

LTE CPE SQI4N4

# Quick Start Guide

FCC ID: 2AI24QCI4NU

FCC ID: 2AI24SQO14

Issue 01

Date 2016-08

## Contents

1	About This Document .....	2
2	Device Panel .....	3
3	What You Need .....	3
4	How It Works.....	4
5	Set Up the Hardware.....	5
5.1	Choose a Location .....	5
5.2	Insert a SIM Card to the Slot .....	6
5.3	Outdoor (SQO14) LED Behavior .....	7
5.4	Connect the SQO14 to the QCI4NU .....	8
5.5	Connect the QCI4NU .....	8
5.6	Mount the SQO14 .....	9
5.6.1	Pole mounting .....	9
6	Connect to the Internet .....	11
7	Wireless.....	13
7.1	Turn the Wireless On or off .....	13
8	Troubleshooting .....	14
8.1	Power LED .....	14
8.2	RESET Button.....	14
8.3	LTE LED .....	15
8.4	Wi-Fi LED .....	15
8.5	ETHERNET 1-4 LEDs.....	16
9	FCC Regulations.....	17

# 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.

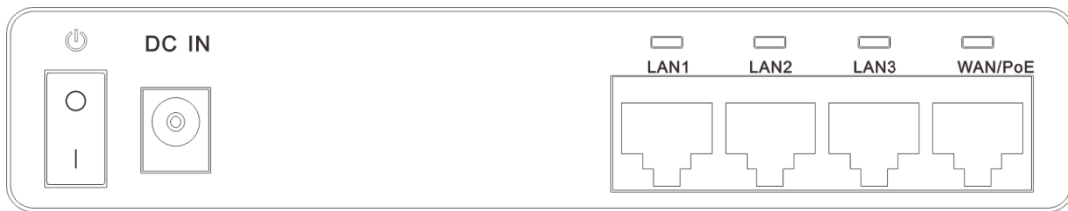


Figure 2-1

Figure 2-2 QCI4NU Front Panel.

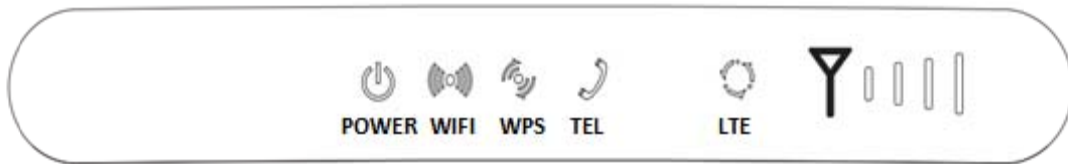






Figure 2-2

## 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.

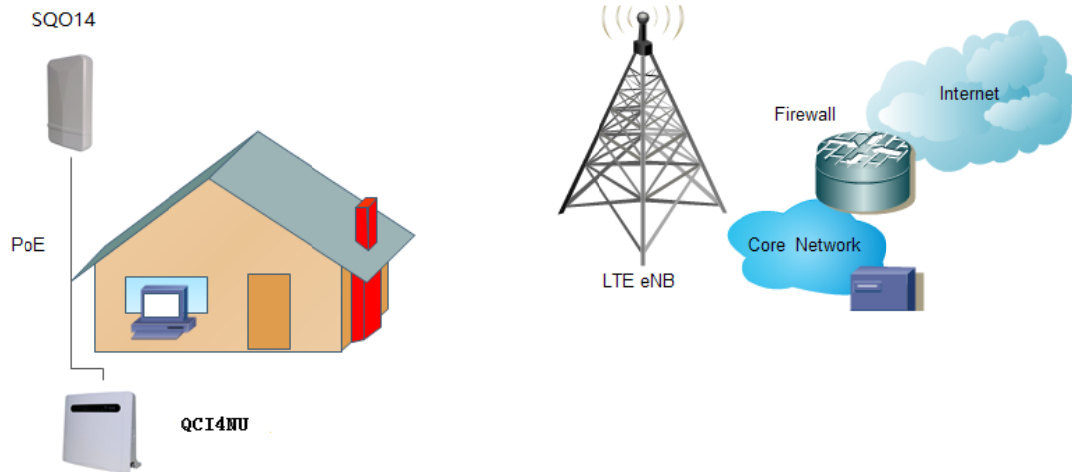


Figure 4-1

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 QCI4NU also serves as telephone adapter.

This Quick Start Guide shows you how to set up your SQO14 and QCI4NU in order to access the Internet.

# 5 Set Up the Hardware

---



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 provide 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.

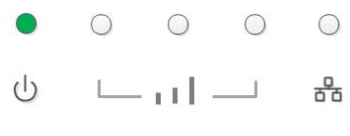

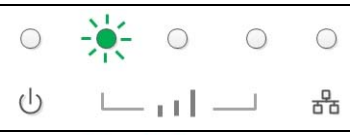





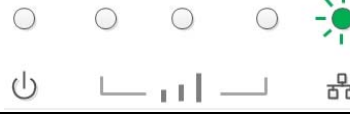



Figure 5-1

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

## 5.3 Outdoor (SQ014) 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 LED 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.

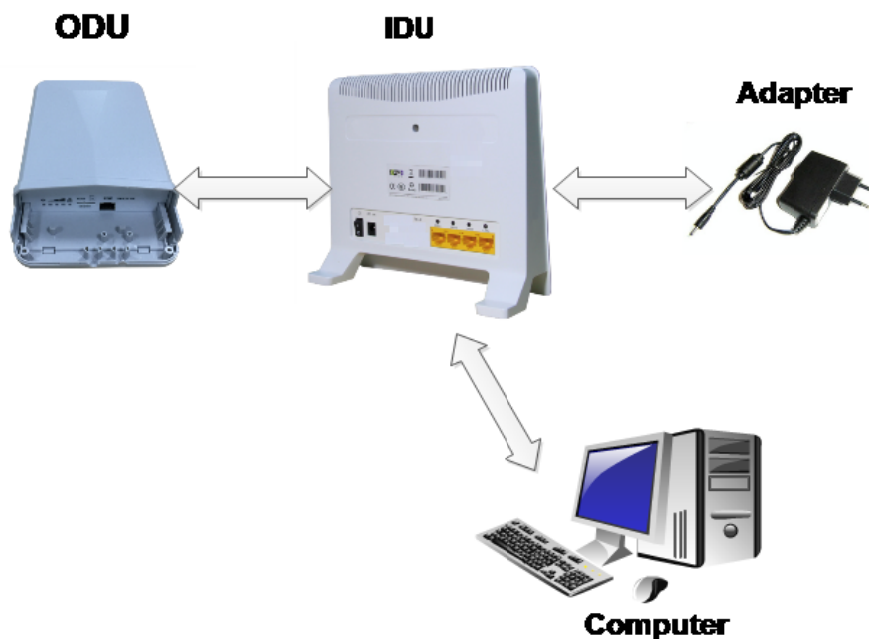


Figure 5-2

**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 SQ014 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 SQ014

See the installation instructions to mount the SQ014 correctly.

### 5.6.1 Pole mounting

Pole diameter type: The mounting pole diameter is  $\Phi 25$  and  $\Phi 45$ MM;

If the pole diameter is less than  $\Phi 30$ , 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;

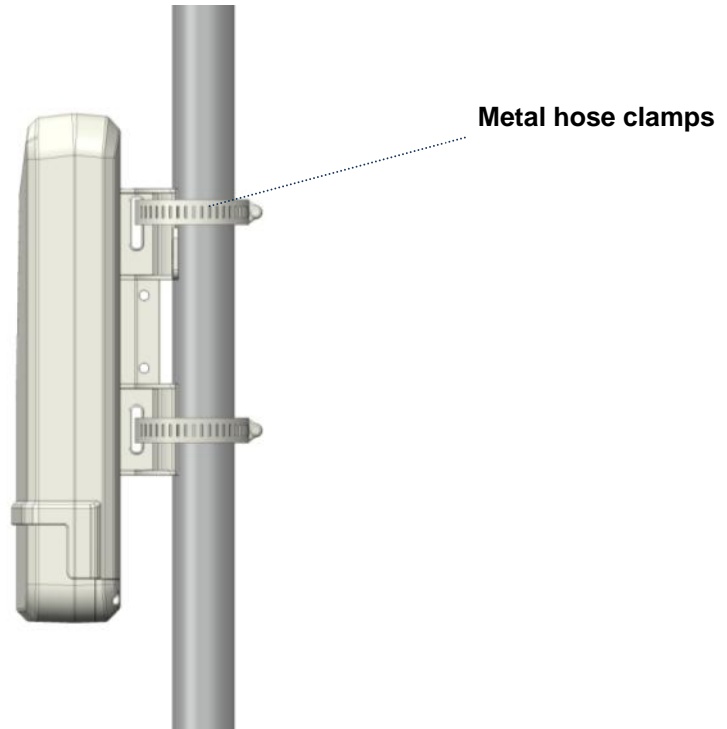


Figure 5-3 pole typemounting A

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.

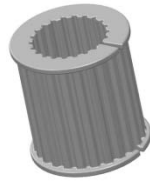


Figure 5-5C-type ring

## 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.

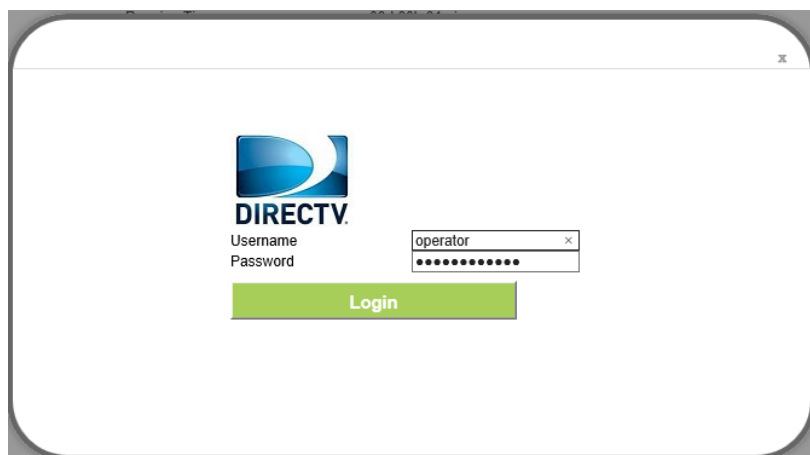


Figure 6-1

### 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

The screenshot shows the main screen of a DIRECTV device. At the top left is the DIRECTV logo. At the top right, there is a language dropdown menu set to 'English' and a 'Logout' button. On the left side, there is a navigation menu with the following items: Overview, Network, Wi-Fi, Security, VPN, VOIP, IPv6, and System. The main content area is titled 'Overview' and contains three sections: System Information, Version Information, and CPU Usage.

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

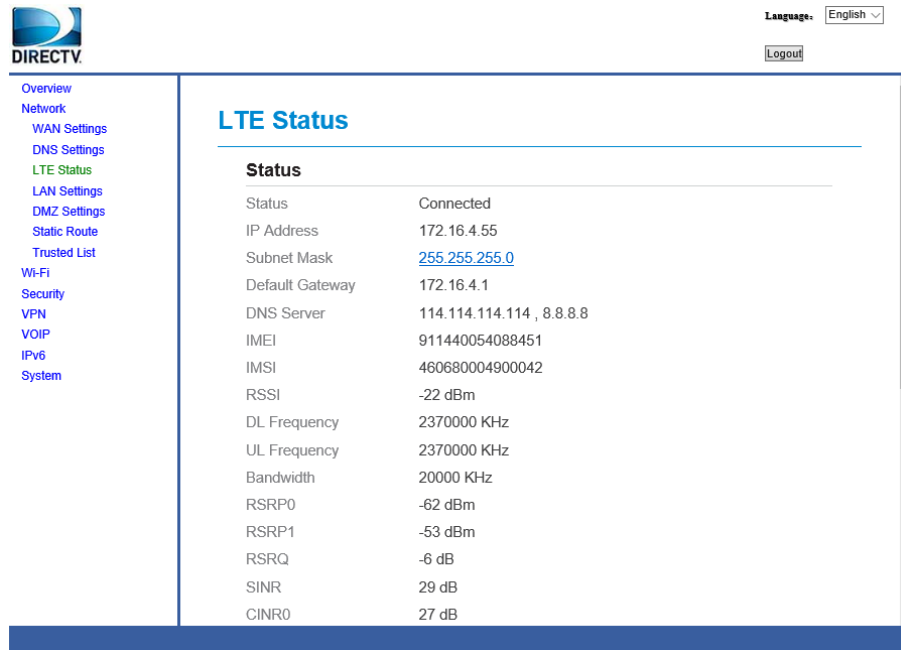


Figure 6-3

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

**Note:** SINR threshold parameters is  $\geq 10$  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

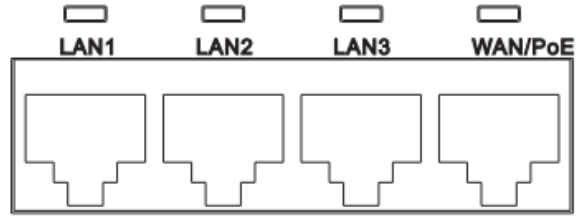


Figure 8-5

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.



# Indoor LTE CPE

Online Help

## Index

1	Getting Started .....	5
1.1	Welcome to the CPE .....	5
1.2	Computer Configuration Requirements .....	5
1.3	Logging In to the Web Management Page .....	5
2	Overview .....	6
2.1	Viewing the System Information .....	6
2.2	Viewing the Version Information .....	7
2.3	Viewing CPU Usage .....	7
2.4	Viewing Memory Usage .....	8
2.5	Viewing LAN Status .....	8
2.6	Viewing Wi-Fi Status .....	9
2.7	Viewing WAN Status .....	9
2.8	Viewing Throughput Statistics .....	10
2.9	Viewing Device List .....	10
3	Network Setting .....	11
3.1	WAN Setting .....	11
3.1.1	Network Mode .....	11
3.1.2	MTU Setting .....	11
3.1.3	Setting Connect ODU .....	12
3.1.4	WAN Network Parameters Setting .....	12
3.2	Outdoor 4G Status .....	13
3.3	LAN Setting .....	14
3.3.1	Setting LAN Host Parameters .....	14
3.3.2	Configuration the DHCP Server .....	15
3.3.3	Bundled Address List .....	16
3.4	DMZ Settings .....	17
3.5	Static Route .....	18
3.5.1	Add Static Route .....	18
3.5.2	Modify Static Route .....	18
3.5.3	Delete Static Route .....	19
4	Wi-Fi .....	19
4.1	WLAN Setting .....	19
4.1.1	Setting General Parameters .....	19
4.1.2	WPS Settings .....	20
4.2	Setting SSID Profile .....	20
4.3	Access Management .....	22
4.3.1	Setting the Access Policy .....	22
4.3.2	Managing the Wi-Fi Access List .....	23
4.4	WDS .....	24
5	Security .....	25
5.1	MAC Filtering .....	25
5.1.1	Enabling MAC Filter .....	25

5.1.2	Disabling MAC Filter .....	26
5.1.3	Setting Allow access network within the rules.....	26
5.1.4	Setting Deny access network within the rules .....	26
5.1.5	Adding MAC Filtering rule .....	27
5.1.6	Modifying MAC Filtering rule .....	27
5.1.7	Deleting MAC Filtering rule .....	28
5.2	IP Filtering .....	28
5.2.1	Enabling IP Filtering.....	28
5.2.2	Disabling IP Filtering.....	28
5.2.3	Setting Allow access network outside the rules.....	29
5.2.4	Setting Deny access network outside the rules.....	29
5.2.5	Adding IP Filtering rule.....	30
5.2.6	Modifying IP Filtering rule.....	30
5.2.7	Deleting IP Filtering rule.....	31
5.3	URL Filtering.....	31
5.3.1	Enabling URL Filtering .....	31
5.3.2	Disabling URL Filtering .....	32
5.3.3	Adding URL Filtering list .....	32
5.3.4	Modify URL Filtering list.....	32
5.3.5	Deleting URL Filtering list.....	33
5.4	Port Forwarding.....	33
5.4.1	Adding Port Forwarding rule .....	33
5.4.2	Modifying Port Forwarding rule .....	34
5.4.3	Deleting Port Forwarding rule .....	35
5.5	UPnP.....	35
6	VPN Setting .....	36
7	VOIP.....	36
7.1	View VOIP Information .....	36
7.2	Configuring SIP Server .....	37
7.3	Configuring SIP Account .....	38
8	System.....	38
8.1	Maintenance .....	38
8.1.1	Restart .....	38
8.1.2	Reset.....	39
8.1.3	Backup Configuration File .....	39
8.1.4	Upload Configuration File .....	40
8.2	Version Manager .....	40
8.2.1	Viewing Version Info .....	40
8.2.2	Version Upgrade .....	41
8.3	FTP auto upgrade .....	41
8.4	TRO69 .....	42
8.5	Date & Time .....	43
8.6	DDNS .....	45
8.7	Diagnosis .....	46

8.7.1	Ping.....	46
8.7.2	Traceroute .....	47
8.8	Syslog.....	48
8.8.1	Local .....	48
8.8.2	Network.....	49
8.9	Account .....	50
8.10	Remote WEB Access.....	51
8.11	Logout .....	52
9	FAQs .....	52

# 1 Getting Started

## 1.1 Welcome 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

## 1.2 Computer 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	<ul style="list-style-type: none"><li>• Microsoft: Windows XP, Windows Vista, or Windows 7</li><li>• Mac: Mac OS X 10.5 or higher</li></ul>
Display resolution	1024 x 768 pixels or higher
Browser	<ul style="list-style-type: none"><li>• Internet Explorer 7.0 or later</li><li>• Firefox 3.6 or later</li><li>• Opera 10 or later</li><li>• Safari 5 or later</li><li>• Chrome 9 or later</li></ul>

## 1.3 Logging 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.



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.

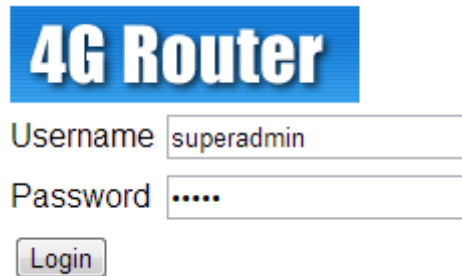


Figure 1-2



The default user name and password are both **admin**.

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

### 2.1 Viewing 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. As shown in Figure 2-1.



Figure 2-1

## 2.2 Viewing the Version Information

To view the Version Information, perform the following steps:

1. Choose **Overview**;
2. In the **Version Information** area, view the version information, such as Product name, Software version, Firmware version, UBoot version. As shown in Figure 2-2.

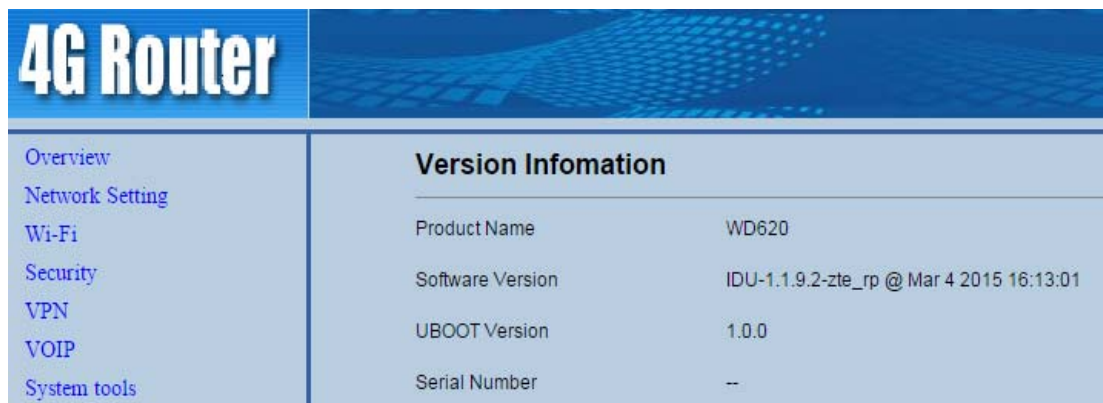


Figure 2-2

## 2.3 Viewing CPU Usage

To view the CPU usage, 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.

4G Router							
<ul style="list-style-type: none"> <li>Overview</li> <li>Network</li> <li>Wi-Fi</li> <li>Security</li> <li>VPN</li> <li>VOIP</li> </ul>	<h3>CPU Usage</h3> <table border="1"> <tbody> <tr> <td>Current</td> <td>28 %</td> </tr> <tr> <td>Max.</td> <td>100 %</td> </tr> <tr> <td>Min.</td> <td>0 %</td> </tr> </tbody> </table>	Current	28 %	Max.	100 %	Min.	0 %
Current	28 %						
Max.	100 %						
Min.	0 %						

Figure 2-3

## 2.4 Viewing Memory Usage

To view the memory usage, 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.

4G Router									
<ul style="list-style-type: none"> <li>Overview</li> <li>Network</li> <li>Wi-Fi</li> <li>Security</li> <li>VPN</li> <li>VOIP</li> <li>System</li> </ul>	<h3>Memory Usage</h3> <table border="1"> <tbody> <tr> <td>Total</td> <td>61704 KB</td> </tr> <tr> <td>Current</td> <td>70 %</td> </tr> <tr> <td>Max.</td> <td>71 %</td> </tr> <tr> <td>Min.</td> <td>49 %</td> </tr> </tbody> </table>	Total	61704 KB	Current	70 %	Max.	71 %	Min.	49 %
Total	61704 KB								
Current	70 %								
Max.	71 %								
Min.	49 %								

Figure 2-4

## 2.5 Viewing LAN Status

To view the LAN status, 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 2-5.



4G Router							
<ul style="list-style-type: none"> <li>Overview</li> <li>Network Setting</li> <li>Wi-Fi</li> <li>Security</li> <li>VPN</li> <li>VOIP</li> </ul>	<h3>LAN Status</h3> <table border="1"> <tr> <td>MAC Address</td> <td>00:12:61:FE:FE:FF</td> </tr> <tr> <td>IP Address</td> <td>192.168.1.1</td> </tr> <tr> <td>Subnet Mask</td> <td>255.255.255.0</td> </tr> </table>	MAC Address	00:12:61:FE:FE:FF	IP Address	192.168.1.1	Subnet Mask	255.255.255.0
MAC Address	00:12:61:FE:FE:FF						
IP Address	192.168.1.1						
Subnet Mask	255.255.255.0						

Figure 2-5

## 2.6 Viewing Wi-Fi Status

To view the Wi-Fi status, perform the following steps:

1. Choose **Overview**;
2. In the **Wi-Fi Status** area, view the information about Wi-Fi status, SSID, Chanel NO., MAC address and WDS status. As shown in Figure 2-6.

4G Router													
<ul style="list-style-type: none"> <li>Overview</li> <li>Network Setting</li> <li>Wi-Fi</li> <li>Security</li> <li>VPN</li> <li>VOIP</li> <li>System tools</li> </ul>	<h3>Wi-Fi Status</h3> <table border="1"> <tr> <td>WLAN</td> <td>Enable</td> </tr> <tr> <td>SSID</td> <td>Airtouch-wuzh01</td> </tr> <tr> <td>Channel</td> <td>11</td> </tr> <tr> <td>Mode</td> <td>auto</td> </tr> <tr> <td>MAC Address</td> <td>00:12:61:FE:FE:FF</td> </tr> <tr> <td>WDS</td> <td>Disable</td> </tr> </table>	WLAN	Enable	SSID	Airtouch-wuzh01	Channel	11	Mode	auto	MAC Address	00:12:61:FE:FE:FF	WDS	Disable
WLAN	Enable												
SSID	Airtouch-wuzh01												
Channel	11												
Mode	auto												
MAC Address	00:12:61:FE:FE:FF												
WDS	Disable												

Figure 2-6

## 2.7 Viewing WAN Status

To view the WAN status, perform the following steps:

1. Choose **Overview**;
2. In the **WAN Status** area, view the information about WAN, such as Connect Mode, MAC Address, IP Address, Subnet Mask, Gateway, DNS Server, Online time, DL&UL Data Rate. As shown in Figure 2-7.



Figure 2-7

## 2.8 Viewing Throughput Statistics

To view the throughput statistics, perform the following steps:

1. Choose **Overview**;
2. In the **Throughput Statistics** area, view the throughput statistics, such as WAN throughput and LAN throughput. As shown in Figure 2-8.

Port	Received				Sent			
	Total Traffic	Packets	Errors	Dropped	Total Traffic	Packets	Errors	Dropped
WAN	0 Bytes	0	0	0	0 Bytes	0	0	0
LAN	59 KB	485	0	0	131 KB	339	0	0

Figure 2-8

## 2.9 Viewing Device List

To view the device list, 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 2-9.

Index	Device Name	MAC Address	IP Address	Lease Time	Type
1	jingjin-PC	c0f8:da:ab:38:64	192.168.1.173	0days 11:59:51	WIFI

Figure 2-9

# 3 Network Setting

## 3.1 WAN Setting

### 3.1.1 Network Mode

To set the network mode, perform the following steps:

1. Choose **Network Setting>WAN Settings**;
2. In the **Network Mode** area, select a mode between **LTE** and **Ethernet**;
3. Click **Submit**. As shown in Figure 3-1.

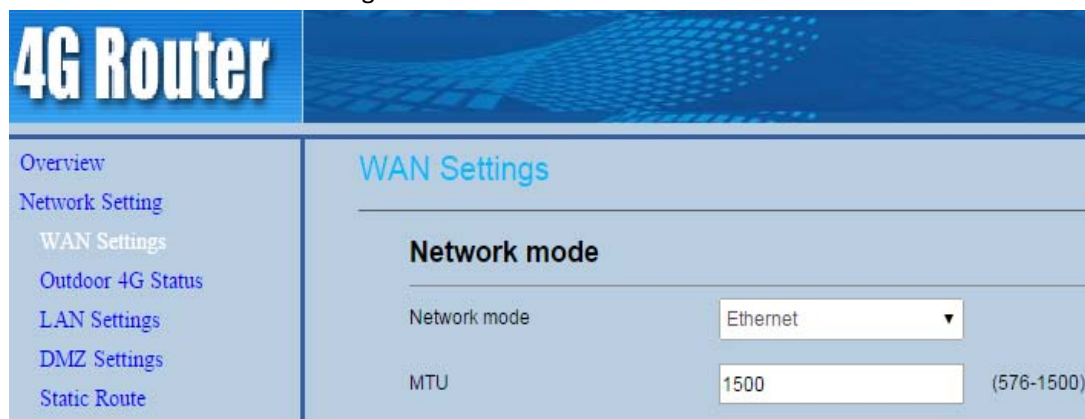


Figure 3-1

### 3.1.2 MTU Setting

To set the WAN MTU size, perform the following steps:

1. Choose **Network Setting>WAN Settings**;
2. In the **Network mode** area, you can configure the MTU size;
3. Click **Submit**. As shown in Figure 3-2.

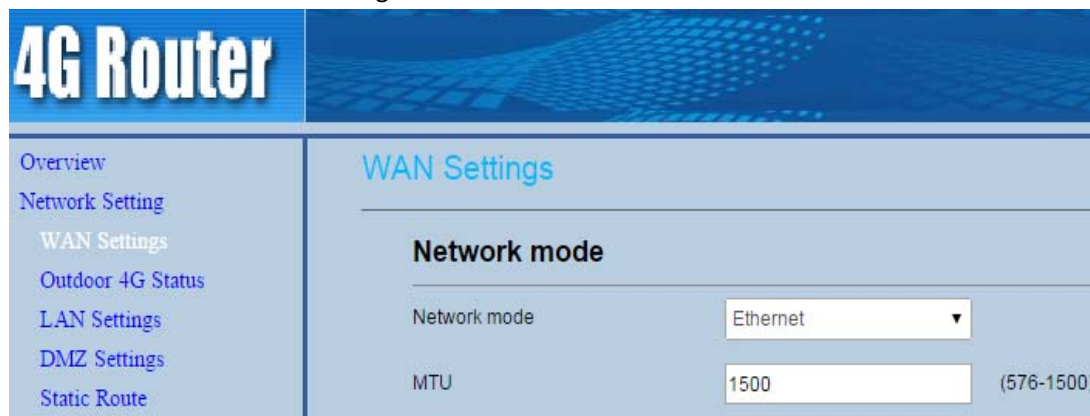


Figure 3-2

### 3.1.3 Setting Connect ODU

To set the WAN connect ODU, perform the following steps:

1. Choose **Network Setting>WAN Settings**;
2. In the **Settings** area, enable Connect ODU;
3. Click **Submit**. As shown in Figure 3-3.

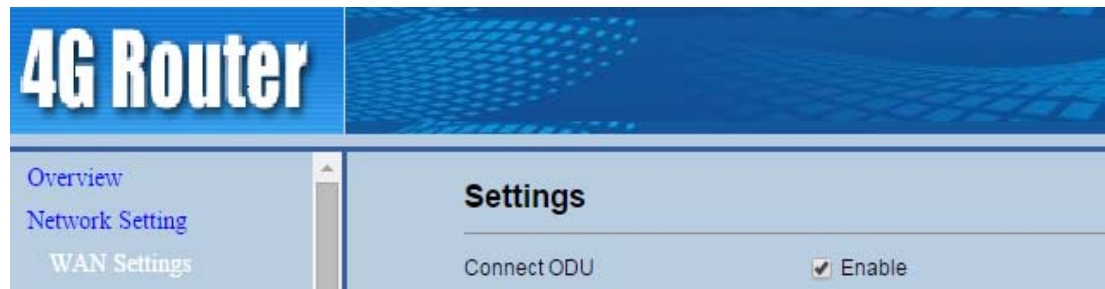


Figure 3-3

### 3.1.4 WAN Network Parameters Setting

Set WAN connect mode as DHCP, perform the following steps:

1. Choose **Network Setting>WAN Settings**;
2. In the **Settings** area, Set connect mode as **DHCP IP**;
3. Click **Submit**. As shown in Figure 3-4.

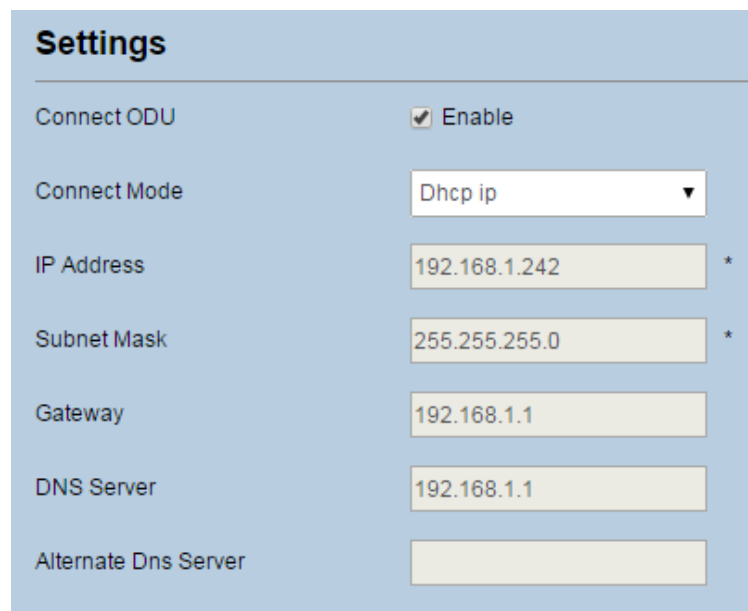


Figure 3-4

Set WAN connect mode as Static IP, perform the following steps:

1. Choose **Network Setting>WAN Settings**;
2. In the **Settings** area, Set connect mode as **Static IP**;
3. Setting IP address, Subnet mask, Gateway and DNS;
4. Click **Submit**. As shown in Figure 3-5.

The screenshot shows a 'Settings' page with the following configuration options:

Setting	Value
Connect ODU	<input checked="" type="checkbox"/> Enable
Connect Mode	Static IP
IP Address	192.168.1.242 *
Subnet Mask	255.255.255.0 *
Gateway	192.168.1.1
DNS Server	192.168.1.1
Alternate Dns Server	

Figure 3-5

### 3.2 Outdoor 4G Status

To view the outdoor 4G status, perform the following steps:

1. Choose **Network Setting>Outdoor 4G Status**;
2. In the **Outdoor 4G Status** area, you can also view the network information such as connect mode, IMSI, RSSI, frequency, DL&UL MCS, RSRP, RSRQ, CINR, SINR, TxPower, Cell ID, PCI, MCC and MNC. As shown in Figure 3-6.

Outdoor 4G Status	
Status	
Status	Connected
IMSI	460001641243191
RSSI	-57 dBm
DL MCS	1
UL MCS	22
DL Frequency	2585000 KHz
UL Frequency	2585000 KHz
Bandwidth	20000 KHz
RSRP0	-97 dBm
RSRP1	-88 dBm
RSRQ	-11 dB
SINR	4 dB
CINR0	-6 dB
CINR1	0 dB

Figure 3-6

## 3.3 LAN Setting

### 3.3.1 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.

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

1. Choose **Network Setting**>**LAN Settings**.
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**. As shown in Figure 3-7.

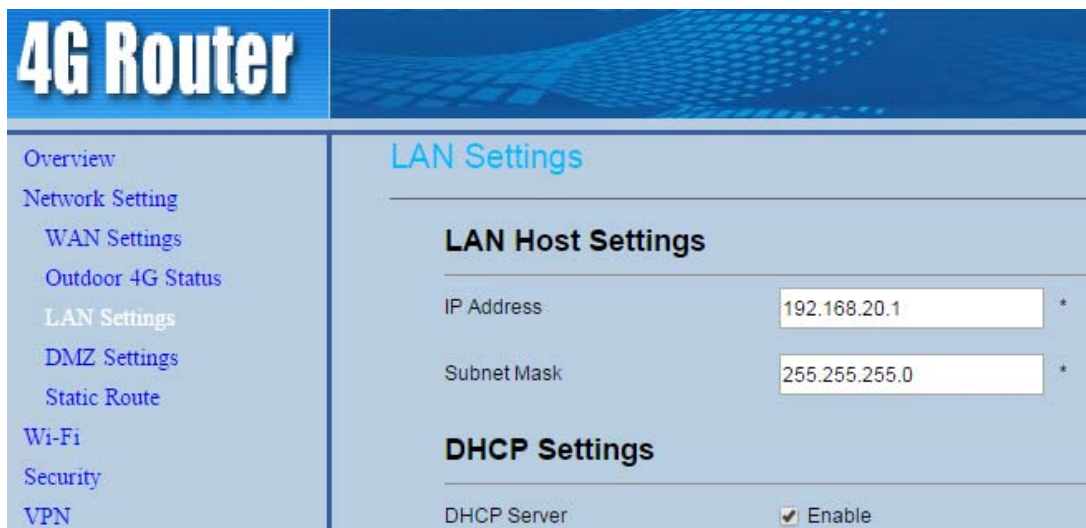


Figure 3-7

### 3.3.2 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 Setting** > **LAN Settings**.
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**. As shown in Figure 3-8.

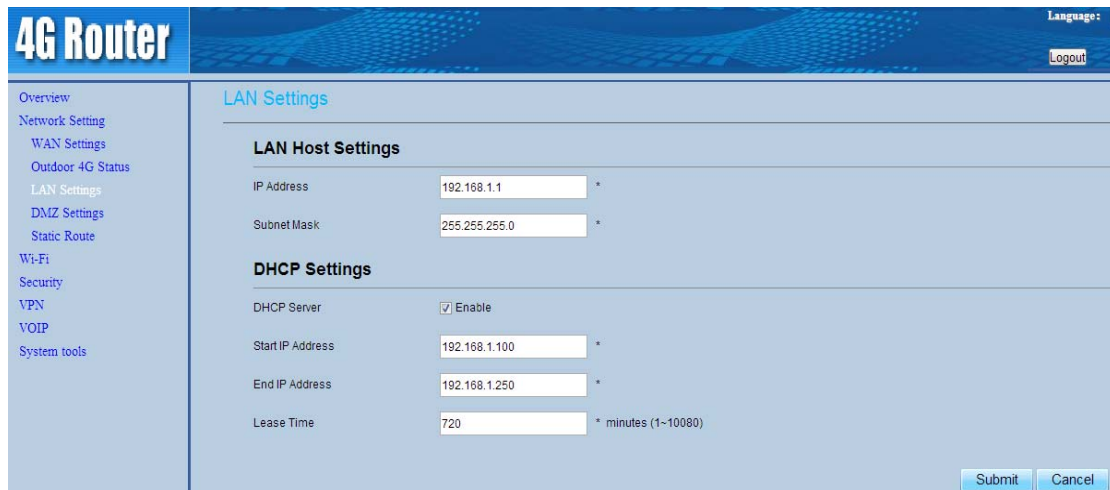


Figure 3-8

### 3.3.3 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.

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

1. Choose **Network Setting > LAN Settings**.
2. Click **Add list**.
3. Set the **MAC address** and **IP Address**.
4. Click **Submit**. As shown in Figure 3-9.

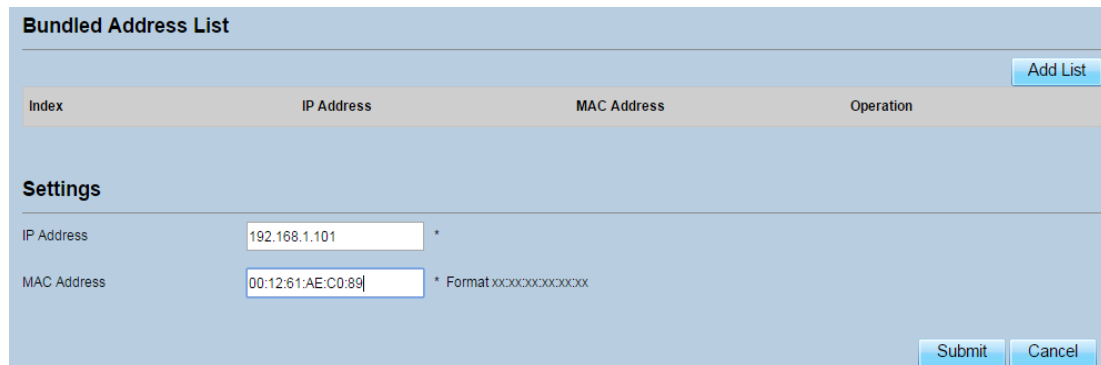


Figure 3-9

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

1. Choose **Network Setting > LAN Settings**.
2. Choose the item to be modified, and click **Edit**.
3. Set the **MAC address** and **IP Address**.
4. Click **Submit**. As shown in Figure 3-10.



**Bundled Address List**

[Add List](#)

Index	IP Address	MAC Address	Operation
1	192.168.20.101	00:12:61:AE:C0:89	<a href="#">Delete</a>   <a href="#">Edit</a>

**Settings**

IP Address:  \*

MAC Address:  \* Format:xxxxxxxxxxxx

[Submit](#) [Cancel](#)

Figure 3-10

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

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

### 3.4DMZ 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 Setting > 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 3-11.

**4G Router** Language: [Logout](#)

Overview  
 Network Setting  
 WAN Settings  
 Outdoor 4G Status  
 LAN Settings  
 DMZ Settings  
 Static Route  
 Wi-Fi  
 Security  
 VPN  
 VOIP  
 System tools

**DMZ Settings**

**DMZ**

DMZ  Enable

ICMP Redirect  Enable

Host Address  \*

[Submit](#) [Cancel](#)

Figure 3-11

## 3.5 Static Route

### 3.5.1 Add Static Route

To add a static route, perform the following steps:

1. Choose **Network Setting>Static Route**.
2. Click **Add list**.
3. Set the **Dest IP address** and **Subnet mask**.
4. Select an **Interface** from the drop-down list.
5. If you select **LAN** as the interface, you need set a Gateway.
6. Click **Submit**. As shown in Figure 3-12.

The screenshot displays the '4G Router' web interface. On the left is a navigation menu with options: Overview, Network Setting (selected), WAN Settings, Outdoor 4G Status, LAN Settings, DMZ Settings, Static Route, Wi-Fi, Security, VPN, VOIP, and System tools. The main content area is titled 'Static Route List' and contains an 'Add List' button. Below this is a table with columns: Index, Dest IP Address, Subnet Mask, Interface, Gateway, Status, and Operation. Underneath the table is the 'Static Route Settings' section, which includes four input fields: 'Dest IP Address' (202.100.14.202), 'Subnet Mask' (255.255.255.255), 'Interface' (LAN), and 'Gateway' (192.168.20.1). Each field has an asterisk to its right. At the bottom right of the settings section are 'Submit' and 'Cancel' buttons.

Figure 3-12

### 3.5.2 Modify Static Route

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

1. Choose **Security>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**. As shown in Figure 3-13.

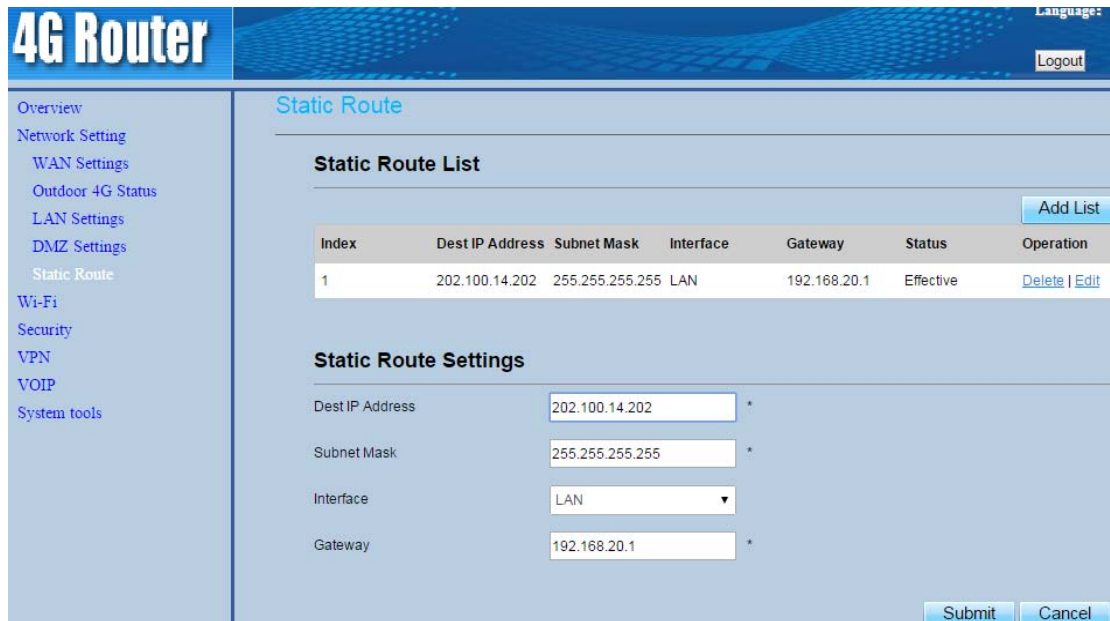


Figure 3-13

### 3.5.3 Delete Static Route

To delete a static route, perform the following steps:

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

## 4 Wi-Fi

### 4.1 WLAN Setting

This function enables you to configure the Wi-Fi parameters.

#### 4.1.1 Setting General Parameters

To configure the general Wi-Fi settings, perform the following steps:

1. Choose **Wi-Fi > Wi-Fi Settings**.
2. In the **General Settings** area, set WLAN to **Enable**.
3. Set **Mode** to one of the values described in the following table:

Parameter Value	Description
802.11b/g/n	The Wi-Fi client can connect to the CPE in 802.11b, 802.11g, or 802.11n mode. If the client connects to the CPE in 802.11n mode, the Advanced Encryption Standard (AES)

	encryption mode is required.
802.11b/g	The Wi-Fi client can connect to the CPE in 802.11b or 802.11g mode.
802.11b	The Wi-Fi client can connect to the CPE in 802.11b mode.
802.11g	The Wi-Fi client can connect to the CPE in 802.11g mode.

4. Set the **Channel No.** from 1 to 11.
5. Click **Submit**. As shown in Figure 4-1.

**General Settings**

WLAN  Enable

Mode

Channel

Figure 4-1

## 4.1.2 WPS Settings

Wi-Fi Protected Setup (WPS) enables you to simply add a wireless client to the network without needing to specifically configure the wireless settings, such as the SSID, security mode and passphrase. You can use either the WPS button or PIN to add the wireless client.

To configure Wi-Fi WPS settings, perform the following steps:

1. Choose **Wi-Fi > WPS Settings**.
2. Set **WPS** to **Enable**.
3. Click **Submit**. As shown in Figure 4-2.

**WPS Settings**

WPS  Enable

Figure 4-2

## 4.2 Setting SSID Profile

After you configure the CPE on the **SSID Profile** page, the Wi-Fi client connects to the CPE based on preset rules, improving access security.

To configure the CPE on the **SSID Profile** page, perform the following steps:

1. Choose **Wi-Fi > Wi-Fi Settings**.
2. Set **SSID**.

The SSID can contain 1 to 32 ASCII characters. It cannot be empty and the last character cannot be a blank character. In addition, the SSID cannot contain the following special characters: / ' = " \ &

The Wi-Fi client connects to the CPE using the found SSID.

3. Set **Maximum number of devices**.

This parameter indicates the maximum number of Wi-Fi clients that connect to the CPE. A maximum of 32 clients can connect to the CPE.

4. Set **Hide SSID broadcast** to **Enable**.

If the SSID is hidden, the client cannot detect the CPE's Wi-Fi information.

5. Set **AP isolation** to **Enable**.

The clients can connect to the CPE but cannot communicate with each other.

6. Set **Security**.

If **Security** is set to **NONE (not recommended)**, Wi-Fi clients directly connect to the CPE. This security level is low.

If **Security** is set to **WEP**, Wi-Fi clients connect to the CPE in web-based encryption mode.

If **Security** is set to **WPA-PSK**, Wi-Fi clients connect to the CPE in WPA-PSK encryption mode.

If **Security** is set to **WPA2-PSK**, Wi-Fi clients connect to the CPE in WPA2-PSK encryption mode. This mode is recommended because it has a high security level.

If **Security** is set to **WPA-PSK & WPA2-PSK**, Wi-Fi clients connect to the CPE in WPA-PSK&WPA2-PSK encryption mode.

7. Set the encryption mode.

If...	Sets to	Description
WEP	Authentication mode	<ul style="list-style-type: none"> <li>● <b>Shared authentication:</b> The client connects to the CPE in shared authentication mode.</li> <li>● <b>Open authentication:</b> The client connects to the CPE in open authentication mode.</li> <li>● <b>Both:</b> The client connects to the CPE in shared or open authentication mode.</li> </ul>
	Encryption password length	<ul style="list-style-type: none"> <li>● <b>128bit:</b> Only 13 ASCII characters or 26 hex characters can be entered in the <b>Key 1</b> to <b>Key 4</b> boxes.</li> <li>● <b>64bit:</b> Only 5 ASCII characters or 10 hex characters can be entered in the <b>Key 1</b> to <b>Key 4</b> boxes.</li> </ul>
	Current password index	This value can be set to <b>1, 2, 3, or 4</b> . After a key index is selected, the corresponding key takes effect.
WPA-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to <b>TKIP+AES, AES, or TKIP</b> .
WPA2-PSK(recommended)	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to <b>TKIP+AES, AES, or</b>

		<b>TKIP.</b>
WPA-PSK & WPA2-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to <b>TKIP+AES, AES, or TKIP.</b>

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

Figure 4-3

## 4.3 Access Management

### 4.3.1 Setting the Access Policy

This function enables you to set access restriction policies for each SSID to manage access to the CPE.

To configure Wi-Fi MAC control settings, perform the following steps:

1. Choose **Wi-Fi > Access Management**.
2. In the **WLAN Access List Settings** area, set Access Policy.  
The access policy can be set to **Disable, Blacklist** or **Whitelist**.
  - If SSID's MAC Access is set to **Disable**, access restrictions do not take effect.
  - If SSID's MAC Access is set to **Blacklist**, only the devices that are not in the blacklist can connect to the CPE.
  - If SSID's MAC Access is set to **Whitelist**, only the devices in the whitelist can connect to the CPE.
3. Click **Submit**. As shown in Figure 4-4.



**WLAN Access List Settings**

Settings  Disable  Whitelist  Blacklist

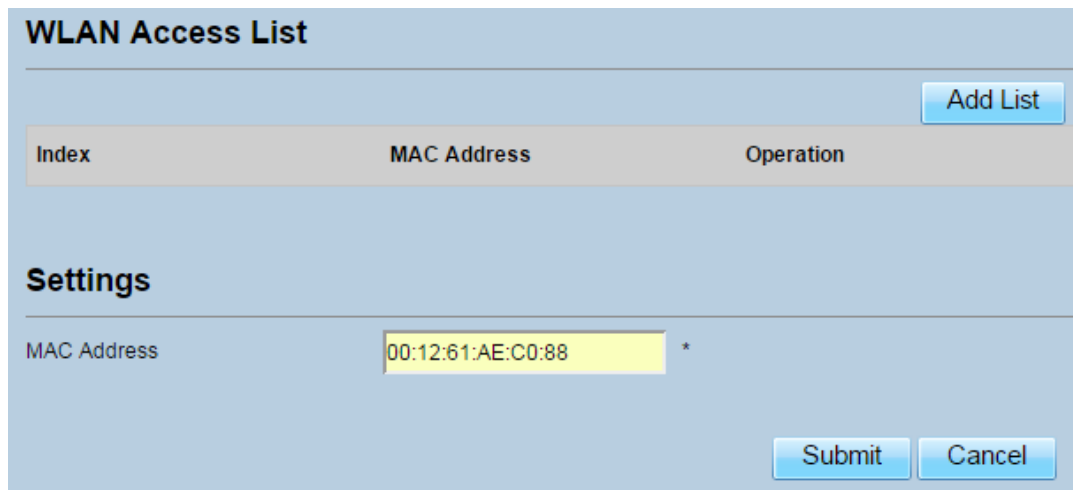
Submit

Figure 4-4

### 4.3.2 Managing the Wi-Fi Access List

This function enables you to set the SSID access policies based on MAC addresses. To add an item to the Wi-Fi access list, perform the following steps:

1. Choose **Wi-Fi > Access Management**.
2. Click **Add**.
3. Set **MAC address**.
4. Click **Submit**. As shown in Figure 4-5.



**WLAN Access List**

Add List

Index	MAC Address	Operation
Settings		
MAC Address	00:12:61:AE:C0:88 *	

Submit Cancel

Figure 4-5

To modify an item in the Wi-Fi access list, perform the following steps:

1. Choose **Wi-Fi > Access Management**.
2. Click **Edit MAC List**.
3. Choose the item to be modified, and click **Edit**.
4. Set MAC address.
5. Set one of the SSID to **Enable** to make the MAC address take effect for the SSID.
6. Click **Submit**. As shown in Figure 4-6.

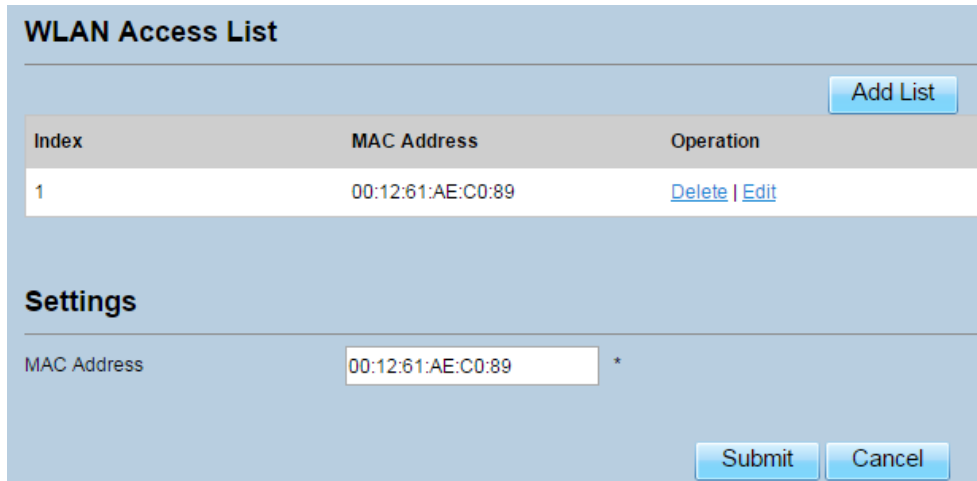


Figure 4-6

To delete an item from the Wi-Fi access list, perform the following steps:

1. Choose **Wi-Fi > Access Management**.
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 4-7.

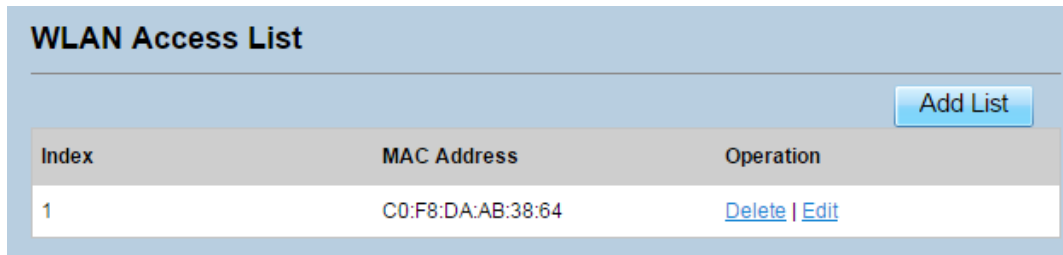


Figure 4-7

## 4.4 WDS

The CPE supports the wireless distribution system (WDS). All Wi-Fi devices in a WDS must be configured to use the same radio channel, encryption mode, SSID, and encryption key. You can set the WDS encryption mode to NONE or WPA/WPA2. If you set the WDS encryption mode to NONE, the Wi-Fi clients can use NONE or WEP encryption mode. If you set the WDS encryption mode to WPA/WPA2-PSK, the Wi-Fi clients can use WPA/WPA2-PSK encryption mode. After WDS is enabled, disable DHCP on CPEs that are not directly connected to the WAN port.

If WDS is enabled, the WPS function will not take effect. If the channel is set to **Auto**, you need to set the channel.

To configure the WDS, perform the following steps:

1. Choose **Wi-Fi > WDS**.
2. Set **WDS** to **Enable**.
3. Set WDS Mode as **Repeater Mode**;
4. Click **Scan**.  
From the search results, choose the SSID of the networking device.
5. Set **Security**.  
**WPA-PSK** can contain 8 to 63 ASCII characters or 64 hex characters.



6. Click **Submit**. As shown in Figure 4-8.

**Settings**

Enable  Enable

WDS Mode

Scan

Index	SSID	BSSID	Select
1	Airtouch-FE9F	00:12:61:fe:fe:ff	<input type="radio"/>
2	CMCC-WEB	30:49:3b:02:eb:9b	<input checked="" type="radio"/>
3	CMCC-CAOHEJING	36:49:3b:02:eb:9b	<input type="radio"/>
4	hello 1xe91w871x911ve61x981x8elwe61xb41x99	ea:06:e6:22:53:dc	<input type="radio"/>

SSID  \*

BSSID  \*

Security:

WPA-PSK  \* (8-63 ASCII characters or 8-64 hexadecimal characters)

Figure 4-8

## 5 Security

### 5.1 MAC Filtering

This page enables you to configure the MAC address filtering rules.

#### 5.1.1 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**. As shown in Figure 5-1.

**MAC Filtering Manager**

MAC Filtering  Enable

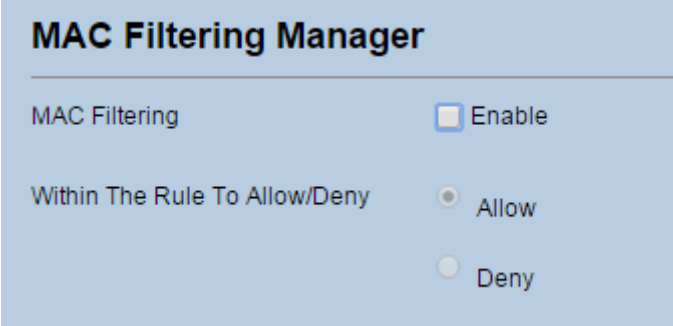
Within The Rule To Allow/Deny  Allow  Deny

Figure 5-1

## 5.1.2 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**. As shown in Figure 5-2.



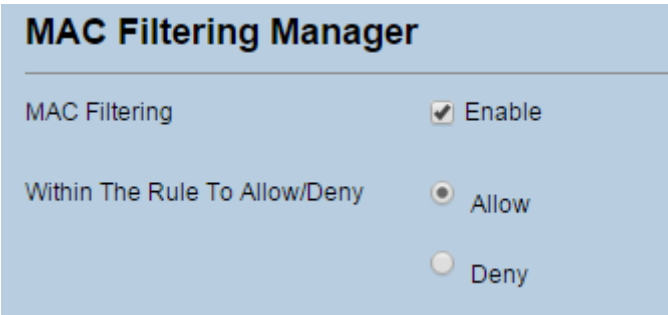
The screenshot shows the 'MAC Filtering Manager' interface. It has a title bar 'MAC Filtering Manager'. Below the title bar, there are two rows of settings. The first row is 'MAC Filtering' with a checkbox that is unchecked, followed by the text 'Enable'. The second row is 'Within The Rule To Allow/Deny' with two radio buttons. The 'Allow' radio button is selected, and the 'Deny' radio button is unselected.

Figure 5-2

## 5.1.3 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**. As shown in Figure 5-3.



The screenshot shows the 'MAC Filtering Manager' interface. It has a title bar 'MAC Filtering Manager'. Below the title bar, there are two rows of settings. The first row is 'MAC Filtering' with a checkbox that is checked, followed by the text 'Enable'. The second row is 'Within The Rule To Allow/Deny' with two radio buttons. The 'Allow' radio button is selected, and the 'Deny' radio button is unselected.

Figure 5-3

## 5.1.4 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**. As shown in Figure 5-4.

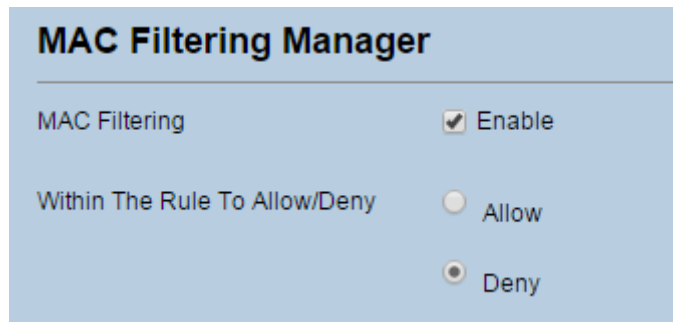


Figure 5-4

### 5.1.5 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**. As shown in Figure 5-5.

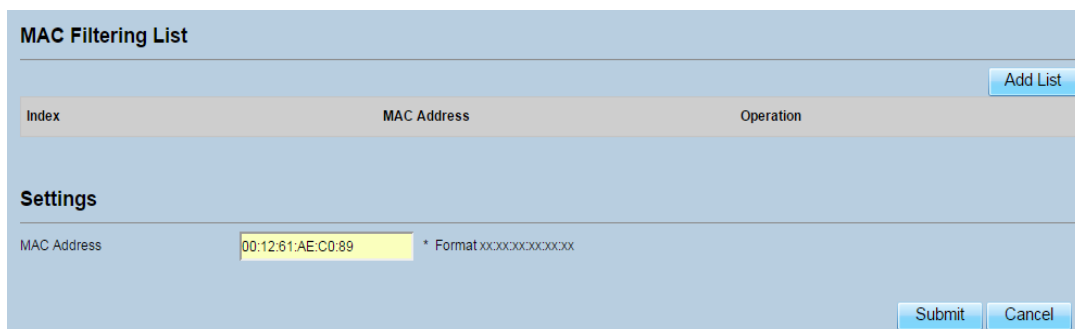


Figure 5-5

### 5.1.6 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**. As shown in Figure 5-6.

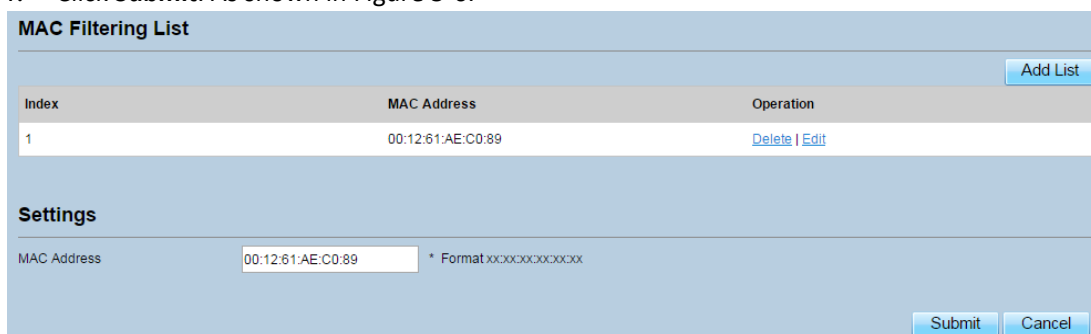
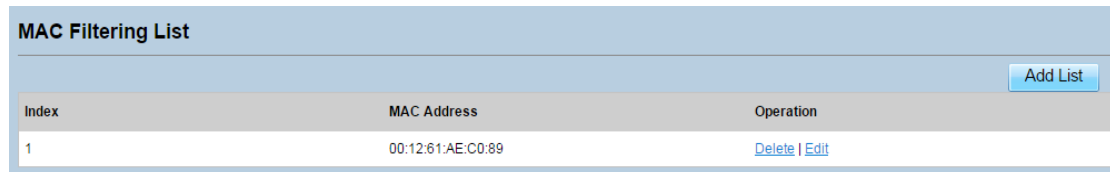


Figure 5-6

## 5.1.7 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**. As shown in Figure 5-7.



The screenshot shows a web interface titled "MAC Filtering List". At the top right, there is a blue button labeled "Add List". Below this is a table with three columns: "Index", "MAC Address", and "Operation". The table contains one row with the following data:

Index	MAC Address	Operation
1	00:12:61:AE:C0:89	<a href="#">Delete</a>   <a href="#">Edit</a>

Figure 5-7

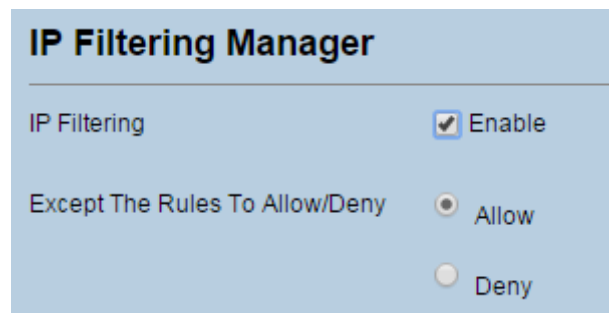
## 5.2 IP Filtering

Data is filtered by IP address. This page enables you to configure the IP address filtering rules.

### 5.2.1 Enabling IP Filtering

To enable IP Filtering, perform the following steps:

1. Choose **Security>IP Filtering**.
2. Set IP Filtering **Enable**.
3. Click **Submit**. As shown in Figure 5-8.



The screenshot shows a web interface titled "IP Filtering Manager". It contains the following configuration options:

- IP Filtering**:  Enable
- Except The Rules To Allow/Deny**:  Allow,  Deny

Figure 5-8

### 5.2.2 Disabling IP Filtering

To disable IP Filtering, perform the following steps:

1. Choose **Security>IP Filtering**.
2. Set IP Filtering **Disable**.
3. Click **Submit**. As shown in Figure 5-9.

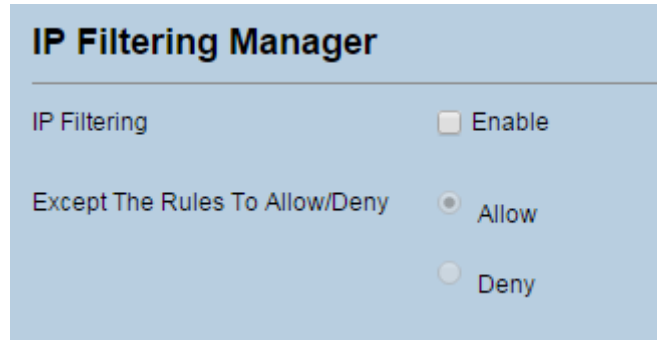


Figure 5-9

### 5.2.3 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**. As shown in Figure 5-10.

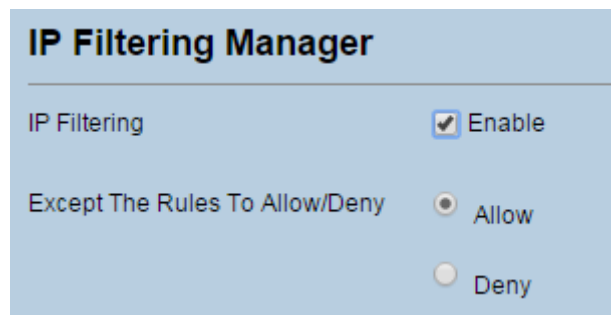


Figure 5-10

### 5.2.4 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**. As shown in Figure 5-11.

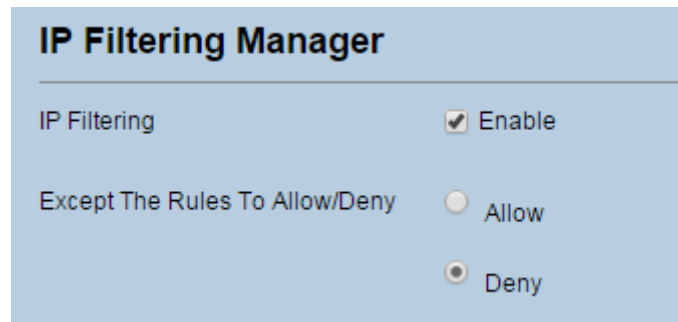


Figure 5-11

## 5.2.5 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**. As shown in Figure 5-12.

The screenshot displays the 'IP Filtering List' configuration page. At the top right is an 'Add List' button. Below it is a table with the following columns: Index, Protocol, Source IP Address Range, Source Port Range, Destination IP Address Range, Destination Port Range, Status, and Operation. Underneath the table is a 'Settings' section with the following fields:

- Service: Custom (dropdown)
- Protocol: ALL (dropdown)
- Source IP Address Range: 192.168.1.20 (text input, with format hint: (Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32])
- Source Port Range: (empty text input, with format hint: (Format: 1000-1500 Or 1000))
- Destination IP Address Range: 112.64.102.13 (text input, with format hint: (Format: x.x.x.x Or x.x.x.x/Mask) Mask Value is [0,32])
- Destination Port Range: (empty text input, with format hint: (Format: 1000-1500 Or 1000))
- Status: Allow (dropdown)

At the bottom right of the settings section are 'Submit' and 'Cancel' buttons.

Figure 5-12

## 5.2.6 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**. As shown in Figure 5-13.

**IP Filtering List**

[Add List](#)

Index	Protocol	Source IP Address Range	Source Port Range	Destination IP Address Range	Destination Port Range	Status	Operation
1	ALL	192.168.1.20		112.64.102.13		Allow	<a href="#">Delete</a>   <a href="#">Edit</a>

**Settings**

Service:

Protocol:

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:

[Submit](#) [Cancel](#)

Figure 5-13

## 5.2.7 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**. As shown in Figure 5-14.

**IP Filtering List**

[Add List](#)

Index	Protocol	Source IP Address Range	Source Port Range	Destination IP Address Range	Destination Port Range	Status	Operation
1	ALL	192.168.1.20		112.64.102.13		Allow	<a href="#">Delete</a>   <a href="#">Edit</a>

Figure 5-14

## 5.3 URL Filtering

Data is filtered by uniform resource locator (URL). This page enables you to configure URL filtering rules.

### 5.3.1 Enabling URL Filtering

To enable URL Filtering, perform the following steps:

3. Choose **Security>URL Filtering**.
4. Set **URL Filtering** to **Enable**.
5. Click **Submit**. As shown in Figure 5-15.

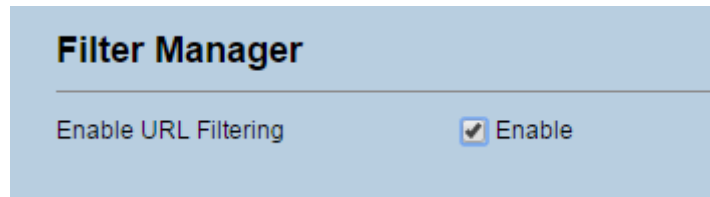


Figure 5-15

### 5.3.2 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**. As shown in Figure 5-16.

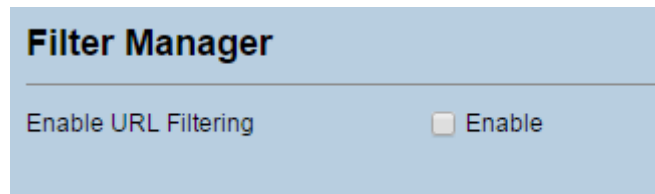


Figure 5-16

### 5.3.3 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**. As shown in Figure 5-17.

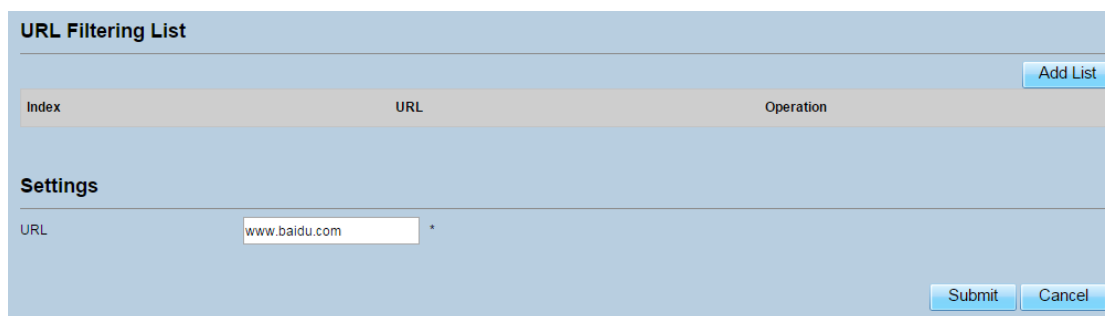


Figure 5-17

### 5.3.4 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**. As shown in Figure 5-18.

Index	URL	Operation
1	www.baidu.com	<a href="#">Delete</a>   <a href="#">Edit</a>

Settings

URL  \*

[Submit](#) [Cancel](#)

Figure 5-18

### 5.3.5 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**. As shown in Figure 5-19.

Index	URL	Operation
1	www.baidu.com	<a href="#">Delete</a>   <a href="#">Edit</a>

Figure 5-19

## 5.4 Port 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.

### 5.4.1 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**. As shown in Figure 5-20.

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
-------	----------	-------------------	------------	------------	-----------

**Settings**

Service: Custom

Protocol: TCP

Remote Port Range: 2000 \* (Format: 1000-1500 Or 1000)

Local Host: 192.168.1.20 \*

Local Port: 3000 \*

Submit Cancel

Figure 5-20

## 5.4.2 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 through 7 in the previous procedure.
4. Click **Submit**. As shown in Figure 5-21.

**Port Forwarding List** [Add List](#)

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	2000	192.168.1.20	3000	<a href="#">Delete</a>   <a href="#">Edit</a>

**Settings**

Service:  ▼

Protocol:  ▼

Remote Port Range:  \* (Format: 1000-1500 Or 1000)

Local Host:  \*

Local Port:  \*

[Submit](#) [Cancel](#)

Figure 5-21

### 5.4.3 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**. As shown in Figure 5-22.

**Port Forwarding List** [Add List](#)

Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	2000	192.168.1.20	3000	<a href="#">Delete</a>   <a href="#">Edit</a>

Figure 5-22

## 5.5 UPnP

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 5-23.

UPnP

**Settings**

UPnP  Enable

Submit

**Current UPNP Status**

Index	Description	Protocol	IP Address	External Port	Internal port
-------	-------------	----------	------------	---------------	---------------

Figure 5-23

## 6 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 6-1.

**VPN Settings**

VPN  Enable

Protocol PPTP

VPN Server 112.64.102.14 \*

Username admin \*

Password .....

**VPN Status**

Username	Local Address	Remote Address	Online Time
----------	---------------	----------------	-------------

Submit Cancel

Figure 6-1

## 7 VOIP

The CPE supports voice services based on the Session Initiation Protocol (SIP) and enables voice service interworking between the Internet and Public Switched Telephone Networks (PSTNs).

### 7.1 View VOIP Information

To view VOIP information, perform the following steps:

1. Choose **VOIP > VOIP Information**;
2. View the **VOIP information**, such as the SIP account and status of the SIP registration server.  
As shown in Figure 7-1.

VoIP Information	
SIP Account	1000
Registration Status	FAILED_OTHER
Line Status	Unknown or undefined

Figure 7-1

## 7.2 Configuring SIP Server

To set the SIP server parameters, perform the following steps:

1. Choose **VOIP > SIP Server**;
2. In the **User Agent port** box, enter the port of the SIP account provided by your service provider.
3. In the **SIP server domain name** box, enter the domain name of the SIP server.
4. In the **Proxy server address** box, enter the address of the proxy server provided by your service provider, for example, **192.168.1.10**.
5. In the **Proxy server port** box, enter the port of the proxy server provided by your service provider, for example, **5060**. The value ranges from 1 to 65535.
6. In the **Registration server address** box, enter the address of the registration server provided by your service provider, for example, **192.168.1.11**.
7. In the **Registration server port** box, enter the port of the registration server provided by your service provider, for example, **5060**. The value ranges from 1 to 65535.
8. Click **Submit**. As shown in Figure 7-2.

Sip Local Port	
User Agent port	<input type="text" value="5060"/> * (1-65535)
Registration Server	
SIP server domain name	<input type="text" value="192.168.1.100"/> * (IP address or domain name)
Proxy server address	<input type="text" value="192.168.1.100"/> * (IP address or domain name)
Proxy server port	<input type="text" value="5060"/> * (1-65535)
Registration server address	<input type="text" value="192.168.1.100"/> * (IP address or domain name)
Registration server port	<input type="text" value="5060"/> * (1-65535)

Figure 7-2

## 7.3 Configuring SIP Account

Before configuring SIP accounts, make sure that the registration server has been properly configured.

To configure SIP account, perform the following steps:

1. Choose **VoIP > SIP Account**.
2. Set SIP Account Enable.
3. In the **User name** and **Password** boxes, enter the user name and password of the SIP account provided by your service provider.
4. In the **Phone Number** box, enter the SIP Phone number provided by your service provider.
5. In the Display Name box, enter the display name provided by your service provider.
6. In the Codec Priority area, set the codec priority.
7. Click **Submit**. As shown in Figure 7-3.

SIP Account	
Enable	<input checked="" type="checkbox"/> Enable
Username	<input type="text" value="1000"/> * (a maximum of 32 characters)
Password	<input type="password" value="****"/> * (a maximum of 32 characters)
Phone Number	<input type="text" value="1000"/> * (a maximum of 32 digits)
Display Name	<input type="text" value="1000"/> * (a maximum of 32 characters)
Codec Priority	
Priority - 1	<input type="text" value="PCMU"/>
Priority - 2	<input type="text" value="PCMA"/>
Priority - 3	<input type="text" value="G723"/>
Priority - 4	<input type="text" value="G729"/>
Priority - 5	<input type="text" value="G722"/>

Figure 7-3

## 8 System

### 8.1 Maintenance

#### 8.1.1 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**. As shown in Figure 8-1.  
The CPE then restarts.

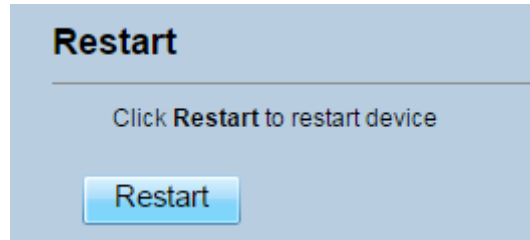


Figure 8-1

## 8.1.2 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**. As shown in Figure 8-2.  
The CPE is then restored to its default settings.

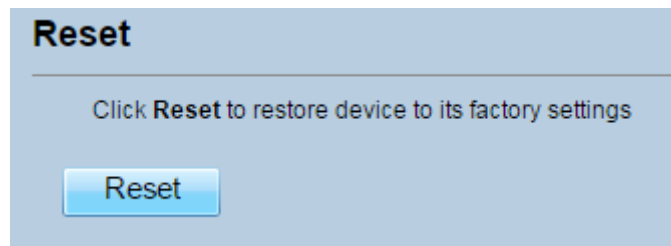


Figure 8-2

## 8.1.3 Backup 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**. As shown in Figure 8-3.

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

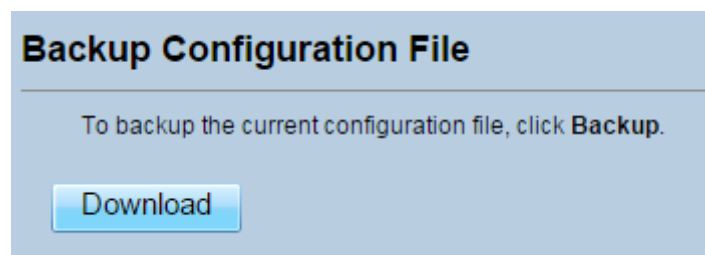


Figure 8-3

## 8.1.4 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 closes. 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**. As shown in Figure 8-4.

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

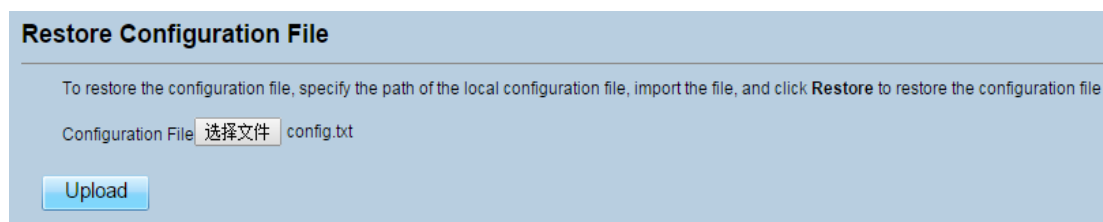


Figure 8-4

## 8.2 Version 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.

### 8.2.1 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 8-5.



Product Name	WD620
Running software version	IDU-1.1.9.2-zte_rp @ Mar 4 2015 16:13:01
Backup software version	IDU-1.1.9.3v-r317-Zte_rp @ Mar 21 2015 16:40:55

Figure 8-5




## 8.2.2 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 closes. 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 8-6.

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

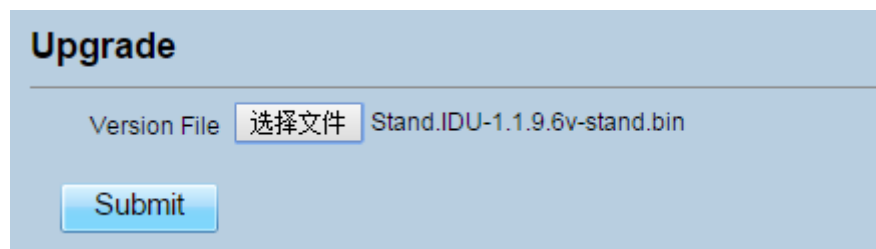


Figure 8-6

## 8.3 FTP auto upgrade

To perform a ftp auto upgrade successfully, make sure the CPE is connected to the Internet.

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**. As shown in Figure 8-7.



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

FTP Auto Upgrade

**Settings**

FTP Auto Upgrade  Enable

Check New FW after connected  Enable

Upgrade Folder  ftp://xxx

Version File  \*

Username  \*

Password  \*

Check New FW Every  24 hrs(1~740)

Start Time(24hrs)

Random Time

Figure 8-7

## 8.4TR069

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.

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**. As shown in Figure 8-8.

## Settings

Enable TR069	<input checked="" type="checkbox"/> Enable
ACS URL Source	URL
ACS URL	http://192.168.1.10:8080 * http://xxx
ACS Username	tr069 *
ACS Password	***** *
Enable Periodic Inform	<input checked="" type="checkbox"/> Enable
Periodic Inform Interval	3600 * (60-86400)seconds
Connection Request Username	tr069 *
Connection Request Password	***** *

Figure 8-8

## 8.5 Date & 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.

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**. As shown in Figure 8-9.

The screenshot shows a 'Settings' interface with a light blue background. At the top, the title 'Settings' is displayed. Below it, the 'Current Time' is shown as '2015-03-26 11:10:44'. There are two radio buttons: 'Set Manually' is selected, and 'Sync from Network' is unselected. Below the radio buttons, the 'Local Time' is displayed as '2015 / 03 / 26 / 11 / 10 / 44' in a grid of input fields, with '(YYYY/MM/DD/HH/MM/SS)' written below it. A blue 'Sync' button is located at the bottom center.

Figure 8-9

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**. As shown in Figure 8-10.

The screenshot shows the 'Settings' interface with 'Sync from Network' selected. The 'Current Time' remains '2015-03-26 11:10:44'. The 'Primary NTP Server' and 'Secondary NTP Server' are both set to 'asia.pool.ntp.org' via dropdown menus. The 'Optional NTP Server' checkbox is checked, and the IP address '192.168.1.10' is entered in the adjacent text field. The 'Time Zone' dropdown menu is set to '(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi'.

Figure 8-10

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**. As shown in Figure 8-11.

**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 8-11

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

## 8.6 DDNS

Dynamic Domain Name Server (DDNS) service is used to map the user's dynamic IP address to a fixed DNS service.

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**. As shown in Figure 8-12.

The image shows a configuration page titled "DDNS Settings". At the top, there is a section for "DDNS" with a checked checkbox labeled "Enable". Below this, there are five input fields: "Service Provider" is a dropdown menu showing "DynDNS.org"; "Domain" is a text box containing "mypersonaldomain.dyndns.c" with an asterisk to its right; "Username" is a text box containing "myusername" with an asterisk to its right; "Password" is a text box filled with dots, also with an asterisk to its right.

Figure 8-12

## 8.7 Diagnosis

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.

### 8.7.1 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](http://www.google.com).
4. Set **Packet size** and **Timeout**.
5. Set **Count**.
6. Click **Ping**. As shown in Figure 8-13.

Wait until the ping command is executed. The execution results are displayed in the Results box.

### Method

---

Method of Diagnostics

Ping

TraceRoute

### Ping

---

Target IP/Domain  \*

Packet Size  \* bytes (1~9000)

Timeout  \* seconds (1~10)

Count  \* times (1~10)

### Result

---

Result Failed

Details

```

PING 192.168.20.10 (192.168.20.10): 56 data bytes
--- 192.168.20.10 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss

```

Figure 8-13

## 8.7.2 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](http://www.google.com).
4. Set **Maximum hops** and **Timeout**.
5. Click **Traceroute**. As shown in Figure 8-14.

Wait until the traceroute command is executed. The execution results are displayed in the Results box.

### Method

Method of Diagnostics

Ping  
 TraceRoute

### Traceroute

Target IP/Domain  \*

Maximum Hops  \* (1~30)

Timeout  \* seconds (1~10)

### Result

Result **Pass**

Details

```

traceroute to 192.168.20.1 (192.168.20.1), 30 hops max, 38 byte
packets
1  ZMWR2500.Jan (192.168.20.1) 0.128 ms

```

Figure 8-14

## 8.8 Syslog

The syslog record user operations and key running events.

### 8.8.1 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**. As shown in Figure 8-15.



The image shows a web-based configuration interface for Syslog. The header is 'Syslog' in blue. Below it is a 'Settings' section. The 'Method' field has two radio buttons: 'Network' (unselected) and 'Local' (selected). The 'Level' field is a dropdown menu currently showing 'INFO'. At the bottom right are 'Submit' and 'Cancel' buttons.

Figure 8-15

### 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.

## 8.8.2 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 8-16.

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

**Syslog**

---

**Settings**

Method  Network  
 Local

Level

---

**Network**

Forward IP address  \*

Figure 8-16

## 8.9 Account

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.

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**. As shown in Figure 8-17.

The screenshot shows a web interface with a light blue background. At the top left, the word "Account" is written in blue. Below it, the section "Change Password" is highlighted in a darker blue. This section contains four input fields: "Username" with a dropdown menu showing "superadmin", "Current Password" with masked characters "\*\*\*\*\*" and an asterisk, "New Password" with masked characters "\*\*\*\*" and an asterisk followed by "(5-15 ASCII characters)", and "Confirm Password" with masked characters "\*\*\*\*\*" and an asterisk followed by "(5-15 ASCII characters)". To the right of these fields are two buttons: "Submit" and "Cancel". Below the "Change Password" section is the "Settings" section, which contains a checkbox labeled "Enable User" that is checked, followed by the text "Enable". To the right of this checkbox are two buttons: "Submit" and "Cancel".

Figure 8-17

## 8.10 Remote WEB Access

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

1. Choose **System > Remote WEB Access**.
2. Set **HTTP** enable. If you set HTTP disable, you will can't login the web management page with the HTTP protocol from WAN side.
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 from WAN side, 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. Click **Submit**. As shown in Figure 8-18.

**Remote Web Access Settings**

Http Access  Enable

HTTP Port  \* (80 , 1024-65534)

Https Access  Enable

HTTPs Port  \* (1-65534)

Figure 8-18

## 8.11 Logout

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

1. Choose **System** and click **Logout**
2. It will back to the login page.

## 9 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.