Welcome to use LTE CPE!

LTE CPE Online Help

Issue 01

Date 2013-01-08

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: terminal@huawei.com

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: terminal@huawei.com

Contents

1 Getting Started

1.1 Welcome to Use the Router

In this document, customer premises equipment (CPE) is referred to as the router. Read the following safety symbols carefully to ensure the correct and safe use of your router:

💬	Indicates additional information about the topic.
☀	Prompts optional methods or the shortcut for an action.
⚠	Warns potential problems or conventions that need to be specified.

1.2 Configuration Requirements for Your Computer

Your computer must meet the requirements of the router. Otherwise, performance will deteriorate.

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
Display resolution	1024 x 768 pixels or higher
Browser	• Internet Explorer 7.0 or a later version • Firefox 3.5 or a later version • Opera 10 or a later version • Safari 5 or a later version • Chrome 9 or a later version

2 Status

2.1 Internet

2.1.1 Status

To view the wide area network (WAN) connection status, perform the following steps:

1. Choose **Status** > **Internet**.
2. View the WAN connection status.

----End

2.1.2 Statistics

To view the statistics for the WAN port, perform the following steps:

1. Choose **Status** > **Internet**.
2. View the statistics for the WAN port, including uplink and downlink rates, uplink and downlink traffic volumes, and online duration.

----End

2.2 LAN

2.2.1 Status

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

1. Choose **Status** > **LAN**.
2. View the LAN connection status, including the IP address, media access control (MAC) address, Dynamic Host Configuration Protocol (DHCP) server, and LAN ports.

----End

2.2.2 Statistics

To view the statistics for LAN ports, perform the following steps:

1. Choose **Status** > **LAN**.

2. View the statistics for LAN ports, including the number of bytes, number of packets, number of erroneous packets, and number of discarded packets transmitted and received on LAN ports.

----End

2.3 WLAN

2.3.1 Status

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

1. Choose **Status** > **WLAN**.
2. View the WLAN connection status, including SSID, IP address, MAC address, broadcast mode, and wireless encryption mode.

----End

2.3.2 Statistics

To view the statistics for WLAN ports, perform the following steps:

1. Choose **Status** > **WLAN**.
2. View the statistics for WLAN ports, including the number of bytes, number of packets, number of erroneous packets, and number of discarded packets transmitted and received on WLAN ports.

----End

3 General Settings

3.1 DHCP Settings

LAN is a shared communication system to which more than one device are attached limited to the immediate area.

With correct LAN settings, network devices such as computers can share communication on the LAN through the router.

3.1.1 LAN Host Settings

You can change the host IP address to another individual IP address that is easy to remember, and make sure that IP address is unique on your network. If you change the IP address of the router, you need to access the web-based utility with the new IP address.

To change the IP address and subnet mask of the router, perform the following steps:

1. Choose **General Settings** > **DHCP Settings**.

   The **DHCP Settings** page is displayed.

2. Set **IP address**.
3. Set **Subnet mask**.
4. Select the **Enable** check box behind **DHCP server**.
5. Click **Submit**.

----End

3.1.2 DHCP Settings

DHCP allows individual clients to obtain TCP/IP configuration automatically upon startup from a server.

You can configure the router as a DHCP server or disable it when the router is working in the routing mode.

When configured as a DHCP server, the router provides the TCP/IP configuration automatically for the LAN clients that support DHCP client capability. 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 **General Settings** > **DHCP Settings**.

   The **DHCP Settings** page is displayed.

2. Select the **Enable** check box behind **DHCP server**.

3. Set **Start IP address**.

   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.

4. Set **End IP address**.

   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.

   The end IP address must be less than or equal to the start IP address.

5. Set **Lease time**.

   This parameter can be set to 1 to 10,080 minutes.

6. Click **Submit**.

----End

The device list indicates the information about active devices.

To view the device list, perform the following steps:

1. Choose **General Settings** > **DHCP Settings**. Click **Connected Devices**. The **Connected Devices** page is displayed.

2. View the device list. It includes **PC 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 bound, **Lease Time** and **PC Name** are displayed as **N/A** and **Unknown** respectively.

----End

3.2 WLAN Settings

3.2.1 General Settings

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

To configure basic WLAN settings, perform the following steps:

1. Choose **General Settings** > **WLAN Settings**.

   The **WLAN Settings** page is displayed.

2. Select the **Enable** check box behind **WLAN**.

3. Set **Mode** to one of the values described in the following table:

Parameter Value	Description
802.11b/g/n	The Wi-Fi station can connect to the router in 802.11b, 802.11g, or 802.11n mode. If the station connects to the router in 802.11n mode, AES encryption mode is required.
802.11b/g	The Wi-Fi station can connect to the router in 802.11b or 802.11g mode.
802.11b	The Wi-Fi station can connect to the router in 802.11b mode.
802.11g	The Wi-Fi station can connect to the router in 802.11g mode.
802.11n	The Wi-Fi station can connect to the router in 802.11n mode.

4. Set **Channel**.

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

   The value **1** to **14** indicates the selected channel.

5. 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.

   If **Mode** is set to **802.11b** or **802.11g**, this parameter does not need to be set.

6. Set **Rate**.

   Rate varies depending on the selected mode.

   If **Rate** is set to **Auto**, the Wi-Fi station connects to the router through the channel with the best signal quality.

   If the rate is specified, the station connects to the router at a specified rate. If the channel conditions do not meet the requirement, connection performance is affected.

7. Set **Transmit power**.

   If this parameter is set to **90%(recommended)**, the Wi-Fi station transmits at the optimal power.

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

   If this parameter is set to **80%**, **60%**, **30%**, or **5%**, the Wi-Fi station transmits at low power. The Wi-Fi station far away from the router may fail to access the router.

8. Click **Submit**.

----End

3.2.2 Interface Profile

After you configure the router on the **Interface Profile** page, the Wi-Fi station connects to the router based on preset rules, improving access security.

To configure the router on the **Interface Profile** page, perform the following steps:

1. Choose **General Settings** > **WLAN Settings**.

   The **WLAN Settings** page is displayed.

2. Set **SSID**.

   > This parameter contains only 1 to 32 ASCII characters.
   >
   > The Wi-Fi station connects to the router using the searched SSID.

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

   > This parameter indicates the maximum number of Wi-Fi stations that connect to the router.
   >
   > A maximum of 16 stations can connect to the router.

4. Select the **Enable** check box behind **Hide SSID broadcast**.

   The SSID is hidden. In this case, the station cannot detect Wi-Fi information about the router.

5. Select the **Enable** check box behind **AP isolation**. The stations can connect to the router but cannot communicate with each other.

6. Set **Security**.

   > If this parameter is set to **NONE(not recommended)**, the Wi-Fi station directly connects to the router. This causes security risks.
   >
   > If this parameter is set to **WEP**, the Wi-Fi station connects to the router in web-based encryption mode.
   >
   > If this parameter is set to **WPA-PSK**, the Wi-Fi station connects to the router in WPA-PSK encryption mode.
   >
   > If this parameter is set to **WPA2-PSK(recommended)**, the Wi-Fi station connects to the router in WPA2-PSK encryption mode. This mode is recommended because it has a high security level.
   >
   > If this parameter is set to **WPA-PSK+WPA2-PSK**, the Wi-Fi station connects to the router in WPA-PSK or WPA2-PSK encryption mode.

7. Set the encryption mode.

If…	Sets to	Description
WEP	BASIC authentication	- **Shared Authentication**: The station connects to the router in shared authentication mode. - **Open Authentication**: The station connects to the router in open authentication mode. - **Both Authentication**: The station connects to the router in shared or open authentication mode.
	Encryption key 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 key index	It can be set to **1**, **2**, **3**, or **4**. After a key index is selected, the corresponding key takes effect.
WPA-PSK	WPA pre-shared key	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	It can be set to **TKIP+AES**, **AES**, or **TKIP**.
WPA2-PSK(recommended)	WPA pre-shared key	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	It can be set to **TKIP+AES**, **AES**, or **TKIP**.
WPA-PSK +WPA2-PSK	WPA pre-shared key	Only 8 to 63 ASCII characters or 8 to 64 hex characters can be entered.
	WPA encryption	It can be set to **TKIP+AES**, **AES**, or **TKIP**.

8. Click **Submit**.

----End

3.3 WLAN Multi SSID

You can set the parameters related to the SSIDs, for example, configure different rates and modes. By default, the SSID with the index of 1 is enabled and cannot be disabled, and Other SSIDs is disabled.

3.3.1 SSID List

The **SSID List** page shows the information about the SSIDs to be configured. To configure an SSID, perform the following steps:

1. Choose **General Settings** > **WLAN Multi SSID**.

The **SSID List** page is displayed.

2. Select an SSID to be configured, and click **Edit**.
3. Select the **Enable** check box behind **SSID**.
4. Set **SSID**.

   The SSID should contain 1 to 32 ASCII characters.

   The SSID cannot contain the following special characters: ‘/’,’'’,’=’,’"’,’\’,’&’.

5. Set **Maximum Number of Connected Devices**.

   The number of accessing devices should be an integer ranging from 1 to 16.

6. Select the **Enable** check box behind **Hide SSID Broadcast**.
7. Set **AP isolation**. If the **Enable** check box is selected, stations can connect to the router but cannot communicate with each other. If the check box is not selected, stations can connect to the router at the same time and communicate with each other.
8. Set **Security**. If **Mode** is set to **802.11n** on the **General Settings** page, **Security** can only be set to **WPA-PSK**, **WPA2-PSK**, or the corresponding encryption mode.

   If **Security** is set to **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK+WPA2-PSK**, set **WPA pre-shared key** and **WPA encryption**.

   The WPA pre-shared key should be 8 to 63 ASCII characters or 64 hex characters.

   If **Security** is set to **WEP, set BASIC authentication**, **Encryption key length**, and **Current key index**, and configure the corresponding keys.

   If **Encryption key length** is set to **128-bit**, the WPA pre-shared key should be 8 to 63 ASCII characters or 64 hex characters.

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

9. Click **Submit**.

   ----End

3.4 WLAN Access Restrictions

3.4.1 WLAN MAC Control

This function enables you to manage the access to the router. You can set access restriction policies for each SSID.

MAC access of each SSID can be set to **Disable**, **Blacklist**, or **Whitelist**.

- If **SSID1 MAC Access** is set to **Disable**, access restriction does not take effect.
- If **SSID1 MAC Access** is set to **Blacklist**, only the devices that are not in the blacklist can connect to the SSID.
- If **SSID1 MAC Access** is set to **Whitelist**, only the devices in the whitelist can connect to the SSID.

To configure WLAN MAC control settings, perform the following steps:

1. Choose **General Settings** > **WLAN Access Restrictions**.

   The **WLAN MAC Control** page is displayed.

2. Set other **SSID MAC Access**.
3. Click **Submit**.

   ----End

3.4.2 WLAN MAC List

This function allows you to set the SSID access policies based on MAC addresses. Set an SSID corresponding to a MAC address.

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

1. Choose **General Settings** > **WLAN Access Restrictions**.

   The **WLAN MAC List** page is displayed.

2. Click **Set Up List**.

   The **WLAN Access List** page is displayed.

3. Click **Add Item**.
4. Set **MAC**.
5. To enable the MAC address to take effect for SSID1, select the **Enable** check box behind **For SSID1**. The operation for other SSIDs is similar to those for SSID1.
6. Click **Submit**.

   ----End

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

1. Choose **General Settings** > **WLAN Access Restrictions**.

   The **WLAN MAC List** page is displayed.

2. Click **Set Up List**.

   The **WLAN Access List** page is displayed.

3. In the entry of the item to be modified, click **Edit**.
4. On the displayed page, set **MAC**.
5. To enable the MAC address to take effect for SSID1, select the **Enable** check box behind **For SSID1**. The operation for other SSID is similar to those for SSID1.
6. Click **Submit**.

   ----End

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

1. Choose **General Settings** > **WLAN Access Restrictions**.

   The **WLAN MAC List** page is displayed.

2. Click **Set Up List**.

   The **WLAN Access List** page is displayed.

3. In the entry of the item to be deleted, click **Delete**.

   A message is displayed.

4. Click **OK**.

----End

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

1. Choose **General Settings** > **WLAN Access Restrict**.

   The **WLAN MAC List** page is displayed.

2. Click **Set Up List**.

   The **WLAN Access List** page is displayed.

3. Click **Delete All**. A message is displayed.

4. Click **OK**.

----End

4 Security Settings

4.1 Firewall General

4.1.1 Firewall Level

This page instructs you to set the firewall level. If **Firewall level** is set to **Custom**, the configuration can be modified.

To set firewall levels, perform the following steps:

1. Choose **Security Settings** > **Firewall General**.

   The **Firewall General** page is displayed.

2. Set **Firewall level**.
3. Click **Submit**.

   ----End

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

1. Choose **Security Settings** > **Firewall General**.

   The **Firewall General** page is displayed.

2. Set **Firewall level** to **Custom**.
3. Set **MAC filtering**.
4. Set **IP filtering**.
5. Set **URL filtering**.
6. Click **Submit**.

   ----End

4.2 MAC Filtering

Data is filtered by MAC address. This page allows you to configure only MAC filtering rules.

4.2.1 MAC Whitelist

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

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.

2. Set **MAC filtering mode** to **Whitelist**.
3. Click **Add Item**.
4. On the displayed page, set **MAC**.
5. Click **Submit**.

----End

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

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.

2. Set **MAC filtering mode** to **Whitelist**.
3. In the entry of the rule to be modified, click **Edit**.
4. On the displayed page, set **MAC**.
5. Click **Submit**.

----End

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

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.

2. Set **MAC filtering mode** to **Whitelist**.
3. In the entry of the rule to be deleted, click **Delete**.

   A message is displayed.

4. Click **OK**.

----End

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

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.

2. Set **MAC filtering mode** to **Whitelist**.
3. Click **Delete All**.

   A message is displayed.

4. Click **OK**.

----End

4.2.2 MAC Blacklist

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

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Blacklist**.
3. Click **Add Item**.
4. On the displayed page, set **MAC**.
5. Click **Submit**.

----End

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

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Blacklist**.
3. In the entry of the rule to be modified, click **Edit**.
4. On the displayed page, set **MAC**.
5. Click **Submit**.

----End

To delete a MAC blacklist rule, perform the following steps:

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Blacklist**.
3. In the entry of the rule to be deleted, click **Delete**.

   A message is displayed.
4. Click **OK**.

----End

To delete all MAC blacklist rules, perform the following steps:

1. Choose **Security Settings** > **MAC Filtering**.

   The **MAC Filtering** page is displayed.
2. Set **MAC filtering mode** to **Blacklist**.

3. Click **Delete All**.

   A message is displayed.

4. Click **OK**.

   ----End

4.3 IP Filtering

Data is filtered by IP address. This page allows you to configure only IP filtering rules.

4.3.1 IP Whitelist

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

1. Choose **Security Settings** > **IP Filtering**.

   The **IP Filtering** page is displayed.

2. Set **IP filtering mode** to **Whitelist**.
3. Click **Add Item**.
4. Set **Application name**.
5. Set **Protocol**.
6. In the **Source address range** box, enter the IP address or IP address segment to be filtered.
7. In the **Source port range** box, enter the port number or port number segment to be filtered.
8. In the **Destination address range** box, enter the IP address or IP address segment to be filtered.
9. In the **Destination port range** box, enter the port number or port number segment to be filtered.
10. Click **Submit**.

    ----End

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

1. Choose **Security Settings** > **IP Filtering**.

   The **IP Filtering** page is displayed.

2. Set **IP filtering mode** to **Whitelist**.
3. In the entry of the rule to be modified, click **Edit**.
4. Set **Application name**.
5. Set **Protocol**.
6. In the **Source address range** box, enter the IP address or IP address segment to be filtered.
7. In the **Source port range** box, enter the port number or port number segment to be filtered.

8. In the **Destination address range** box, enter the IP address or IP address segment to be filtered.
9. In the **Destination port range** box, enter the port number or port number segment to be filtered.
10. Click **Submit**.

----End

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

1. Choose **Security Settings** > **IP Filtering**.

   The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Whitelist**.
3. In the entry of the rule to be deleted, click **Delete**.

   A message is displayed.
4. Click **OK**.

----End

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

1. Choose **Security Settings** > **IP Filtering**.

   The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Whitelist**.
3. Click **Delete All**.

   A message is displayed.
4. Click **OK**.

----End

4.3.2 IP Blacklist

On the **Firewall General** page, if **IP filtering** is set to **Blacklist**, only the IP addresses in the IP blacklist cannot be accessed.

To add an IP blacklist rule, perform the following steps:

1. Choose **Security Settings** > **IP Filtering**.

   The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Blacklist**.
3. Click **Add Item**.
4. Set **Application name**.
5. Set **Protocol**.

6. In the **Source address range** box, enter the IP address or IP address segment to be filtered.
7. In the **Source port range** box, enter the port number or port number segment to be filtered.
8. In the **Destination address range** box, enter the IP address or IP address segment to be filtered.
9. In the **Destination port range** box, enter the port number or port number segment to be filtered.
10. Click **Submit**.

----End

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

1. Choose **Security Settings** > **IP Filtering**.

   The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Blacklist**.
3. In the entry of the rule to be modified, click **Edit**.
4. Set **Application name**.
5. Set **Protocol**.
6. In the **Source address range** box, enter the IP address or IP address segment to be filtered.
7. In the **Source port range** box, enter the port number or port number segment to be filtered.
8. In the **Destination address range** box, enter the IP address or IP address segment to be filtered.
9. In the **Destination port range** box, enter the port number or port number segment to be filtered.
10. Click **Submit**.

----End

To delete an IP blacklist rule, perform the following steps:

1. Choose **Security Settings** > **IP Filtering**.

   The **IP Filtering** page is displayed.
2. Set **IP filtering mode** to **Blacklist**.
3. In the entry of the rule to be deleted, click **Delete**.

   A message is displayed.
4. Click **OK**.

----End

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

1. Choose **Security Settings** > **IP Filtering**.

The **IP Filtering** page is displayed.

2. Set **IP filtering mode** to **Blacklist**.
3. Click **Delete All**.

   A message is displayed.
4. Click **OK**.

----End

4.4 URL Filtering

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

4.4.1 URL Whitelist

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

1. Choose **Security Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.
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 Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.
2. Set **URL filtering mode** to **Whitelist**.
3. In the entry of the rule to be modified, 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 Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.
2. Set **URL filtering mode** to **Whitelist**.

3. In the entry of the rule to be deleted, click **Delete**.

   A message is displayed.

4. Click **OK**.

   ----End

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

1. Choose **Security Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.

2. Set **URL filtering mode** to **Whitelist**.
3. Click **Delete All**.

   A message is displayed.

4. Click **OK**.

   ----End

4.4.2 URL Blacklist

On the **Firewall General** page, if **URL filtering** is set to **Blacklist**, only the URLs in the URL blacklist cannot be accessed.

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

1. Choose **Security Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.

2. Set **URL filtering mode** to **Blacklist**.
3. Click **Add Item**.
4. Set **URL**.
5. Click **Submit**.

   ----End

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

1. Choose **Security Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.

2. Set **URL filtering mode** to **Blacklist**.
3. In the entry of the rule to be modified, click **Edit**.
4. On the displayed page, set **URL**.
5. Click **Submit**.

   ----End

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

1. Choose **Security Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.

2. Set **URL filtering mode** to **Blacklist**.

3. In the entry of the rule to be deleted, click **Delete**.

   A message is displayed.

4. Click **OK**.

----End

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

1. Choose **Security Settings** > **URL Filtering**.

   The **URL Filtering** page is displayed.

2. Set **URL filtering mode** to **Blacklist**.

3. Click **Delete All**.

   A message is displayed.

4. Click **OK**.

----End

5 USB Management

5.1 Server Settings

The **Server Settings** page displays basic USB information, for example, storage space, used space, free space, and whether to enable FTP server.

5.1.1 Network Server

The **Network Server** page allows you to view and set the status of the FTP server.

To enable the FTP server, perform the following steps:

1. Choose **USB Management** > **Server Settings**.

   The **Network Server** page is displayed.

2. Select the **Enable** check box behind **FTP Server**.
3. Click **Submit**.

   ----End

5.1.2 USB Storage

The **USB Storage** page displays the USB storage space, for example, total storage space, used space, and free space. To view USB storage space, perform the following steps:

1. Choose **USB Management** > **Server Settings**.

   The **USB Storage** page is displayed.

2. Click **Refresh** to manually update the USB storage space.

   ----End

5.2 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.

5.2.1 User List

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 **USB Management** > **User Settings**.

   The **User List** page is displayed.

2. Click **Add Item**.
3. On the displayed page, set the parameters related to the user, including user name, password, confirm password, shared device, shared directory, and permission.
4. Click **Submit**.

----End

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

1. Choose **USB Management** > **User Settings**.

   The **User List** page is displayed.

2. In the entry of the user to be modified, click **Edit**.
3. On the displayed page, modify the parameter settings related to the user.
4. Click **Submit**.

----End

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

1. Choose **USB Management** > **User Settings**.

   The **User List** page is displayed.

2. In the entry of the user to be deleted, click **Delete**.

   A message is displayed.

3. Click **OK**.

----End

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

1. Choose **USB Management** > **User Settings**.

   The **User List** page is displayed.

2. Click **Delete All**.

   A message is displayed.

3. Click **OK**.

----End

6 System

6.1 Device Information

This page shows basic information about the router, for example, name, serial number (SN), international mobile equipment identity (IMEI), software version, and hardware version.

To view system information, perform the following steps:

1. Choose **System**> **Device Information**. The **Device Information** page is displayed.
2. View the information in each row.

----End

6.2 Reset

6.2.1 Reboot

This function enables you to reboot the router when it is not powered off. The parameter settings take effect only after the router is rebooted.

To reboot the router, perform the following steps:

1. Choose **System**> **Reset**. The **Reset** page is displayed.
2. Click **Reboot**. A dialog box is displayed, asking you whether to reboot the router.
3. Click **OK**. The router is automatically restarted.

----End

6.2.2 Restore

This function enables you to restore the default values of the parameters. After the router is restored, the configured parameters are replaced by default values.

To restore the router, perform the following steps:

1. Choose **System**> **Reset**. The **Reset** page is displayed.
2. Click **Restore**. A dialog box is displayed, asking you whether to restore the router to factory settings.

3. Click **OK**. The router is restored to factory settings.

----End

6.3 Backup & Recovery

This function enables you to back up the existing configuration file on the computer so that the backup configuration file can be used to restore the router when the router does not function properly.

6.3.1 Backup

To back up the existing configuration file, perform the following steps:

1. Choose **System**> **Backup & Recovery**. The **Backup & Recovery** page is displayed.
2. Click **Backup** on the **Backup** page. In the displayed dialog box, select the save path and name of the configuration file to be backed up. Click **Save**. The procedure for file downloading may vary depending on the used browser.

----End

6.3.2 Recovery

To reload the backup configuration file, perform the following steps:

1. Choose **System**> **Backup & Recovery**. The **Backup & Recovery** page is displayed.
2. Click **Browse** on the **Recovery** page. In the displayed dialog box, select the backup configuration file.
3. Click **Open**. The dialog box closes. In the box on the right of **Configuration file**, the save path and name of the backup configuration file are displayed.
4. Click **Recover**. A dialog box is displayed, asking you whether to upgrade the software version.
5. Click **OK**. The router reloads the backup configuration file. After reloading, the router is automatically restarted.

----End

6.4 Password Change

This function enables you to change the login password of the admin user. After the password is changed, the new password is used upon next login.

To change the password, perform the following steps:

1. Choose **System**> **Password Change**. The **Password Change** page is displayed.
2. Set **Current password**, **New password**, and **Confirm password**. The new password and confirm password must contain 6 to 15 ASCII characters.
3. Click **Submit**.

----End

6.5 Date & Time

6.5.1 Settings

You can manually configure the system time or synchronize the system time with the network. If **Synchronize with network time** is selected, the router regularly obtains time from the server for synchronization. If daylight saving time (DST) is enabled, the router also adjusts the system time based on the DST time.

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

1. Choose **System**> **Date & Time**. The **Settings** page is displayed.
2. Click the **Manual set with local time** option button.
3. Set **Local time** or click **Time From PC**.
4. Click **Submit**.

----End

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

1. Choose **System**> **Date** & **Time**. The **Settings** page is displayed.
2. Click the **Synchronize with network time** option button.
3. Set **NTP server 1**. It is the primary server for time synchronization.
4. Set **NTP server 2**. It is the secondary server for time synchronization.
5. Set **Time zone**. Different countries and areas have their own time zones. You can select a time zone from the drop-down list.
6. Select the **Enable daylight saving time** check box.

   If DST is enabled, the start and end time of DST must be configured. The router automatically provides the default DST time based on the time zone. **Daylight saving time start**, **Daylight saving time end**, and **Daylight saving time offset** can be set as required.
7. Click **Submit**.

----End

6.6 Diagnosis

When the router does not function properly, the diagnosis tools on the **Diagnosis** page can be used to preliminarily identify the problem so that actions are taken to solve the problem.

6.6.1 Ping

When the router fails to access the Internet, run the ping command to preliminarily identify the problem.

To run the ping command to preliminarily identify the problem, perform the following steps:

1. Choose **System**> **Diagnosis**. On the **Diagnosis** page, set Diagnosis **method** to **Ping**. The **Ping** page is displayed.
2. Enter the domain name in the **Destination IP address or domain** box, for example, www.google.com.
3. Set **Packet size** and **Timeout** and select the **Enable** check box behind **Do not Fragment**.
4. Click **Ping**.
5. Wait until the ping operation is performed. The command output is displayed in the **Result** box.

----End

6.6.2 Traceroute

When the router fails to access the Internet, run the Traceroute command to preliminarily identify the problem.

To run the Traceroute command to preliminarily identify the problem, perform the following steps:

1. Choose **System**> **Diagnosis**. On the **Diagnosis** page, set Diagnosis **method** to **Traceroute**. The **Traceroute** page is displayed.
2. Enter the domain name in the **Destination IP address or domain** box, for example, www.google.com.
3. Set **Maximum Hops** and **Timeout**.
4. Click **Traceroute**.
5. Wait until the Traceroute operation is performed. The command output is displayed in the **Result** box.

----End

6.6.3 System Check

When the router does not function properly, the System Check tool can be used to preliminarily identify the problem.

To use the System Check tool to preliminarily identify the problem, perform the following steps:

1. Choose **System**> **Diagnosis**. On the **Diagnosis** page, set Diagnosis **method** to **System Check**. The **System Check** page is displayed.
2. Click **Check**.
3. Wait until the system check is performed. The possible causes will be 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

6.6.4 Wireless Status

This page displays information about the wireless network status, such as the PLMN, service status, bandwidth, cell ID, signal strength, RSRP, RSRQ and roaming status.

To view the wireless status, perform the following steps:

1. Choose **System > Diagnosis**. On the Method page, set Diagnosis method to **Wireless Status.**The **Wireless Status** page is then displayed.
2. View the information in each row.

----End

6.7 Log

Logs record user operations and key running events. To view logs, perform the following steps:

1. Choose **System**> **Log**. The **Log** page is displayed.
2. Select the corresponding log level from the **Log level** drop-down list. The number of logs of this level is displayed on the right of the drop-down list, and all logs are detailed in the output box.
3. Select the operation mode.
   - **Clear**: Clears all logs in the router.
   - **Export**: Exports all logs in the router to a file in the computer.

----End

7 FAQs

The POWER indicator is not off.
• Check that the power cable is connected properly and that the router is powered on. • Check that the power adapter meets specifications.
Login to the web management page fails.
• Check that the router is started. • Check that the network cable between the router and the computer is connected properly. • Check that the IP address of the computer is set correctly. If the problem persists, contact authorized local service suppliers.
The router fails to search for the wireless network.
• Check that the power adapter is connected properly. • Check that the router is placed at an open area that is far away from obstructions such as concrete or wooden walls. • Check that the router 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 router is overheated.
• The router will be overheated after being used for a long time. Therefore, power off the router when you do not use it. • Check that the router is properly ventilated and kept far away from direct sunlight.
The parameters are restored to default values.
• If the router is powered off unexpectedly during the configuration, the parameters may be restored to default settings. • Huawei recommends that you export the parameter settings after the set the parameters so that the router can be quickly restored to the previous status using the exported settings.

8 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
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
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

9 Copyright Notice and Warranty Disclaimer

This product incorporates open source software components covered by the terms of third party copyright notices and license agreements contained below.

Samba

Copyright© Andrew Tridgell 1994-2002

GNU General Public License V2.0

http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html

DJV Image and Movie Viewersg

Copyright© 2004-2009 Darby Johnston

http://djv.sourceforge.net/legal.html

BSD License/ Modified BSD License

http://www.opensource.org/licenses/bsd-license

EasySoap++

Copyright© 2001 David Crowley; SciTegic, Inc.

GNU Library or "Lesser" General Public License V2.0

http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html

Open BSD

Copyright©1996-2011 OpenBSD

BSD License/ Modified BSD License

http://www.opensource.org/licenses/bsd-license

m2sc

Copyright© 2009 Google

http://code.google.com/p/m2sc/

GNU General Public License 3.0

http://www.gnu.org/licenses/gpl.html

WRITTEN OFFER

If you would like a copy of the GPL source code contained in this product shipped on a CD, for a charge $20 no more than the cost of preparing and mailing a CD to you, please contact mobile@huawei.com.