Welcome to the LTE CPE!

Online Help

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://www.huaweidevice.com/mbb_copyright or contact: **mobile@huawei.com**.

Contents

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	• Microsoft: Windows XP, Windows Vista, or Windows 7 • Mac: Mac OS X 10.5 or higher
Display resolution	1024 x 768 pixels or higher
Browser	• Internet Explorer 7.0 or later • Firefox 3.6 or later • Opera 10 or later • Safari 5 or later • Chrome 9 or later

1.3 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.

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

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

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

   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**, I**P 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. Click **Next** to view and set Internet connection parameters.
3. Click **Next** to view and set Wi-Fi-related parameters, including **Wi-Fi**, **Country/Region**, **Mode**, **Channel**, **SSID**, and **Hide SSID broadcast**.
4. Click **Next** to view and set Wi-Fi security-related parameters, such as **Security**.

   The displayed parameters vary depending on the **Security** setting. For example, if **Security** is set to **WPA-PSK&WPA2-PSK**, then **WPA-PSK** and **WPA encryption** are displayed and must be set.
5. Click **Next** to view the settings you just configured.
6. 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.

Remove the USB Dongle before you perform a local upgrade.

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 through a USB Dongle or Internet port.

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

2.4.3 Updating Using CWMP

To update the CPE software using the CPE WAN Management Protocol (CWMP), perform the following steps:

1. Choose **Home** > **Update**.
2. Click **CWMP Update**.

---End

3 Internet

3.1 Network Connection

3.1.1 Selecting a Network Mode

To select a network mode for the CPE, perform the following steps:

Insert a valid USIM card into the CPE.

Power on the CPE, and then log in to the web management page as the admin user.

1. Choose **Internet > Network Connection**.
2. Set **Network mode** to one of the following values:

Value	Description
Auto	The CPE automatically selects its working mode, with an order of preference of 4G, 3G and 2G.
4G	The CPE accesses 4G networks only.
3G	The CPE accesses 3G networks only.
2G	The CPE accesses 2G networks only.

3. Click **Submit**.

----End

3.1.2 Selecting a Connection Mode

To select a network connection mode, perform the following steps:

1. Choose **Internet > Network Connection**.
2. Set **Connection mode**.

Value	Description
Always on	If the conditions permit, the CPE automatically connects to the Internet. When roaming, accessing the network automatically may incur additional charges.
Manual	The CPE disconnects from the Internet upon startup. You can connect or disconnect the CPE to or from the Internet manually.

3. Click **Submit**.

----End

3.1.3 Selecting an APN Profile

You can select an APN profile for the CPE to access the Internet.

To set the APN profile, perform the following steps:

1. Choose **Internet > Network Connection**.
2. Select a profile from the **Profile** drop-down list.
3. Click **Submit**.

----End

3.1.4 Selecting PDP Type

You can select a PDP (Packet Data Protocol) to set the dial-up type, perform the following steps:

1. Choose **Internet > Network Connection**.
2. Set **PDP type** to one of the following values described in the following table:

Value	Description
IPv4	Internet Protocol version 4 (IPv4) that is the foundation for current Internet technologies. Because IP resources are limited, an IP address is shared by different persons in different time periods, that is, an IP address is not allocated to only one network subscriber. Thus, the real-name system cannot be implemented over the IPv4-based networks.
IPv4/IPv6	IPv4-to-IPv6 transition technology that is used when IPv4 and IPv6 coexist.

3. Click **Submit**.

----End

3.1.5 Setting Data Roaming

To turn roaming on or off, perform the following steps:

1. Choose **Internet > Network Connection**.
2. Do as follows:
   - Select the **Enable** check box behind the **Data Roaming** to turn it on.
   - Clear the **Enable** check box behind the **Data Roaming** to turn it off.
3. Click **Submit**.

----End

3.2 APN Management

To create an APN profile, perform the following steps:

1. Choose **Internet** >**APN Management**.
2. Click **Add**.
3. Set **Profile name**, **APN**, **User Name** and **Password**.
4. Set **Authentication** to **None**, **PAP**, **CHAP** or **Auto**.
5. Click **Submit**.

----End

To modify an APN profile, perform the following steps:

1. Choose **Internet** >**APN Management**.
2. Choose the APN profile item to be modified, and click **Edit**.
3. Modify **Profile name**, **APN**, **User Name** or **Password**.
4. Set **Authentication** to **None**, **PAP**, **CHAP** or **Auto**.
5. Click **Submit**.

----End

To delete an APN profile, perform the following steps:

1. Choose **Internet** >**APN Management**.
2. Choose the APN profile item to be deleted, and click **Delete**.
3. Click **OK**.

----End

3.3 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

3.3.1 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

3.3.2 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

3.3.3 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

3.3.4 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

3.3.5 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

3.3.6 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

3.3.7 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

3.4 Setting the Internet MTU

A maximum transmission unit (MTU) is defined as the maximum packet size (in bytes) at a communication protocol layer. It relates to communication ports, for example, network interface cards and serial ports.

To set the MTU, perform the following steps:

1. Choose **Internet** > **Internet MTU**.
2. Set **Internet MTU** to a value in the range of 1280 to 1500.
3. 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 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

4.2 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

4.3 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

5 Wi-Fi

5.1 Wi-Fi Settings

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

5.1.1 Setting General Parameters

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

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

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

4. Click **Submit**.

----End

5.1.2 Setting SSID Profile

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

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

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

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

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

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

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

   A maximum of 32 clients can connect to the CPE.

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

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

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

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

6. Set **Security**.

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

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

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

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

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

7. Set the encryption mode.

If…	Sets to	Description
WEP	Authentication mode	• **Shared authentication**: The client connects to the CPE in shared authentication mode. • **Open authentication**: The client connects to the CPE in open authentication mode. • **Both**: The client connects to the CPE in shared or open authentication mode.
	Encryption password length	• **128bit**: Only 13 ASCII characters or 26 hex characters can be entered in the **Key 1** to **Key 4** boxes. • **64bit**: Only 5 ASCII characters or 10 hex characters can be entered in the **Key 1** to **Key 4** boxes.
	Current password index	This value can be set to **1**, **2**, **3**, or **4**. After a key index is selected, the corresponding key takes effect.
WPA-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to **TKIP+AES**, **AES**, or **TKIP**.

If…	Sets to	Description
WPA2-PSK(recommended)	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to **TKIP+AES**, **AES**, or **TKIP**.
WPA-PSK & WPA2-PSK	WPA-PSK	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	This value can be set to **TKIP+AES**, **AES**, or **TKIP**.

8. 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 **Status** to **Enable**.
4. 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: / ' = " \ &

5. Set **Maximum number of devices**.

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

   A maximum of 32 clients can connect to the CPE.

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

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

7. Set **AP isolation** to **Enable**.

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

8. Set **Security**.

   If **Security** is set to **WPA-PSK, WPA2-PSK** or **WPA-PSK & WPA2-PSK**, you can set **WPA encryption** and **WPA-PSK.**

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

   If **Security** is set to **WEP**, set **Authentication mode**, **Password length** and **Current password index**, and configure the corresponding keys.

   If **Password length** is set to **128-bit**, **WPA-PSK** can contain 8 to 63 ASCII characters or 64 hex characters.

If **Password length** is set to **64-bit**, the 64-bit encryption key must contain 5 ASCII characters or 10 hex characters.

9. Click **Submit**.

----End

5.5 Advanced Settings

Advanced Settings affect Wi-Fi performance. The settings help you to obtain the maximum rate through optimal access performance.

To configure the advanced settings, perform the following steps:

1. Choose **Wi-Fi** > **Advanced Settings**.
2. Set **Country/Region**.
3. Set **Channel**.

   Auto indicates that the channel with the best signal quality is selected.

   The value **1** to **13** indicates the selected channel.

4. Set **802.11n bandwidth**.

   If this parameter is set to **20MHz**, 802.11n supports only 20 MHz bandwidth.

   If this parameter is set to **20/40MHz**, 802.11n supports 20 MHz or 40 MHz bandwidth.

5. Set **Transmit power**.

   If this parameter is set to **100%**, the Wi-Fi client transmits at full power.

   If this parameter is set to **80%**, **60%**, or **40%**, the Wi-Fi client transmits signals at low power. The Wi-Fi client located far away from the CPE may fail to access the CPE.

6. Set **WMM** to **Enable**.

   Wi- Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard. It provides basic quality of service (QoS) features for IEEE 802.11 networks. WMM prioritizes traffic according to four access categories (AC): voice, video, best effort, and background. However, WMM does not provide guaranteed throughput. WMM applies to simple applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones.

7. Click **Submit**.

----End

5.6 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 6.2.1 "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 6.3.1 "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 6.4.1 "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

7 Services

7.1 Setting 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 **Services** > **DDNS**.
2. In **Service provider**, choose **DynDNS.org**.
3. Set **DDNS** to **Enable**.
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**.

----End

7.2 SMS Settings

7.2.1 Viewing SMS Messages

You can check the messages in your inbox, drafts, and outbox folders.

To view a message, perform the following steps:

1. Choose **Services** > **SMS Messages**.
2. Do as follows:
   - Click **Inbox** to view received messages.
   - Click **Drafts** to view draft messages.
   - Click **Outbox** to view sent messages.

----End

7.2.2 Sending SMS Messages

To send a message, perform the following steps:

1. Choose **Services** > **SMS Messages**.
2. In **Phone number**, enter the recipient's phone number.

   If you want to send a message to multiple recipients, use semicolons (;) to separate the phone numbers.
3. In **Content**, edit a message.
4. Click **Send**.

   ----End

7.2.3 Saving SMS Messages

To save a message, perform the following steps:

1. Choose **Services** > **SMS Messages**.
2. In **Phone number**, enter the recipients' phone numbers.
3. In **Content**, edit a message.
4. Click **Save**.

   ----End

7.2.4 Forwarding SMS Messages

To forward a message, perform the following steps:

1. Choose **Services** > **SMS Messages**.
2. Choose the message to be forwarded, and click **Forward.**
3. In **Phone number**, enter the recipients' phone numbers.
4. Click **Send**.

   ----End

7.2.5 Replying to SMS Messages

To reply to a message, perform the following steps:

1. Choose **Services** > **SMS Messages**.
2. Choose the message to be replied, and click **Reply.**
3. In **Content**, edit a message.
4. Click **Send**.

   ----End

7.2.6 Deleting SMS Messages

To delete one or more SMS messages, perform the following steps:

1. Choose **Services** > **SMS Messages**.
2. Do as follows:
   - Choose the message to be deleted, and click **Delete.**
   - To delete all messages on a page, click **Delete Page**.

   ----End

7.3 Setting SMS

You can configure SMS settings, such as setting the SMS center number, enabling or disabling an SMS report, and setting whether to save sent messages.

1. Choose **Services** > **SMS Settings**.
2. In the **Service center address** box, enter the SMS center number.
3. Set whether to enable **SMS report**.
4. Set whether to enable **Save sent messages**.

   A message sent to multiple recipients cannot be saved.

5. Select the save time from the drop-down list.
6. Click **Submit**.

   ----End

7.4 Setting FTP Server

The FTP server enables you to share data on your USB storage device.

To enable the FTP server, perform the following steps:

1. Choose **Services** > **Ftp server**.
2. Set **Ftp** to **Enable**.
3. Click **Submit**.

   ----End

7.5 Setting Samba Server

Samba is a software package for sharing files and printers between computers running Windows and computers running Unix on a Wi-Fi network.

To enable the Samba server, perform the following steps:

1. Choose **Services** > **Samba server**.
2. Set **Samba** to **Enable**.

3. Click **Submit**.

----End

7.6 Setting DLNA Server

Digital Living Network Alliance (DLNA) support enables you to access your music, photos and videos anywhere, anytime.

To enable the DLNA server, perform the following steps:

1. Choose **Services** > **DLNA server**.
2. Set **DLNA server** to **Enable**.
3. Click **Submit**.

----End

7.7 Configuring User Settings

You can add users to the user list to share the files and directories in the USB disk. Using the configured account, users can access the FTP server through the FTP client.

The user list shows the added users and related information, for example, user names, shared directories, and permissions. In addition, you can add, edit, or delete the users.

To add a user to the user list, perform the following steps:

1. Choose **Services** > **User Settings**.
2. Click **Add**.
3. Set the parameters related to the user.
4. Click **Submit**.

----End

To modify a user in the user list, perform the following steps:

1. Choose **Services** > **User Settings**.
2. Choose the user to be modified, and click **Edit**.
3. Modify the parameter settings.
4. Click **Submit**.

----End

To delete a user from the user list, perform the following steps:

1. Choose **Services** > **User Settings**.
2. Choose the user to be deleted, and click **Delete**.

3. Click **OK**.

----End

To delete all users from the user list, perform the following steps:

1. Choose **Services** > **User Settings**.
2. Click **Delete All**.
3. Click **OK**.

----End

7.8 Viewing USB Storage

The **USB Storage** page displays the USB storage space, for example, total storage space, used space, and free space.

To view the USB storage space, perform the following steps:

1. Choose **Services** > **USB Storage**.
2. View the information about the USB storage space.

----End

8 VoIP

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

8.1 Viewing VoIP Information

To view the VoIP information, perform the following steps:

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

----End

8.2 Configuring a SIP Server

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

1. Choose **VoIP** > **SIP Server**.
2. In the **User Agent port** box, enter the port of the SIP account provided by your service provider.
3. In the **Proxy server address** box, enter the address of the proxy server provided by your service provider, for example, **192.168.1.10**.
4. In the **Proxy server port** box, enter the port of the proxy server provided by your service provider, for example, **5060**.

   The value ranges from 1 to 65535.
5. In the **Registration server address** box, enter the address of the registration server provided by your service provider, for example, **192.168.1.11**.
6. In the **Registration server port** box, enter the port of the registration server provided by your service provider, for example, **5060**.

   The value ranges from 1 to 65535.
7. In the **SIP server domain name** box, enter the domain name of the SIP server.

   If you set **Secondary server** to **Enable**, you should set the previous parameters again.
8. Click **Submit**.

----End

8.3 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 **VoIP** > **SIP Account**.
2. Click **Add**.
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 **VoIP** > **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 **VoIP** > **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 **VoIP** > **SIP Account**.
2. Click **Delete All**.
3. Click **OK**.

----End

8.4 Managing Speed Dial

Speed dial enables you to quickly dial a telephone number. Once you assign a speed dial number to a telephone number, you can use the former to dial the latter. You can configure up to 10 speed dial numbers.

To add a speed dial number, perform the following steps:

1. Choose **VoIP** > **Speed Dial**.
2. Click **Add**.
3. In the **Speed Dial Number** box, enter an easily remembered number.
4. In the **Actual Number** box, enter the actual telephone number.
5. In the **Description** box, enter a description for the speed dial number.
6. Click **Submit**.

----End

To modify a speed dial number, perform the following steps:

1. Choose **VoIP** > **Speed Dial**.
2. Choose the item to be modified, and click **Edit**.
3. Repeat steps 3 through 5 in the previous procedure.
4. Click **Submit**.

----End

To delete a speed dial number, perform the following steps:

1. Choose **VoIP** > **Speed Dial**.
2. Choose the number to be deleted, and click **Delete**.
3. Click **OK**.

----End

To delete all speed dial numbers, perform the following steps:

1. Choose **VoIP** > **Speed Dial**.
2. Click **Delete All**.
3. Click **OK**.

----End

8.5 Setting Advanced SIP Parameters

On the **Advanced SIP** page, you can set advanced SIP parameters. It is recommended that you retain the default settings.

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

1. Choose **VoIP** > **Advanced SIP**.
2. Set the following parameters:

- **Registration timeout (seconds)**: specifies the validity period for registration. The value ranges from 60 to 65535.
- **Session timeout (seconds)**: specifies the validity period for a server session. The value ranges from 100 to 3600.
- **Minimum session timeout (seconds)**: specifies the shortest validity period for a server session. The value ranges from 90 to 1800. If you set both **Minimum session timeout (seconds)** and **Session timeout (seconds)**, the **Minimum session timeout (seconds)** settings prevail.
- **Call waiting**: specifies whether to enable call waiting.

3. Click **Submit**.

----End

8.6 Setting Advanced Voice Parameters

On the **Advanced Voice** page, you can set advanced voice parameters. It is recommended that you retain the default settings.

To set the advanced voice parameters, perform the following steps:

1. Choose **VoIP** > **Advanced Voice**.
2. Set the following parameters:
   - **DTMF Method**: specifies the Dual Tone Multi-Frequency (DTMF) transmission mode.
   - **Fax Option**: specifies the Fax over IP mode.
   - **Country/Region**: specifies the country or region where the CPE is located.

     If you change the **Country/Region** settings, you must restart the CPE for the settings to take effect.

   - **Outgoing List**: Select the primary outgoing account from the drop-down list.
   - **RTP Start Port**: specifies the Real-time Transfer Protocol (RTP) port number. The value is an even number ranging from 50000 to 65514.
   - Set other parameters, it is recommended that you retain the default settings.
3. Click **Submit**.

----End

8.7 Setting Advanced Codec Parameters

On the **Advanced Codec** page, you can set advanced voice codec parameters. It is recommended that you retain the default settings.

To set the advanced codec parameters, perform the following steps:

1. Choose **VoIP** > **Advanced Codec**.

2. Set the following parameters:
   - **Primary codec type**: specifies the primary voice codec type. The default value is **G.711-PCMA**.
   - **Secondary codec type**: specifies the secondary voice codec type. The default value is **G.711-PCMU**.
   - **Third codec type**: specifies the third voice codec type. The default value is **G.726-32**.
   - **Fourth codec type**: specifies the fourth voice codec type. The default value is **G.726-24**.
   - **Fifth codec type**: specifies the fifth voice codec type. The default value is **G.729**.
   - **Sixth codec type**: specifies the sixth voice codec type. The default value is **G.722**.
3. Click **Submit**.

----End

9 System

9.1 Maintenance

9.1.1 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

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

   The CPE is then restored to its default settings.

   ----End

9.1.3 Downloading a 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.

   In the displayed dialog box, select the save path and name of the configuration file to be backed up.
3. Click **Save**.

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

   ----End

9.1.4 Uploading a 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.

   In the displayed dialog box, select the backed up configuration file.
3. Click **Open**.

   The dialog box closes. In the box to the right of **Configuration file**, the save path and name of the backed up configuration file are displayed.
4. Click **Upload**.
5. Click **OK**.

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

   ----End

9.2 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

9.3 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

9.4 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.

9.4.1 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

9.4.2 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

9.4.3 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

9.4.4 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

9.5 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

9.6 System Notification

This page enables you to configure the notification methods of key device status changes.

1. Choose **System** > **System Notification**.
2. Set **Frequency** from the drop-down list**.**

   Set **Web popup receiving IP.** If **Web popup receiving IP** is left blank, notifications are randomly sent to connected clients.
3. Set **Send SMS notification to**, and **Forward SMS from**.

   After **Send SMS notification to** setting takes effect, message test, forwarding, and notification settings can be configured.
4. Configure the notification settings for each **Events**.
5. Click **Submit**.

   ----End

9.7 Setting TR-069

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

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

1. Choose **System** > **TR-069 Settings**.
2. To enable the CPE to send inform packets to the ACS at predefined intervals, set **Periodic inform** to **Enable**.
3. If you set **Periodic inform** to **Enable**, set **Periodic inform interval**.
4. In the **ACS URL** box, enter the ACS URL address.
5. Enter **ACS user name** and **ACS password** for 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.
6. Click **Submit**.

   ----End

9.8 Setting Antenna

To set the antenna type, perform the following steps:

1. Choose **System** > **Antenna Settings**.
2. Select the antenna type from the drop-down list.
3. Click **Submit**.

----End

10 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.

11 Acronyms and Abbreviations

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

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