LTE CPE SQI4N4

Quick Start Guide

FCC ID: 2AI24QCI4NU
FCC ID: 2AI24SQO14

Issue 01

Date 2016-08

Contents

1 About This Document

The document will serve as a quick start guide for LTE device model SQI4N4. The SQI4N4 includes two parts, an indoor unit and an outdoor unit. Please see following matrixshows for detailed information.

LTE CPE SQI4N4	Indoor Unit	FCC ID: 2AI24QCI4NU	Model: QCI4NU
	Outdoor Unit	FCC ID: 2AI24SQO14	Model: SQO14

2 Device Panel

Figure 2-1 QCI4NU Rear Panel.

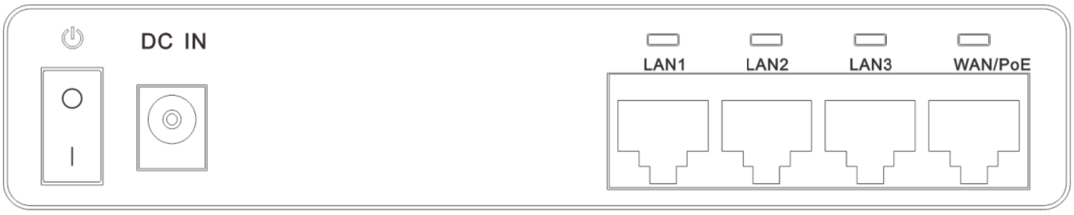


Figure 2-1

Figure 2-2 QCI4NU Front Panel.

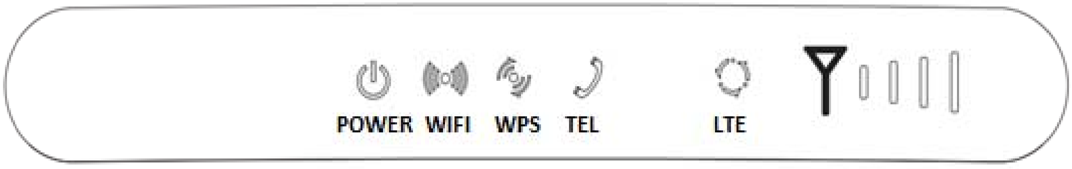
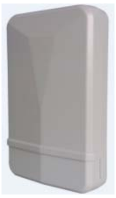


Figure 2-2

3 What You Need

Ensure that you have everything required to properly set up your device.

SQO14	QCI4NU	POWER SUPPLY	Ethernet CABLE
			

4 How It Works

Figure 4-1 LAN and WAN.

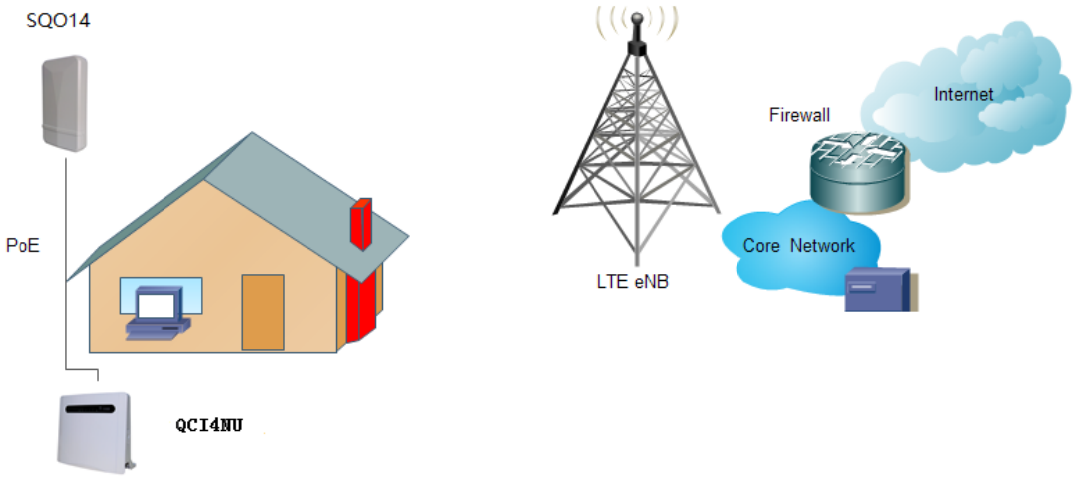


Figure 4-1

1. The SQO14 connects to the LTE network.
2. The SQO14 is connected to the QCI4NU.
3. The QCI4NU functions as a LAN & Wi-Fi access gateway.
4. The QCI4NUalso serves as telephone adapter.

This Quick Start Guide shows you how to set up your SQO14 and QCI4NUin order to access the Internet.

5 Set Up the Hardware

⚠ **CAUTION**

Before you begin, ensure that you are familiar with all safety and accident prevention procedures necessary for working at heights and with electricity.

Do NOT install the SQO14 during a lightning storm.

5.1 Choose a Location

The SQO14 can be mounted on a pole or antenna mast or on a wall using the supplied bracket mount.

- Choose a mounting point that is sturdy enough to hold the SQO14, even during high winds.
- When choosing a location to install the SQO14, remember that the SQO14's front panel should point towards your service provider's nearest base station. You do not need to be able to see the base station from the SQO14's position. However, if you experience difficulties with signal reception, a Line of Sight (LoS) connection may prSQO14ce better results.
- It is suggested that you transport the SQO14 to its intended installation location in its original protective packaging.

5.2 Insert a SIM Card to the Slot

CAUTION

Make sure the SQO14 is turned off before you insert your SIM card. It is recommended to NOT connect the PoE cable you do this step. Otherwise, the SIM card may be damaged.

Step 1 Remove the cover from the SQO14.

Figure 5-1 Remove the cover.

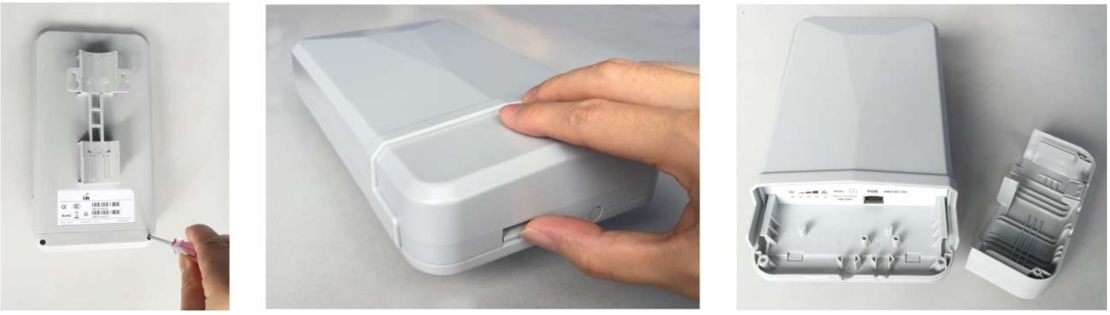


Figure 5-2

Step 2 Insert your SIM card.

Figure 5-2 Insert SIM Card.

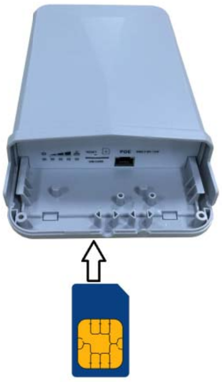
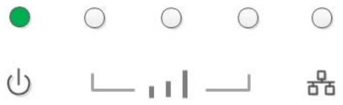
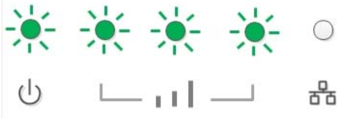
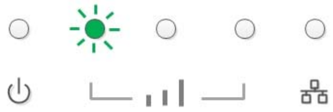
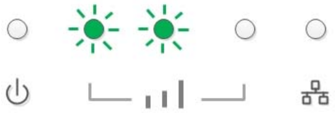
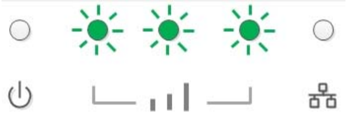
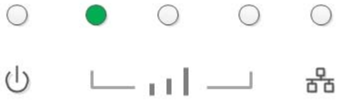
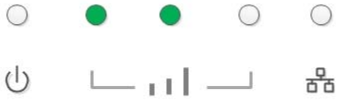
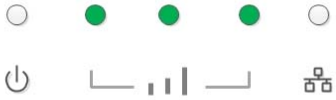
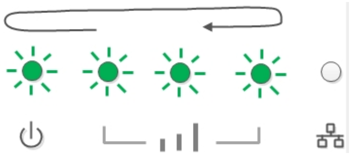
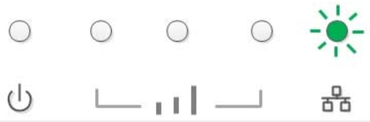


Figure 5-1

Step 3 Align and put the cover to protect it in the SQO14.

5.3 Outdoor (SQO14) LED Behavior

When set up the Outdoor Unit, the LED will have the following behavior.

CPE State	Description	LED Behavior	LED illustration
Power On	Power supply normal	Power LED on	
Detect with no SIM card	After CPE power on，detecting no SIM card	Power LET and three signal strength LEDs blinking together, the frequency is 2 times per second.	
Scanning the LTE network	Scanning the LTE network	The first signal strength LED blinking	
Network Authentication	CPE is authenticating	Two signal strength LEDs blinking	
Getting IP Address	CPE getting IP address from LTE network	Three signal strength LEDs blinking	
Signal Strength weak	Signal strength is weak	Only first signal strength LED on, the other two off	
Signal Strength good	Signal strength is good	Two signal strength LEDs on	
Signal Strength strong	Signal strength is strong	Three signal strength LEDs on	
Firmware Upgrading	CPE starting the firmware upgrading	The first four LEDs blinking alternately	
LAN connected	With local LAN connected	LAN LED indicator flashing	

5.4 Connect the SQO14 to the QCI4NU

Lay a CAT5e Ethernet cable (not included) from your intended QCI4NU location to our intended SQO14 location.

The maximum distance of the CAT5e cable is limited to 100 meters.

Signal attenuation may result if you use cable extenders to cover a greater distance.

If you intend to use cable ties or other methods to secure the cable, do not tighten them yet. Leave the cable loose until after you finish installing the QCI4NU and SQO14.

To connect the CAT5e Ethernet cable:

Step 1 Open the cover of SQO14 by take of the screws on the housing.

Step 2 Feed the end of the CAT5e Ethernet cable through the rubber, and connect the end of the cable to the SQO14.

Step 3 Put the cover on the SQO14 housing and twist the screw.

5.5 Connect the QCI4NU

Figure 5-3QCI4NU Hardware Connections.

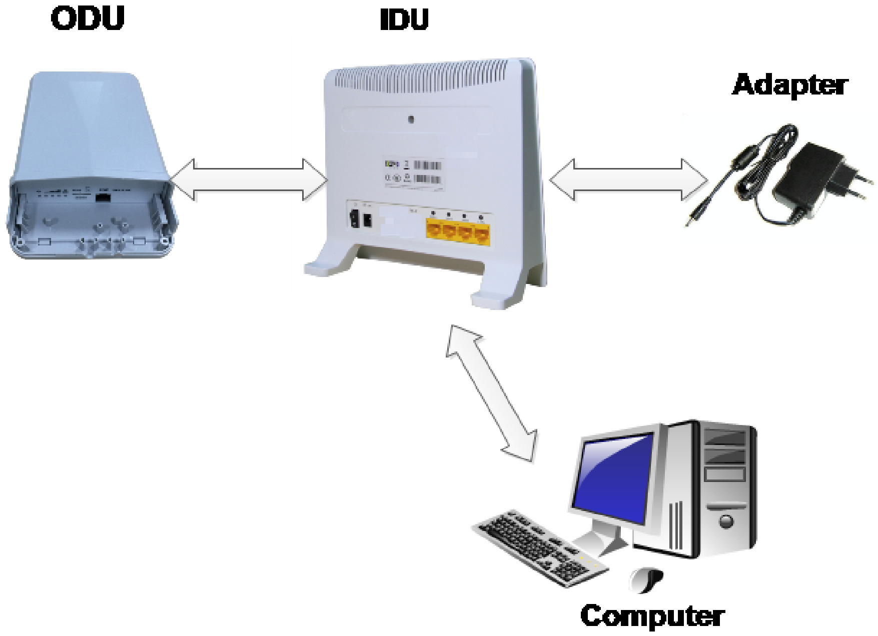


Figure 5-2

NOTE: Make sure you have inserted your SIM card into the SQO14.

Step 1 Connect the CAT5e Ethernet cable which is already connected to the SQO14 to the QCI4NU’s RJ-45 PoE port.

⚠ CAUTION

Do not connect a computer or a switch directly to the QCI4NU’s PoE port due to the high PoE power.

Step 2 Connect the supplied power adapter to the QCI4NU. The POWER LED shines a steady green once connected.

Step 3 Connect the included Ethernet cable from the computer to one of the QCI4NU’s ETHERNET ports.

Step 4 Connect an analog phone to the PHONE port to use VoIP. The PHONE LTE should light on.

5.6 Mount the SQO14

See the installation instructions to mount the SQO14 correctly.

5.6.1 Pole mounting

Pole diameter type： The mounting pole diameter is Φ25 and Φ45MM;

If the pole diameter is less thanΦ30, you need to add a C-type ring to make sure the device can be mounted on the pole.

The specific mounting steps are as follows:

1. Using a screwdriver to loosen the metal hose clamps，through the terminal equipment mounting hole, the metal hose clamps and the pole is fixed；

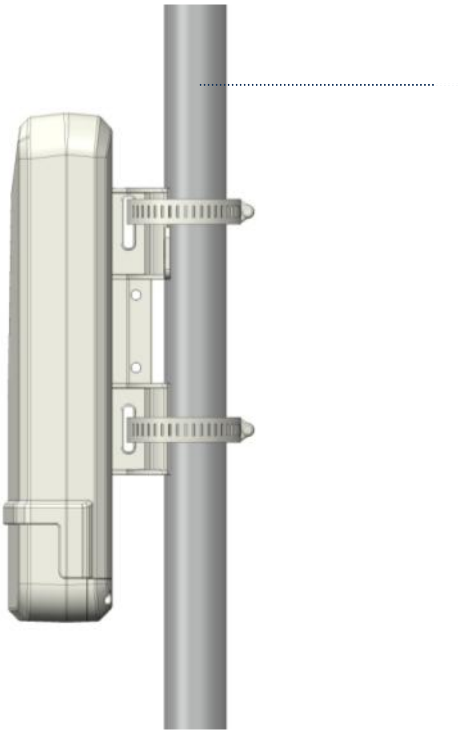


Figure 5-3 pole typemounting A

2. Using a screwdriver to lock the metal hose clamps, fixed terminal equipment.(Using software to enable terminal equipment aligned in the direction of the base station, achieve the best effect.)

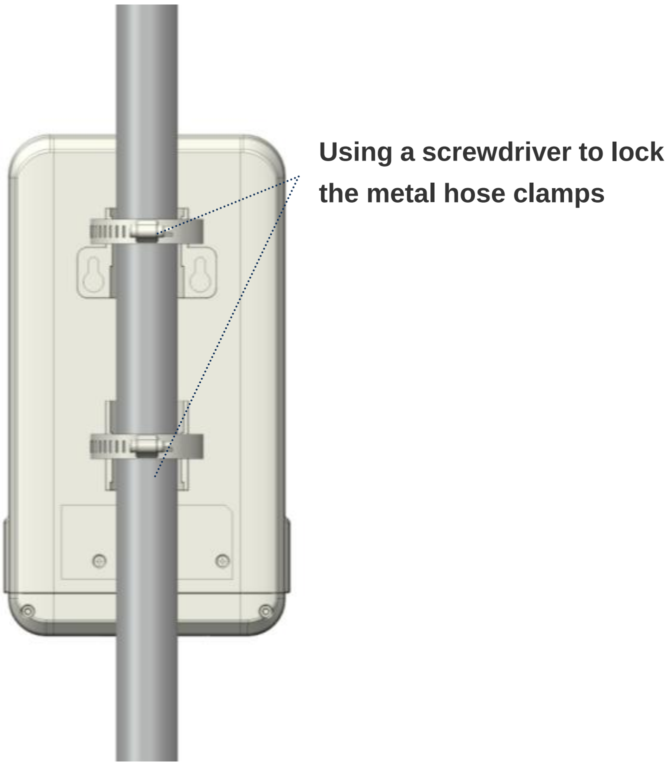


Figure 5-4 pole typemounting B

Note :(terminal equipment cable outlet must be installed downward direction.)

3. If the diameter of pole between 25mm and 30mm, it’s needed to use the rubber C-type ring to add the diameter of the pole.

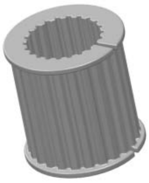


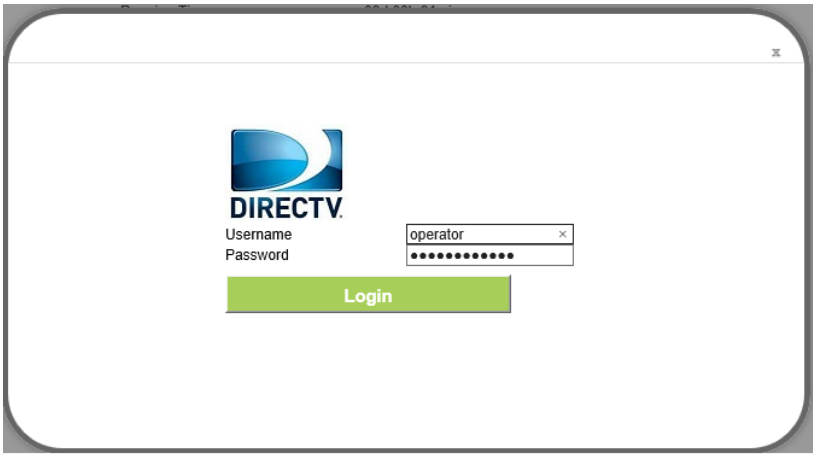
Figure 5-5C-type ring

6 Connect to the Internet

Step 1 Open a web browser and enter the URL http://192.168.100.1 of indoor unit

Step 2 Enter the default Username and Password. Click Login. (Fields are case-sensitive.)

Figure 6-1 Login Screen.



Username: operator

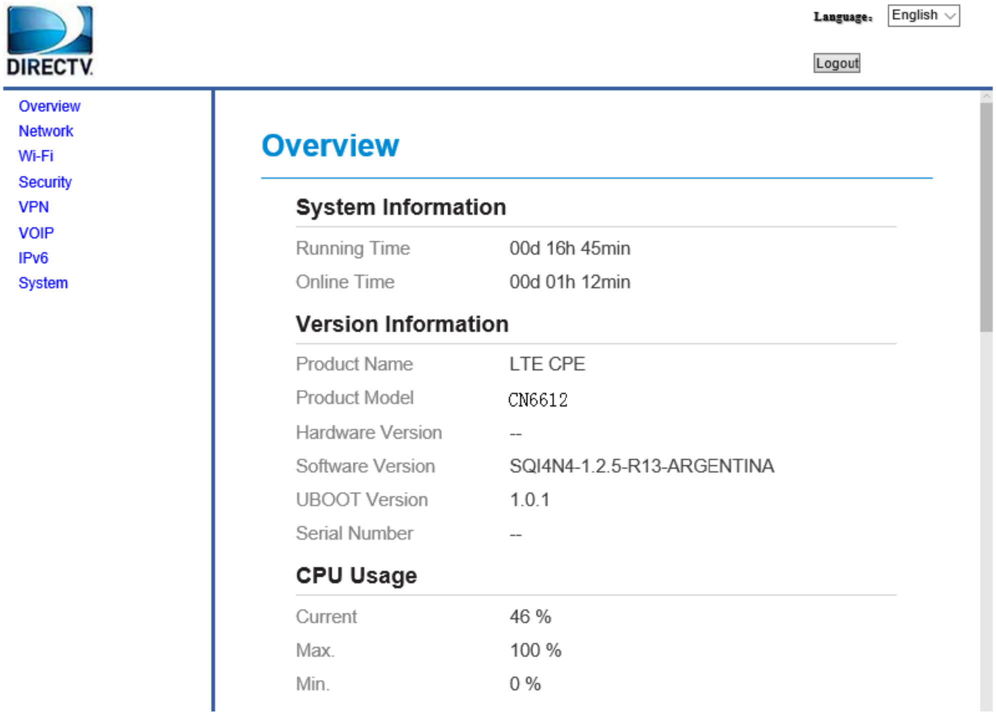
Password: •••••••••••••

Figure 6-1

NOTE

If the login screen does not open, make sure internet browser’s proxy settings disabled. Your computer should also be set to get an IP address automatically from the LTE Router DHCP Server, 192.168.100.100 to 254.

Figure 6-2 Main Screen



Overview

System Information

Running Time	00d 16h 45min
Online Time	00d 01h 12min

Version Information

Product Name	LTE CPE
Product Model	CN6612
Hardware Version	--
Software Version	SQI4N4-1.2.5-R13-ARGENTINA
UBOOT Version	1.0.1
Serial Number	--

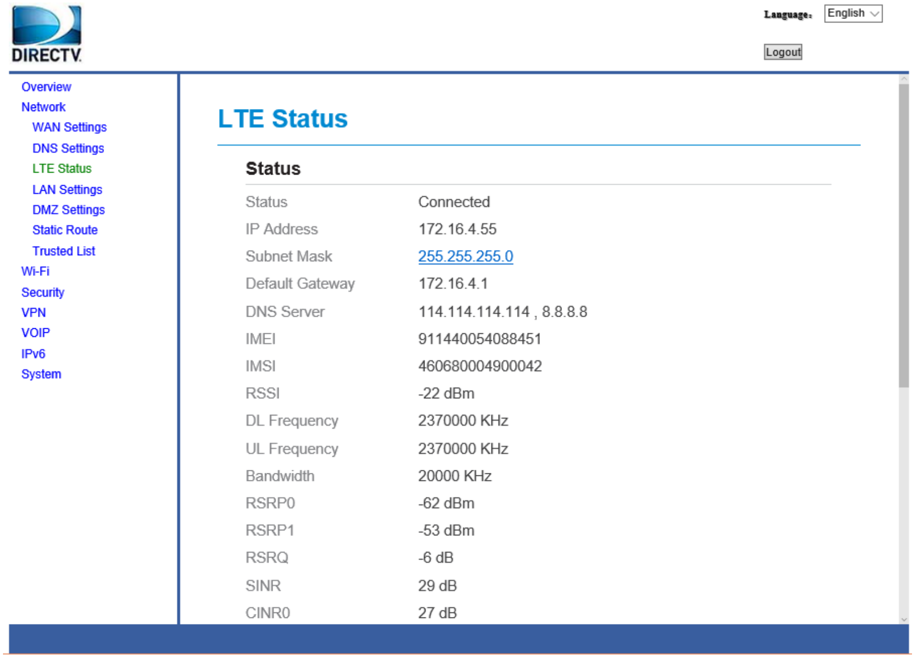
CPU Usage

Current	46 %
Max.	100 %
Min.	0 %

Figure 6-2

If the LTE Signal Bar & Internet Icons located above of the page are grayed out, it means that it cannot acquire LTE Signal. To check signal, go to Network Menu

Figure 6-3 Network



LTE Status

Status

Status	Connected
IP Address	172.16.4.55
Subnet Mask	255.255.255.0
Default Gateway	172.16.4.1
DNS Server	114.114.114.114 , 8.8.8.8
IMEI	911440054088451
IMSI	460680004900042
RSSI	-22 dBm
DL Frequency	2370000 KHz
UL Frequency	2370000 KHz
Bandwidth	20000 KHz
RSRP0	-62 dBm
RSRP1	-53 dBm
RSRQ	-6 dB
SINR	29 dB
CINR0	27 dB

Figure 6-3

If the SINR is below 10db, replanning or repositioning of the outdoor (SQO14) antenna is required.

Note: SINR threshold parameters is ≥10 db

7 Wireless

7.1 Turn the Wireless On or off

Step 1 The WIFI is set to default as ON.
Step 2 You can also press the WIRELESS On/Off button for one second and release it.

8 Troubleshooting

Use this section if you have problems with your LTE Device.

8.1 Power LED

Figure 9-1 Power LED Symbol

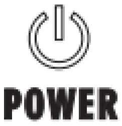


Figure 8-1

Table 9-1 Power LED Definition

LED	COLOR	STATUS	DESCRIPTION
PWR	Blue	OFF	No Power Supply
		Steady On	Power on

If the power LED is off, please check.

Step 1 Power adapter MUST be plugged into device.

Step 2 If the problem still persists, device hardware component or power adapter may be defective, please contact your local vendor.

8.2 RESET Button

Figure 9-2 RESET Button

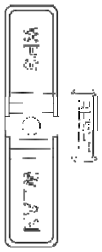


Figure 8-2

To reset the device to default, press the RESET button until the power LED begins to blink. Then check the other LEDs.

Based on the following definitions of the other LEDs, it can diagnose if there’s any hardware defect.

8.3 LTE LED

Figure 9-3 LTE LED Symbol

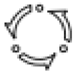


Figure 8-3

Table 9-2 LTE LED Definition

LED	COLOR	STATUS	DESCRIPTION
LTE	Blue	Steady On	In LTE network
		Blinking	LTE scan, connect, complete LTE connectivity
		OFF	No access in LTE network

If the LTE LED is off or blinking continuously, please check:

Step 1 PoE cable MUST be connected between QCI4NU and SQO14 device.

Step 2 Re-power on the QCI4NU device.

Step 3 Wait until the LED indicator steadies.

Step 4 If the problem still persists, device hardware component may be defective, please contact our technical support.

8.4 Wi-Fi LED

Figure 9-4 WIFI LED Symbol

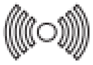


Figure 8-4

Table 9-3 WLAN LED Definition

LED	COLOR	STATUS	DESCRIPTION
WIFI	Blue	OFF	WLAN function disable
		Blinking	Data transmission through WLAN
		Steady On	WLAN function enable

If the WIFI LED is off, please check:

WIFI: Enable wireless function and all configuration parameters MUST be correct. See the WIFI configuration for more information.

8.5 ETHERNET 1-4 LEDs

Figure 9-6 ETHERNET 1~3 LEDs Symbol

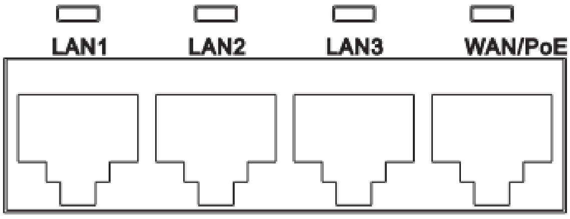


Figure 8-5

Table 9-5 ETHERNET 1-3 LEDs Definition

LED	COLOR	STATUS	DESCRIPTION
LAN1~LAN3	Green	Steady On	Ethernet connection is normal
		Blinking	Ethernet interface data being transmitted
		OFF	Ethernet connection is not established
WAN/POE	Green	Steady On	WAN connection is normal
		Blinking	WAN interface data being transmitted
		OFF	WAN connection is not established

If the LED is off , please check:

Step 1 The LAN cable MUST be connected between device and PC.

Step 2 NIC function on the PC MUST be enabled.

Step 3 If the problem still persists, device hardware component may be defective, please contact your local vendor.

LTE Outdoor CPE

User Guide

Index

1 Getting Started

1.1Welcome to the CPE

In this document, the LTE (Long Term Evolution) CPE (customer premises equipment) will be replaced by the CPE. Carefully read the following safety symbols to help you use your CPE safely and correctly:

💬	Additional information
☀	Optional methods or shortcuts for an action
⚠	Potential problems or conventions that need to be specified

1.2Computer Configuration Requirements

For optimum performance, make sure your computer meets the following requirements.

Item	Requirement
CPU	Pentium 500 MHz or higher
Memory	128 MB RAM or higher
Hard disk	50 MB available space
Operating system	• Microsoft: Windows XP, Windows Vista, or Windows 7 • Mac: Mac OS X 10.5 or higher
Display resolution	1024 x 768 pixels or higher
Browser	• Internet Explorer 7.0 or later • Firefox 3.6 or later • Opera 10 or later • Safari 5 or later • Chrome 9 or later

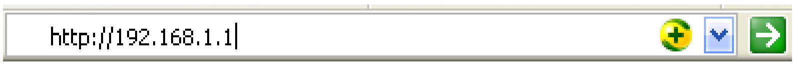
1.3Logging In to the Web Management Page

Use a browser to log in to the web management page to configure and manage the CPE.

The following procedure describes how to use a computer running Windows XP and Internet Explorer 7.0 to log in to the web management page of the CPE.

1. Connect the CPE properly.

2. Launch Internet Explorer, enter **http://192.168.1.1** in the address bar, and press **Enter**. As shown in Figure 1-1.

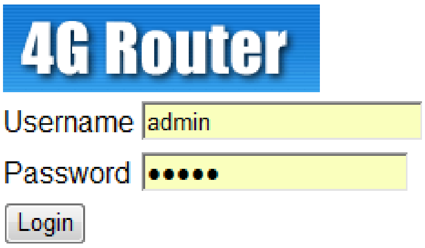


http://192.168.1.1

Figure 1-1

3. Enter the user name and password, and click **Log In**.

You can log in to the web management page after the password is verified. As shown in Figure 1-2.



4G Router

Username admin

Password ●●●●●

Figure 1-2

The default user name and password are both **admin**. If you want to check the details of the CPE, please use the super user login the CPE, the username and password both are **administrator.**

To protect your CPE from unauthorized access, change the password after your first login.

The CPE supports diagnostic function. If you encounter problems, please contact customer service for the specific using method.

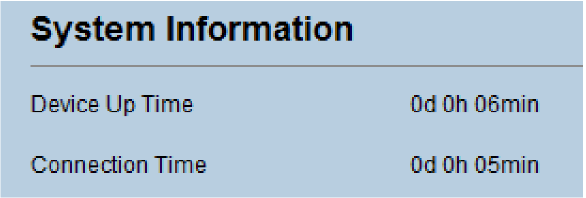
To ensure your data safety, it is recommended that you turn on the firewall, and conserve your login and FTP password carefully.

2 Overview

2.1Viewing the System Information

To view the System Information, perform the following steps:

1. Choose **Overview**;
2. In the **System Information** area, view the system status, such as Running time and Online time. As shown in Figure 2-1.



System Information

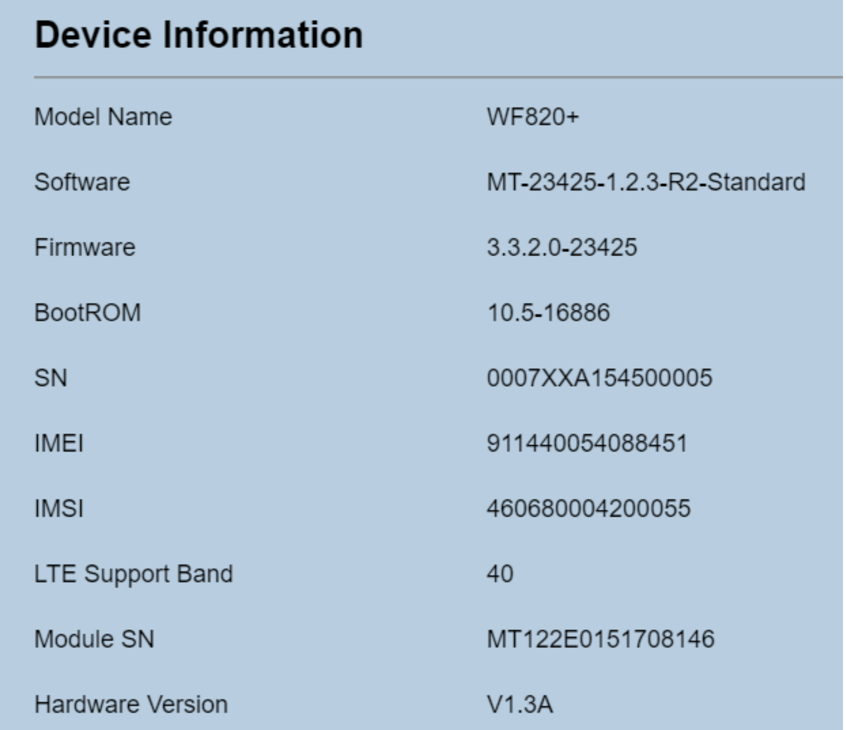
Device Up Time	0d 0h 06min
Connection Time	0d 0h 05min

Figure 2-1

2.2Viewing the Device Information

To view the Device Information, perform the following steps:

1. Choose **Overview**;
2. In the **Device Information** area, view the device information, such as Product name, Software version, Firmware version, Bootrom version, CPE SN, IMEI, IMSI,LTE support band and Module SN . As shown in Figure 2-2.



Device Information

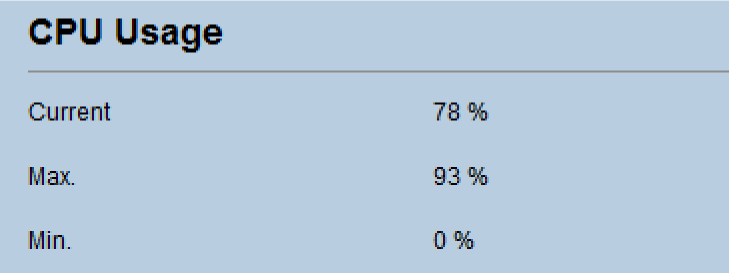
Model Name	WF820+
Software	MT-23425-1.2.3-R2-Standard
Firmware	3.3.2.0-23425
BootROM	10.5-16886
SN	0007XXA154500005
IMEI	911440054088451
IMSI	460680004200055
LTE Support Band	40
Module SN	MT122E0151708146
Hardware Version	V1.3A

Figure 2-2

2.3Viewing CPU Usage

To view the Device Information, perform the following steps:

1. Choose **Overview**;
2. In the **CPU Usage** area, view the cpu usage information, such as Current cpu usage, Max cpu usage, Min cpu usage. As shown in Figure 2-3.



CPU Usage

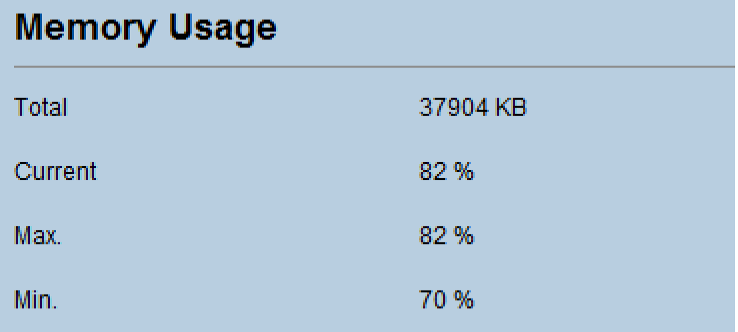
Current	78 %
Max.	93 %
Min.	0 %

Figure 2-3

2.4Viewing Memory Usage

To view the Device Information, perform the following steps:

1. Choose **Overview**;
2. In the **Memory Usage** area, view the memory usage information, such as Total memory, Current memory usage, Max memory usage and Min memory usage. As shown in Figure 2-4.



Memory Usage

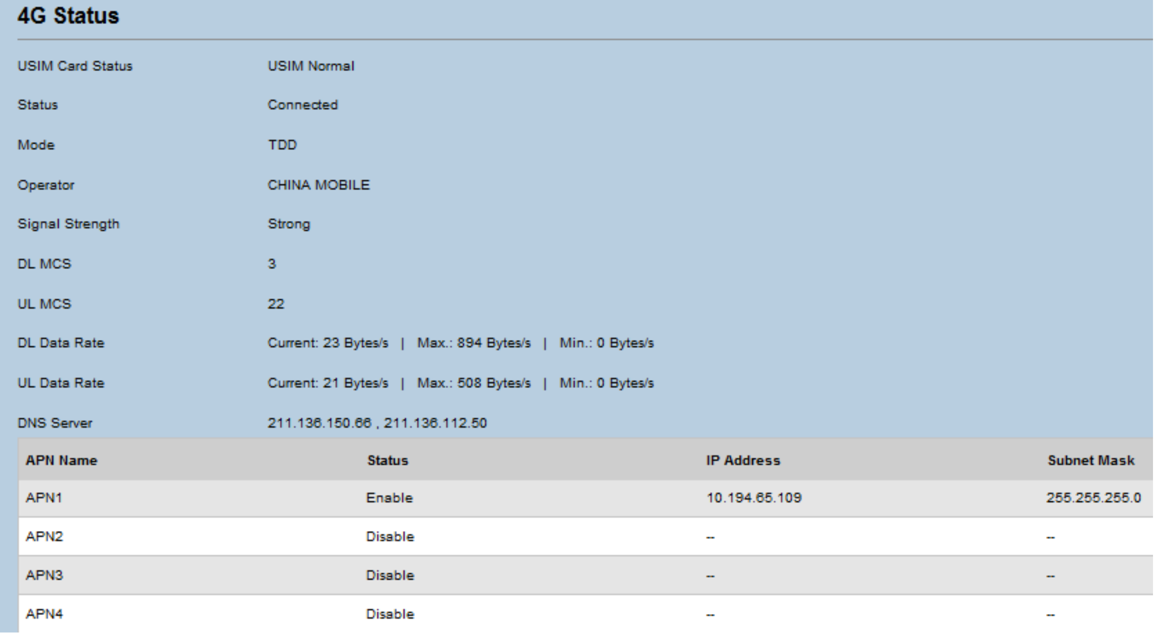
Total	37904 KB
Current	82 %
Max.	82 %
Min.	70 %

Figure 2-4

2.5Viewing 4G Status

To view the Device Information, perform the following steps:

1. Choose **Overview**;
2. In the **4G Status** area, view the information about lte network, such as USIM card status, Connect Status, Network mode, Operator information, Signal Strength indicator, DL&UL MCS, DNS Server and APN information. As shown in Figure 2-5.



4G Status

USIM Card Status	USIM Normal
Status	Connected
Mode	TDD
Operator	CHINA MOBILE
Signal Strength	Strong
DL MCS	3
UL MCS	22
DL Data Rate	Current: 23 Bytes/s | Max.: 894 Bytes/s | Min.: 0 Bytes/s
UL Data Rate	Current: 21 Bytes/s | Max.: 508 Bytes/s | Min.: 0 Bytes/s
DNS Server	211.136.150.66 , 211.136.112.50

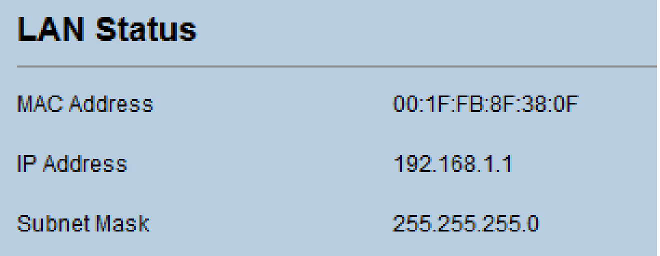
APN Name	Status	IP Address	Subnet Mask
APN1	Enable	10.194.65.109	255.255.255.0
APN2	Disable	--	--
APN3	Disable	--	--
APN4	Disable	--	--

Figure 2-5

2.6Viewing LAN Status

To view the Device Information, perform the following steps:

1. Choose **Overview**;
2. In the **LAN Status** area, view the lan status, such as Mac address, IP address and Subnet mask. As shown in Figure 2-6.



LAN Status

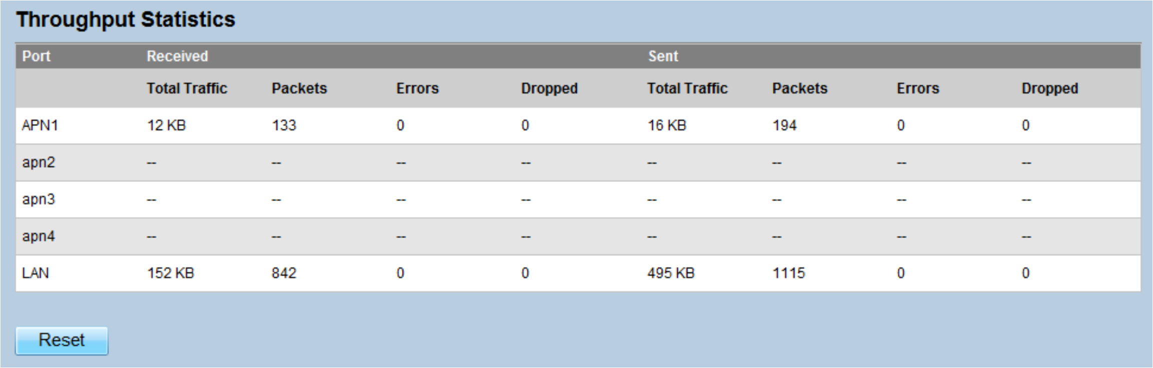
MAC Address	00:1F:FB:8F:38:0F
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

Figure 2-6

2.7Viewing Throughput Statistics

To view the Device Information, perform the following steps:

1. Choose **Overview**;
2. In the **Throughput Statistics** area, view the throughput statistics, such as APN throughput and LAN throughput.
3. In this area, also you can choose and click the button **Reset** to empty the throughput statistics. As shown in Figure 2-7.



Throughput Statistics

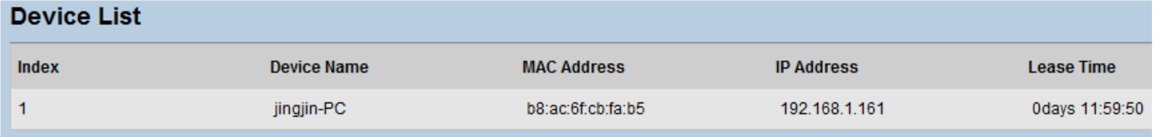
Port	Received				Sent			
	Total Traffic	Packets	Errors	Dropped	Total Traffic	Packets	Errors	Dropped
APN1	12 KB	133	0	0	16 KB	194	0	0
apn2	--	--	--	--	--	--	--	--
apn3	--	--	--	--	--	--	--	--
apn4	--	--	--	--	--	--	--	--
LAN	152 KB	842	0	0	495 KB	1115	0	0

Figure 2-7

2.8Viewing Device List

To view the Device Information, perform the following steps:

1. Choose **Overview**;
2. In the **Device List** area, view the device information which connect to the CPE, such as Device name, Mac address, IP address and Lease time. As shown in Figure 2-8.



Device List

Index	Device Name	MAC Address	IP Address	Lease Time
1	jingjin-PC	b8:ac:6f:cb:fa:b5	192.168.1.161	0days 11:59:50

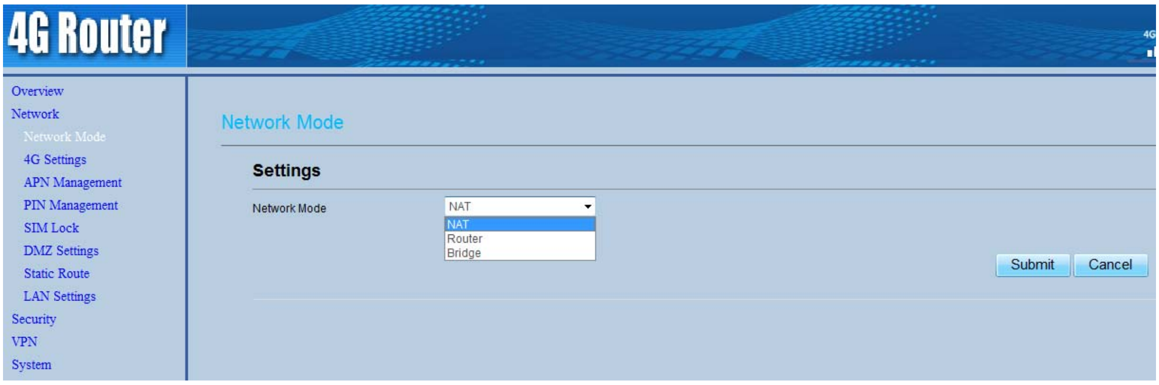
Figure 2-8

3 Network Setting

3.1Network Mode

To set the network mode, perform the following steps:

1. Choose **Network** >**Network Mode**;
2. In the **Network Mode** area, select a mode between **Route** and **Bridge**;
3. Click **Submit**. As shown in Figure 3-1.



Network Mode

Settings

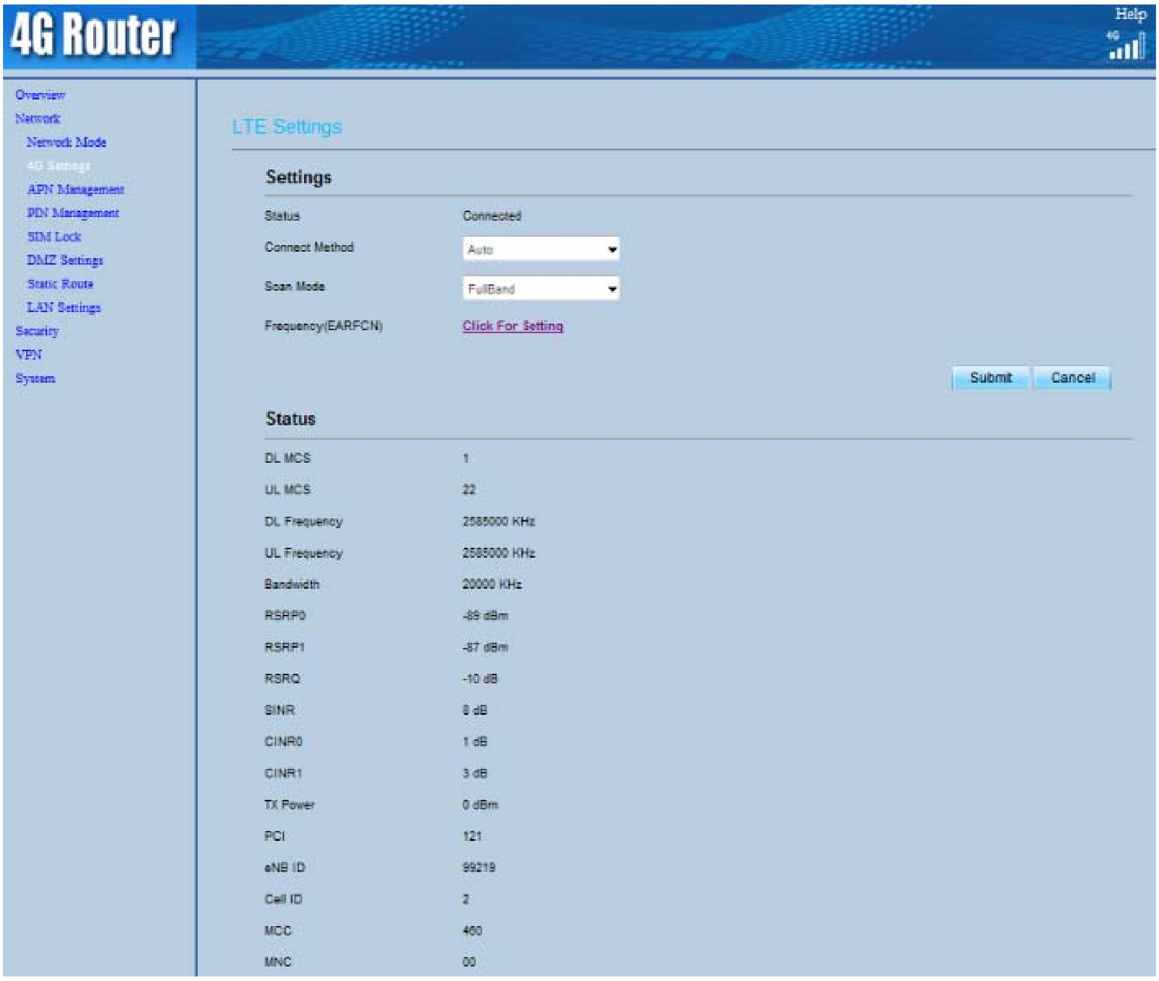
Network Mode: NAT

Figure 3-1

3.24G Setting

To set the LTE Network, perform the following steps:

1. Choose **Network** >**4G Setting**;
2. In the **4G Setting** area, you can configure the lte network
3. In the **4G Setting** area, you can also view the network information such as frequency, DL&UL MCS, RSRP, RSRQ, CINR, SINR, TxPower, Cell ID, PCI, MCC and MNC. As shown in Figure 3-2.



LTE Settings

Settings

Status	Connected
Connect Method	Auto
Scan Mode	FullBand
Frequency(EARFCN)	Click For Setting

Status

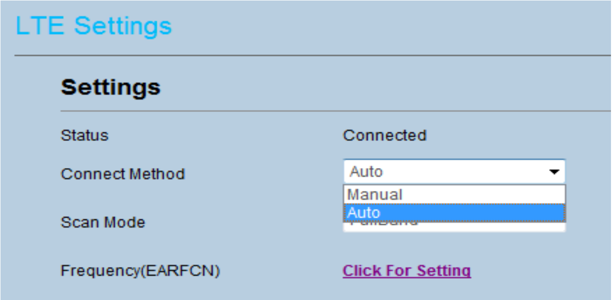
DL MCS	1
UL MCS	22
DL Frequency	2585000 KHz
UL Frequency	2585000 KHz
Bandwidth	20000 KHz
RSRP0	-89 dBm
RSRP1	-87 dBm
RSRQ	-10 dB
SINR	8 dB
CINR0	1 dB
CINR1	3 dB
TX Power	0 dBm
PCI	121
eNB ID	99219
Cell ID	2
MCC	460
MNC	00

Figure 3-2

3.2.1 Setting Connect Method

To set the lte network connect method, perform the following steps:

1. Choose **Network** >**4G Setting**;
2. In the **4G Setting area**, you can set the **connect method**;
3. There are two methods to connect the lte network , it is needed to choose a method between **Auto** and **Manual**, if you want to auto connect to the lte network you should choose the **Auto**, otherwise you should choose **Manual**;
4. Click **Submit**. As shown in Figure 3-3.



LTE Settings

Settings

Status	Connected
Connect Method	Auto
Scan Mode	
Frequency(EARFCN)	Click For Setting

Figure 3-3

3.2.1.1 Manual Connect Network

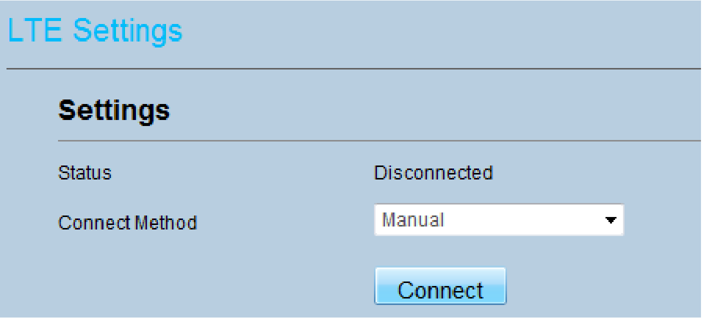
To manual connect the network, perform the following steps:

1 Choose **Network** >**4G Setting**;

2 Set the **Connect Method** to **Manual**;

3 Click **PLMN** to scan the network and select a network you want to connect. If you don't want to use this function, it will auto select a network to connect.

4 If you want to connect to the LTE network, you should click **connect** button to connect the network, otherwise you can click the button **Disconnect** to disconnect from lte network. As shown in Figure 3-4.



LTE Settings

Settings

Status Disconnected

Connect Method Manual ▾

Connect

Figure 3-4

3.2.1.2 Setting Scan Mode

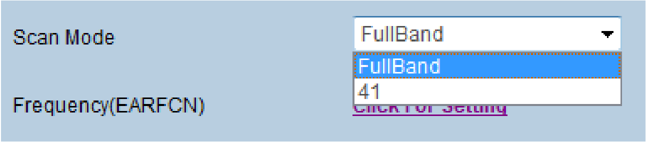
To set the lte network scan mode, perform the following steps:

1 choose **Network>4G Setting**;

2 In the **lte setting** area, you can set the **scan mode**;

3 You can choose **full mode** or a band the CPE supported.

4 Click **Submit**. As shown in Figure 3-5.



Scan Mode FullBand ▾

FullBand

41

Frequency(EARFCN) Click For Setting

Figure 3-5

3.2.2 Setting Frequency (Earfcn)

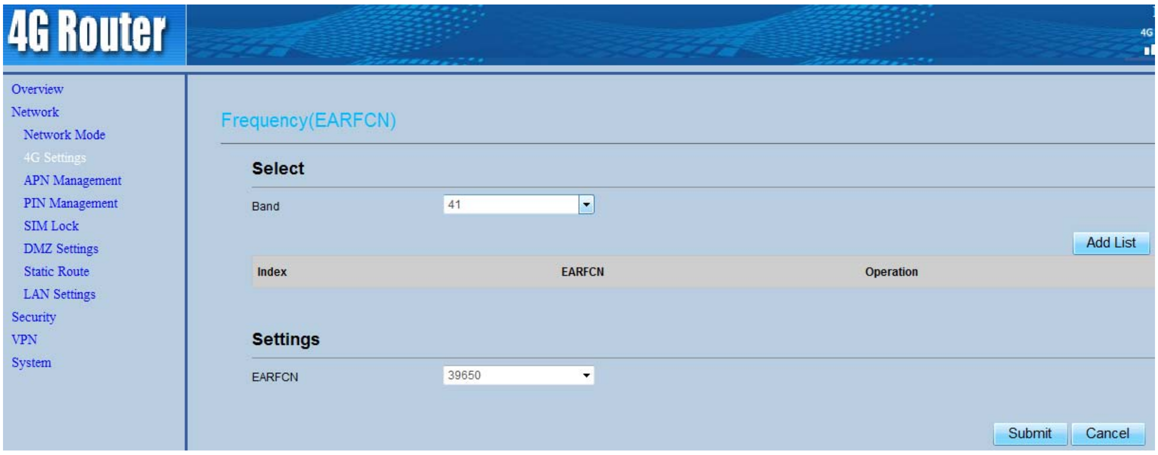
To set the frequency, perform the following steps:

1 Choose **Network** >**4G Setting**.

2 In the **lte setting** area, click to set the **frequency**.

3 In the **Frequency Setting** area, you can choose a band, then click **Add list** to choose a **Earfcn Number**.

4 Click **Submit**. As shown in Figure 3-6.



Frequency(EARFCN)

Select

Band: 41

Index	EARFCN	Operation

Settings

EARFCN: 39650

Figure 3-6

3.3APN Management

To set and manage APN, perform the following steps:

1 Choose **Network**>**APN Management**.

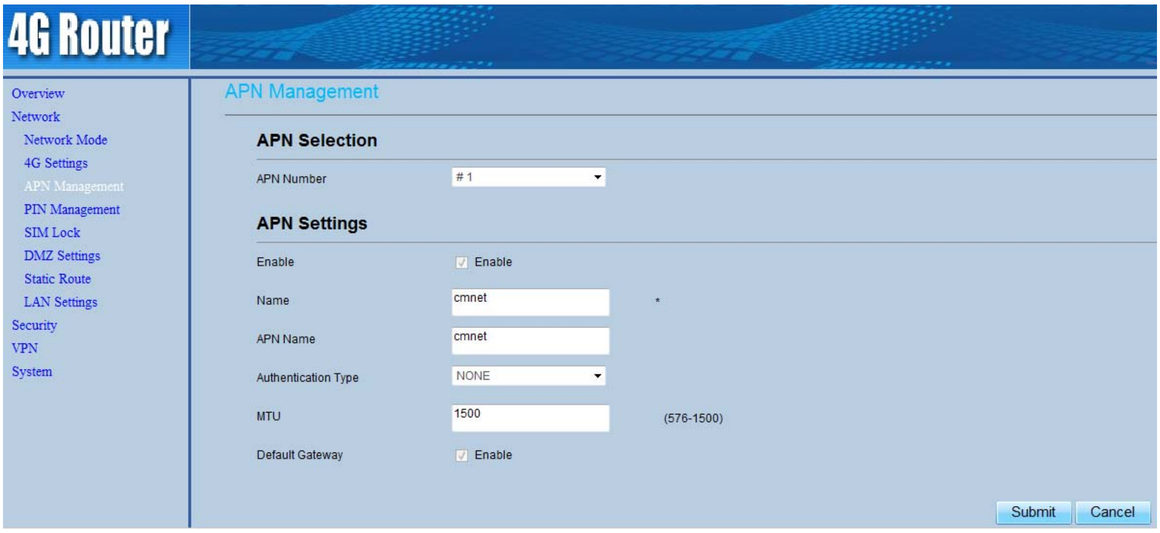
2 In the **APN Management** area, you can set the APN.

3 Choose a **APN number** which you want to set.

4 In the **APN Setting** area you can set the APN parameters, such as enable or disable the apn, apn name, username, password and so on.

5 If you want set a APN as **default gateway**, you should check that is enabled.

6 Click **Submit.** As shown in Figure 3-7.



APN Management

APN Selection

APN Number: # 1

APN Settings

Enable: ☑ Enable

Name: cmnet *

APN Name: cmnet

Authentication Type: NONE

MTU: 1500 (576-1500)

Default Gateway: ☑ Enable

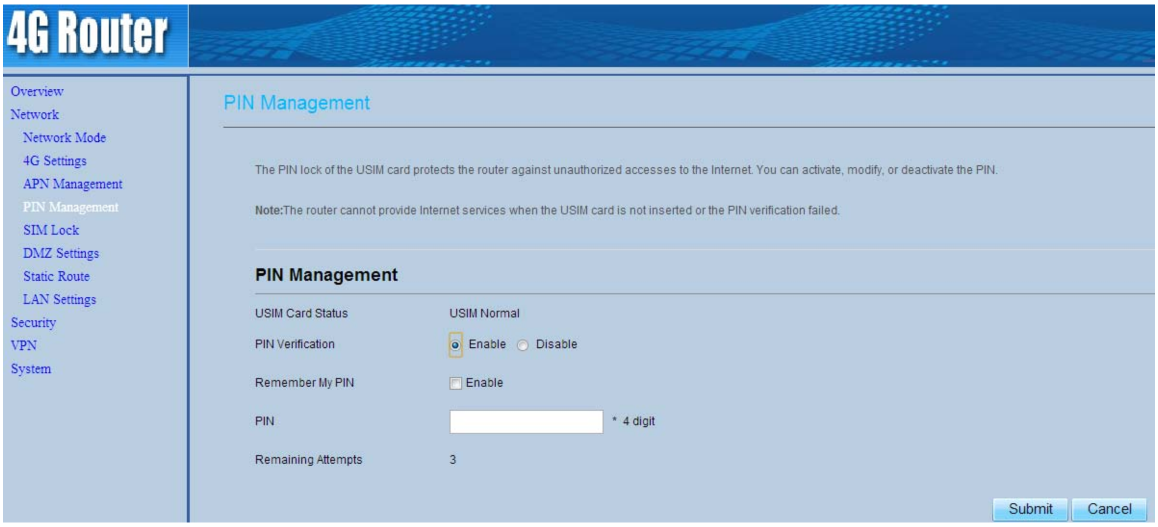
Figure 3-7

3.4PIN Management

To manage the PIN, you can perform the following operations on the PIN Management page:

- Enable or disable the PIN verification.
- Verify the PIN.

- Change the PIN.
- Set automatic verification of the PIN. As shown in Figure 3-8.



PIN Management

The PIN lock of the USIM card protects the router against unauthorized accesses to the Internet. You can activate, modify, or deactivate the PIN.

Note: The router cannot provide Internet services when the USIM card is not inserted or the PIN verification failed.

PIN Management

USIM Card Status	USIM Normal
PIN Verification	● Enable ○ Disable
Remember My PIN	□ Enable
PIN	* 4 digit
Remaining Attempts	3

Figure 3-8

3.4.1 Viewing the Status of the USIM Card

To view the status of the USIM card, perform the following steps:

1 Choose **Network** >**PIN Management**.

2 View the status of the USIM card in the **USIM card status** field.

3.4.2 Enabling PIN Verification

To enable PIN verification, perform the following steps:

1 Choose **Network** >**PIN Management**.

2 Set **PIN verification** to **Enable**.

3 Enter the PIN (4 to 8 digits) in the **Enter PIN** box.

4 Click **Submit**.

3.4.3 Disabling PIN Verification

To disable PIN verification, perform the following steps:

1 Choose **Network** >**PIN Management**.

2 Set **PIN verification** to **Disable**.

3 Enter the PIN (4 to 8 digits) in the **Enter PIN** box.

4 Click **Submit**.

3.4.4 Verifying the PIN

If PIN verification is enabled but the PIN is not verified, the verification is required. To verify the

PIN, perform the following steps:

1 Choose **Network** >**PIN Management**.
2 Enter the PIN (4 to 8 digits) in the **PIN** box.
3 Click **Submit**.

3.4.5 Changing the PIN

The PIN can be changed only when PIN verification is enabled and the PIN is verified.
To change the PIN, perform the following steps:

1 Choose **Network**>**PIN Management**.
2 Set PIN verification to **Enable**.
3 Set **Change PIN** to **Enable**.
4 Enter the current PIN (4 to 8 digits) in the **PIN** box.
5 Enter a new PIN (4 to 8 digits) in the **New PIN** box.
6 Repeat the new PIN in the **Confirm PIN** box.
7 Click **Submit**.

3.4.6 Setting Automatic Verification of the PIN

You can enable or disable automatic verification of the PIN. If automatic verification is enabled, the CPE automatically verifies the PIN after restarting. This function can be enabled only when PIN verification is enabled and the PIN is verified.

To enable automatic verification of the PIN, perform the following steps:

1. Choose **Network** > **PIN Management**.
2. Set **Pin verification** to **Enable**.
3. Set **Remember my PIN** to **Enable**.
4. Click **Submit**.

3.4.7 Verifying the PUK

If PIN verification is enabled and the PIN fails to be verified for three consecutive times, the PIN will be locked. In this case, you need to verify the PUK and change the PIN to unlock it.

To verify the PUK, perform the following steps:

1. Choose **Network**> **PIN Management**.
2. Enter the PUK in the **PUK** box.
3. Enter a new PIN in the **New PIN** box.
4. Repeat the new PIN in the **Confirm PIN** box.

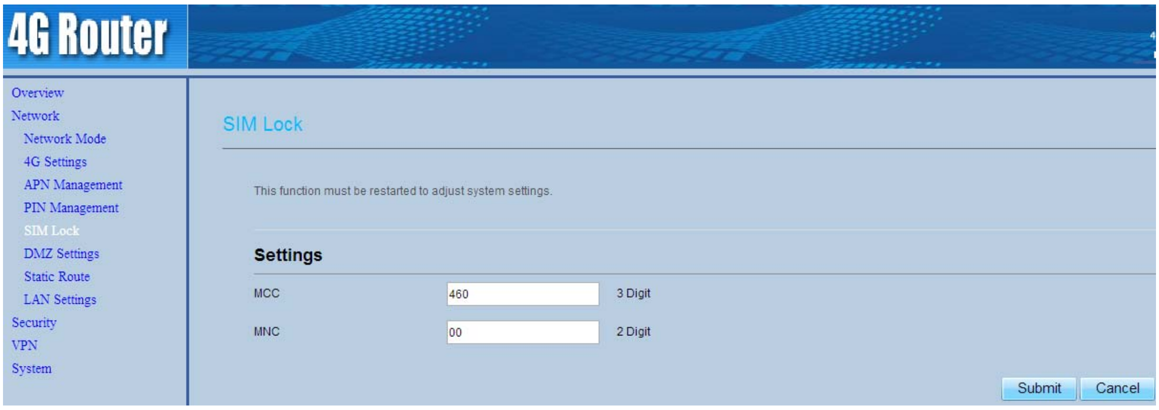
5. Click **Submit**.

3.5SIM Lock

If you want to connect a specify network, and the CPE can’t connect other network, you can set a SIM lock.

To set the SIM lock, perform the following steps:

1. Choose **Network**>**SIM Lock.**
2. Enter the MCC (3 digits) in the **MCC** box.
3. Enter the MNC (2 digits) in the **MNC** box.
4. Click **Submit**. As shown in Figure 3-9.



SIM Lock

This function must be restarted to adjust system settings.

Settings

MCC 460 3 Digit

MNC 00 2 Digit

Figure 3-9

3.6DMZ Settings

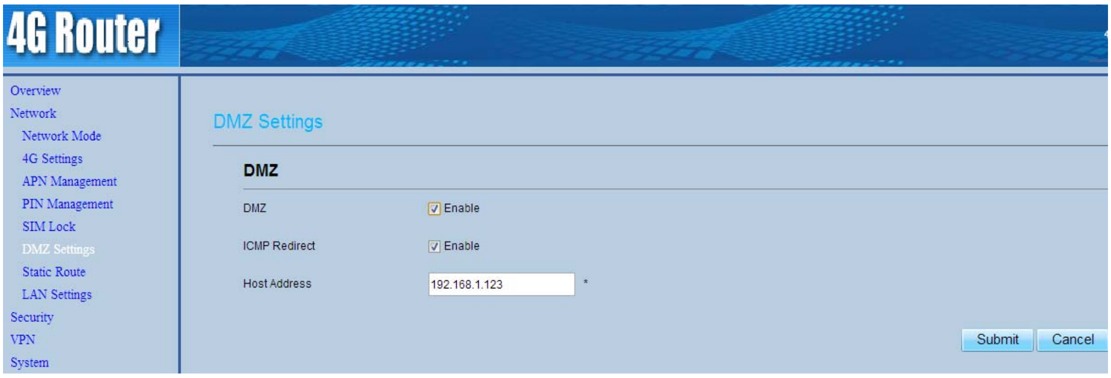
If the demilitarized zone (DMZ) is enabled, the packets sent from the WAN are directly sent to a specified IP address on the LAN before being discarded by the firewall.

To set DMZ, perform the following steps:

1. Choose **Network** > **DMZ Settings**.
2. Set **DMZ** to **Enable**.
3. (Optional) Set **ICMP Redirect** to Enable.
4. Set **Host address**.

This IP address must be different from the IP address set on the **LAN Host Settings** page, but they must be on the same network segment.

5. Click **Submit**. As shown in Figure 3-10.



DMZ Settings

DMZ

DMZ ☑ Enable

ICMP Redirect ☑ Enable

Host Address 192.168.1.123 *

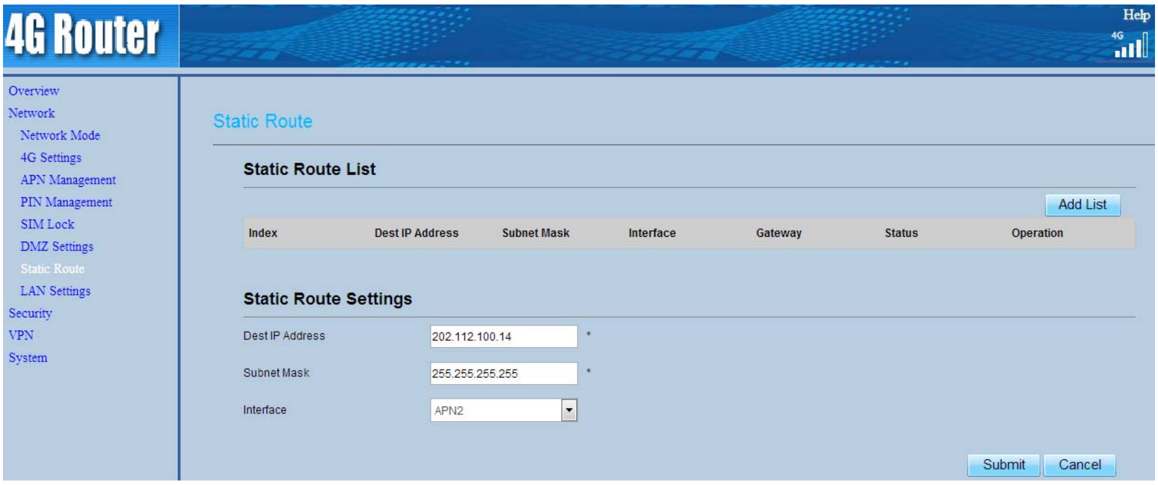
Figure 3-10

3.7Static Route

3.7.1 Add Static Route

To add a static route, perform the following steps:

1. Choose **Network**>**Static Route**.
2. Click **Add list**.
3. Set the **Dest IP address** and **Subnet mask**.
4. Select a **Interface** from the drop-down list.
5. If you select **LAN** as the interface, you need set a LAN IP addess.
6. Click **Submit.** As shown in Figure 3-11.



Static Route

Static Route List

Index	Dest IP Address	Subnet Mask	Interface	Gateway	Status	Operation

Static Route Settings

Dest IP Address 202.112.100.14 *

Subnet Mask 255.255.255.255 *

Interface APN2

Figure 3-11

3.7.2 Modify Static Route

To modify a access restriction rule, perform the following steps:

1. Choose **Network**>**Static Route**.
2. Choose the item to be modified, and click **Edit**.
3. Repeat steps 3 through 5 in the previous procedure.

4. Click **Submit**.

3.7.3 Delete Static Route

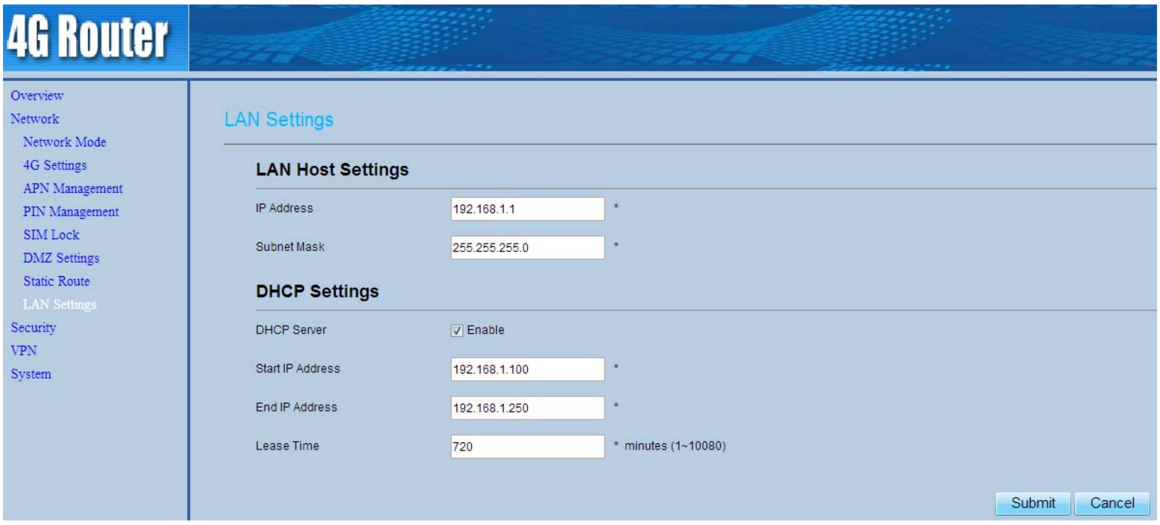
To delete a static route, perform the following steps:

1. Choose **Netwok**>**Static Route**.
2. Choose the item to be deleted, and click **Delete**.

3.8LAN Setting

3.8.1 Setting LAN Host Parameters

By default, the IP address is 192.168.1.1 with a subnet mask of 255.255.255.0. You can change the host IP address to another individual IP address that is easy to remember. Make sure that IP address is unique on your network. If you change the IP address of the CPE, you need to access the web management page with the new IP address. As shown in Figure 3-12.



LAN Settings

LAN Host Settings

IP Address 192.168.1.1 *

Subnet Mask 255.255.255.0 *

DHCP Settings

DHCP Server ☑ Enable

Start IP Address 192.168.1.100 *

End IP Address 192.168.1.250 *

Lease Time 720 * minutes (1~10080)

Figure 3-12

To change the IP address of the CPE, perform the following steps:

1 Choose **Network**>**LAN Setting**.

2 In the **LAN Host Settings** area, set IP address and subnet mask.

3 In the **DHCP Setting** area, set the DHCP server to **Enable**.

4 Click **Submit**.

3.8.2 Configuration the DHCP Server

DHCP enables individual clients to automatically obtain TCP/IP configuration when the server powers on.You can configure the CPE as a DHCP server or disable it.When configured as a DHCP server, the CPE automatically provides the TCP/IP configuration for the LAN clients that support

DHCP client capabilities. If DHCP server services are disabled, you must have another DHCP server on your LAN, or each client must be manually configured.

To configure DHCP settings, perform the following steps:

1. Choose **Network**> **LAN Setting**.

2. Set the **DHCP server** to **Enable**.

3. Set **Start IP address**.

   This IP address must be different from the IP address set on the **LAN Host Settings** area, but they must be on the same network segment.

4. Set **End IP address**.

   This IP address must be different from the IP address set on the **LAN Host Settings** area, but they must be on the same network segment.

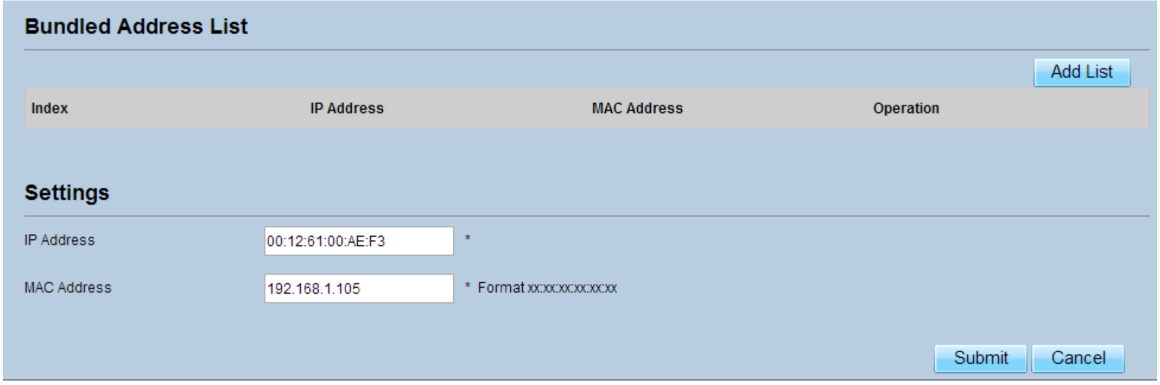
5. Set **Lease time**.

   Lease time can be set to 1 to 10,080 minutes. It is recommended to retain the default value.

6. Click **Submit**.

3.8.3 Bundled Address List

You can bind an IP address to a device based on its MAC address. The device will receive the same IP address each time it accesses the DHCP server. For example, you can bind an IP address to an FTP server on the LAN. As shown in Figure 3-13.



Bundled Address List

Index	IP Address	MAC Address	Operation

Settings

IP Address: 00:12:61:00:AE:F3 *

MAC Address: 192.168.1.105 * Format xx:xx:xx:xx:xx:xx

Figure 3-13

To add an item to the setup list, perform the following steps:

1. Choose **Network**> LAN **Setting**.

2. Click **Add list**.

3. Set the MAC address and **IP Address**.

4. Click **Submit**.

To modify an item in the setup list, perform the following steps:

1. Choose **Network**> LAN **Setting**.
2. Choose the item to be modified, and click **Edit**.
3. Set the MAC address and **IP Address**.
4. Click **Submit**.

To delete an item in the setup list, perform the following steps:

1. Choose **Network** > LAN **Setting**.
2. Choose the item to be deleted, and click **Delete**.

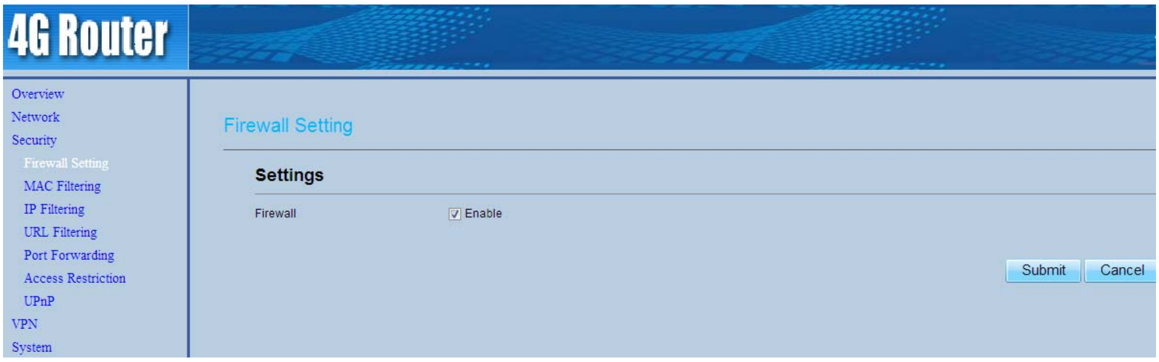
4 Security

4.1Setting Firewall

This page describes how to set the firewall. If you enable or disable the firewall, you can modify the configuration.

To set the firewall, perform the following steps:

1. Choose **Security**>**Firewall**.
2. Choose **Enable** or **Disable** to modify the configuration.
3. Click **Submit**. As shown in Figure 4-1.



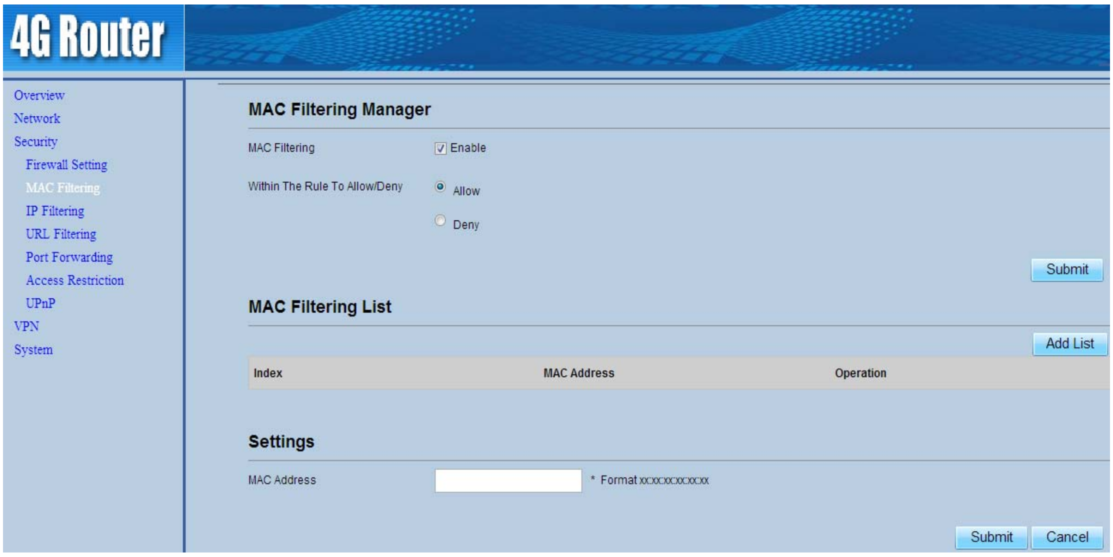
Firewall ☑ Enable

Figure 4-1

If you choose enable the firewall, you can modify the configuration about firewall, such as Mac filter, IP filter, URL filter and so on. If you choose disable, you can’t modify any configurations about the firewall.

4.2MAC Filtering

This page enables you to configure the MAC address filtering rules. As shown in Figure 4-2.



MAC Filtering Manager

MAC Filtering ☑ Enable

Within The Rule To Allow/Deny ● Allow ○ Deny

MAC Filtering List

Index	MAC Address	Operation

Settings

MAC Address * Format xx:xx:xx:xx:xx:xx

Figure 4-2

4.2.1 Enabling MAC Filter

To enable MAC address filter, perform the following steps:

1. Choose **Security**>**MAC Filtering**
2. Set MAC filtering to **Enable**.
3. Click **Submit**.

4.2.2 Disabling MAC Filter

To disable MAC address filter, perform the following steps:

1. Choose **Security**>**MAC Filtering**
2. Set MAC filtering to **Disable**.
3. Click **Submit**.

4.2.3 Setting Allow access network within the rules

To set allow access network within the rules, perform the following steps:

1. Choose **Security**>**MAC Filtering**.
2. Set **Allow access network** within the rules.
3. Click **Submit**.

4.2.4 Setting Deny access network within the rules

To set deny access network within the rules, perform the following steps:

1. Choose **Security**>**MAC Filtering**.
2. Set **Deny access network** within the rules.

3. Click **Submit**.

4.2.5 Adding MAC Filtering rule

To add a MAC filtering rule, perform the following steps:

1. Choose **Security**>**MAC Filtering**.
2. Click **Add list**.
3. Set **MAC address**.
4. Click **Submit**.

4.2.6 Modifying MAC Filtering rule

To modify a MAC address rule, perform the following steps:

1. Choose **Security**>**MAC Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **MAC address**.
4. Click **Submit**.

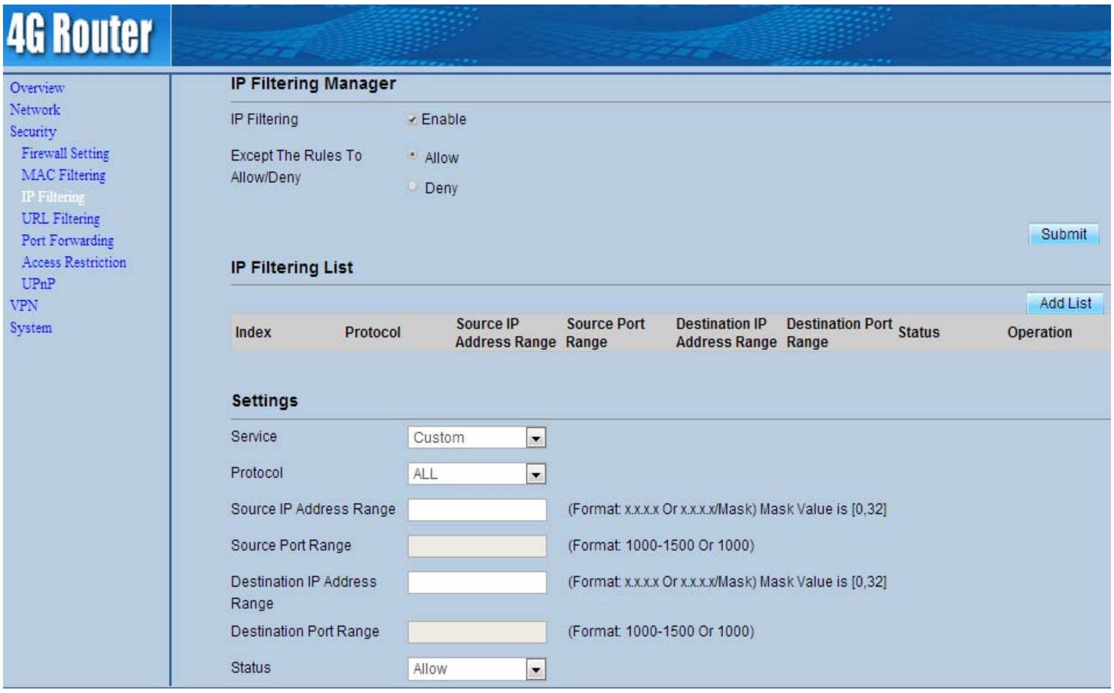
4.2.7 Deleting MAC Filtering rule

To delete a MAC address filter rule, perform the following steps:

1. Choose **Security**>**MAC Filtering**.
2. Choose the rule to be deleted, and click **Delete**.

4.3IP Filtering

Data is filtered by IP address. This page enables you to configure the IP address filtering rules. As shown in Figure 4-3.



IP Filtering Manager

IP Filtering ☑ Enable

Except The Rules To Allow/Deny ● Allow ○ Deny

IP Filtering List

Index	Protocol	Source IP Address Range	Source Port Range	Destination IP Address Range	Destination Port Range	Status	Operation

Settings

Service	Custom	
Protocol	ALL	
Source IP Address Range		(Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32]
Source Port Range		(Format: 1000-1500 Or 1000)
Destination IP Address Range		(Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32]
Destination Port Range		(Format: 1000-1500 Or 1000)
Status	Allow	

Figure 4-3

4.3.1 Enabling IP Filtering

To enable IP Filtering, perform the following steps:

1. Choose **Security**>**IP Filtering**.
2. Set IP Filtering **Enable**.
3. Click **Submit**.

4.3.2 Disabling IP Filtering

To disable IP Filtering, perform the following steps:

1. Choose **Security**>**IP Filtering**.
2. Set IP Filtering **Disable**.
3. Click **Submit**.

4.3.3 Setting Allow access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Security**>**IP Filtering**.
2. Set **Allow access network** outside the rules.
3. Click **Submit**.

4.3.4 Setting Deny access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Security**>**IP Filtering**.
2. Set **Deny access network** outside the rules.
3. Click **Submit**.

4.3.5 Adding IP Filtering rule

Add an IP address filtering rule, perform the following steps:

1. Choose **Security**>**IP Filtering**.
2. Click **Add list**.
3. Set **Service**.
4. Set **Protocol**.
5. In the **Source IP Address Range** box, enter the source IP address or IP address segment to be filtered.
6. In the **Source port range** box, enter the source port or port segment to be filtered.
7. In the **Destination IP Address Range** box, enter the destination IP address or IP address segment to be filtered.
8. In the **Destination port Range** box, enter the destination port or port segment to be filtered.
9. In the **Status** box, choose a status the rule will be executed.
10. Click **Submit**.

4.3.6 Modifying IP Filtering rule

To modify an IP filtering rule, perform the following steps:

1. Choose **Security** > **IP Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Repeat steps 3 through 9 in the previous procedure.
4. Click **Submit**.

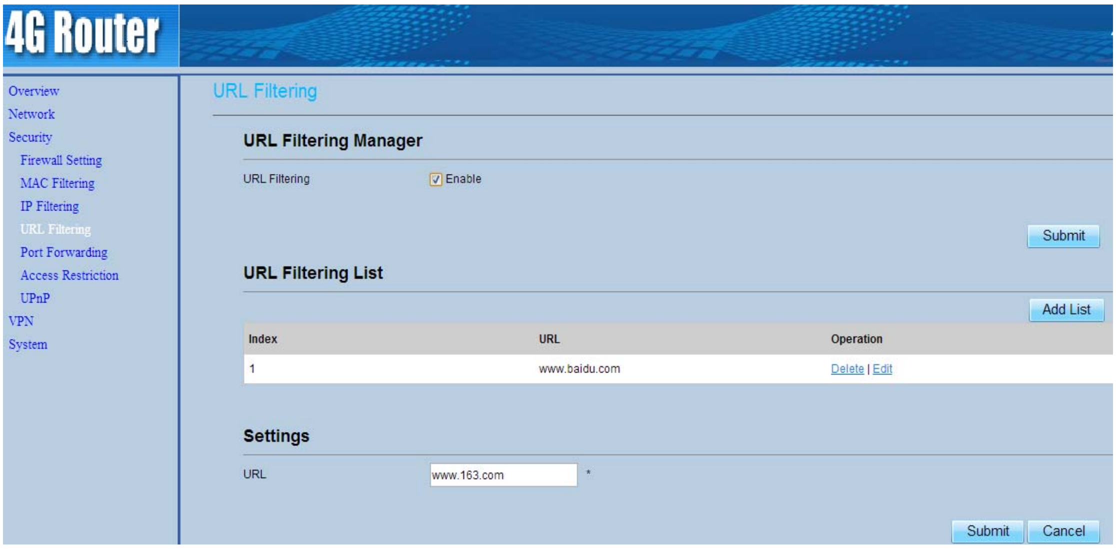
4.3.7 Deleting IP Filtering rule

To delete an IP address filtering rule, perform the following steps:

1. Choose **Security** > **IP Filtering**.
2. Choose the rule to be deleted, and click **Delete**.

4.4URL Filtering

Data is filtered by uniform resource locator (URL). This page enables you to configure URL filtering rules. As shown in Figure 4-4.



URL Filtering

URL Filtering Manager

URL Filtering ☑ Enable

URL Filtering List

Index	URL	Operation
1	www.baidu.com	Delete | Edit

Settings

URL www.163.com *

Figure 4-4

4.4.1 Enabling URL Filtering

To enable URL Filtering, perform the following steps:

1. Choose **Security**>**URL Filtering**.
2. Set **URL Filtering** to **Enable**.
3. Click **Submit**.

4.4.2 Disabling URL Filtering

To disable URL Filtering, perform the following steps:

1. Choose **Security**>**URL Filtering**.
2. Set **URL Filtering** to **Disable**.
3. Click **Submit**.

4.4.3 Adding URL Filtering list

To add a URL filtering list, perform the following steps:

1. Choose **Security**>**URL Filtering**.
2. Click **Add list**.
3. Set **URL**.
4. Click **Submit**.

4.4.4 Modify URL Filtering list

To modify a URL filtering rule, perform the following steps:

1. Choose **Security**>**URL Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **URL** address.
4. Click **Submit**.

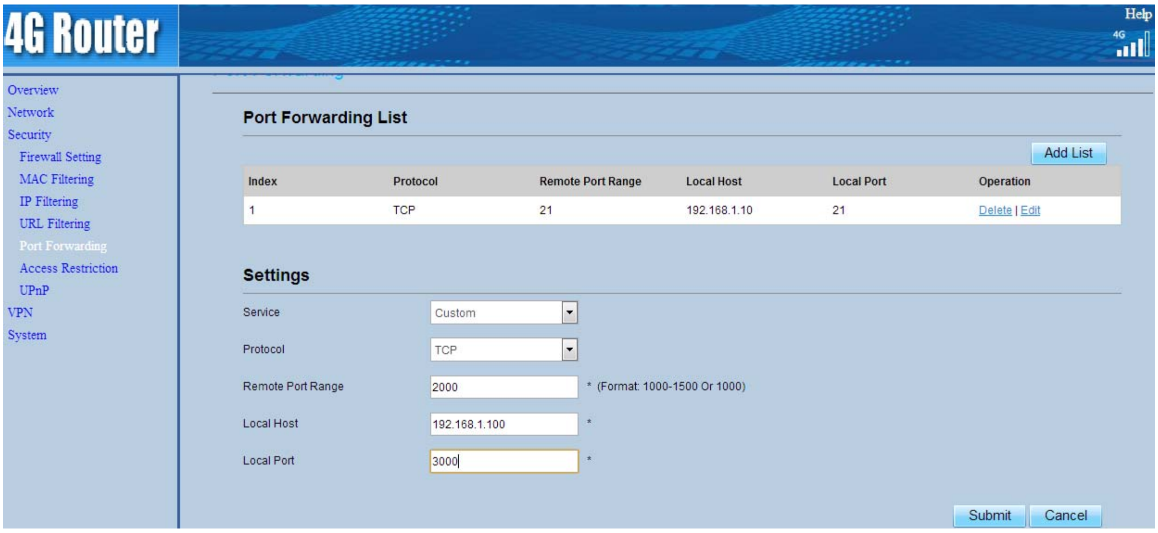
4.4.5 Deleting URL Filtering list

To delete a URL list, perform the following steps:

1. Choose **Security**>**URL Filtering**.
2. Choose the item to be deleted, and click **Delete**.

4.5Port Forwarding

When network address translation (NAT) is enabled on the CPE, only the IP address on the WAN side is open to the Internet. If a computer on the LAN is enabled to provide services for the Internet (for example, work as an FTP server), port forwarding is required so that all accesses to the external server port from the Internet are redirected to the server on the LAN. As shown in Figure 4-5.



Port Forwarding List

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	21	192.168.1.10	21	Delete | Edit

Settings

Service	Custom
Protocol	TCP
Remote Port Range	2000 * (Format: 1000-1500 Or 1000)
Local Host	192.168.1.100 *
Local Port	3000 *

Figure 4-5

4.5.1 Adding Port Forwarding rule

To add a port forwarding rule, perform the following steps:

1. Choose **Security** > **Port Forwarding**.

2. Click **Add list**.

3. Set **Service**.

4. Set **Protocol**.

5. Set **Remote port range**.

💬 The port number ranges from 1 to 65535.

6. Set **Local host**.

💬 This IP address must be different from the IP address that is set on the **LAN Host Settings** page, but they must be on the same network segment.

7. Set **Local port**.

💬 The port number ranges from 1 to 65535.

8. Click **Submit**.

4.5.2 Modifying Port Forwarding rule

To modify a port forwarding rule, perform the following steps:

1. Choose **Security** > **Port Forwarding**.

2. Choose the item to be modified, and click **Edit**.

3. Repeat steps 3 through7 in the previous procedure.

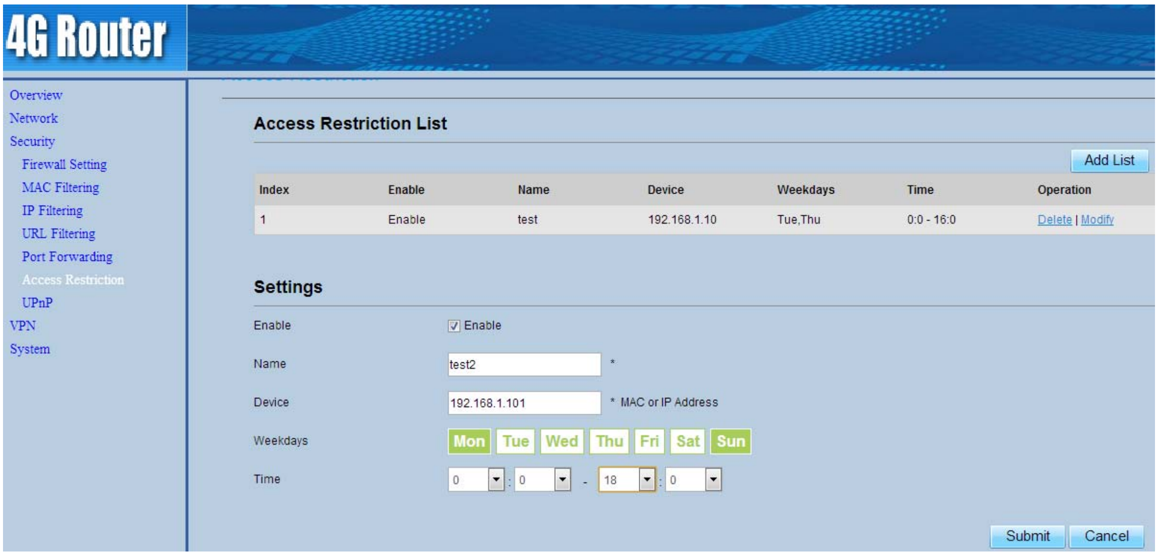
4. Click **Submit**.

4.5.3 Deleting Port Forwarding rule

To delete a port forwarding rule, perform the following steps:

1. Choose **Security** > **Port Forwarding**.
2. Choose the item to be deleted, and click **Delete**.

4.6Access Restriction



Access Restriction List

Index	Enable	Name	Device	Weekdays	Time	Operation
1	Enable	test	192.168.1.10	Tue,Thu	0:0 - 16:0	Delete | Modify

Settings

Enable ☑ Enable

Name test2 *

Device 192.168.1.101 * MAC or IP Address

Weekdays Mon Tue Wed Thu Fri Sat Sun

Time 0 : 0 - 18 : 0

Figure 4-6

4.6.1 Add Access Restriction

To add a access restriction rule, perform the following steps:

1. Choose **Security**>**Access Restriction**.
2. Click **Add list**.
3. Set **Access Restriction** to **Enable**.
4. Set **Access Restriction Name**.
5. Set Device **MAC address** or **IP address**.
6. Set **Weekdays** and **time**.
7. Click **Submit**.

4.6.2 Modify Access Restriction

To modify a access restriction rule, perform the following steps:

1. Choose **Security**>**Access Restriction**.
2. Choose the item to be modified, and click **Edit**.
3. Repeat steps 4 through 6 in the previous procedure.
4. Click **Submit**.

4.6.3 Delete Access Restriction

To delete a access restriction rule, perform the following steps:

1. Choose **Security**>**Access Restriction**.

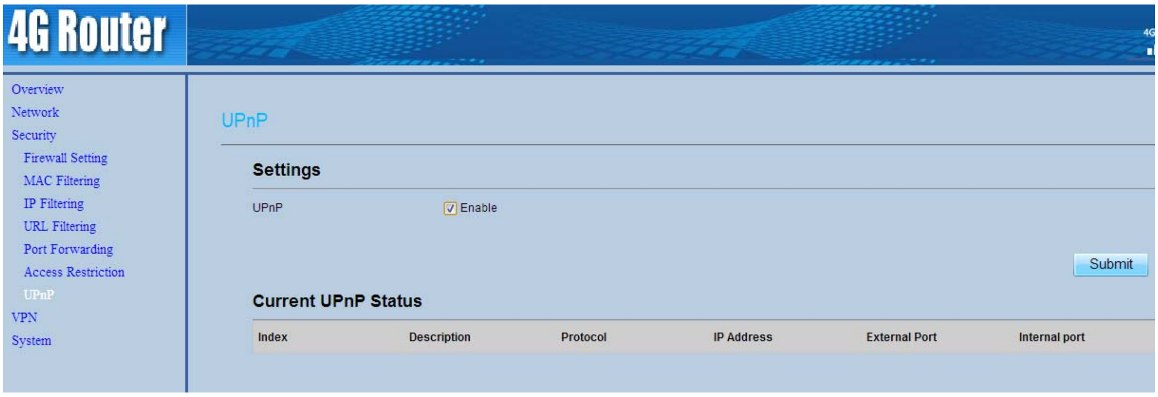
2. Choose the item to be deleted, and click **Delete**.

4.7UPnP

On this page, you can enable or disable the Universal Plug and Play (UPnP) function.

To enable UPnP, perform the following steps:

1. Choose **Security > UPnP**.
2. Set UPnP to **Enable**.
3. Click **Submit**. As shown in Figure 4-7.



UPnP

Settings

UPnP ☑ Enable

Current UPnP Status

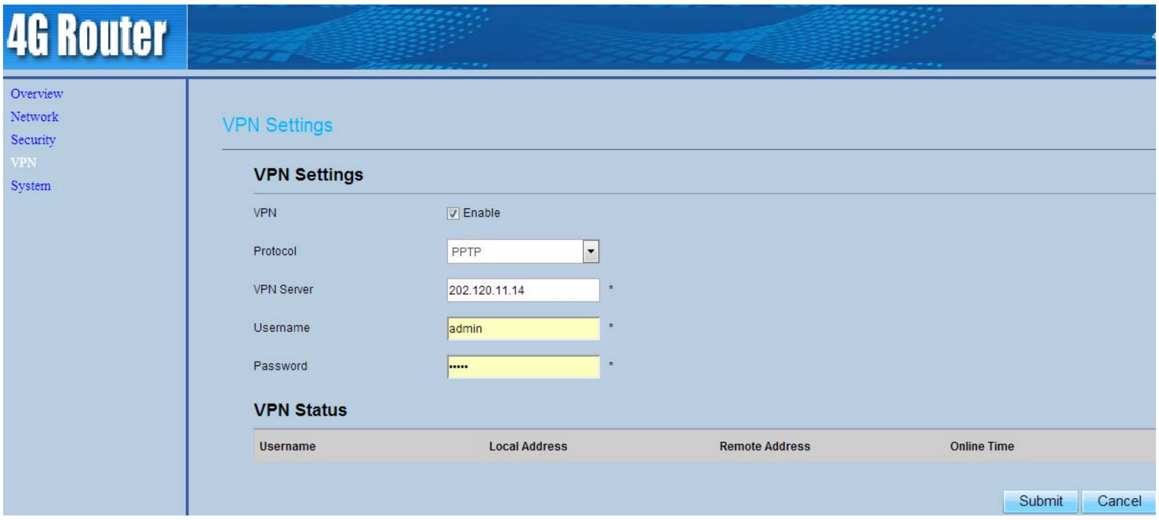
Index	Description	Protocol	IP Address	External Port	Internal port

Figure 4-7

5 VPN Setting

This function enables you to connect the virtual private network (VPN).
To connect the VPN, perform the following steps:

1. Choose **VPN Setting.**
2. In the **VPN Setting** area, enable VPN.
3. Select a protocol from **Protocol** drop-down list.
4. Enter **Username** and **Password**.
5. Click **Submit**.
6. You can view the status in **VPN Status** area. As shown in Figure 5-1.



VPN Settings

VPN Settings

VPN ☑ Enable

Protocol PPTP

VPN Server 202.120.11.14 *

Username admin *

Password ••••• *

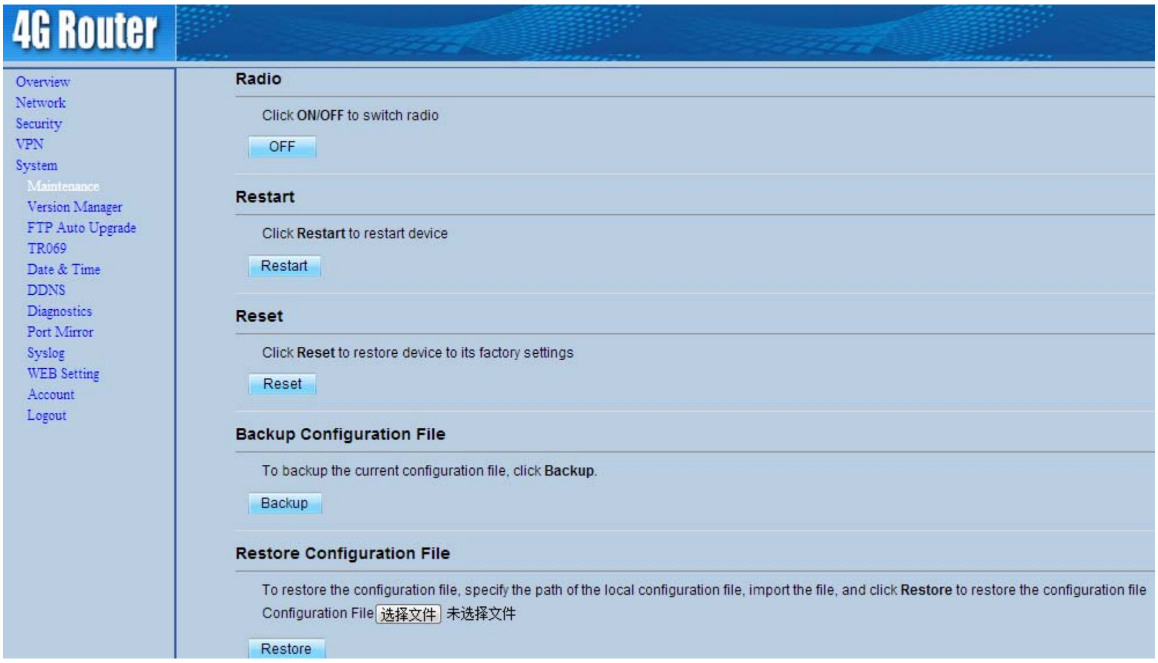
VPN Status

Username	Local Address	Remote Address	Online Time

Figure 5-1

6 System

6.1Maintenance



Radio

Click **ON/OFF** to switch radio

Restart

Click **Restart** to restart device

Reset

Click **Reset** to restore device to its factory settings

Backup Configuration File

To backup the current configuration file, click **Backup**.

Restore Configuration File

To restore the configuration file, specify the path of the local configuration file, import the file, and click **Restore** to restore the configuration file

Configuration File 选择文件 未选择文件

Figure 6-1

6.1.1 Radio

To switch the radio, perform the following steps:

1. Choose **System**>**Maintenance**.

2. Click **ON/OFF** to switch radio.

6.1.2 Restart

This function enables you to restart the CPE. Settings take effect only after the CPE restarts. To restart the CPE, perform the following steps:

1. Choose **System**>**Maintenance**.
2. Click **Restart**.

The CPE then restarts.

6.1.3 Reset

This function enables you to restore the CPE to its default settings.

To restore the CPE, perform the following steps:

1. Choose **System**>**Maintenance**.
2. Click **Reset.**

The CPE is then restored to its default settings.

6.1.4 Download Configuration File

You can download the existing configuration file to back it up. To do so:

1. Choose **System**>**Maintenance**.
2. Click **Download** on the **Maintenance** page.
3. In the displayed dialog box, select the save path and name of the configuration file to be backed up.
4. Click **Save**.

The procedure for file downloading may vary with the browser you are using.

6.1.5 Upload Configuration File

You can upload a backed up configuration file to restore the CPE. To do so:

1. Choose **System**>**Maintenance**.
2. Click **Browse** on the **Maintenance** page.
3. In the displayed dialog box, select the backed up configuration file.
4. Click **Open**.
5. The dialog box choses. In the box to be right of Configuration file, the save path and name of the backed up configuration file are displayed.
6. Click **Upload**.

The CPE uploads the backed up configuration file. The CPE then automatically restarts.

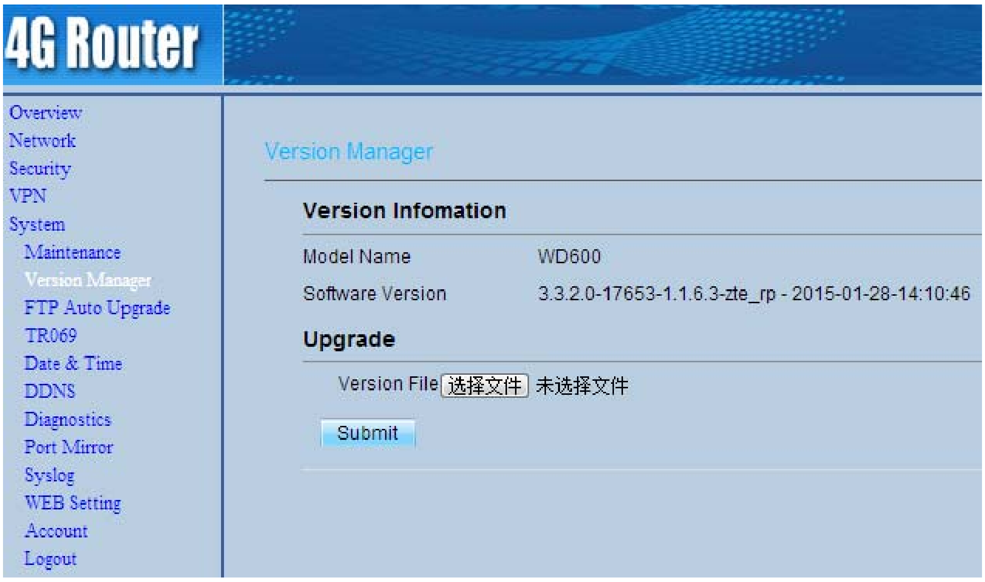
6.2Version Manager

This function enables you to upgrade the software version of the CPE to the latest version. It is recommended that you upgrade the software because the new version, certain bugs have been fixed and the system stability is usually improved.

6.2.1 Viewing Version Info

To view the version info, perform the following steps:

1. Choose **System**>**Version Manager**.
2. In the **Version Info** area, you can view the product name and software version. As shown in Figure 6-2.



Version Manager

Version Infomation

Model Name	WD600
Software Version	3.3.2.0-17653-1.1.6.3-zte_rp - 2015-01-28-14:10:46

Upgrade

Version File 选择文件 未选择文件

Submit

Figure 6-2

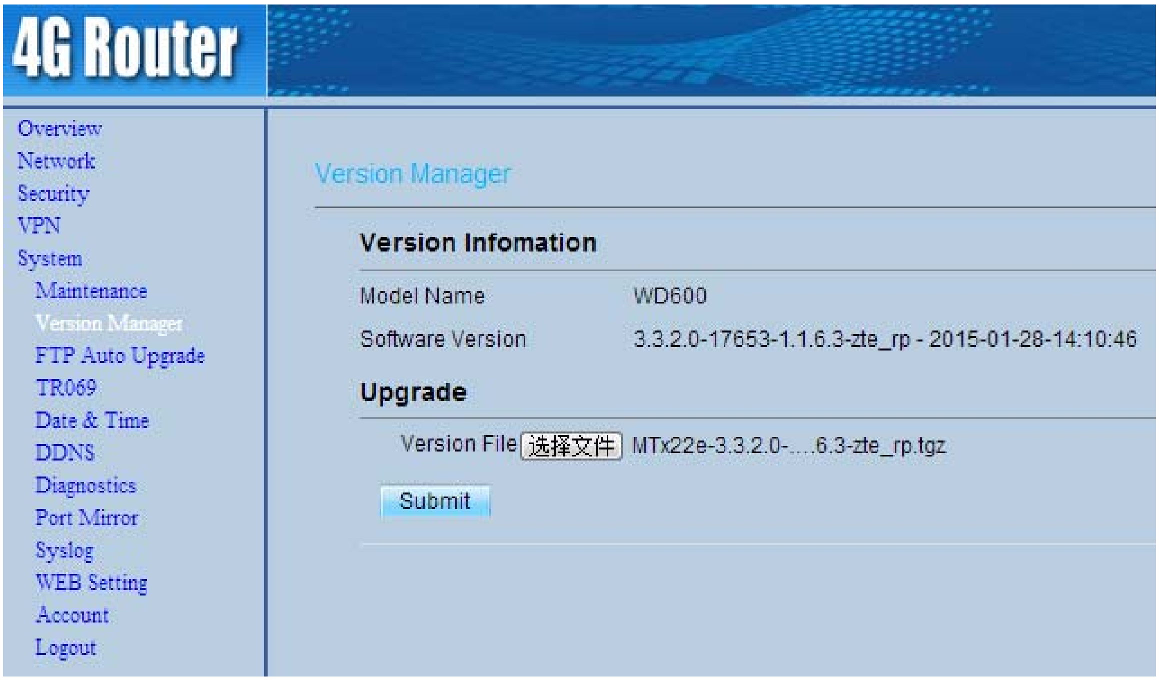
6.2.2 Version Upgrade

To perform an upgrade successfully, connect the CPE to your computer through a network cable, save the upgrade file on the computer, and make sure the CPE is not connected to anything other than a power adapter and the computer.

To perform an upgrade, perform the following steps:

1. Choose **System**>**Version Manager**.
2. In the **Version Upgrade** area, click **Browse**. In the displayed dialog box, select the target software version file.
3. Click **Open**. The dialog box choses. The save path and name of the target software version file are displayed in the Update file field.
4. Click **Submit**.
5. The software upgrade starts. After the upgrade, the CPE automatically restarts and runs the new software version. As shown in Figure 6-3.

⚠ During an upgrade, do not power off the CPE or disconnect it from the computer.



Version Manager

Version Infomation

Model Name	WD600
Software Version	3.3.2.0-17653-1.1.6.3-zte_rp - 2015-01-28-14:10:46

Upgrade

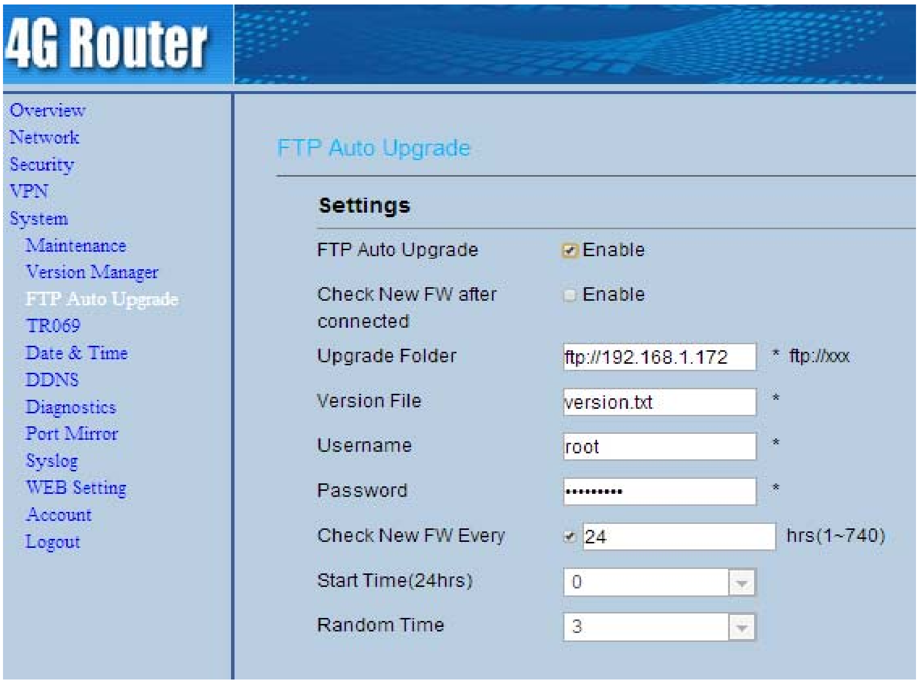
Version File 选择文件 MTx22e-3.3.2.0-....6.3-zte_rp.tgz

Submit

Figure 6-3

6.3FTP auto upgrade

To perform a ftp auto upgrade successfully, make sure the CPE is connected to the Internet. As shown in Figure 6-4.



FTP Auto Upgrade

Settings

FTP Auto Upgrade	☑ Enable	
Check New FW after connected	□ Enable	
Upgrade Folder	ftp://192.168.1.172	* ftp://xxx
Version File	version.txt	*
Username	root	*
Password	•••••••••	*
Check New FW Every	☑ 24	hrs(1~740)
Start Time(24hrs)	0	
Random Time	3	

Figure 6-4

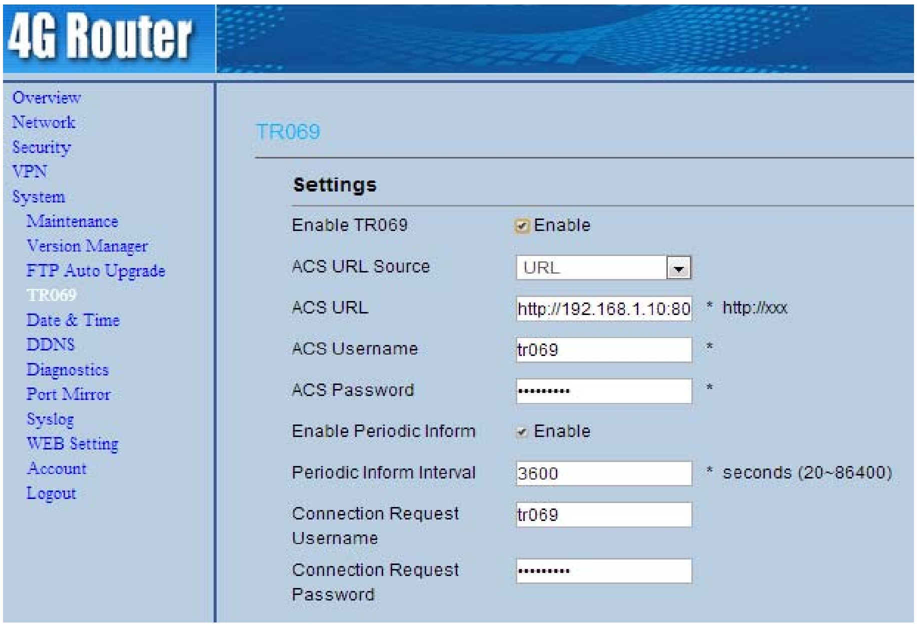
To perform a ftp auto upgrade, perform the following steps:

1. Choose **System**>**FTP auto upgrade**.
2. Enable **FTP auto upgrade**.
3. If you want to check new firmware after connect to Internet, you need to enable the item of **Check new firmware after connect to Internet**.
4. Set a ftp address to the **Upgrade folder** box.
5. Set **Version file**.
6. Set **User name** and **Password**.
7. Set the **Interval** of checking new firmware.
8. Set **Start time**.
9. Set **Random time**.
10. Click **Submit**.

⚠ The CPE will automatically upgrade according to the setting. During an upgrade, do not disconnect the power supply or operate the CPE.

6.4TR069

TR-069 is a standard for communication between CPEs and the auto-configuration server (ACS). If your service provider uses the TR069 automatic service provision function, the ACS automatically provides the CPE parameters. If you set the ACS parameters on both the CPE and ACS, the network parameters on the CPE are automatically set using the TR-069 function, and you do not need to set other parameters on the CPE. As shown in Figure 6-5.



TR069

Settings

Enable TR069	☑ Enable	
ACS URL Source	URL	
ACS URL	http://192.168.1.10:80	* http://xxx
ACS Username	tr069	*
ACS Password	•••••••••	*
Enable Periodic Inform	☑ Enable	
Periodic Inform Interval	3600	* seconds (20~86400)
Connection Request Username	tr069	
Connection Request Password	•••••••••	

Figure 6-5

To configure the CPE to implement the TR-069 function, perform the following steps:

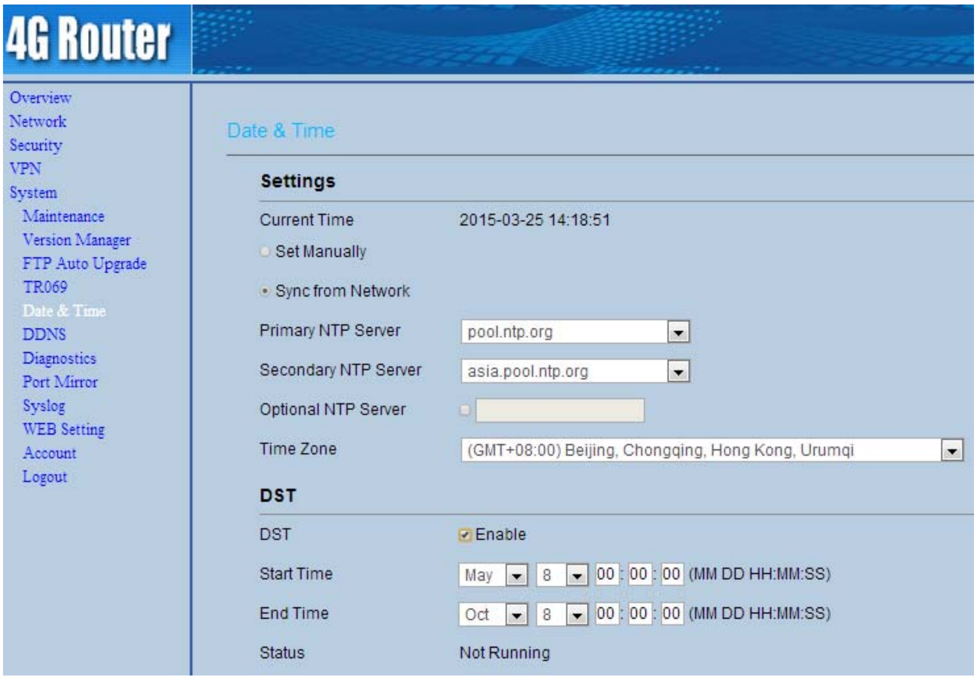
1. Choose **System**>**TR-069 Settings**.
2. Set **acs URL source**. There are two methods, such as **URL** and **DHCP**.
3. In the **ACS URL** box, enter the **ACS URL** address.
4. Enter ACS **user name** and **password** for the CPE authentication.

   To use the CPE to access the ACS, you must provide a user name and password for authentication. The user name and the password must be the same as those defined on the ACS.

5. If you set **Periodic inform** to **Enable**, set **Periodic inform interval**.
6. Set **connection request user name** and **password**.
7. Click **Submit**.

6.5Date & Time

You can set the system time manually or synchronize it with the network. If you select **Sync from network**, the CPE regularly synchronizes the time with the specified Network Time Protocol (NTP) server. If you enable daylight saving time (DST), the CPE also adjusts the system time for DST. As shown in 6-6.



Date & Time

Settings

Current Time 2015-03-25 14:18:51

○ Set Manually

● Sync from Network

Primary NTP Server pool.ntp.org

Secondary NTP Server asia.pool.ntp.org

Optional NTP Server □

Time Zone (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

DST

DST ☑ Enable

Start Time May 8 00 : 00 : 00 (MM DD HH:MM:SS)

End Time Oct 8 00 : 00 : 00 (MM DD HH:MM:SS)

Status Not Running

Figure 6-6

To set the date and time, perform the following steps:

1. Choose **System** > **Date & Time**.

2. Select **Set manually**.

3. Set **Local time** or click **Sync** to automatically fill in the current local system time.

4. Click **Submit**.

To synchronize the time with the network, perform the following steps:

1. Choose **System** > **Date & Time**.

2. Select **Sync from network**.

3. From the **Primary NTP server** drop-down list, select a server as the primary server for time synchronization.

4. From the **Secondary NTP server** drop-down list, select a server as the IP address of the secondary server for time synchronization.

5. If you don’t want to use other NTP server, you need to enable Optional ntp server, and set a server IP address.

6. Set **Time zone**.

7. Click **Submit**.

To set DST, perform the following steps:

1. Choose **System**>**Date&Time**.

2. Set **DST** enable.

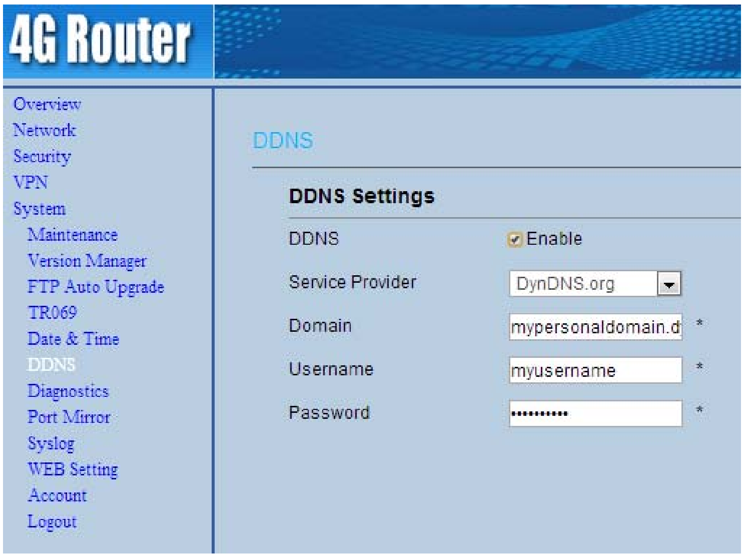
3. Set **Start Time** and **End Time**.

4. Click **Submit**.

The CPE will automatically provide the DST time based on the time zone.

6.6DDNS

Dynamic Domain Name Server (DDNS) service is used to map the user's dynamic IP address to a fixed DNS service. As shown in Figure 6-7.



DDNS

DDNS Settings

DDNS	☑ Enable
Service Provider	DynDNS.org
Domain	mypersonaldomain.d *
Username	myusername *
Password	•••••••••• *

Figure 6-7

To configure DDNS settings, perform the following steps:

1. Choose **System** > **DDNS**.

2. Set **DDNS** to **Enable**.

3. In **Service provider**, choose **DynDNS.org** or **oray.com**.

4. Enter **Domain name** and **Host name.** For example, if the domain name provided by your service provider is **test.customtest.dyndns.org**, enter **customtest.dyndns.org** as **Domain name**, and **test** as **Host name**.

5. Enter **User name** and **Password.**

6. Click **Submit**.

6.7Diagnosis

If the CPE is not functioning correctly, you can use the diagnosis tools on the **Diagnosis** page to preliminarily identify the problem so that actions can be taken to solve it.

6.7.1 Ping

If the CPE fails to access the Internet, run the ping command to preliminarily identify the problem. To do so:

1. Choose **System**>**Diagnosis**.

2. In the Method area, select **Ping**.

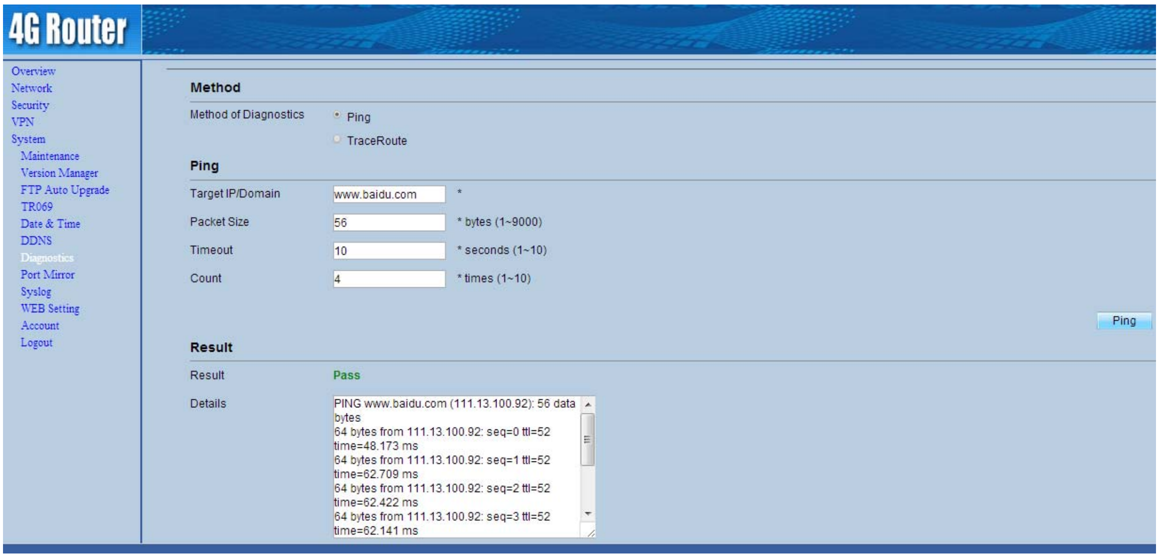
3. Enter the domain name in the **Target IP or domain** field, for example, www.google.com.

4. Set **Packet size** and **Timeout**.

5.	Set **Count**.

6.	Click **Ping**.

Wait until the ping command is executed. The execution results are displayed in the Results box. As shown in Figure 6-8.



Method

Method of Diagnostics ● Ping ○ TraceRoute

Ping

Target IP/Domain	www.baidu.com	*
Packet Size	56	* bytes (1~9000)
Timeout	10	* seconds (1~10)
Count	4	* times (1~10)

Result

Result: Pass

Details:

```
PING www.baidu.com (111.13.100.92): 56 data
bytes
64 bytes from 111.13.100.92: seq=0 ttl=52
time=48.173 ms
64 bytes from 111.13.100.92: seq=1 ttl=52
time=62.709 ms
64 bytes from 111.13.100.92: seq=2 ttl=52
time=62.422 ms
64 bytes from 111.13.100.92: seq=3 ttl=52
time=62.141 ms
```

Figure 6-8

6.7.2 Traceroute

If the CPE fails to access the Internet, run the Traceroute command to preliminarily identify the problem. To do so:

1.	Choose **System**>**Diagnosis**.

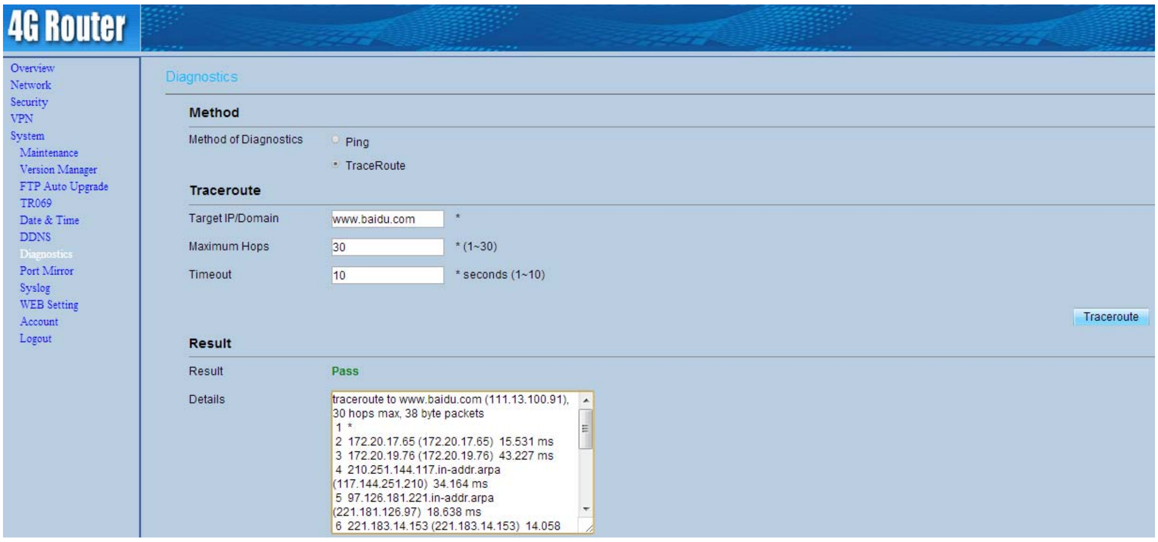
2.	In the Method area, select **Traceroute**.

3.	Enter the domain name in the **Target IP or domain** field. For example, www.google.com.

4.	Set **Maximum hops** ad **Timeout**.

5.	Click **Traceroute**.

Wait until the traceroue command is executed. The execution results are displayed in the Results box. As shown in Figure 6-9.



Diagnostics

Method

Method of Diagnostics ○ Ping ● TraceRoute

Traceroute

Target IP/Domain: www.baidu.com *

Maximum Hops: 30 * (1~30)

Timeout: 10 * seconds (1~10)

Result

Result: Pass

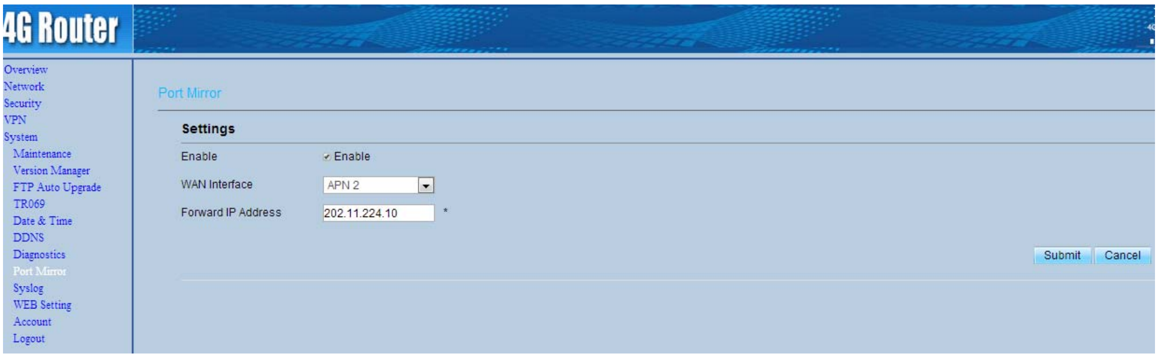
Details:

```
traceroute to www.baidu.com (111.13.100.91),
30 hops max, 38 byte packets
 1  *
 2  172.20.17.65 (172.20.17.65)  15.531 ms
 3  172.20.19.76 (172.20.19.76)  43.227 ms
 4  210.251.144.117.in-addr.arpa
(117.144.251.210)  34.164 ms
 5  97.126.181.221.in-addr.arpa
(221.181.126.97)  18.638 ms
 6  221.183.14.153 (221.183.14.153)  14.058
```

Figure 6-9

6.8Port Mirror

This function enables you to monitor or analysis the data flow of one or more network interface. As shown in Figure 6-10.



Port Mirror

Settings

Enable: ☑ Enable

WAN Interface: APN 2

Forward IP Address: 202.11.224.10 *

Figure 6-10

To enable the Port Mirror, perform the following steps:

1. Choose **System**>**Port Mirror**.
2. Set **Port Mirror** to **Enable**.
3. From the **WAN interface** drop-down list, select an interface.
4. In the **Forward IP address** box, enter the IP address.
5. Click **Submit**.

6.9Syslog

The syslog record user operations and key running events.

6.9.1 Local

To set the syslog to local, perform the following steps:

1. Choose **System**>**Syslog**.

2. In the **Setting** area, set the method to **Local**.

3. In the **Level** drop-down list, select a log level.

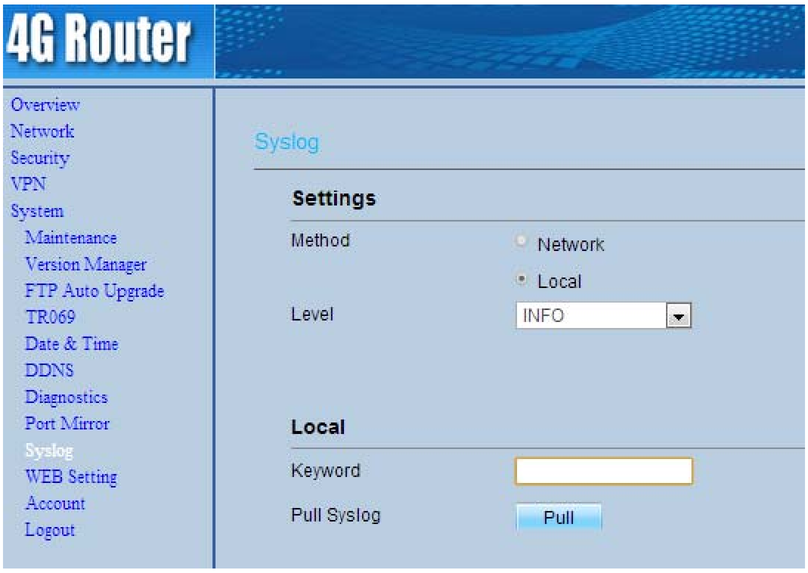
4. Click **Submit**.

Viewing local syslog

To view the local syslog, perform the following steps:

1. In the **Keyword** box, set a keyword.

2. Click **Pull**, the result box will display. As shown in Figure 6-11.



Syslog

Settings

Method ○ Network ● Local

Level INFO

Local

Keyword

Pull Syslog

Figure 6-11

6.9.2 Network

To set the syslog to network, perform the following steps:

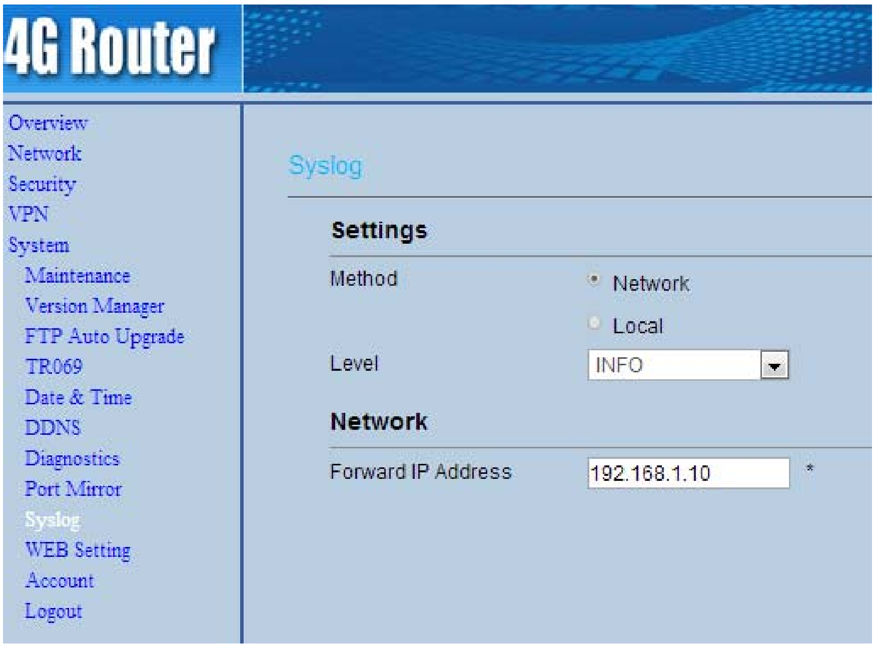
1. Choose **System**>**Syslog**.

2. In the **Setting** area, set the method to **Network**.

3. In the **Level** drop-down list, select a log level.

4. In the **Forward IP address** box, set a IP address.

5. Click **Submit**. As shown in Figure 6-12.



Syslog

Settings

Method ● Network ○ Local

Level INFO

Network

Forward IP Address 192.168.1.10 *

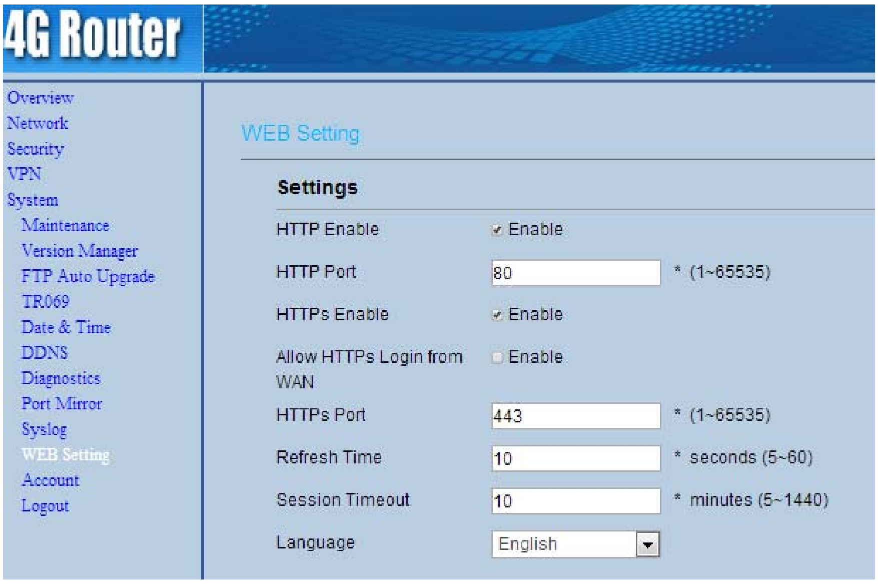
Figure 6-12

The syslog will transmit to some client to display through network.

6.10WEB setting

To configure the parameters of WEB, perform the following steps:

1. Choose **System**>**WEB Setting**.
2. Set **HTTP** enable. If you set HTTP disable, you will can't login the web management page with the HTTP protocol.
3. Set **HTTP port**. If you want to change the login port, you can set a new port in the box, the default HTTP port is 80.
4. Set **HTTPS** enable. If you want to login the web management page with the HTTPS protocol, you need to enable the HTTPS.
5. If you want to login the web management page form the **WAN**, you need to Enable **Allowing login from WAN**.
6. Set the **HTTPS port**.
7. Set **Refresh time**.
8. Set **Session timeout**.
9. Click **Submit**. As shown in Figure 6-13.



WEB Setting

Settings

HTTP Enable ☑ Enable

HTTP Port 80 * (1~65535)

HTTPs Enable ☑ Enable

Allow HTTPs Login from WAN □ Enable

HTTPs Port 443 * (1~65535)

Refresh Time 10 * seconds (5~60)

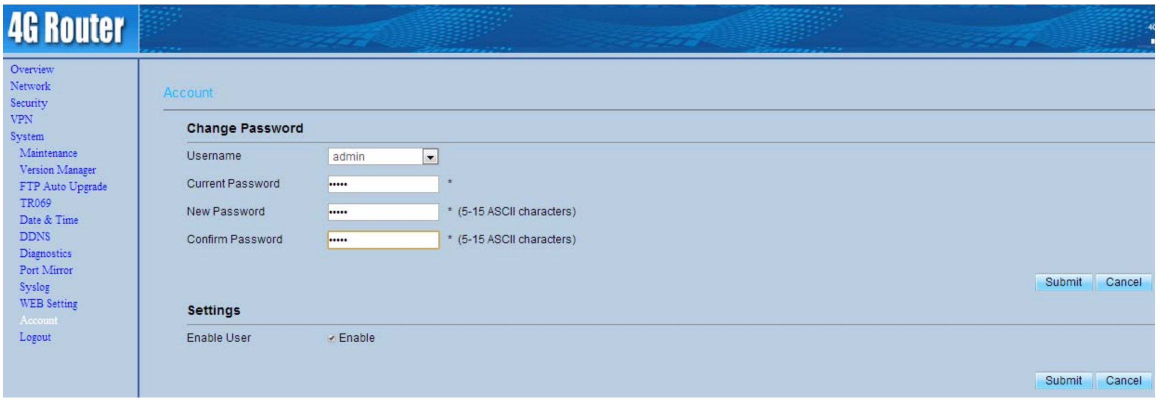
Session Timeout 10 * minutes (5~1440)

Language English

Figure 6-13

6.11Account

This function enables you to change the login password of the user. After the password changes, enter the new password the next time you login. As shown in Figure 6-14.



Account

Change Password

Username admin

Current Password ••••• *

New Password ••••• * (5-15 ASCII characters)

Confirm Password ••••• * (5-15 ASCII characters)

Settings

Enable User ☑ Enable

Figure 6-14

To change the password, perform the following steps:

1. Choose **System**>**Account**.
2. Select the **user name**, if you want to change the password of normal user, you need to set **Enable User** enable.
3. Enter the **current password**, set a **new password** ,and **confirm the new password**.
4. **New password** and **Confirm password** must contain 5 to 15 characters.
5. Click **Submit**.

6.12Logout

To logout the web management page, perform the following steps:

1. Choose **System** and click **Logout**

2. It will back to the login page.

7 FAQs

The POWER indicator does not turn on.

- Make sure that the power cable is connected properly and the CPE is powered on.
- Make sure that the power adapter is compatible with the CPE.

Fails to Log in to the web management page.

- Make sure that the CPE is started.
- Verify that the CPE is correctly connected to the computer through a network cable. If the problem persists, contact authorized local service suppliers.

The CPE fails to search for the wireless network.

- Check that the power adapter is connected properly.
- Check that the CPE is placed in an open area that is far away from obstructions, such as concrete or wooden walls.
- Check that the CPE is placed far away from household electrical appliances that generate strong electromagnetic field, such as microwave ovens, refrigerators, and satellite dishes.

If the problem persists, contact authorized local service suppliers.

The power adapter of the CPE is overheated.

- The CPE will be overheated after being used for a long time. Therefore, power off the CPE when you are not using it.
- Check that the CPE is properly ventilated and shielded from direct sunlight.

The parameters are restored to default values.

- If the CPE powers off unexpectedly while being configured, the parameters may be restored to the default settings.
- After configuring the parameters, download the configuration file to quickly restore the CPE to the desired settings.

FCC Regulations

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

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

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/ TV technician for help.

Caution ：

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

This equipment complies with the FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator and any part of your body. The antennas must not be co-located with other transmitter antennas.