

## **Welcome to the LTE CPE!**

Online Help

## **Copyright © Huawei Technologies Co., Ltd. 2014. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

The product described in this manual may include copyrighted software of Huawei Technologies Co., Ltd and possible licensors. Customers shall not in any manner reproduce, distribute, modify, decompile, disassemble, decrypt, extract, reverse engineer, lease, assign, or sublicense the said software, unless such restrictions are prohibited by applicable laws or such actions are approved by respective copyright holders under licenses.

## **Trademarks and Permissions**



 are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

Other trademarks, product, service and company names mentioned are the property of their respective owners.

## **Notice**

Some features of the product and its accessories described herein rely on the software installed, capacities and settings of local network, and may not be activated or may be limited by local network operators or network service providers, thus the descriptions herein may not exactly match the product or its accessories you purchase.

Huawei Technologies Co., Ltd reserves the right to change or modify any information or specifications contained in this manual without prior notice or obligation.

## **NO WARRANTY**

THE 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 CASE SHALL HUAWEI TECHNOLOGIES CO., LTD BE LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS, BUSINESS, REVENUE, DATA, GOODWILL OR ANTICIPATED SAVINGS.

## **Import and Export Regulations**

Customers shall comply with all applicable export or import laws and regulations and will obtain all necessary governmental permits and licenses in order to export, re-export or import the product mentioned in this manual including the software and technical data therein.

## **Copyright Notice**

To view more details about the copyright notice of this product, please visit URL:

[http://consumer.huawei.com/minisite/copyright\\_notice/](http://consumer.huawei.com/minisite/copyright_notice/) or contact: **mobile@huawei.com**.

---

# Contents

---

<b>1 Getting Started.....</b>	<b>1</b>
1.1 Welcome to the CPE.....	1
1.2 Computer Configuration Requirements .....	1
1.3 Logging In to the Web Management Page .....	1
<b>2 Home.....</b>	<b>3</b>
2.1 Overview .....	3
2.1.1 Viewing the Internet Status .....	3
2.1.2 Viewing the Internet Usage .....	3
2.1.3 Viewing the Wi-Fi Status .....	3
2.1.4 Viewing the LAN Usage .....	3
2.1.5 Viewing the Antenna Status .....	4
2.2 Product Information .....	4
2.2.1 Viewing the Product Information.....	4
2.2.2 Viewing the Device List.....	4
2.3 Quick Setup .....	4
2.4 Update .....	5
2.4.1 Updating on Local.....	5
2.4.2 Updating Online.....	5
<b>3 PIN Management .....</b>	<b>7</b>
3.1 Viewing the Status of the USIM Card.....	7
3.2 Enabling PIN Verification .....	7
3.3 Disabling PIN Verification .....	7
3.4 Verifying the PIN .....	8
3.5 Changing the PIN.....	8
3.6 Setting Automatic Verification of the PIN.....	8
3.7 Verifying the PUK.....	9
<b>4 LAN.....</b>	<b>10</b>
4.1 DHCP Settings .....	10
4.1.1 Setting LAN Host Parameters .....	10
4.1.2 Configuring the DHCP Server .....	10
4.1.3 Bundled Address List .....	11
4.2 Static Routing.....	12
4.3 Dynamic Routing .....	12
<b>5 Wi-Fi .....</b>	<b>14</b>
5.1 Wi-Fi Settings.....	14
5.2 Access Management .....	14

5.2.1 Setting the Access Policy .....	14
5.2.2 Managing the Wi-Fi Access List .....	15
5.3 WPS Settings.....	16
5.4 Wi-Fi Multi-SSID Settings.....	16
5.5 WDS.....	17
<b>6 Security.....</b>	<b>18</b>
6.1 Setting Firewall Level .....	18
6.2 MAC Filtering.....	18
6.2.1 Managing MAC Address Whitelist .....	18
6.2.2 Managing MAC Address Blacklist .....	19
6.3 URL Filtering .....	19
6.3.1 Managing URL Whitelist.....	20
6.3.2 Managing URL Blacklist .....	20
6.4 IP Filtering.....	21
6.4.1 Managing IP Address Whitelist.....	21
6.4.2 Managing IP Blacklist.....	22
6.5 Setting Service Access Control .....	22
6.6 Setting ALG .....	22
6.7 Setting Port Forwarding .....	23
6.8 Setting UPnP .....	24
6.9 Setting DMZ.....	24
6.10 Turning On or Off Bridge Mode .....	24
<b>7 Voice .....</b>	<b>26</b>
7.1 Viewing Voice Information .....	26
7.2 Configuring a SIP Account.....	26
<b>8 System .....</b>	<b>28</b>
8.1 Maintenance .....	28
8.1.1 Restart .....	28
8.1.2 Reset.....	28
8.2 Changing the Password .....	28
8.3 Setting the Date and Time .....	29
8.4 Diagnosis.....	29
8.4.1 Ping .....	29
8.4.2 Traceroute .....	30
8.4.3 System Check.....	30
8.4.4 Checking the Wireless Status .....	30
8.5 Logs.....	31
<b>9 FAQs .....</b>	<b>32</b>
<b>10 Acronyms and Abbreviations.....</b>	<b>33</b>



# 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**.
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.



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.

Please change the default WiFi password as soon as possible.

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

**---End**

# 2 Home

---

## 2.1 Overview

### 2.1.1 Viewing the Internet Status

To view the Internet connection status, perform the following steps:

1. Choose **Home > Overview**.
2. In the **Internet Status** area, view the Internet status, such as **USIM card status**, **Network mode**, and **IP address**.

----End

### 2.1.2 Viewing the Internet Usage

To view the network data usage, perform the following steps:

1. Choose **Home > Overview**.
2. In the **Internet Usage** area, view the network data usage, including total traffic, uplink and downlink traffic volumes, uplink and downlink rates, and time spent online.

----End

### 2.1.3 Viewing the Wi-Fi Status

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

1. Choose **Home > Overview**.
2. In the **Wi-Fi Status** area, view the following information.

View the Wi-Fi network connection status, including the **SSID**, **IP Address**, **MAC Address**, **Broadcast mode**, and **Wireless Encryption mode**.

View the statistics of the Wi-Fi network, including the total traffic, packets, erroneous packets, and discarded packets transmitted and received over the Wi-Fi network.

----End

### 2.1.4 Viewing the LAN Usage

To view the local area network (LAN) connection status, perform the following steps:

1. Choose **Home > Overview**.
2. In the **LAN Usage** area, view the following information.



View the LAN status, such as **IP address**, **MAC address**, **DHCP server**.

View the statistics of the LAN, including the total traffic, packets, erroneous packets, and discarded packets transmitted and received over the LAN.

----End

## 2.1.5 Viewing the Antenna Status

To view the antenna status, perform the following steps:

1. Choose **Home > Overview**.
2. In the **Antenna** area, view the antenna status.

----End

## 2.2 Product Information

### 2.2.1 Viewing the Product Information

To view the basic product information, perform the following steps:

1. Choose **Home > Product Information**.
2. In the **Product Information** area, view the basic information about the CPE.

For example, the name, serial number (SN), international mobile equipment identity (IMEI).

----End

### 2.2.2 Viewing the Device List

To view the device list, perform the following steps:

1. Choose **Home > Product Information**.
2. In the **Device List** area, view the information about the devices, such as **Computer Name**, **MAC Address**, **IP Address**, and **Lease Time**.

**Lease Time** indicates the remaining lease duration of the dynamic DHCP server. If a static IP address is bundled with the device, **Lease Time** and **Computer Name** are N/A and Unknown respectively.

----End

## 2.3 Quick Setup

The setup wizard guides you to configure the most important settings of the CPE. After the configurations are complete, the CPE can access the Internet.

To configure the CPE, perform the following steps:

1. Choose **Home > Quick Setup**.

2. Set **SSID**.
  3. Click **Next** to view and set Wi-Fi security-related parameters, including **Display password** and **WPA-PSK**.
  4. Click **Next** to view the settings you just configured.
  5. Click **Submit** for the settings to take effect.
- End

## 2.4 Update

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

### 2.4.1 Updating on Local

To perform a local upgrade successfully, connect the CPE to your computer through Wi-Fi or 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 a local upgrade, perform the following steps:

1. Choose **Home > Update**.
2. In the **Local Update** 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 **Update**.



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

5. Click **OK**.

The software upgrade starts. After the upgrade, the CPE automatically restarts and runs the new software version.

----End

### 2.4.2 Updating Online

To perform an online upgrade successfully, make sure the CPE is connected to the Internet.

To perform an online upgrade, perform the following steps:

1. Choose **Home > Update**.
2. Click **Check** to detect the latest version.



After updates are found, the CPE retains the server address and informs you if any subsequent updates are found on the server.

If...	Then...
Updates are found.	Go to step 3.
Updates are not found.	The upgrade ends.

3. Click **Update** to download the updates.

After downloading the updates, the CPE automatically upgrades and restarts.

A message is displayed, indicating that the upgrade is complete. Then, the login dialog box is displayed.



During an upgrade, do not disconnect the power supply or operate the CPE.

**---End**

# 3 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
- Chang the PIN
- Set automatic verification of the PIN

## 3.1 Viewing the Status of the USIM Card

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

1. Choose **Internet > PIN Management**.
2. View the status of the USIM card in the **USIM card status** field.

----End

## 3.2 Enabling PIN Verification

To enable PIN verification, perform the following steps:

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

----End

## 3.3 Disabling PIN Verification

To disable PIN verification, perform the following steps:

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

----End

## 3.4 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 **Internet > PIN Management**.
2. Enter the PIN (4 to 8 digits) in the **PIN** box.
3. Click **Submit**.

----End

## 3.5 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 **Internet > 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**.

----End

## 3.6 Setting Automatic Verification of the PIN

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

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

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

----End

## 3.7 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 **Internet > 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**.

----End

# 4 LAN

---

A local area network (LAN) is a shared communication system to which multiple devices are attached.

When correctly configured, devices on the LAN can use the CPE to share data.

## 4.1 DHCP Settings

### 4.1.1 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 **LAN > DHCP Settings**.
2. In the **LAN Host Settings** area, set **IP address**.
3. Set the **DHCP server** to **Enable**.
4. Click **Submit**.

----End

### 4.1.2 Configuring 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 the CPE is working in the routing mode.

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 **LAN > DHCP 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**.

----End

### 4.1.3 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.



After you change the settings, click **Submit** for the changes to take effect. The DHCP server may need to restart.

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

1. Choose **LAN > DHCP Settings**.
2. Click **Edit List**.
3. Click **Add**.
4. Set the MAC address and **IP Address**.
5. Click **Submit**.

----End

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

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

----End

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

1. Choose **LAN > DHCP Settings**.



2. Click **Edit List**.
3. Choose the item to be deleted, and click **Delete**.
4. Click **OK**.

----End

To delete all items from the setup list, perform the following steps:

1. Choose **LAN > DHCP Settings**.
2. Click **Edit List**.
3. Click **Delete All**.
4. Click **OK**.

----End

## 4.2 Static Routing

If cascaded routers are used on the LAN, add static routing rules to ensure that the devices connected to the cascaded routers can be accessed. Static routing is similar to dynamic routing. However, manual configuration is required and the router must always be available.



If the IP address of the cascaded router is fixed, static routing is recommended.

If the IP address of the cascaded router is changeable, dynamic routing is recommended.

To configure static routing settings, perform the following steps:

1. Choose **LAN > Static Routing**.
2. Click **Add**.
3. Set **Destination IP address**.
4. Set **Subnet mask**.
5. Set **Router IP address**.

This IP address is obtained from the CPE and used for data transmission to the cascading devices. This IP address must be reachable.

6. Click **Submit**.

----End

## 4.3 Dynamic Routing

This function is enabled when cascaded routers are used on the LAN and the cascaded routers comply with the Routing Information Protocol (RIP). This page allows you to enable or disable RIP and set its version and operation mode.

To configure dynamic routing settings, perform the following steps:

1. Choose **LAN > Dynamic Routing**.

2. Set **RIP** to **Enable**.

3. Set **Operation**.

If it is set to **Active**, the CPE actively makes route changes and notifies surrounding routers of the changes. If it is set to **Passive**, the CPE does not make route changes until it is notified.

4. Set **Version** to **RIP v1**, **RIP v2**, or **RIP v1/RIP v2**.

5. Click **Submit**.

----End

# 5 Wi-Fi

## 5.1 Wi-Fi Settings

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

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 **WPA-PSK**.



**WPA-PSK** can contain 8 to 63 ASCII characters or 64 hex characters.

If set **Display password** to **Enable**, **WPA-PSK** will be visible.

4. Click **Submit**.

----End

## 5.2 Access Management

### 5.2.1 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 **Settings** area, set SSID's MAC Access.

The MAC access of each SSID 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**.

----End

## 5.2.2 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 **Edit MAC List**.
3. Click **Add**.
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**.

----End

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**.

----End

To delete an item from 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 deleted, and click **Delete**.
4. Click **OK**.

----End

To delete all items from the Wi-Fi access list, perform the following steps:

1. Choose **Wi-Fi > Access Management**.
2. Click **Edit MAC List**.

3. Click **Delete All**.
4. Click **OK**.

----End

## 5.3 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. Set **WPS Mode**.



If **WPS Mode** is set to **PBC**, the client can connect to the CPE after you press the WPS button on the CPE and the client.

If **WPS Mode** is set to **Route PIN**, the client can connect to the CPE after you enter the Router PIN on the client.

If **WPS Mode** is set to **Client PIN**, the client can connect to the CPE after you enter the correct PIN and click **Connect to Client**.

4. Click **Submit**.

----End

## 5.4 Wi-Fi Multi-SSID Settings

The **SSID List** page shows information about the SSIDs to be configured.

To configure an SSID, perform the following steps:

1. Choose **Wi-Fi > Wi-Fi Multi-SSID**.
2. Choose an SSID to be configured, and click **Edit**.
3. 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: / ' = " \ &

4. Set **WPA-PSK**.



**WPA-PSK** can contain 8 to 63 ASCII characters or 64 hex characters.

If set **Display password** to **Enable**, **WPA-PSK** will be visible.

5. Click **Submit**.

----End

## 5.5 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**, go to the **Advanced Settings** page to set the channel.

To configure the WDS, perform the following steps:

1. Choose **Wi-Fi > WDS**.
2. Set **WDS** to **Enable**.
3. Click **Scan**.
4. 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**.

----End

# 6 Security

## 6.1 Setting Firewall Level

This page describes how to set the firewall level. If **Firewall level** is set to **Custom**, you can modify the configuration.

To set the firewall level, perform the following steps:

1. Choose **Security > Firewall Level**.
2. Set **Firewall level** from the drop-down list.
3. Set **DoS attack** to **Enable**.

To block Denial of Service (DoS) attacks from the LAN and Internet.

4. Click **Submit**.

----End

To set filtering functions of the firewall, perform the following steps:

1. Choose **Security > Firewall Level**.
2. Set **Firewall level** to **Custom**.
3. Set **MAC filtering**.
4. Set **IP filtering**.
5. Set **URL filtering**.
6. Click **Submit**.

----End

## 6.2 MAC Filtering

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

### 6.2.1 Managing MAC Address Whitelist

To add a MAC address whitelist rule, perform the following steps:

1. Choose **Security > MAC Filtering**.
2. Set **MAC filtering mode** to **Whitelist**.
3. Click **Add Item**.

4. Set the MAC address.
5. Click **Submit**.

----End

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

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

----End

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

1. Choose **Security > MAC Filtering**.
2. Set **MAC filtering mode** to **Whitelist**.
3. Choose the rule to be deleted, and click **Delete**.
4. Click **OK**.

----End

To delete all MAC address whitelist rules, perform the following steps:

1. Choose **Security > MAC Filtering**.
2. Set **MAC filtering mode** to **Whitelist**.
3. Click **Delete All**.
4. Click **OK**.

----End

## 6.2.2 Managing MAC Address Blacklist

Choose **Security > MAC Filtering**, and then set **MAC filtering mode** to **Blacklist**.

The other steps are the same as those for managing the MAC address whitelist. For details, see section "Managing MAC Address Whitelist".

## 6.3 URL Filtering

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



## 6.3.1 Managing URL Whitelist

To add a URL whitelist rule, perform the following steps:

1. Choose **Security > URL Filtering**.
2. Set **URL filtering mode** to **Whitelist**.
3. Click **Add Item**.
4. Set URL.
5. Click **Submit**.

----End

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

1. Choose **Security > URL Filtering**.
2. Set **URL filtering mode** to **Whitelist**.
3. Choose the rule to be modified, and click **Edit**.
4. On the displayed page, set URL.
5. Click **Submit**.

----End

To delete a URL whitelist rule, perform the following steps:

1. Choose **Security > URL Filtering**.
2. Set **URL filtering mode** to **Whitelist**.
3. Choose the rule to be deleted, and click **Delete**.
4. Click **OK**.

----End

To delete all URL whitelist rules, perform the following steps:

1. Choose **Security > URL Filtering**.
2. Set **URL filtering mode** to **Whitelist**.
3. Click **Delete All**.
4. Click **OK**.

----End

## 6.3.2 Managing URL Blacklist

Choose **Security > URL Filtering**, and then set **URL filtering mode** to **Blacklist**.

The other steps are the same as those for managing the URL address whitelist. For details, see section "Managing URL Whitelist".

## 6.4 IP Filtering

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

### 6.4.1 Managing IP Address Whitelist

To add an IP address whitelist rule, perform the following steps:

1. Choose **Security > IP Filtering**.
2. Set **IP filtering mode** to **Whitelist**.
3. Click **Add Item**.
4. Set **Service**.
5. Set **Protocol**.
6. In the **Source IP Address Range** box, enter the source IP address or IP address segment to be filtered.
7. In the **Source port range** box, enter the source port or port segment to be filtered.
8. In the **Destination IP Address Range** box, enter the destination IP address or IP address segment to be filtered.
9. In the **Destination port Range** box, enter the destination port or port segment to be filtered.
10. Click **Submit**.

----End

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

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

----End

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

1. Choose **Security > IP Filtering**.
2. Set **IP filtering mode** to **Whitelist**.
3. Choose the rule to be deleted, and click **Delete**.
4. Click **OK**.

----End

To delete all IP whitelist rules, perform the following steps:

1. Choose **Security > IP Filtering**.
2. Set **IP filtering mode** to **Whitelist**.
3. Click **Delete All**.
4. Click **OK**.

----End

## 6.4.2 Managing IP Blacklist

Choose **Security > IP Filtering**, and then set **IP filtering mode** to **Blacklist**.

The other steps are the same as those for managing the IP address whitelist. For details, see section "Managing IP Address Whitelist".

## 6.5 Setting Service Access Control

This function enables you to control the number of users connecting to the CPE.

The access control list shows the types of services that are controlled by the CPE. By default, the access control rules are not in effect.

To set the access control list, perform the following steps:

1. Choose **Security > Service Access Control**.
2. Choose the item to be configured, and click **Edit**.
3. Set **IP address range**.



If **Access Source** is set to **LAN**, the IP address must be on the same network segment as the IP address set on the **LAN Host Settings** page.

If **Access Source** is set to **Internet**, the IP address must be on different network segments from the IP address that is set on the **LAN Host Settings** page.

4. Set **Status**.
5. Click **Submit**.

----End

## 6.6 Setting ALG

To enable ALG(Application Layer Gateway), perform the following steps:

1. Choose **Security > ALG**.
2. Set **SIP ALG** to **Enable**.
3. Set **SIP port**.



It is recommended to retain the default port **5060**. If you use another port, you cannot use VoIP software.

4. Click **Submit**.


----End

## 6.7 Setting 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.

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


1. Choose **Security > Port Forwarding**.
2. Click **Add Item**.
3. Set **Type**.
4. Set **Protocol**.
5. (Optional) Set **Remote host**.
6. Set **Remote port range**.

 The port number ranges from 1 to 65535.

7. 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.

8. Set **Local port**.

 The port number ranges from 1 to 65535.

9. Set **Status** to **Enabled** or **Disabled**.

10. Click **Submit**.

----End

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 9 in the previous procedure.
4. Click **Submit**.

----End

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**.
3. Click **OK**.

----End

To delete all port forwarding rules, perform the following steps:

1. Choose **Security > Port Forwarding**.
2. Click **Delete All**.
3. Click **OK**.

----End

## 6.8 Setting 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**.

----End

## 6.9 Setting DMZ

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 **Security > DMZ**.
2. Set **DMZ** to **Enable**.
3. 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.

4. Click **Submit**.

----End

## 6.10 Turning On or Off Bridge Mode

CPE supports bridge mode. Bridge mode allows for faster Internet access speeds of the device connected to the CPE.



In bridge mode, only one device can be connected to the CPE at a time.

In bridge mode, the CPE 's data services are disabled.

To turn bridge mode on or off, perform the following steps:

1. Choose **Security > IP Pass Through**.
2. Do as follows:
  - Select **Enable** to turn on bridge mode.
  - Clear **Enable** to turn off bridge mode.
3. Click **Submit**.

----End

# 7 Voice

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 Viewing Voice Information

To view the Voice information, perform the following steps:

1. Choose **Voice > Voice Information**.
  2. View the Voice information, such as the SIP account and status of the SIP registration server.
- End

## 7.2 Configuring a SIP Account

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

To add a SIP account, perform the following steps:

1. Choose **Voice > SIP Account**.
  2. Click **Add Item**.
  3. In the **SIP Account** box, enter the SIP account number provided by your service provider.
  4. In the **User name** and **Password** boxes, enter the user name and password of the SIP account provided by your service provider.
  5. Click **Submit**.
- End

To modify a SIP account, perform the following steps:

1. Choose **Voice > SIP Account**.
  2. Choose the item to be modified, and click **Edit**.
  3. Repeat steps 3 and 4 in the previous procedure.
  4. Click **Submit**.
- End

To delete a SIP account, perform the following steps:

1. Choose **Voice > SIP Account**.
2. Choose the item to be deleted, and click **Delete**.
3. Click **OK**.

----**End**

To delete all SIP accounts, perform the following steps:

1. Choose **Voice > SIP Account**.
2. Click **Delete All**.
3. Click **OK**.

----**End**



# 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**.
3. Click **OK**.

The CPE then restarts.

----End

### 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**.
3. Click **OK**.

The CPE is then restored to its default settings.

----End

## 8.2 Changing the Password

This function enables you to change the login password of the admin user. After the password changes, enter the new password the next time you log in.

To change the password, perform the following steps:

1. Choose **System** > **Change Password**.
2. Enter the current password, set a new password, and confirm the new password.  
**New password** and **Confirm password** must contain 8 to 15 ASCII characters.
3. Click **Submit**.

----End

## 8.3 Setting the Date and 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 from PC** to automatically fill in the current local system time.
4. Click **Submit**.

----End

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. Set **Time zone**.
6. Select **Daylight saving time**. The CPE automatically provides the default DST time based on the time zone.
7. Click **Submit**.

----End

## 8.4 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.

### 8.4.1 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 **Do not fragment** to **Enable**.
6. Click **Ping**.

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

----End

## 8.4.2 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**.

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

----End

## 8.4.3 System Check

If the CPE malfunctions, you can use the System Check tool to preliminarily identify the problem. To do so:

1. Choose **System > Diagnosis**.
2. In the **Method** area, select **System check**.
3. Click **Check**.

Wait until the system check is performed. The possible causes of the CPE problem are displayed on the page.

4. Click **Export** to export the detailed information to the computer.

If necessary, send the detailed information to maintenance personnel.

----End

## 8.4.4 Checking the Wireless Status

This page displays information about the wireless network status, such as the **PLMN**, **service status**.

To view the wireless status, perform the following steps:

1. Choose **System > Diagnosis**.
2. In the **Method** area, select **Wireless status check**.

The **Wireless Status** page is displayed.

----End

## 8.5 Logs

Logs record user operations and key running events. To view logs:

1. Choose **System > Logs**.
2. Select the corresponding log level from the **Log level** drop-down list.

The number of logs in this level is displayed to the right of the drop-down list, and all logs are displayed in the output box.

3. Select the operation mode.
  - **Clear**: Clear all logs in the CPE.
  - **Export**: Export all logs in the CPE to a file in the computer.

----End

# 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 Wi-Fi or 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.

# 10

## Acronyms and Abbreviations

---

<b>ACL</b>	Access Control List
<b>AES</b>	Advanced Encryption Standard
<b>ALG</b>	Application Layer Gateway
<b>AP</b>	Access Point
<b>CPE</b>	Customer-Premises Equipment
<b>CWMP</b>	CPE WAN Management Protocol
<b>DDNS</b>	Dynamic Domain Name Server
<b>DDoS</b>	Distributed Denial of Service
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DMZ</b>	Demilitarized Zone
<b>DNS</b>	Domain Name Server/Domain Name System
<b>DoS</b>	Denial-of-Service
<b>DST</b>	Daylight Saving Time
<b>FTP</b>	File Transfer Protocol
<b>GSM</b>	Global System for Mobile Communications
<b>GUI</b>	Graphical User Interface
<b>HTTP</b>	Hypertext Transfer Protocol
<b>ICMP</b>	Internet Control Message Protocol
<b>IMEI</b>	International Mobile Station Equipment Identity
<b>IP</b>	Internet Protocol
<b>IPSec</b>	Internet Protocol Security
<b>ISP</b>	Internet Service Provider
<b>LAN</b>	Local Area Network
<b>LTE</b>	Long Term Evolution
<b>MAC</b>	Media Access Control
<b>MTU</b>	Maximum Transmission Unit
<b>NAT</b>	Network Address Translation
<b>NTP</b>	Network Time Protocol

<b>PBC</b>	Push Button Configuration
<b>PIN</b>	Personal Identification Number
<b>PKM</b>	Privacy Key Management
<b>PPPoE</b>	Point-to-Point Protocol over Ethernet
<b>PPTP</b>	Point-to-Point Tunneling Protocol
<b>RIP</b>	Routing Information Protocol
<b>RTSP</b>	Real Time Streaming Protocol
<b>QoS</b>	Quality of Service
<b>SIM</b>	Subscriber Identity Module
<b>SIP</b>	Session Initiation Protocol
<b>SN</b>	Serial Number
<b>SNTP</b>	Simple Network Time Protocol
<b>SSID</b>	Service Set Identifier
<b>SSH</b>	Secure Shell
<b>SYN</b>	Synchronous Idle
<b>TKIP</b>	Temporal Integrity Protocol
<b>TLS</b>	Transport Layer Security
<b>TTLS</b>	Tunneled Transport Layer Security
<b>UDP</b>	User Datagram Protocol
<b>UPnP</b>	Universal Plug and Play
<b>URL</b>	Uniform Resource Locator
<b>VLAN</b>	Virtual Local Area Network
<b>VoIP</b>	Voice over Internet Protocol
<b>WAN</b>	Wide Area Network
<b>WCDMA</b>	Wideband Code Division Multiple Access
<b>WEP</b>	Wired Equivalent Privacy
<b>WLAN</b>	Wireless Local Area Network
<b>WPA</b>	Wi-Fi Protected Access
<b>WPA-PSK</b>	Wi-Fi Protected Access-Pre-Shared Key
<b>WPS</b>	Wi-Fi Protected Setup