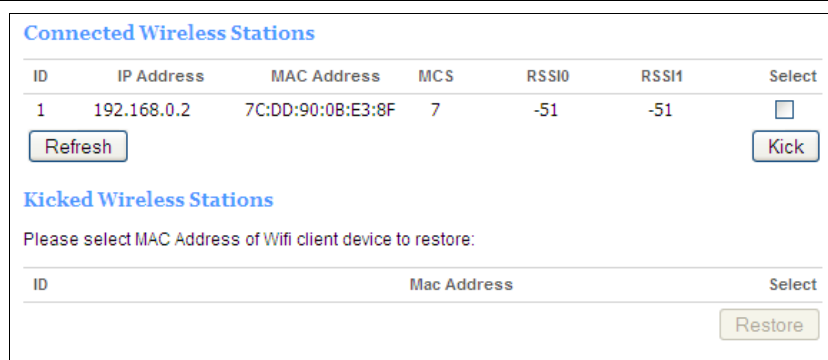


Figure4-4-2-9-1 Connected Wireless Stations



Figure 4-4-2-9-2 Kicked Wireless Stations

4.4.2.10 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 4-4-2-10-1 Backup & Restore

4.4.2.11 System Settings

Clicking on the header of the “System Settings” tab will take you to the “System Security Settings” page. From this page, 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 ▼
Respond to PING on WAN	Enabled ▼
SPI Firewall	Disabled ▼
UPnP	Disabled ▼
HTTPS Web Login	Disabled ▼
Apply Reset	

Figure 4-4-2-11-1 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.

➤ **UPNP**

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

➤ **HTTPS Web Login**

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

4.4.2.12 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 4-4-2-12-1 NTP Setting

4.4.2.13 VoIP

Clicking on the header of the “VoIP” tab will take you to “VoIP” page.

The screenshot shows the 'VoIP Settings' page with the following configuration:

VoIP Settings	Enable
Status	Registered
Config Mode	☐ SIM ☒ Memory
Use second APN	Disable
Main SIP/Register Server Address	voip2.net1.se
SIP Service Domain	ims.claro.com.pe
Username	softphone225
Password	••••••••
APN	voip.claro.pe

Buttons: Apply, Register

Please wait 1-3 min after you click button...

Figure 4-4-2-14-1 VoIP page

From this page, choose Memory, you can set up VoIP configuration.

The screenshot shows the 'VoIP Settings' page with the 'Memory' config mode selected. The configuration is as follows:

VoIP Settings	Enable
Status	Unregistered
Config Mode	☐ SIM ☒ Memory
Use second APN	Disable
Server Address	
Username	
Password	
APN	Default

Buttons: Apply, Register

Please wait 1-3 min after you click button...

Figure 4-4-2-13-2 Set VoIP

- **Status** – the default status is “Unregistered”, after setting up the VoIP information and clicking the “Register” button, the status will be changed to “Registered”.
- **Config Mode** – SIM, Memory(the default is SIM)

- **Server Address** – inputting the server IP that you register.
- **Username** – inputting the username that you register.
- **Password** – inputting the password that you register.

After setting up the above informations and clicking the “Register” button to register the server, you can call up via the device.

4.4.3 System Settings



The screenshot shows the 'System Settings' page. On the left is a sidebar menu with options: Basic Settings, Advanced Settings, System Settings, Local Upgrade (highlighted), Device Settings, and Factory Reset. The main content area is titled 'Local Upgrade' and contains two sections. The first section is for 'Location' with a '选择文件' (Select File) button and the text '未选择任何文件' (No file selected), followed by an 'Apply' button. The second section is for 'LTE Upgrade' with another '选择文件' (Select File) button and the text '未选择任何文件' (No file selected), followed by an 'Apply' button.

Figure 4-4-3-1 System Settings

4.4.3.1 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.



The screenshot shows the 'Firmware Upgrade' page. It has two main sections. The first section is for 'Router Upgrade' with a '浏览...' (Browse...) button and the text '未选择文件。' (No file selected), followed by an 'Apply' button. The second section is for 'LTE Upgrade' with another '浏览...' (Browse...) button and the text '未选择文件。' (No file selected), followed by an 'Apply' button.

Figure 4-4-3-1-1 Firmware 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.

4.4.3.2 Device Security

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: 1admin0

New Password: (32 characters max.)

Repeat Password: (32 characters max.)

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

4.4.3.3 Factory Reset

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

Factory Reset

Click button to restore default settings

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

4.5 4G

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

Dashboard	Status	Settings	4G
APN Settings			
PIN Management			
APN Settings			
Mode: ☐ Auto ☒ Manual			
Host Name: Add New			
APN Type: IPv4			
Profile Name: Claro			
APN: datacell.claro.pe			
Authentication: None			
User Name: Claro			
Password: 			
Set as default			

Figure 4-5-1 4G

4.5.1 APN Settings

The default APN mode is Manual and the default APN has value, if you want to configure the LTE APN, then you can configure the APN settings by clicking on the “Add New” button (Figure 4-5-1-2).

APN Settings

Mode: ☐ Auto ☒ Manual

Host Name: Add New

APN Type:

Profile Name:

APN:

Authentication:

User Name:

Password:

Set as default

Figure 4-5-1-1 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 Cancel

APN Type:

Profile Name:

APN:

Authentication:

User Name:

Password:

Save

Figure 4-5-1-2 APN Configuration

APN Settings

Mode: ☐ Auto ☒ Manual

Host Name: Add New

APN Type:

Profile Name:

APN:

Authentication:

User Name:

Password:

Set as default Save Delete

Figure4-5-1-3 Choose the user-defined APN

4.5.2 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;
- **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
Apply	

Figure 4-5-2-1 PIN Management page

PIN Management	
USIM Card Status	USIM Ready
PIN Status	PIN Enabled
Remaining PIN Attempts	3
PIN Lock	☐ Enable ☒ Disable
Apply	
PIN change	
Current PIN	
New PIN	
Confirm New PIN	
Apply	

Figure 4-5-2-2 Enable the PIN

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

Figure 4-5-2-3 PUK Management page