

Horizon 2100F12

LTE CBRS Outdoor CPE



Index


CHAPTER 1: Introduction.....	3
1 Introduction to Indoor CPE.....	3
2 Features & Specifications	3
3 Application Diagram.....	5
CHAPTER 2: Product Overview	5
1 Important Note for Using This Router	5
2 Packing List	5
3 Device Description.....	Error! Bookmark not defined.
3.1 Panel of router.....	5
1 Getting Started	7
1.1 Welcome to the CPE.....	7
1.2 Computer Configuration Requirements	7
1.3 Login the Web Management Page.....	7
2 Overview.....	9
2.1 Viewing Current Connection.....	9
2.2 Viewing LTE Status.....	9
2.3 Viewing WAN Status	10
3 Status.....	11
3.1 Statistics	11
3.2 WAN Status.....	12
3.3 LAN Status.....	14
4 Update	15
4.1 Version Manager	15
4.2 Auto upgrade	16
5 Settings.....	18
5.1 Device Information	18
5.2 Network.....	19
5.3 Ethernet.....	31
5.4 Parental Controls.....	32
5.5 Firewall	34
5.6 VPN.....	48
5.7 IPv6.....	49
5.8 System.....	50
FAQs	65

CHAPTER 1: Introduction

1 Introduction to Indoor CPE

2100F12 is a highly advanced LTE indoor multi-service product solution specifically designed to meet integrated data. The product supports advanced Gigabit networking with POE power. It enables wide service coverage and provides high data throughput and networking features to customers who needs rural easy broadband access, connectivity.

2 Features & Specifications















Made for the Outdoors
Last Mile Ready Fixed Wireless Access
LTE Outdoor CBRs Router

The Horizon 2100F12 is a secured, highly advanced, LTE outdoor multi-service CAT B CPE-CBSD designed to meet the needs of residential, business and enterprise users. Service providers can deliver high-speed broadband services to their customers over the last mile using the shared-spectrum of the CBRs over 4G technology.

Our device is FCC part 96 certified with an built-in SAS (Spectrum Access System) client to increase your service reach thanks to high-power signal transmissions and 4x4 MIMO high-gain directional antennas.

The rugged IP68 rated outdoor design enables it to work in rough weather and remote locations, can be installed in farms, manufacturing plants, stadiums, schools, hospitals, parks or anywhere requiring a robust wireless solution.

 CBRS Supports LTE band 48 (CBRS)	 IP68 IP68 hardened enclosure with industrial grade components
 LTE 3GPP Release 12 with up to 560 Mbps /30Mbps (DL/UL)	 High Temperature and Freeze resistant, protects from Rain, Sun, Snow, Frost and Flurry
 SAS High-power CPE-CBSD with built-in SAS client	 ESD 15KV ESD & Surge Protection
 Antenna Built-in 4x4 MIMO, high power dual- polarized and dual-slant directional antennas	 Mounting Easy install, Pole/Wall Mounting Kit Included
 PoE Standard Gigabit PoE Injector Included	 Management Remote Management supports TR-069, SNMP, FOTA, HTTP/Web GUI
 Mode Supports Bridge/Router Mode	 Security SECURE NETWORK with advanced VPN features

Below is the detail info about 2100F12

Basic Information	LTE CAT12 LTE-TDD: B48
	Downlink speeds up to 560Mbps // Uplink speeds up to 30Mbps
	Carrier Aggregation; up to 4 carriers downlink
	4x4 MIMO
	1.4MHz, 3MHz, 5MHz, 10MHz, 15MHz, 20MHz
	256QAM DL / 64QAM UL
	Maximum Transmit Power 23±2dBm (Power class 3)
	Four (4) internal directional antennas with high gain
	Maximum Peak Gain: Up to 16dBi
Operational Modes	Route Mode
	Bridge Mode / Supports remote management under bridge mode
	NAT mode
	Static Route
Network Protocols and Features	NAT, static routing
	Vlan in Bridge mode
	DMZ
	DNS relay, NTP and DDNS
	IGMP proxy
	Supports DHCP server
	Support VPN (PPTP/L2TPv2/L2TPv3/GRE L2/GRE L3)/VPN Passthrough
	ICMP supported
	Port Mirror and Port Forwarding
Quality of Service Control	LTE QoS Support
	Supports the DiffServ approach
Firewall	Built-in NAT Firewall
	SPI (Based on Iptables)
	Support DDOS
	Access Control (Parental Controls)
	IP Address Filtering, URL Filtering, MAC Filtering
	Firewall can be enabled or disabled via GUI
	Web-based GUI for remote and local management
	Up to 3 level of access account
	Firmware upgrade and configuration data upload/download via web GUI
	FOTA Upgrade
	Local/Remote device management and firmware update via TR069 and web GUI
	IPv4 only, IPv6 only, IPv4/IPv6 Dual Stack
Hardware Specifications	1 x USIM/SIM (2FF)
Physical Interface	4 LED Indicators, PWR, NET, SIM, SIG
Physical Specifications	Dimensions: 288mm x 288 mm x 82mm
	Weight: <2Kg
	IP Rating: IP68 Rated Enclosure
	Back Enclosure Material: SurTec Treated Die-Cast Alloy Enclosure
Operating Environment	Front Enclosure Material: PC 143R. Meets the standard of UL 746C
	-40°C to 60°C (-40°F to 140°F)
Certification	FCC Part 96 Authorized, FCC ID: 2ADX3-2100F12

3 Application Diagram



CHAPTER 2: Product Overview

1 Important Note for Using This Router



- 1, Do not remove, open or repair the case yourself. Contact with your Internet Service Provider or have it repaired at a qualified service center.
- 2, Do not plug and unplug SIM card when device is power on.

2 Packing List

Product Images







What's in the Box?

- Horizon 2100/F12 Router
- Quick Start Guide
- Power Adapter
- Gigabit PoE Injector
- Ethernet Cable
- Cable Gland
- Pole Mounting Kit

3 Panel of router



4 LED Indicators
(PWR, NET, SIM, RF Signal)

Outdoor Router		
 POWER	Steady on	Power On
	Off	No Power Supply
 INTERNET	Steady on	Internet Available
	Off	Internet Unavailable
	Blinking (500ms interval)	Data Transmission
 SIM	Steady on	SIM ready
	Off	No SIM detected
	Blinking (1sec interval)	SIM LOCK or PIN/PUK LOCK
 SIGNAL	Green	Signal strong
	Yellow	Signal good
	Red	Signal weak

CHAPTER 3: Software Features

1 Getting Started

1.1 Welcome to the CPE

In this document, the LTE (Long Term Evolution) CPE (customer premises equipment) will be short for 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">• 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	<ul style="list-style-type: none">• Internet Explorer 7.0 or later• Firefox 3.6 or later• Opera 10 or later• Safari 5 or later• Chrome 9 or later

1.3 Login the Web Management Page

Launch web browser to login 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://192.168.0.1> in the address bar, and press Enter. As shown in Figure 1-1.

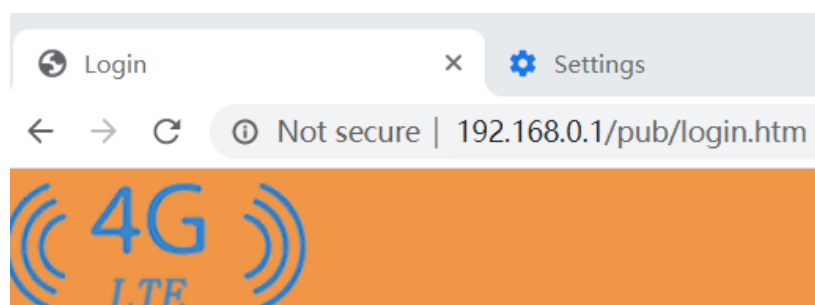


Figure 1-1

3. Enter the user name and password, and click Login.
4. You can login 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**. If you want to view or configure the CPE more, you should use the super account to log in to the web management page. The default super user name is **superadmin**, and the password is **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.

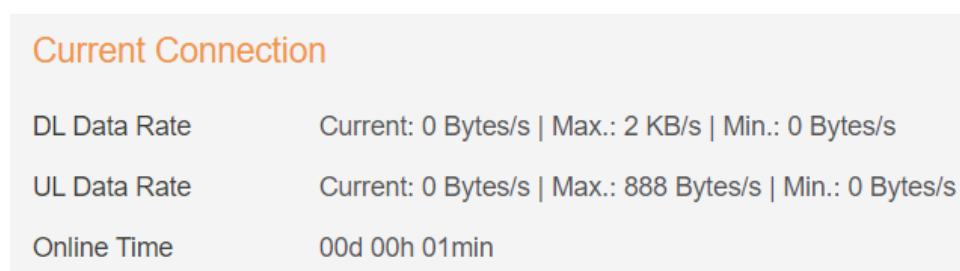
To ensure your data safety, it is recommended that you turn on the firewall, and conserve your login and FTP password carefully.

1 Overview

2.1 Viewing Current Connection

To view the current connection, perform the following steps:

1. Choose **Overview**;
2. In the **Current Connection** area, view the connection status, such as DL/UL Data Rate and Online time. As shown in Figure 2-1.



Current Connection	
DL Data Rate	Current: 0 Bytes/s Max.: 2 KB/s Min.: 0 Bytes/s
UL Data Rate	Current: 0 Bytes/s Max.: 888 Bytes/s Min.: 0 Bytes/s
Online Time	00d 00h 01min

Figure 2-1

2.3 Viewing LTE Status

To view the LTE network status, perform the following steps:

1. Choose **Overview**;
2. In the **LTE Status** area, view the information about Connect status, Mode, Cell ID, Signal quality and so on. As shown in Figure 2-3.

The screenshot displays the 'LTE Settings' interface. It is divided into two main sections: 'Settings' and 'Status'.

Settings Section:

- Status:** Connected
- Connect Method:** Auto (dropdown menu)
- Buttons:** Submit and Cancel

Status Section:

DL MCS	0
UL MCS	0
DL Frequency	2679.0 MHz
UL Frequency	2559.0 MHz
Bandwidth	20 MHz
RSSI	-53 dBm
RSRP0	-79 dBm
RSRP1	-77 dBm
RSRQ	-5 dB
SINR	32 dB
TX Power	-55 dBm

Figure 2-3

2.4 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 Connect Mode, IP, Subnet Mask, DNS Server and so on. As shown in Figure 2-4.

The screenshot displays the 'WAN Status' interface, which lists various connection parameters in a table format.

Connect Method	LTE
Connect Mode	NAT
IP Address	172.16.15.156
Subnet Mask	255.255.255.0
DNS Server	114.114.114.114 8.8.8.8

Figure 2-4

3 Status

3.1 Statistics

3.1.1 Viewing CPU Usage

To view the CPU usage, perform the following steps:

1. Choose **Status**;
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 3-1.

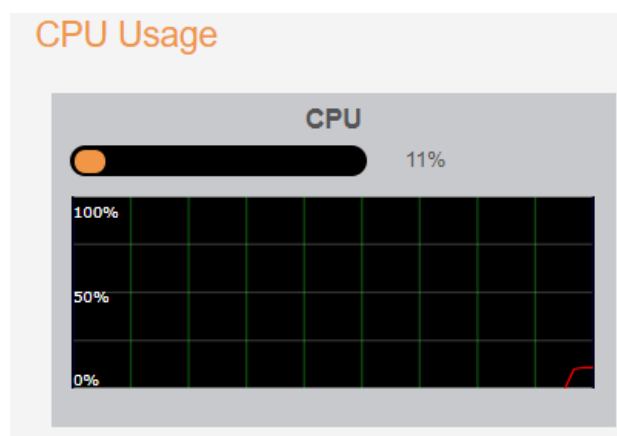


Figure 3-1

3.1.2 Viewing Memory Usage

To view the memory usage, perform the following steps:

1. Choose **Status**;
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 3-2.

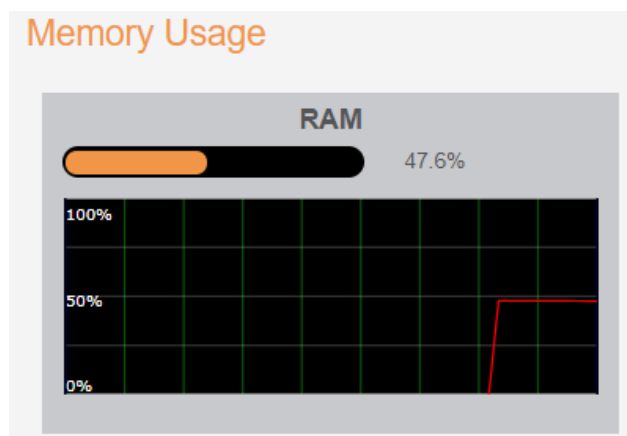


Figure 3-2

3.1.3 Viewing APN List

To view the APN list, perform the following steps:

1. Choose **Status**;
2. In the **APN List**, view the information about APN information. As shown in Figure 3-3.

APN List

Profile Name	Status	IP Address	Subnet Mask
APN1	Enable	172.16.15.156	255.255.255.0
APN2	Disable	--	--
APN3	Disable	--	--
APN4	Disable	--	--

Figure 3-3

3.1.4 Viewing Throughput Statistics

To view the Throughput Statistics, perform the following steps:

1. Choose **Status**;
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 3-4.

Throughput Statistics

Port	Received		Sent	
	Total Traffic	Packets	Total Traffic	Packets
LAN	491KB	2289	1.33 MB	2218
APN1	66KB	305	64KB	380
APN2	0 Bytes	0	0 Bytes	0
APN3	0 Bytes	0	0 Bytes	0
APN4	0 Bytes	0	0 Bytes	0

Figure 3-4

3.2 WAN Status

3.2.1 WAN Status

To view the WAN status, perform the following steps:

1. Choose **Status**;
2. Choose **WAN Status**
3. In the **WAN Status** area, view the **WAN Status** such as IP Address, Primary DNS and Secondary DNS. As shown in Figure 3-5.

WAN Status

WAN Status

IP Address	10.35.226.121
Primary DNS	211.136.150.86
Secondary DNS	211.136.150.88

Figure 3-5

3.2.2 Connection Status

To view the connection status, perform the following steps:

1.Choose **Status**;

2.Choose **WAN Status**

2.In the **Connection Status** area, view the **Connection Status** such as Connection mode, Connection Status, USIM Status, IMEI, IMSI, RSRP0, RSRP1, RSRQ, RSSI, SINR, E-cell ID, EnodeB ID and Cell ID. As shown in Figure 3-6.

Connection Status

Connection mode	LTE
Connection Status	No Service
USIM Status	Ready
IMEI	862165040901371
IMSI	460680058800102
RSRP0	0 dBm
RSRP1	0 dBm
RSRQ	0 dB
RSSI	0 dBm
SINR	0 dB
E-cell ID	--
EnodeB ID	--
Cell ID	--

Figure 3-6

3.3 LAN Status

3.3.1 LAN Status

To view the WAN status, perform the following steps:

1. Choose **Status**;
2. Choose **LAN Status**
3. In the **LAN Status** area, view the **LAN Status** such as LAN IP and DHCP Server. As shown in Figure 3-7.

LAN Status

LAN Status

LAN IP	192.168.1.1
DHCP Server	192.168.1.100-192.168.1.249

Figure 3-7

3.3.2 Device List

To view the device list, perform the following steps:

1. Choose **Status**;
2. Choose **LAN Status**;
3. 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 3-8.

Device List

Index	Device Name	MAC Address	IP Address	Lease Time	Type
1	LAPTOP-4MDE6LLJ	B4 A9 FC E8 80 4F	192.168.1.219	00d 11h 31min	LAN DHCP

Figure 3-8

4 Update

4.1 Version Manager

This function enables you to upgrade the software version of the CPE to a new version.

Viewing Version Info

To view the version info, perform the following steps:

1. Choose **Update>Version Manager**.
2. In the **Version Info** area, you can view the product name and software version. As shown in Figure 4-1.

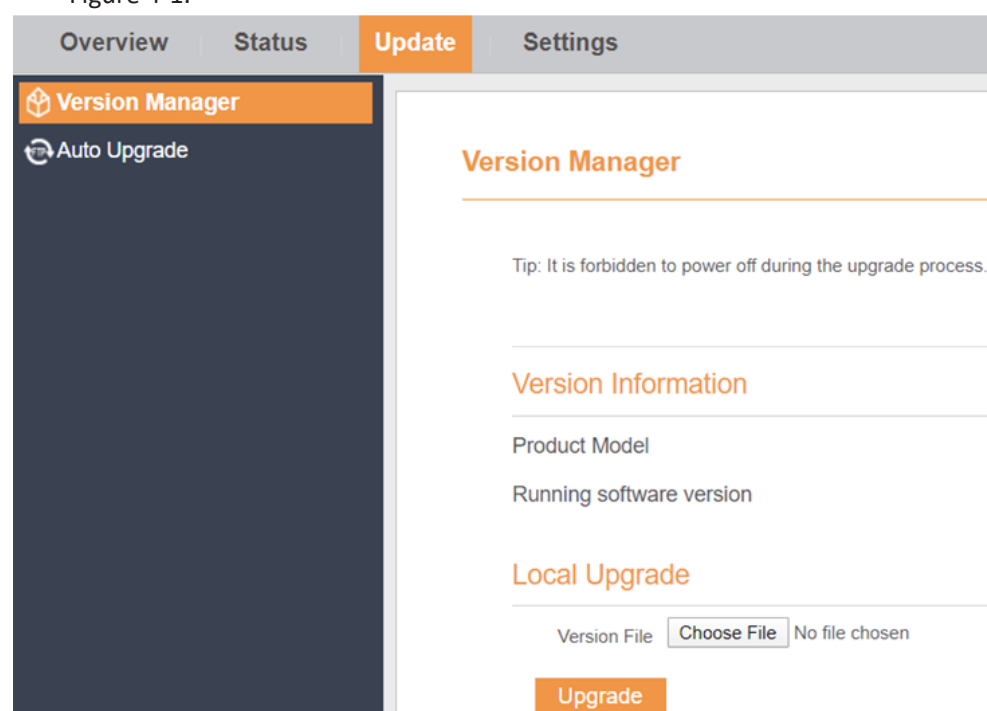


Figure 4-1

4.1.1 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 **Update>Version Manager**.
2. In the **Version Upgrade** area, click **Browser**. 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 4-2.



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

Local Upgrade

Version File No file chosen

Figure 4-2

4.2 Auto upgrade

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

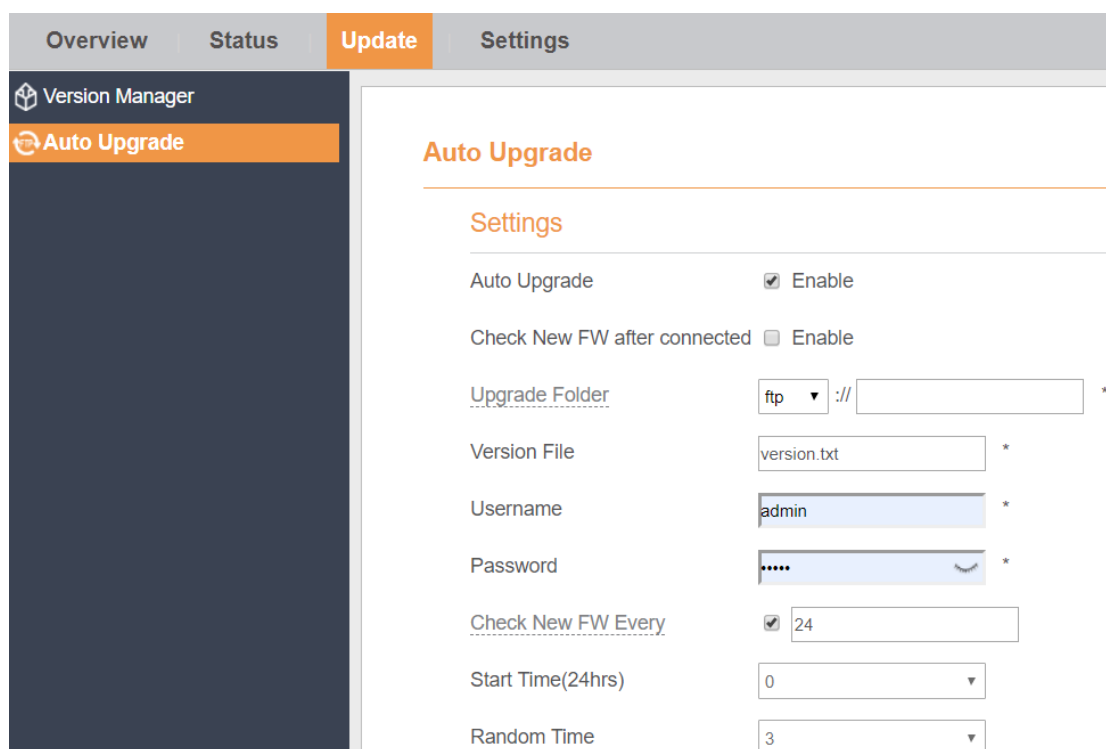
To perform a ftp auto upgrade, perform the following steps:

1. Choose **Update>Auto upgrade**.
2. Enable **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 the ftp server address to the **Upgrade folder** box.
5. Set **Version file**. //This contain the new FW name
6. Set **User name** and **Password**.
7. Set the **Interval** of checking new firmware. //Check upgrade periodic
8. Set **Start time**. // The time of upgrade begin
9. Set **Random time**. // Out of this time, UE will not upgrade.
10. Click **Submit**. As shown in Figure 4-3.



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

2,If set interval of checking new FW, the start time and random time will shouldn't be set.



The screenshot displays the 'Auto Upgrade' settings page in a web interface. The top navigation bar includes 'Overview', 'Status', 'Update' (highlighted), and 'Settings'. The left sidebar shows 'Version Manager' and 'Auto Upgrade' (highlighted). The main content area is titled 'Auto Upgrade' and contains a 'Settings' section with the following options:

- Auto Upgrade**: ☒ Enable
- Check New FW after connected**: ☐ Enable
- Upgrade Folder**: ftp :// [] *
- Version File**: version.txt *
- Username**: admin *
- Password**: [] *
- Check New FW Every**: ☒ 24
- Start Time(24hrs)**: 0 ▼
- Random Time**: 3 ▼

Figure 4-3

5 Settings

5.1 Device Information

To view the System Information, perform the following steps:

1. Choose **Settings**;
2. In the **System Information** area, view the system status, such as Running time. As shown in Figure 5-1.



System Information	
Running Time	00d 00h 14min

Figure 5-1

5.1.1 Viewing the Version Information

To view the Version Information, perform the following steps:

1. Choose **Settings**;
2. In the **Device Information** area, view the device information, such as Product name, Product Model, Hardware Version, Software version, UBoot version and CPE SN . As shown in Figure 5-2.



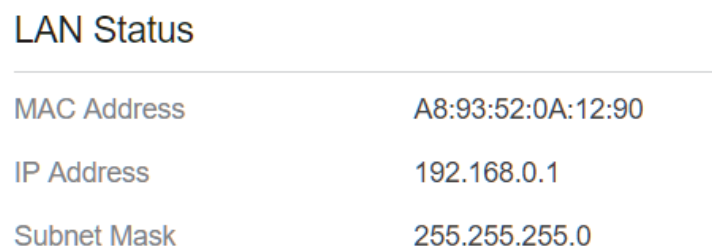
Device Information	
System Information	
Running Time	00d 00h 16min
Version Information	
Product Model	
Hardware Version	
Software Version	
UBOOT Version	V1.0.2
Serial Number	RP410201200000004
IMEI	862165040656108
IMSI	460680058800030

Figure 5-2

5.1.2 Viewing LAN Status

To view the LAN status, perform the following steps:

1. Choose **Settings**;
2. In the **LAN Status** area, view the LAN status, such as Mac address, IP address and Subnet mask. As shown in Figure 5-3.



MAC Address	A8:93:52:0A:12:90
IP Address	192.168.0.1
Subnet Mask	255.255.255.0

Figure 5-3

5.2 Network

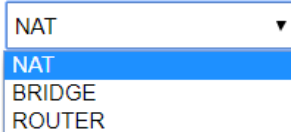
5.2.1 WAN Settings

1. To set the network mode, perform the following steps:
2. Choose **Network >WAN Settings**;
3. In the **Network Mode** area, select a mode between **NAT** and **ROUTER** and **Bridge**
4. Click **Submit**. As shown in Figure 5-4.

WAN Settings

Settings

Network Mode



NAT ▼
NAT
BRIDGE
ROUTER

Figure 5-4

5.2.2 DNS

To set the DNS settings, perform the following steps:

1. Choose **Network >DNS Settings**;
2. In the **Settings** area, you can set the Primary DNS and Secondary DNS. As shown in Figure 5-5.

DNS Settings

Static DNS has the highest priority, VPN DNS follows it and LTE DNS has the lowest priority. If you want to restore the VPN/LTE DNS, please clear the two DNS configuration and submit.

Settings

Primary DNS	114.114.114.114
Secondary DNS	8.8.8.8

Figure 5-5

5.2.3 LTE Settings

To set the LTE network, perform the following steps:

1. Choose **Network > LTE Settings**;
2. In the **Settings** area, you can set the configuration of LTE network;
3. In the **Status** area, you can view the LTE network connect status, such as Frequency, RSSI, RSRP, RSRQ, CINR, SINR, Cell ID and so on. As shown in Figure 5-6.

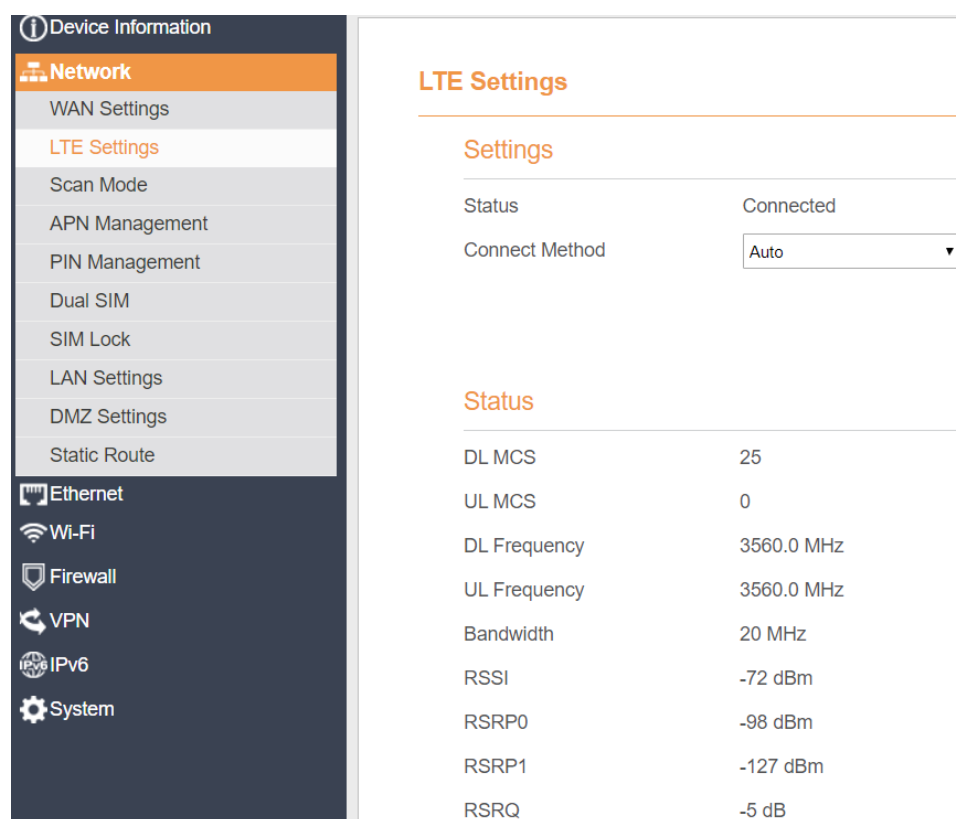


Figure 5-6

5.2.3.1 Connect Method Setting

To set the connect method, perform the following steps:

1. Choose **Network > LTE Settings**;

- In the **Setting** area, Select a connect method between **Auto** and **Manual**. As shown in Figure 5-7.

The screenshot shows the 'LTE Settings' page. Under the 'Settings' section, the 'Status' is 'Connected' and the 'Connect Method' is set to 'Auto' in a dropdown menu. At the bottom right, there are 'Submit' and 'Cancel' buttons.

Figure 5-7

5.6.2.2 5.2.3.2 Auto Connect LTE Network

To set the CPE automatically connect to the internet, perform the following steps:

- Choose **Network > LTE Settings**;
- In the **Setting** area, set the connect method as **Auto**. When the LTE network is ready, the CPE will be connected automaticity. As shown in Figure 5-8.

The screenshot shows the 'LTE Settings' page. Under the 'Settings' section, the 'Status' is 'Connected' and the 'Connect Method' is set to 'Auto' in a dropdown menu. Below this, there is a 'Status' section with a table of network parameters.

Status	
DL MCS	28
UL MCS	2
DL Frequency	3560.0 MHz
UL Frequency	3560.0 MHz
Bandwidth	20 MHz
RSSI	-71 dBm
RSRP0	-97 dBm
RSRP1	-128 dBm
RSRQ	-5 dB

Figure 5-8

5.6.2.3 5.2.3.3 Manual Connect Mobile Network

To set the mobile network manual connect to the internet, perform the following steps:

1. Choose **Network > LTE Settings**;
2. In the **Setting** area, set the connect method as **Manual**, when the LTE network is ready, you can set the CPE connect to the LTE network or disconnect from the LTE network. As shown in Figure 5-9.

LTE Settings

Settings

Status	Disconnected
Connect Method	<div>Manual ▼</div>
<div>Connect</div>	

Status

DL MCS	0
UL MCS	0
DL Frequency	2624.6 MHz
UL Frequency	2624.6 MHz
Bandwidth	20 MHz
RSSI	-53 dBm
RSRP0	-93 dBm
RSRP1	-85 dBm
RSRQ	-15 dB
SINR	0 dB
TX Power	0 dBm
PCI	20
CINR0	-6.7 dB
CINR1	4.6 dB
Cell ID	193
MCC	460
MNC	00

Figure 5-9

5.2.4 Scan Mode

This function is used to configure UE mode of scan network. The default scan mode is full band.

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

1. choose **Network>Scan mode**;
2. If select **Bandlock**, UE will only connect to the checked bands. Others will not be scanned.
3. Click **Submit**. As shown in Figure 5-10.

The screenshot shows a web-based configuration interface. At the top, there is a 'Scan Mode' label followed by a dropdown menu currently set to 'Band Lock'. Below this, the text 'Band Lock' is displayed in orange. Underneath, there is a section titled 'Band Select' followed by a list of bands: Band 2, Band 4, Band 5, Band 12, Band 13, Band 14, Band 17, Band 25, Band 26, Band 38, Band 41, Band 42, Band 43, Band 48, Band 53, and Band 66. Each band has a checkbox to its left. The checkbox for 'Band 42' is checked, while all other checkboxes are unchecked.

Figure 5-10

5.6.2.4 5.2.4.1 Setting EARFCN

To set the frequency, perform the following steps:

- 1 Choose **Network>Scan Mode**.
- 2 In the **Scan Mode** area, choose **EARFCN Lock**.
- 3 In the **EARFCN Lock** area, you can set an **EARFCN**, then click **Add** to add it to the EARFCN lock list.
- 4 Click **Submit**. As shown in Figure 5-11.

Settings

Scan Mode: EARFCN Lock

EARFCN Lock

EARFCN: 44500 * **Add**

EARFCN Lock List (Max Limit :5)

Index	EARFCN	Operation
1	44500	Delete

Submit **Cancel**

Figure 5-11

5.6.2.5 5.2.4.2 Setting PCI LOCK

To set the PCI lock perform the following steps:

1. Choose **Network>Scan Mode**.
2. In the **Scan Mode** area, choose **PCI Lock**.
3. In the **PCI Lock** area, you can set **PCI** of the cell, then click **Add** to add it to the PCI lock list.
4. Click **Submit**. As shown in Figure 5-12.

Update **Settings**

Scan Mode

Settings

Scan Mode: PCI Lock

PCI Lock

PCI: * **Add**

PCI Lock List (MAX:5)

Index	PCI	Operation
-------	-----	-----------

Submit **Cancel**

Nearby Cell List

Refresh eNB List **Clear**

Index	Band	EARFCN	PCI	RSRP(dBm)	RSRQ(dB)	RSSI(dBm)	CINR(dB)
-------	------	--------	-----	-----------	----------	-----------	----------

Figure 5-12

5.2.5 APN 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 an **APN number** which you want to set, there are 4 APNs selected.

4. In the **APN Setting** area you can set the APN parameters, such as enable or disable the apn, apn name, profile name.
5. Set the authentication type (chap or pap or none) and the username, password of it.
6. Set the PDN type: IPv4 or IPv6 or IPv4/v6 dual stack.
7. Click **Submit**. As shown in Figure 5-13.

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

And we can also set the APN apply to SNMP or TR069.

The screenshot shows the 'Settings' tab of the router's web interface. On the left, a sidebar menu lists various settings categories: Device Information, Network (selected), APN Management, PIN Management, Dual SIM, SIM Lock, LAN Settings, DMZ Settings, Static Route, Ethernet, Wi-Fi, Firewall, VPN, IPv6, and System. The main content area is titled 'APN Management' and contains two sections: 'APN Selection' and 'APN Settings'. In 'APN Selection', the 'APN Number' is set to '# 1'. In 'APN Settings', the 'Enable' checkbox is checked, 'Profile Name' is 'APN1', 'APN Name' is 'APN1', 'Authentication Type' is 'NONE', 'PDN Type' is 'IPv4', 'Default Gateway' is checked, and 'Apply To' includes 'TR069' and 'SNMP'.

Figure 5-13

5.2.6 PIN 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 5-14

The screenshot shows the 'Settings' tab of the router's web interface. On the left, a sidebar menu lists various settings categories: Device Information, Network (selected), APN Management, PIN Management (selected), Dual SIM, SIM Lock, LAN Settings, DMZ Settings, Static Route, Ethernet, Wi-Fi, Firewall, VPN, IPv6, and System. The main content area is titled 'PIN Management' and contains a description: 'The PIN lock of the USIM card protects the router against unauthorized accesses to the Internet. You can activate, modify, or deactivate the PIN.' Below this is a note: 'Note: The router cannot provide Internet services when the USIM card is not inserted or the PIN verification failed.' The 'PIN Management' section includes fields for 'USIM Card Status' (set to 'USIM Normal'), 'PIN Verification' (radio buttons for 'Enable' and 'Disable', with 'Enable' selected), 'PIN' (a text input field), and 'Remaining Attempts' (set to '3'). At the bottom right, there are 'Submit' and 'Cancel' buttons.

Figure 5-14

5.6.2.6 5.2.6.1 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.

5.6.2.7 5.2.6.2 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**.

5.6.2.8 5.2.6.3 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**.

5.6.2.9 5.2.6.4 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**.

5.6.2.10 5.2.6.5 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**.

5.6.2.11 5.2.6.6 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.

- 1 To enable automatic verification of the PIN, perform the following steps:
- 2 Choose **Network > PIN Management**.
- 3 Set Pin verification to Enable.
- 4 Set **Remember my PIN** to Enable.
- 5 Click Submit.

5.6.2.12 5.2.6.7 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**.

5.2.7 SIM 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. Input the PLMN you want to lock in the **PLMN** box.
3. Click **add** to add the PLMN in the lock list.
4. Click **Submit**. As shown in Figure 5-15.

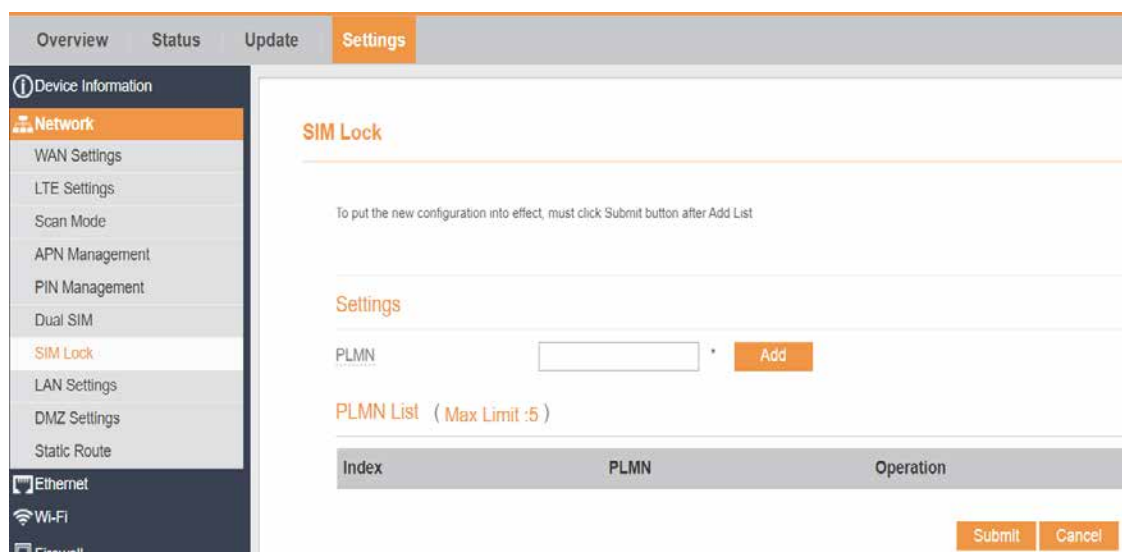


Figure 5-15

5.2.8 LAN Setting

5.6.2.13 5.2.8.1 Setting LAN Host Parameters

By default, the IP address is 192.168.0.1 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>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 5-16.

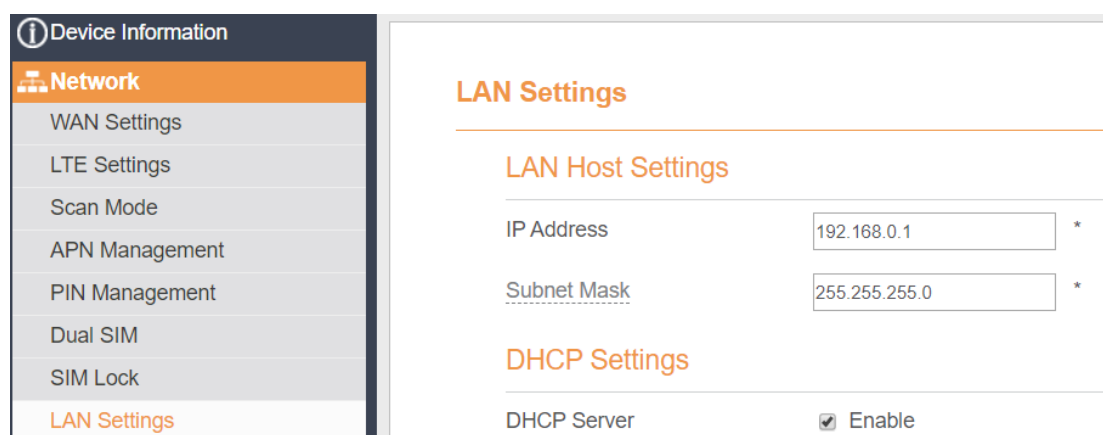


Figure 5-16

5.6.2.14 5.2.8.2 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 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 5-17.

LAN Settings	
LAN Host Settings	
IP Address	192.168.0.1 *
Subnet Mask	255.255.255.0 *
DHCP Settings	
DHCP Server	<input checked="" type="checkbox"/> Enable
Start IP Address	192.168.0.10 *
End IP Address	192.168.0.100 *
Lease Time	720 *
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

Figure 5-17

5.2.9 DMZ 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**.

- (Optional) Set **ICMP Redirect** to **Enable**.
- 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.

- Click **Submit**. As shown in Figure 5-18.

Figure 5-18

5.2.10 Static Route

5.6.2.15 5.2.10.1 Add Static Route

To add a static route, perform the following steps:

- Choose **Network Setting>Static Route**.
- Click **Add list**.
- Set the **Dest IP address** and **Subnet mask**.
- Select an **Interface** from the drop-down list.
- If you select **LAN** as the interface, you need set a Gateway.
- Click **Submit**. As shown in Figure 5-19.

Figure 5-19

5.6.2.16 5.2.10.2 Modify Static Route

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

- Choose **Firewall>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 5-20.

Figure 5-20

5.6.2.17 5.2.10.3 Delete Static Route

To delete a static route, perform the following steps:

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

5.3 Ethernet

5.3.1 Ethernet Settings

In this area, you can select the connection mode of Ethernet, and there are three modes that you could choose. They are Dynamic IP, Static IP and LAN Only. perform the following steps:

1. Choose **Ethernet > Ethernet Settings**;
2. Set **Connection mode** to **Dynamic IP/Static IP/LAN Only**.
3. Click **Save**. As shown in Figure 5-21.



If you choose Static IP, you need to configure manually.

Figure 5-21

5.3.2 Ethernet Status

In this area, you can view the status about the Ethernet. To view the Ethernet status, perform the following steps:

1. Choose **Ethernet > Ethernet Status**;
2. In the **Ethernet Status** area, view the information about Connection mode, Link Status, Connect Status, Online Time, IP Address, Subnet Mask, Default Gateway, Primary DNS and Secondary DNS (the figure below is about **Dynamic IP mode**). As shown in Figure 5-22.

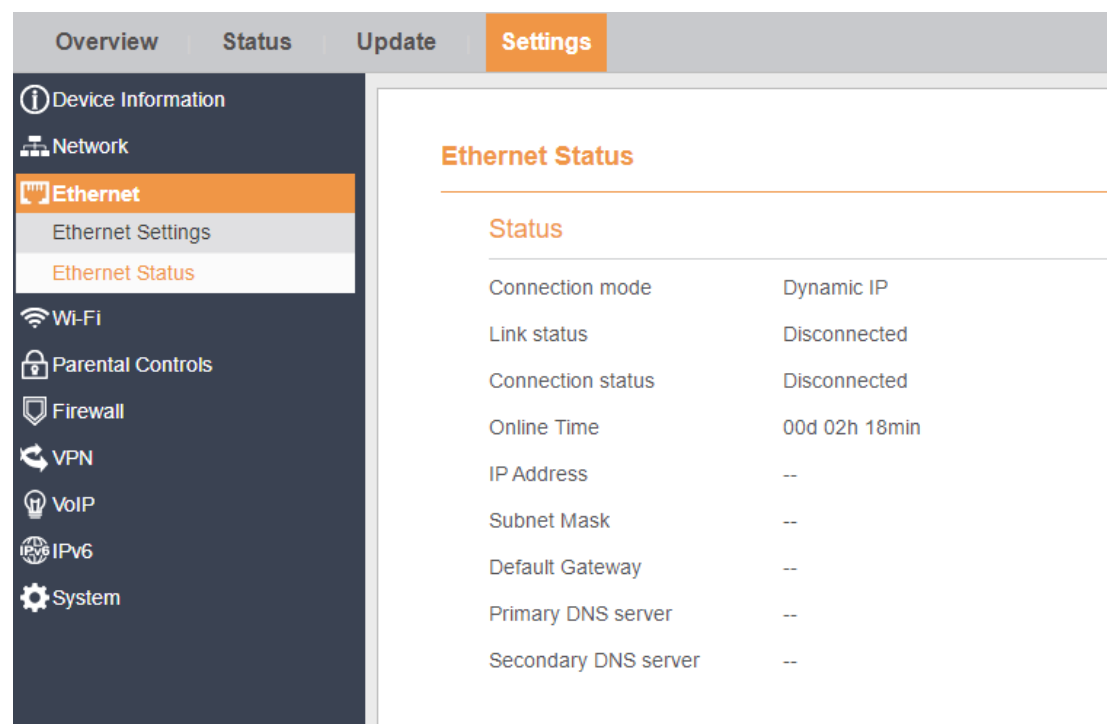


Figure 5-24

5.5 Parental Controls

5.5.1 Enabling Parental Controls

To enable Parental Controls, perform the following steps:

1. Choose **Settings > Parental Controls**.
2. Set **Parental Controls** to **Enable**.
3. Click **Save**. As shown in Figure 5-33.

Parental Controls

Parental Controls Manager

Enable

☒ Enable

Submit

Figure 5-33

5.5.2 Disabling Parental Controls

To disable Parental Controls, perform the following steps:

- 1.Choose **Settings > Parental Controls**.
- 2.Set **Parental Controls** to **Disable**.
- 3.Click **Save**. As shown in Figure 5-34.

Parental Controls

Parental Controls Manager

Enable

☐ Enable

Submit

Figure 5-34

5.5.3 Adding Parental Controls list

To add a Parental Controls list, perform the following steps:

- 1.Choose **Settings >Parental Controls**.
- 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.Set **Access Restriction status**
- 8.Click **Save**. As shown in Figure 5-35.

Parental Controls List (Max Limit :32)

Add List

Index	Name	Device	Weekdays	Time	Operation
-------	------	--------	----------	------	-----------

Settings

Name

test

Device

192.168.1.1

Weekdays

Mon Tue Wed Thu Fri Sat Sun

Time

10

0

-

15

0

Submit

Cancel

Figure 5-35

5.6 Firewall

5.6.1 Setting 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 **Firewall>Firewall Setting**.
2. Choose **Enable** or **Disable** to modify the configuration.
3. Click **Submit**. As shown in Figure 5-36.

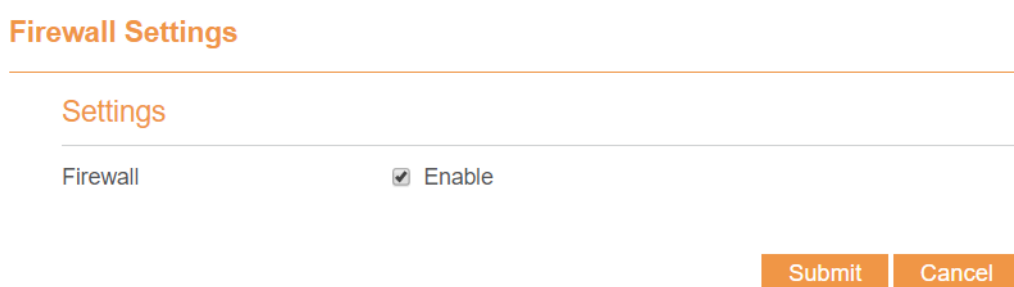


Figure 5-36

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.

5.6.3 MAC Filtering

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

5.6.3.1 Enabling MAC Filter

To enable MAC address filter, perform the following steps:

1. Choose **Firewall>MAC Filtering**
2. Set MAC filtering to **Enable**.
3. Click **Submit**. As shown in Figure 5-37.

MAC Filtering

MAC Filtering Manager

MAC Filtering	<input checked="" type="checkbox"/> Enable
Within The Rule To Allow/Deny	<input checked="" type="radio"/> Allow
	<input type="radio"/> Deny

Figure 5-37

5.6.3.2 Disabling MAC Filter

To disable MAC address filter, perform the following steps:

1. Choose **Firewall>MAC Filtering**
2. Set MAC filtering to **Disable**.
3. Click **Submit**. As shown in Figure 5-38.

MAC Filtering

MAC Filtering Manager

MAC Filtering	<input checked="" type="checkbox"/> Enable
Within The Rule To Allow/Deny	<input type="radio"/> Allow
	<input checked="" type="radio"/> Deny

Figure 5-38

5.6.3.3 Setting Allow access network within the rules

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

1. Choose **Firewall>MAC Filtering**.
2. Set **Allow access network** within the rules.
3. Click **Submit**. As shown in Figure 5-39.

MAC Filtering

MAC Filtering Manager

MAC Filtering	<input checked="" type="checkbox"/> Enable
Within The Rule To Allow/Deny	<input checked="" type="radio"/> Allow
	<input type="radio"/> Deny

Figure 5-39

5.6.3.4 Setting Deny access network within the rules

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

1. Choose **Firewall>MAC Filtering**.
2. Set **Deny access network** within the rules.
3. Click **Submit**. As shown in Figure 5-40.

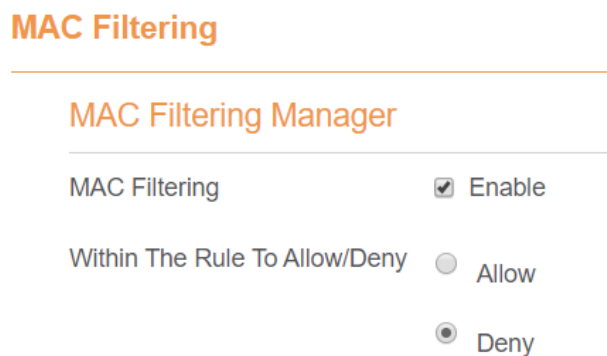


Figure 5-40

5.6.3.5 Adding MAC Filtering rule

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

1. Choose **Firewall>MAC Filtering**.
2. Click **Add list**.
3. Set **MAC address**.
4. Click **Submit**. As shown in Figure 5-41.

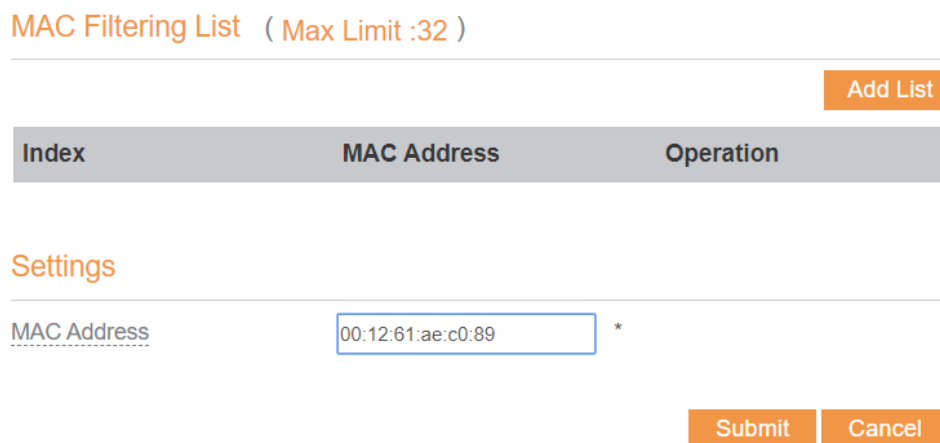


Figure 5-41

5.6.3.6 Modifying MAC Filtering rule

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

1. Choose **Firewall>MAC Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **MAC address**.
4. Click **Submit**. As shown in Figure 5-42.

MAC Filtering List (Max Limit :32)

MAC Filtering List (Max Limit :32)		
Add List		
Index	MAC Address	Operation
1	00:12:61:AE:C0:89	Delete Edit

Settings

MAC Address

*

Submit

Cancel

Figure 5-42

5.6.3.7 Deleting MAC Filtering rule

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

1. Choose **Firewall>MAC Filtering**.
2. Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-43.

MAC Filtering List (Max Limit :32)

MAC Filtering List (Max Limit :32)		
Add List		
Index	MAC Address	Operation
1	00:12:61:AE:C0:89	Delete Edit

Figure 5-43

5.6.4 IP Filtering

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

5.6.4.1 Enabling IP Filtering

To enable IP Filtering, perform the following steps:

1. Choose **Firewall>IP Filtering**.
2. Set IP Filtering **Enable**.
3. Click **Submit**. As shown in Figure 5-44.

IP Filtering Manager

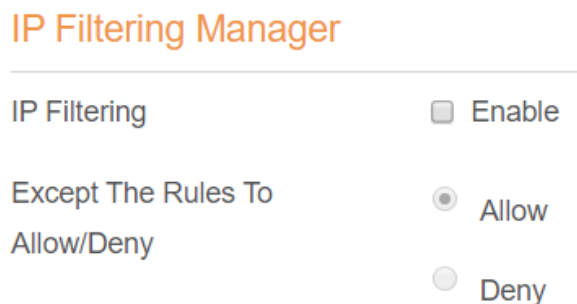
IP Filtering	<input checked="" type="checkbox"/> Enable
Except The Rules To Allow/Deny	<input checked="" type="radio"/> Allow
	<input type="radio"/> Deny

Figure 5-44

5.6.4.2 Disabling IP Filtering

To disable IP Filtering, perform the following steps:

1. Choose **Firewall>IP Filtering**.
2. Set IP Filtering **Disable**.
3. Click **Submit**. As shown in Figure 5-45.



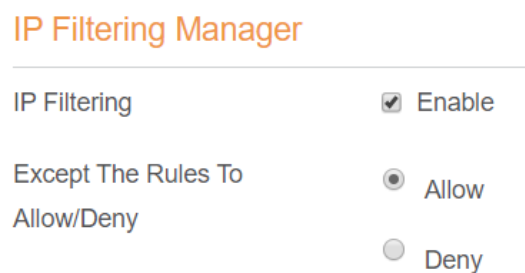
The screenshot shows the 'IP Filtering Manager' interface. It has a title bar 'IP Filtering Manager' in orange. Below it, there are two settings: 'IP Filtering' with a checkbox that is unchecked and the label 'Enable' to its right; and 'Except The Rules To Allow/Deny' with two radio buttons, 'Allow' (selected) and 'Deny' (unselected).

Figure 5-45

5.6.4.3 Setting Allow access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Firewall>IP Filtering**.
2. Set **Allow access network** outside the rules.
3. Click **Submit**. As shown in Figure 5-46.



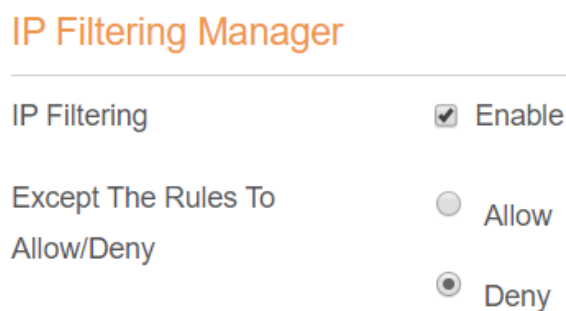
The screenshot shows the 'IP Filtering Manager' interface. It has a title bar 'IP Filtering Manager' in orange. Below it, there are two settings: 'IP Filtering' with a checked checkbox and the label 'Enable' to its right; and 'Except The Rules To Allow/Deny' with two radio buttons, 'Allow' (selected) and 'Deny' (unselected).

Figure 5-46

5.6.4.4 Setting Deny access network outside the rules

To set allow access network, perform the following steps:

1. Choose **Firewall>IP Filtering**.
2. Set **Deny access network** outside the rules.
3. Click **Submit**. As shown in Figure 5-47.



The screenshot shows the 'IP Filtering Manager' interface. It has a title bar 'IP Filtering Manager' in orange. Below it, there are two settings: 'IP Filtering' with a checked checkbox and the label 'Enable' to its right; and 'Except The Rules To Allow/Deny' with two radio buttons, 'Allow' (unselected) and 'Deny' (selected).

Figure 5-47

5.6.4.5 Adding IP Filtering rule

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

1. Choose **Firewall>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 5-48.

IP Filtering List (Max Limit :32)

[Add List](#)

Index	Protocol	Source IP	Source Port Range	Destination IP	Destination Port Range	Status	Operation
<p>Settings</p> <p>Service: <input type="text" value="Custom"/></p> <p>Protocol: <input type="text" value="ALL"/></p> <p>Source IP: <input type="text" value="192.10.64.123"/></p> <p>Source Port Range: <input type="text"/></p> <p>Destination IP: <input type="text"/></p> <p>Destination Port Range: <input type="text"/></p> <p>Status: <input type="text" value="Allow"/></p> <p style="text-align: right;">Submit Cancel</p>							

Figure 5-48

5.6.4.6 Modifying IP Filtering rule

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

1. Choose **Firewall > 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 5-49.

IP Filtering List (Max Limit :32)

[Add List](#)

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

Settings

Service

Custom ▼

Protocol

ALL ▼

Source IP

192.10.64.123

Source Port Range

Destination IP

100.10.64.123

Destination Port Range

Status

Allow ▼

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

Figure 5-49

5.6.4.7 Deleting IP Filtering rule

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

1. Choose **Firewall > IP Filtering**.
2. Choose the rule to be deleted, and click **Delete**. As shown in Figure 5-50.

IP Filtering List (Max Limit :32)

[Add List](#)

Index	Protocol	Source IP	Source Port Range	Destination IP	Destination Port Range	Status	Operation
1	ALL	192.10.64.123	N/A	100.10.64.123	N/A	Allow	Delete Edit

Figure 5-50

5.6.5 URL Filtering

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

5.6.5.1 Enabling URL Filtering

To enable URL Filtering, perform the following steps:

1. Choose **Firewall>URL Filtering**.
2. Set **URL Filtering** to **Enable**.
3. Click **Submit**. As shown in Figure 5-51.

URL Filtering

URL Filtering Manager

URL Filtering ☒ Enable

Figure 5-51

5.6.5.2 Disabling URL Filtering

To disable URL Filtering, perform the following steps:

1. Choose **Firewall>URL Filtering**.
2. Set **URL Filtering** to **Disable**.
3. Click **Submit**. As shown in Figure 5-52.

URL Filtering

URL Filtering Manager

URL Filtering ☐ Enable

Figure 5-52

5.6.5.3 Adding URL Filtering list

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

1. Choose **Firewall>URL Filtering**.
2. Click **Add list**.
3. Set **URL**.
4. Click **Submit**. As shown in Figure 5-53.

URL Filtering List (Max Limit :32)

Index	URL	Operation

Settings

URL *

Figure 5-53

5.6.5.4 Modify URL Filtering list

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

1. Choose **Firewall>URL Filtering**.
2. Choose the rule to be modified, and click **Edit**.
3. Set **URL** address.
4. Click **Submit**. As shown in Figure 5-54.

URL Filtering List (Max Limit :32)

			Add List
Index	URL	Operation	
1	www.google.com	Delete Edit	

Figure 5-54

5.6.5.5 Deleting URL Filtering list

To delete an URL list, perform the following steps:

1. Choose **Firewall>URL Filtering**.
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-55.

URL Filtering List (Max Limit :32)

			Add List
Index	URL	Operation	
1	www.google.com	Delete Edit	

Figure 5-55

5.6.6 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.

5.6.6.1 Adding Port Forwarding rule

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

1. Choose **Firewall > 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 5-56.

Port Forwarding

Port Forwarding List (Max Limit :32)

[Add List](#)

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

Settings

Service Custom ▼

Protocol TCP ▼

Remote Port Range 2000 *

Local Host 192.168.0.1 *

Local Port 3000 *

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

Figure 5-56

5.6.6.2 Modifying Port Forwarding rule

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

1. Choose **Firewall > Port Forwarding**.
2. Choose the item to be modified, and click **Edit**.
3. Re-config the service, protocol, and ports.
4. Click **Submit**. As shown in Figure 5-57.

Port Forwarding

Port Forwarding List (Max Limit :32)

Add List					
Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	2000	192.168.0.1	3000	Delete Edit

Settings

Service	Custom ▼	
Protocol	TCP ▼	
Remote Port Range	2000	*
Local Host	192.168.0.1	*
Local Port	3000	*

Submit Cancel

Figure 5-57

5.6.6.3 Deleting Port Forwarding rule

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

1. Choose **Firewall > Port Forwarding**.
2. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-58.

Port Forwarding List (Max Limit :32)

Add List					
Index	Protocol	Remote Port Range	Local Host	Local Port	Operation
1	TCP	2000	192.168.0.1	3000	Delete Edit

Figure 5-58

5.6.7 Port Triggering

5.6.7.1 Enabling Port Triggering

To enable **Port Triggering**, perform the following steps:

1. Choose **Firewall > Port Triggering**.
2. Set **Port Triggering** to **Enable**.
3. Click **Submit**. As shown in Figure 5-59.

Port Triggering

Port Triggering Manager

Port Triggering ☒ Enable

Figure 5-59

5.6.7.2 Disabling Port Triggering

To disable URL Filtering, perform the following steps:

- 1.Choose **Firewall> Port Triggering**.
- 2.Set **Port Triggering** to **Disable**.
- 3.Click **Submit**. As shown in Figure 5-60.

Port Triggering

Port Triggering Manager

Port Triggering ☐ Enable

Figure 5-60

5.6.7.3 Adding Port Triggering

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

- 1.Choose **Firewall> Port Triggering**.
- 2.Click **Add list**.
- 3.Set Triggered Port and Forwarded Port.
- 4.Click **Submit**. As shown in Figure 5-61.

Port Triggering List (Max Limit :32)

Index	Triggered Port	Triggered Protocol	Forwarded Port	Forwarded Protocol	Operation
-------	----------------	--------------------	----------------	--------------------	-----------

Settings

Triggered Port

Triggered Protocol

Forwarded Port

Forwarded Protocol

Figure 5-61

5.6.7.4 Edit Port Triggering

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

- 1.Choose **Firewall> Port Triggering**.
- 2.Choose the rule to be modified, and click **Edit**.

3. Set Triggered Port and Forwarded Port.
5. Click **Submit**. As shown in Figure 5-62.

Port Triggering List (Max Limit :32)

Index	Triggered Port	Triggered Protocol	Forwarded Port	Forwarded Protocol	Operation
1	80	TCP	80	TCP	Delete Edit

[Add List](#)

Figure 5-62

5.6.7.5 Deleting Port Triggering list

To delete an **Port Triggering** list, perform the following steps:

3. Choose **Firewall> Port Triggering**.
4. Choose the item to be deleted, and click **Delete**. As shown in Figure 5-63.

Port Triggering List (Max Limit :32)

Index	Triggered Port	Triggered Protocol	Forwarded Port	Forwarded Protocol	Operation
1	80	TCP	80	TCP	Delete Edit

[Add List](#)

Figure 5-63

5.6.8 Access Restriction

Access Restriction

Access Restriction List (Max Limit :32)

[Add List](#)

Index	Enable	Name	Device	Weekdays	Time	Operation
<div>Settings</div> <div> <div>Enable <input checked="" type="checkbox"/> Enable</div> <div> <div>Name</div> <div>ABC *</div> </div> <div> <div>Device</div> <div>00:12:61:AE:C0:89 *</div> </div> <div> <div>Weekdays</div> <div> <div>Mon</div> <div>Tue</div> <div>Wed</div> <div>Thu</div> <div>Fri</div> <div>Sat</div> <div>Sun</div> </div> </div> <div> <div>Time</div> <div> <div>0 ▾</div> <div>:</div> <div>0 ▾</div> <div>-</div> <div>23 ▾</div> <div>:</div> <div>59 ▾</div> </div> </div> <div> <div>Submit</div> <div>Cancel</div> </div> </div>						

Figure 5-64

5.6.8.1 Add Access Restriction

To add an 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**.

5.6.8.2 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**.

5.6.8.3 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**.

5.6.9 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 **Firewall > UPnP**.
2. Set **UPnP** to **Enable**.
3. Click **Submit**. As shown in Figure 5-65.

UPnP

Settings

UPnP ☒ Enable

Submit

Current UPnP Status

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

Figure 5-65

5.6.10 DoS

On this page, you can enable or disable the Denial of service (DoS) function.

1. Choose **Firewall > DoS**.
2. Set **UPnP** to **Enable**.
3. Click **Submit**. As shown in Figure 5-66.

DoS

DoS Settings	
DoS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Sync flood	<input checked="" type="checkbox"/> Enable
Ping flood	<input checked="" type="checkbox"/> Enable
TCP port scan	<input type="checkbox"/> Enable
UDP port scan	<input type="checkbox"/> Enable

Figure 5-66

5.7 VPN

This function enables you to connect the virtual private network (VPN).

To connect the VPN, perform the following steps:

1. Choose **VPN**.
2. In the **VPN Settings** 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 5-67.

VPN Settings

VPN ☒ Enable

Protocol L2TP ▾

VPN Server 172.16.34.120 *

Username TEST *

Password **** *

Host Name cpe_lac

Bear Device APN1 ▾

Default Gateway ☐ Enable

IPsec Enable ☐ Enable

IPsec Password ▾ *

VPN Status

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

Figure 5-67

5.8 IPv6

Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP). Every device on the Internet is assigned an unique IP address for identification and location definition.

5.8.1 Status

The status page shows IPv6 information. As shown in Figure 5-68.

Status

IPv6 Information

IPv6 Status	Enable
WAN Connection Type	AutoConfiguration
IPv6 MGMT Global Address	--

LAN Address

IPv6 DATA Global Address	--
IPv6 Link-Local Address	fe80::1
AutoConfiguration Type	SLAAC

Figure 5-68

5.8.2 IPv6 WAN Settings

In this page, user can enable or disable IPv6 function. Meanwhile, user can set WAN Connection Type and the type of DNS. As shown in Figure 5-69

IPv6 WAN Settings

WAN

IPv6 Enable ☒ Enable

WAN Settings

WAN Connection Type AutoConfiguration ▼

IPv6 MGMT Global Address --

DNS From DHCPv6 ▼

Bear Device APN1 ▼

Submit Cancel

Figure 5-69

5.8.3 IPv6 LAN Settings

In this page, user can choose the Autoconfiguration Type. As shown in Figure 5-70.

IPv6 LAN Settings

LAN Settings

IPv6 Link-Local Address fe80::1

AutoConfiguration Type SLAAC ▼

Submit Cancel

Figure 5-70

5.9 System

5.9.1 Maintenance

5.9.1.1 Reboot

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 **Reboot**. As shown in Figure 5-71
The CPE then restarts.

Reboot

Click **Reboot** to reboot device

Reboot

Figure 5-71

5.9.1.2 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 **Factory Reset**. As shown in Figure 5-72.
The CPE is then restored to its default settings.

Factory Reset

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

Factory Reset

Figure 5-72

5.9.1.3 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 5-73.
The procedure for file downloading may vary with the browser you are using.

Backup Configuration File

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

Download

Figure 5-73

5.9.1.4 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 chooses. 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 5-74.

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

Restore Configuration File

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

Configuration File No file chosen

Figure 5-74

5.9.1.5 CBSD

You can input SAS Server setting in CBSD page

1. Choose **System>CBSD**. Figure 5.74A
 2. Click **Browse** on the **CBSD** page.
 3. In the displayed dialog box, Input **SAS User ID**.
 4. In the displayed dialog box, Device **FCC ID** will show for SAS requirement.
 5. In the display dialog box, Select **SAS Grant Renew Range** Value Default is 50.
 6. In the display dialog box, Input your **SAS URL**
 7. In the Display **Save** option will save the setting and device will send registration request to SAS sever.

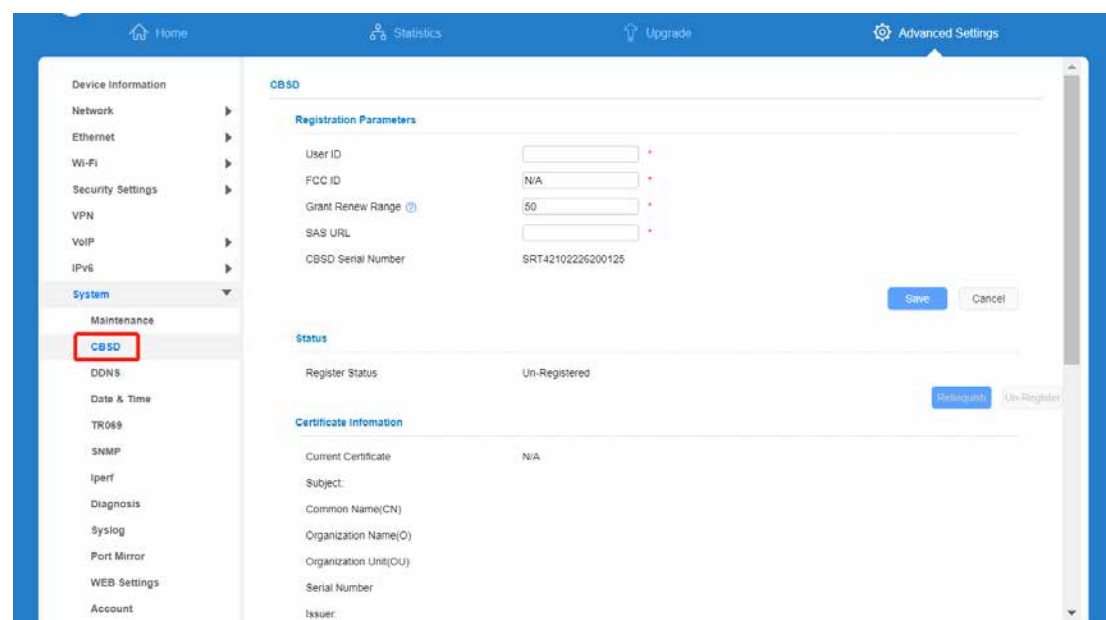



Figure 5.74A

5.9.2 TR069

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>TR069**.
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 5-75.

TR069

Settings

Enable TR069	<input checked="" type="checkbox"/> Enable
ACS URL Source	URL ▼
ACS URL	http://192.168.0.10/acs *
ACS Username	tr069 *
ACS Password	***** *
Enable Periodic Inform	<input checked="" type="checkbox"/> Enable
Periodic Inform Interval	3600 *
Connection Request Username	tr069
Connection Request Password	*****

Submit

Cancel

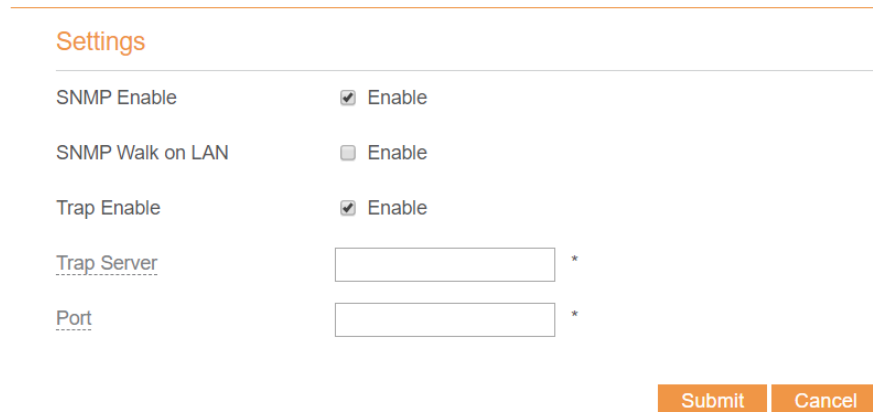
Figure 5-75

5.9.3 SNMP

You can enable SNMP and set config SNMP trap.

The UE will actively report changes of some certain values to the SNMP server. As shown in Figure 5-76.

SNMP



The figure shows a web-based configuration page for SNMP settings. At the top, there is a title bar with the word "Settings" in orange. Below this, the settings are organized into a table-like structure. The first row is "SNMP Enable" with a checked checkbox and the text "Enable". The second row is "SNMP Walk on LAN" with an unchecked checkbox and the text "Enable". The third row is "Trap Enable" with a checked checkbox and the text "Enable". The fourth row is "Trap Server" with a text input field and an asterisk. The fifth row is "Port" with a text input field and an asterisk. At the bottom right, there are two orange buttons: "Submit" and "Cancel".

SNMP Enable	<input checked="" type="checkbox"/> Enable
SNMP Walk on LAN	<input type="checkbox"/> Enable
Trap Enable	<input checked="" type="checkbox"/> Enable
Trap Server	<input type="text"/> *
Port	<input type="text"/> *

Submit Cancel

Figure 5-76

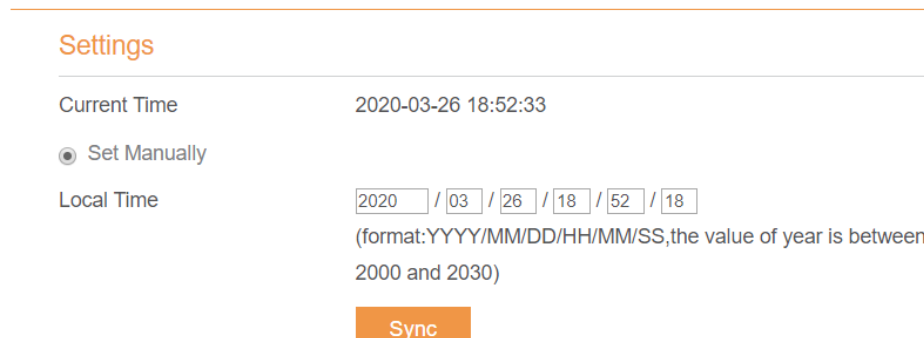
5.9.4 Date & Time

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 5-77.

Date & Time



The figure shows a web-based configuration page for Date & Time settings. At the top, there is a title bar with the word "Settings" in orange. Below this, the settings are organized into a table-like structure. The first row is "Current Time" with the value "2020-03-26 18:52:33". The second row is "Set Manually" with a selected radio button. The third row is "Local Time" with a date and time input field showing "2020 / 03 / 26 / 18 / 52 / 18". Below the input field, there is a note: "(format:YYYY/MM/DD/HH/MM/SS,the value of year is between 2000 and 2030)". At the bottom, there is an orange button labeled "Sync".

Current Time	2020-03-26 18:52:33
<input checked="" type="radio"/> Set Manually	
Local Time	<input type="text" value="2020"/> / <input type="text" value="03"/> / <input type="text" value="26"/> / <input type="text" value="18"/> / <input type="text" value="52"/> / <input type="text" value="18"/>

(format:YYYY/MM/DD/HH/MM/SS,the value of year is between 2000 and 2030)

Sync

Figure 5-77

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 5-78.

Date & Time

Settings

Current Time	2020-03-26 18:53:43
<input type="radio"/> Set Manually	
<input checked="" type="radio"/> Sync from Network	
Primary NTP Server	<input type="text" value="pool.ntp.org"/>
Secondary NTP Server	<input type="text" value="asia.pool.ntp.org"/>
Optional NTP Server	<input type="checkbox"/> <input type="text"/>
Time Zone	<input type="text" value="(GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi"/>

Figure 5-78

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 5-79.

DST

DST	<input type="checkbox"/> Enable
Start Time	<input type="text" value="Mar"/> <input type="text" value="Second"/> <input type="text" value="Mon"/> (2020-03-09) at <input type="text" value="2"/> o'clock
End Time	<input type="text" value="Nov"/> <input type="text" value="First"/> <input type="text" value="Sun"/> (2020-11-01) at <input type="text" value="2"/> o'clock
Status	Not Running

Figure 5-79

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

5.9.5 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 5-80.

DDNS

DDNS (Dynamic Domain Name System) is a service that allows network clients to connect to the wireless router, even with a dynamic public IP address, through its registered domain name.

DDNS Settings

DDNS	<input checked="" type="checkbox"/> Enable
Service Provider	WWW.DYNDNS.ORG ▼
Domain	<input type="text"/> *
Username	<input type="text"/> *
Password	<input type="password"/> *
Refresh	<input type="text" value="0"/> *
Enable Wildcard	<input type="checkbox"/> Enable
WAN IP and domain verification	<input type="checkbox"/> Enable

Submit**Cancel**

Figure 5-80

5.9.6 Iperf

Iperf is a network performance testing tool. You can test TCP and UDP bandwidth quality. It can test the maximum TCP bandwidth, with a variety of parameters and UDP characteristics. Bandwidth, delay jitter and packet loss can be given.

5.9.6.1 TCP

To set TCP, perform the following steps:

1. Choose **System>Iperf**.
2. Set Trap Server.
3. Set Server Port (1024~65535).
4. Set Management Port (1024~65535).
5. Set Measurement Time (10~86400).
6. Set Protocol, select TCP.
7. Click **Save** and wait for few minutes, the results will be shown in the Result area. As shown in Figure 5-81.

The screenshot shows the Iperf configuration interface. It has a title bar 'Iperf' and two main sections: 'Settings' and 'Result'.

Settings

Server Address	10.0.4.98	*
Server Port	5001	*
Management Port	5001	*
Measurement Time	30	*
Protocol Type	TCP	*

At the bottom right of the Settings section are two buttons: 'Start' and 'Stop'.

Result

Status	Running
Uplink Speed	—
Downlink Speed	—

Figure 5-81

5.9.6.2 UDP

To set UDP, perform the following steps:

1. Choose **System>Iperf**.
2. Set Trap Server.
3. Set Server Port (1024~65535).
4. Set Management Port (1024~65535).
5. Set Measurement Time (10~86400).
6. Set Protocol, select UDP.
7. Set Packet Length (1~1470).

8.Set Udp Bandwidth.

9.Click **Save** and wait for few minutes, the results will be shown in the Result area. As shown in Figure 5-82.

The screenshot shows the Iperf web interface. The 'Settings' section includes the following fields:

Field	Value
Server Address	10.0.4.98
Server Port	5001
Management Port	5001
Measurement Time	30
Protocol Type	UDP
Data Length	1024
UDP Bandwidth	15M

Below the settings are 'Start' and 'Stop' buttons. The 'Result' section shows the following data:

Field	Value
Status	Running
Uplink Latency	--
Downlink Latency	--
Uplink Speed	--
Downlink Speed	--

Figure 5-82

5.9.7 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.

5.9.7.1 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**. As shown in Figure 5-83.

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

Diagnostics

Method

Method of Diagnostics: ☒ Ping ☐ TraceRoute

Ping

Target IP/Domain	www.baidu.com	*
Packet Size	56	*
Timeout	10	*
Count	4	*

Result

Result: **Pass**

Details:

```

PING www.baidu.com (112.80.248.75): 56 data bytes
64 bytes from 112.80.248.75: seq=0 ttl=54 time=163.447 ms
64 bytes from 112.80.248.75: seq=1 ttl=54 time=51.388 ms
64 bytes from 112.80.248.75: seq=2 ttl=54 time=61.369 ms
64 bytes from 112.80.248.75: seq=3 ttl=54 time=59.464 ms

--- www.baidu.com ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 51.388/83.917/163.447 ms
  
```

Figure 5-83

5.9.7.2 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** and **Timeout**.
5. Click **Traceroute**. As shown in Figure 5-84

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

Diagnostics

Method

Method of Diagnostics

- ☐ Ping
- ☒ TraceRoute

Traceroute

Target IP/Domain *

Maximum Hops *

Timeout *

Traceroute

Cancel

Result

Result **Pass**

Details

```

traceroute to www.baidu.com (112.80.248.75), 30 hops max, 38
byte packets
 1 192.168.23.50 (192.168.23.50) 758.544 ms
 2 *
 3 10.0.10.1 (10.0.10.1) 224.854 ms
 4 58.246.124.193 (58.246.124.193) 50.321 ms
 5 112.64.249.145 (112.64.249.145) 31.167 ms
 6 139.226.203.122 (139.226.203.122) 44.152 ms
 7 139.226.225.153 (139.226.225.153) 58.233 ms
 8 219.158.97.106 (219.158.97.106) 198.055 ms

```

Figure 5-84

5.9.8 Port Mirror

Port mirroring is used on a network switch to send a copy of network packets seen on one switch port. To do so:

1. Choose **System>Port Mirror**.
2. Enable Port Mirror.
3. Select the **WAN Interface** which you want a copy.
4. Type the **Monitor IP**, where the copy will send to.
5. Click **Submit**. As shown in Figure 5-85.

Port Mirror

Settings

Enable ☒ EnableWAN Interface Forward IP Address *

Submit

Cancel

Figure 5-85

5.9.9 Syslog

The syslog record user operations and key running events.

5.9.9.1 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**. As shown in Figure 5-86.

The screenshot shows the 'Syslog' configuration page. Under the 'Settings' tab, the 'Method' is set to 'Local' (radio button selected). The 'Level' is set to 'INFO' in a dropdown menu. There are 'Submit' and 'Cancel' buttons. Below the settings, there is a 'Local' section with a 'Keyword' input field containing 'sys', and 'Pull Syslog' and 'Clear Syslog' buttons. At the bottom, the 'Result' section displays a list of log entries, each starting with a timestamp and the text 'OpenWrt user notice syslog: Receive reply: getspeed-1-1'.

Figure 5-86

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.

5.9.9.2 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 5-87.

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

Syslog

Settings

Method

☒ Network

☐ Local

Network

Forward IP Address

192.168.1.120

*

Submit

Cancel

Figure 5-87

5.9.10 WEB 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 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 5-88.

WEB Settings

Settings

HTTP Enable	<input checked="" type="checkbox"/> Enable
HTTP Port	<input type="text" value="80"/> *
HTTPs Enable	<input checked="" type="checkbox"/> Enable
Allow HTTPs Login from WAN	<input type="checkbox"/> Enable
Allow PING from WAN	<input type="checkbox"/> Enable
HTTPs Port	<input type="text" value="443"/> *
Refresh Time	<input type="text" value="10"/> *
Session Timeout	<input type="text" value="10"/> *
Language	<input type="text" value="English"/> ▼

Figure 5-88

5.9.11 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 5-89.

Account

Change Password

Username	<input type="text" value="superadmin"/> ▼
Current Password	<input type="password"/> *
New Password	<input type="password"/> *
Confirm Password	<input type="password"/> *

Figure 5-89

5.9.12 Logout

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

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

It will return to the login page.

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.

DISCLAIMER

ALL CONTENTS OF THIS MANUAL ARE PROVIDED "AS IS". EXCEPT AS REQUIRED BY APPLICABLE LAWS, NO WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE MADE IN RELATION TO THE ACCURACY, RELIABILITY OR CONTENTS OF THIS MANUAL.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOSS OF PROFITS, BUSINESS, REVENUE, DATA, GOODWILL SAVINGS OR ANTICIPATED SAVINGS REGARDLESS OF WHETHER SUCH LOSSES ARE FORSEEABLE OR NOT.

THE MAXIMUM LIABILITY (THIS LIMITATION SHALL NOT APPLY TO LIABILITY FOR PERSONAL INJURY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH A LIMITATION) OF ARISING FROM THE USE OF THE PRODUCT DESCRIBED IN THIS MANUAL SHALL BE LIMITED TO THE AMOUNT PAID BY CUSTOMERS FOR THE PURCHASE OF THIS PRODUCT.

Safety Information

This section contains important information about the operation of your device. It also contains information about how to use the device safely. Read this information carefully before using your device.

Electronic device

Do not use your device if using the device is prohibited. Do not use the device if doing so causes danger or interference with other electronic devices.

Interference with medical equipment

Follow rules and regulations set forth by hospitals and health care facilities. Do not use your device where prohibited:

- Some wireless devices may affect the performance of hearing aids or pacemakers. Consult your service provider for more information.
- Pacemaker manufacturers recommend that a minimum distance of 15 cm be maintained between a device and a pacemaker to prevent potential interference with the pacemaker. If using a pacemaker, hold the device on the side opposite the pacemaker and do not carry the device in your front pocket.

Areas with flammables and explosives

- Do not use the device where flammables or explosives are stored (in a gas station, oil depot, or chemical plant, for example). Using your device in these environments increases the risk of explosion or fire. In addition, follow the instructions indicated in

text or symbols.

- Do not store or transport the device in containers with flammable liquids, gases, or explosives.

Operating environment

- Avoid dusty, damp, or dirty environments. Avoid magnetic fields. Using the device in these environments may result in circuit malfunctions.
- Before connecting and disconnecting cables, stop using the device and disconnect it from the power supply. Ensure that your hands are dry during operation.
- Place the device on a stable surface.
- Keep the device away from electronic appliances that generate strong magnetic or electric fields, such as a microwave oven or refrigerator.
- During thunderstorms, power off your device and remove all cables connected to it to protect against lightning strikes.
- Do not use your device during thunderstorms to protect your device against any danger caused by lightning.
- Ideal operating temperatures are 0°C to 40°C. Ideal storage temperatures are -20°C to +70°C. Extreme heat or cold may damage your device or accessories.
- Keep the device and accessories in a well-ventilated and cool area away from direct sunlight. Do not enclose or cover your device with towels or other objects. Do not place the device in a container with poor heat dissipation, such as a box or bag.
- To protect your device or accessories from fire or electrical shock hazards, avoid rain and moisture.
- Keep the device away from sources of heat and fire, such as a heater, microwave oven, stove, water heater, radiator, or candle.
- Do not place any object, such as a candle or a water container, on the device. If any foreign object or liquid enters the device, immediately stop using it, power it off, and remove all cables connected to it. Then, contact an authorized service center.
- Do not block device openings. Reserve a minimum of 10 cm around the device to dissipate heat.
- Stop using your device or applications for a while if the device is overheated. If skin is exposed to an overheated device for an extended period, low temperature burn symptoms, such as red spots and darker pigmentation, may occur.
- Do not touch the device's antenna. Otherwise, communication quality may be reduced.
- Do not allow children or pets to bite or suck the device or accessories. Doing so may result in damage or explosion.
- Observe local laws and regulations, and respect the privacy and legal rights of others.
- The device should be installed and operated with a minimum distance of 20 cm between the radiator and your body.
- Keep the device in a place with good reception. The distance between the device and other metal materials (such as metal brackets or metal doors and windows) should be greater than 25 cm and the distance between the device should be greater than 30 cm.

Child's safety

- Comply with all precautions with regard to child's safety. Letting children play with the device or its accessories may be dangerous. The device includes detachable parts that may present a choking hazard. Keep away from children.
- The device and its accessories are not intended for use by children. Children should only use the device with adult supervision.

Accessories

- Using an unapproved or incompatible power adapter, charger or battery may cause fire, explosion or other hazards.
- Choose only accessories approved for use with this model by the device manufacturer. The use of any other types of accessories may void the warranty, may violate local regulations and laws, and may be dangerous. Please contact your retailer for information about the availability of approved accessories in your area.

Power adapter safety

- The power plug is intended to serve as a disconnect device.
- For pluggable devices, the socket-outlet shall be installed near the devices and shall be easily accessible.
- Unplug the power adapter from electrical outlets and the device when not in use.
- Do not drop or cause an impact to the power adapter. If it is damaged, take it to an authorized service center for inspection.
- If the power cable is damaged (for example, the cord is exposed or broken), or the plug loosens, stop using it at once. Continued use may lead to electric shocks, short circuits, or fire.
- Do not touch the power cord with wet hands or pull the power cord to disconnect the power adapter.
- Do not touch the device or the power adapter with wet hands. Doing so may lead to short circuits, malfunctions, or electric shocks.
- If your power adapter has been exposed to water, other liquids, or excessive moisture, take it to an authorized service center for inspection.
- Ensure that the power adapter meets the requirements of Clause 2.5 in IEC60950-1/EN60950-1/UL60950-1 and has been tested and approved according to national or local standards.

Cleaning and maintenance

- During storage, transportation, and operation of the device, keep it dry and protect it from collision.
- Keep the device and accessories dry. Do not attempt to dry it with an external heat source, such as a microwave oven or hair dryer.
- Do not expose your device or accessories to extreme heat or cold. These environments may interfere with proper function and may lead to fire or explosion.
- Avoid collision, which may lead to device malfunctions, overheating, fire, or explosion.

- If the device is not going to be used for an extended period of time, power it off, and remove all cables connected to it.
- If anything unusual occurs (for example, if the device emits smoke or any unusual sound or smell), immediately stop using it, power it off, remove all cables connected to it, and contact an authorized service center.
- Do not trample, pull, or excessively bend any cable. Doing so may damage the cable, causing the device to malfunction.
- Before you clean or maintain the device, stop using it, stop all applications, and disconnect all cables connected to it.
- Do not use any chemical detergent, powder, or other chemical agents (such as alcohol and benzene) to clean the device or accessories. These substances may cause damage to parts or present a fire hazard. Use a clean, soft, and dry cloth to clean the device and accessories.
- Do not place magnetic stripe cards, such as credit cards and phone cards, near the device for extended periods of time. Otherwise the magnetic stripe cards may be damaged.
- Do not dismantle or remanufacture the device and its accessories. This voids the warranty and releases the manufacturer from liability for damage. In case of damage, contact an authorized service center for assistance or repair.

Emergency calls

The availability of emergency calls is subject to your cellular network quality, service provider policy, and local laws and regulations. Never rely solely on your device for critical communications like medical emergencies.