Wonderful Communication, Mobile Life.

Welcome to HUAWEI E960 Wireless Gateway.

HUAWEI E960 Wireless Gateway

User Guide

Copyright © 2007 Huawei Technologies Co., Ltd.

All Rights Reserved

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

Trademarks

and HUAWEI are trademarks of Huawei Technologies Co., Ltd. All other trademarks and trade names mentioned in this manual are the property of their respective holders.

Notice

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

Safety Precautions

Read the safety precautions carefully to ensure the correct and safe use of your wireless device. For detailed information, see Chapter 15 "Warnings and Precautions."

	Do not switch on your device when the device use is prohibited or when the device use may cause interference or danger.
	Do not use your device while driving.
	Follow the rules or regulations in hospitals and health care facilities. Switch off your device near medical apparatus.
	Switch off your device in an aircraft. The device may cause interference to control signals of the aircraft.
	Switch off your device near high-precision electronic devices. The device may affect the performance of these devices.
	Do not attempt to disassemble your device or its accessories. Only qualified personnel are allowed to service or repair the device.
	Do not place your device or its accessories in containers with strong electromagnetic field.
	Do not place magnetic storage media near your device. Radiation from the device may erase the information stored on them.
	Do not put your device in a high-temperature place or use it in a place with flammable gas such as a gas station.
	Keep your device and its accessories away from children. Do not allow children to use your device without guidance.
	Use approved batteries and chargers only to avoid explosion.
	Observe the laws or regulations on device use. Respect others' privacy and legal rights when using your device.

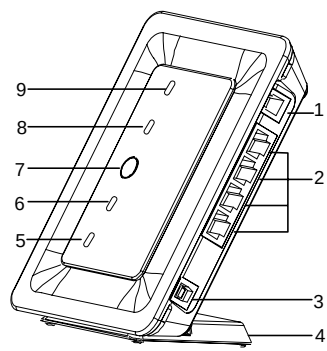
Table of Contents

1 Getting to Know Your E960

Your E960 supports HSDPA/WCDMA 2100, GSM/GPRS/EDGE 1900/1800/900/850, and network auto-switch. With the E960, you can experience wireless gateway and USB modem at any time and any place.

Appearance

1. Phone cable interface
2. Ethernet cable interface
3. Power adapter/USB cable interface
4. Pedestal
5. Network mode indicator
6. Signal strength indicator
7. ON/OFF key
8. WLAN indicator
9. Power indicator



Indicator and Button

The following table introduces the indicator and button of your E960.

Indicator	
Power	When it is steady on in yellow, the E960 is switched on successfully.
WLAN	If it is steady on and in yellow, the WLAN is enabled. If it is blinking, data is transmitting

Indicator	
Signal strength	• Fast blinking in red: SIM card faults (SIM card does not exist or the PIN code is not verified) • Steady on and in red: signal strength in level one (weak) • Steady on and in yellow: signal strength in level two or three (middle) • Steady on and in green: signal strength in level four or five (strong)
Network mode	• Double blinking in green: searching the network • Blinking in green: registering with the 2G network • Steady on and in green: GPRS/EDGE data service connected • Fast blinking in green: Downloading the upgrade mode • Blinking in blue: registering with the 3G network • Steady on and in blue: WCDMA data service connected • Steady on and in cyan: HSDPA data service connected 🕮 **Note:** When the gateway is initialized, it is steady on and in green for three seconds.
Button	
ON/ OFF	Press and hold it to power on or off the E960

Interfaces

- Power adapter/USB cable interface: When connected with the power adapter, the E960 functions as a wireless gateway. When connected to the PC with a USB data cable, the E960 functions as a USB modem.
- Ethernet cable interface: Insert an Ethernet cable connected to the PC or other network equipments.
- Phone cable interface: Insert a phone cable connected with a telephone to realize the voice service.

PC Configuration Requirements

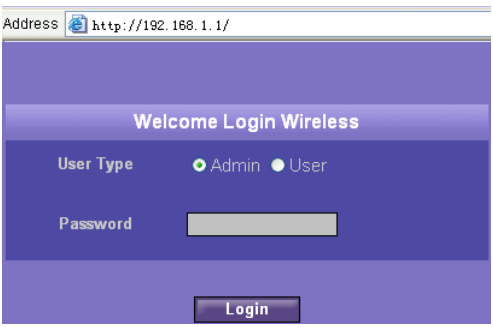
The recommended PC configurations for using the E960 are as follows:

- CPU: Pentium 500 MHz or above
- Memory: 128 MB RAM or above
- Hard disk: 100 MB available space
- Operating System: Windows 2000, Windows XP, or Windows Vista
- LCD resolution: 800*600 pixel or above, recommended 1024*768 pixel
- Interface: standard USB interface
- Internet Browser: Internet Explorer 6.0 or above, Firefox 1.5 or above, Netscape 8.0 or above

2 Using the E960 Configuration Page

Logging in to the Management Page

1. Start the IE browser, and then enter the address **http://192.168.1.1** in the address bar.
2. Select **User Type**, enter **Password**, and then click Login.

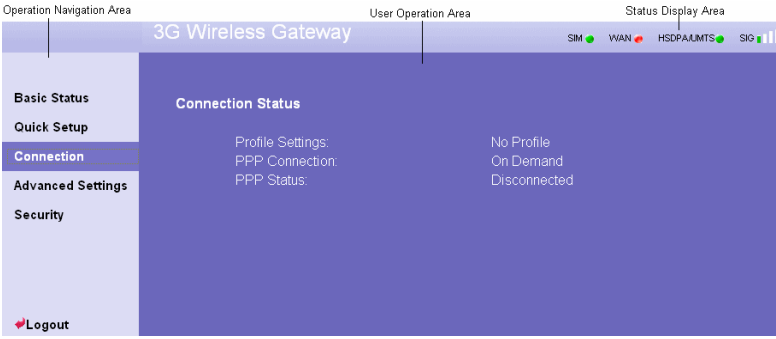


- **Admin**: Has the rights to view and modify the configurations. The default password is **admin**;
- **User**: Has the right to view only the basic information. The default password is **user**.

Note:

To avoid the configuration conflict, only one user can log in to the E960 management page at a time.

Describing the Management Page



- **Operation Navigation Area**: Shows the main functions of the management console.
- **User Operation Area**: Shows configuration information, data information, help information, and function operation area of the gateway. The user operation window varies with different function operations.
- **Status Display Area**: Shows the network mode, PPP dial-up status, network signal strength, and SIM card status in real-time.

Operation Functions

The following table shows the main operations in the gateway management page.

Item	Description
Basic Status	Displays the parameter configuration status of the gateway. For details, see "Viewing the Gateway Configuration Information."
Quick Setup	Configures the gateway quickly. For details, see Chapter 4 "Quickly Configuring the Gateway."
Connection	Displays the network connection status and connects to the network. For details, see "Connecting to the Internet."
Advanced Settings	Configures the advanced settings of the gateway, which includes the following settings: system, SIM card, UMTS, dial-up, DHCP, and WLAN. For details, see Chapter 6 "Describing Advanced Settings."
Security	Configures the Security settings of the gateway, For details, see “Security Settings”.
Logout	Log out of the gateway page

Gateway Status

The following table shows the gateway status information.

Item	Description	
SIM	 The SIM card is valid.	 The SIM card is not inserted or invalid.
WAN	 The PPP dial-up connection is successful.	 The PPP dial-up connection is failed.
WCDMA	 The WCDMA network is connected. **Note:** If the gateway is registered with other network modes, the corresponding network connection status is displayed.	 The WCDMA network is unavailable.
SIG	The signal strength from weak to strong is shown as follows: 	

Using the Quick Setup Wizard

The quick setup wizard guides you to configure the most important settings of the gateway.

If you are using the gateway configuration page for the first time, the system displays the quick setup wizard page by default after you log in. You can configure the basic parameters quickly by following the prompts. For details, refer to Chapter 4 "Quickly Configuring the Gateway."

Connecting to the Internet

Accessing the Connection Status Page

- Click **Connection** to access the page.
- After you log in to the management page again, you can automatically access the connection status page.

Connecting to the Internet

1. If the PIN code protection is enabled, the system prompts you to validate the PIN code. For details, see "Validating the PIN Code."
2. If **PPP Connection** is **Auto** or **Demand**, refresh the page to view the current network connection status.
3. If **PPP Connection** is **Manual**, click Connect or Disconnect to connect or disconnect from the network.

4. Wait for several minutes, if you are prompted that the connection is successful, you can start the IE browser and enter the website address to access the Internet.

Validating the PIN Code

If the PIN code protection is enabled, you are prompted to validate the PIN code when you restart the gateway and log in to the management page.

1. Enter the correct PIN code, and then click Apply.

Note:

- For the initial PIN code, consult your service provider.
- If you enter wrong PIN codes for three successive times, the PIN is locked. For details, see "Unlocking the PIN Code."
- If the PIN validation fails, you cannot use the network-related functions.

2. When you succeed in validating the PIN code, click Continue to access the network connection page.

Viewing the Gateway Configuration Information

On the gateway configuration page, you can view the current parameter configuration information of the gateway and the network connection status. The network connection status includes **WAN**, **LAN**, and **WLAN**.

1. Click **Basic Status** in the operation navigation area.
2. Click Advanced... on the right part of the page to view the status of the gateway.
3. Click Refresh to view the current status of the gateway on the advanced status page.

3 Quickly Configuring the Gateway

You can use the quick setup wizard to configure and maintain the basic parameters of the gateway. Click **Quick Setup** in the operation navigation to access the welcome page. Click Next> to access the PPP profile setting page following the page prompts.

Configuring PPP Profile Settings

- **Profile Name**: Enter the profile name when the text box is null.
- **Dial-up Number/PPP User Name/PPP Password:** Enter these three parameters provided by the internet service provider (ISP). The dial-up number is used to initiate the network call; and the PPP user name and password is used to gain the service authorization provided by the ISP.
- **APN/IP Address:** Select the mode for obtaining the APN or IP address. If the carrier provides the relevant parameters, select **Static** and enter the APN and IP address. Otherwise, you need to select **Dynamic** and the gateway automatically obtains them.

Selecting the PPP Connection Mode

PPP Connection: It is used to select the dial-up access mode.

- **Auto**: After the gateway is switched on, it automatically connects to the Internet and will not disconnect regardless of the data transmission.
- **On Demand**: The gateway automatically connects to the Internet when there is data transmission. It automatically closes the connection when there is no data transmission.
- **Manual**: Manual dial-up. For details, see "Connecting to the Internet."

PPP Authentication: The service is provided by your Internet Service Provider (ISP). For details, consult your ISP.

Configuring the WLAN Setting

SSID: Enter a name for your WLAN.

The service set identifier (SSID) is used to identify a WLAN. A wireless terminal (such as a PC) and the wireless gateway can perform normal data communication only when they have the same SSIDs. To ensure the WLAN security, do not use the default SSID. You can enter a character string as the SSID, such as **MyHome**.

SSID Broadcast: Enable or disable the SSID broadcast.

- **Enabled**: The E960 broadcasts the SSID of the WLAN, and users can easily access the WLAN. Unauthorized users, however, can also easily access the WLAN because the SSID is broadcasted.
- **Disabled**: The E960 does not broadcast the SSID of the WLAN. Before accessing the WLAN, the user must obtain the SSID of the WLAN. Thus, the WLAN security is improved.

Note:

For the convenience of the client accessing the WLAN, you can select **Enabled** for **SSID Broadcast** when you configure the WLAN setting. Once you finish setting up the WLAN, you can disable the SSID broadcast to improve the security of the WLAN.

Configuring the WLAN Encryption Mode

To access the wireless network, you must set the wireless security key of your PC be consistent with that of the wireless gateway.

No Encryption

For the convenience of the client accessing the WLAN, you can set the **Encryption mode** to **NO ENCRYPTION** when you set up a WLAN. In daily use, however, this option is not recommended for the security of the WLAN.

WPA-PSK/WPA2-PSK

- **WPA-PSK** is a 256-bit data encryption method that can automatically change the key.
- **WPA2-PSK** is a more secure version of **WPA-PSK**, and it supports the IEEE 802.11 standard.
- **WPA Encryption** is algorithms for selecting the WPA data encryption. There are three algorithms: **TKIP**, **AES**, and **TKIP+AES**.
- **WPA Pre-Shared Key**: You can enter 64-character hexadecimal value or 8–63-character ASCII value as the key. The ASCII value contains all characters that can be entered through the PC keyboard, and the hexadecimal value contains numbers of 0–9 and characters of A–F. For example, you can enter the ASCII value of **1234abcde** as the key.
- **Network Key Rotation Interval**: It is used to set how long a network key is dynamically changed. By default, it is **0**. To disable this function, you can set the value to **0** or **Null**.

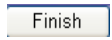
WEP

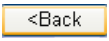
Wireless Equivalent Privacy, a 64-bit or 128-bit data encryption method. The 128-bit WEP encryption provides higher security level.

Network key 1: You can enter 5 ASCII characters or 10-character hexadecimal numeral to form a 64-bit key. You can also enter 13 ASCII characters or 26-character hexadecimal numeral to form a 128-bit key.

Validating Quick Setup

The last page of the wizard displays the all settings you have configured.

- To accept settings, click 

to submit the information.
- To make changes, click 

to return.
- Click 

to quit the settings.

4 Configuring Your Computer

In this part, take the Window XP operating system (OS) as an example to describe how to configure your computer. For other OSs, the configuration may be different; thus, you need to configure it according to the actual situation.

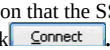
Wireless Configuration

The wireless configuration enables your PC connect to the E960 through the wireless network. If you need only the Ethernet to connect your PC, you do not need to configure this.

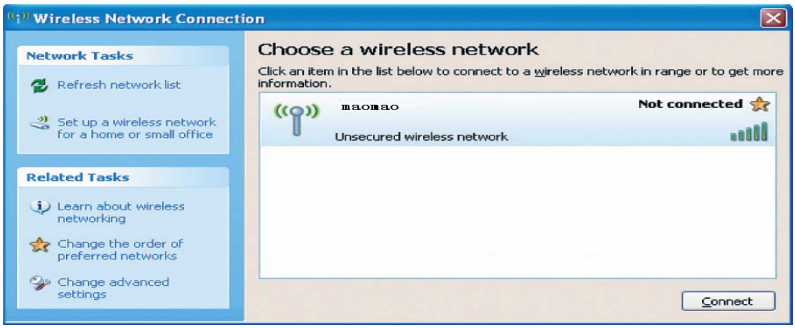
Configuration Requirements

- To set up wireless network connection, your PC must have been configured with the WLAN adapter that supports the IEEE 802.11 b/g protocol.
- If the encryption function is enabled, you need to ensure that all PCs connecting to the E960 use the same key with the E960.
- For the use of WLAN adapter, refer to the WLAN adapter user guide provided by the manufacturer.
- See "Configuring the WLAN Encryption Mode" for the encryption configuration.
- See "Configuring the WLAN Setting" for SSID parameters configuration.

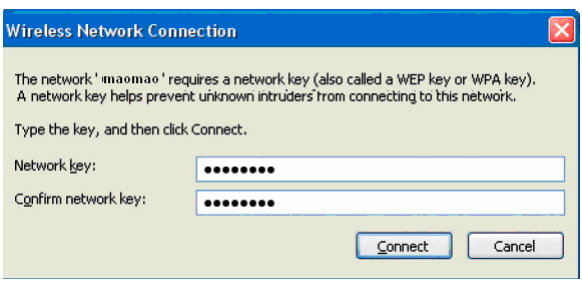
Configuring the Wireless Network Connection

1. Select **Start** > **Control Panel** > **Network Connections** > **Wireless Network Connection**.
2. Click **Show Wireless Networks** to display the wireless network connection list.
3. Select the network connection that the SSID is consistent with that in the E960 WEB configuration, and then click 

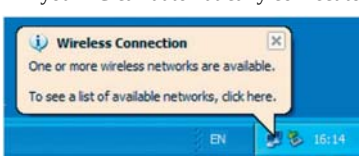
.



4. If the encryption parameter is set for the E960, the **Wireless Network Connection** dialog box is displayed and requires the network key and confirmation. The value you entered must be consistent with the **WPA Pre-Shared Key** or **Network Key** of the E960.



5. Wait for several minutes after you enter the correct network key. The wireless connection icon displays in the status area in the lower right corner of the screen. Then, your PC can automatically connect to the E960.



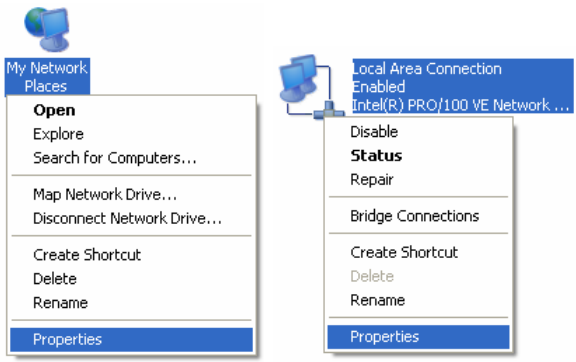
Configuring the PC Network

The recommended configurations of the gateway are as follows:

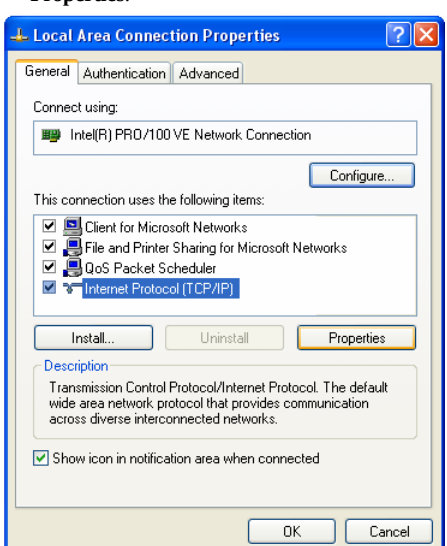
- Obtain an IP address automatically.
- Deselect **Use a proxy server for your LAN**.

Configuring the Network Connection

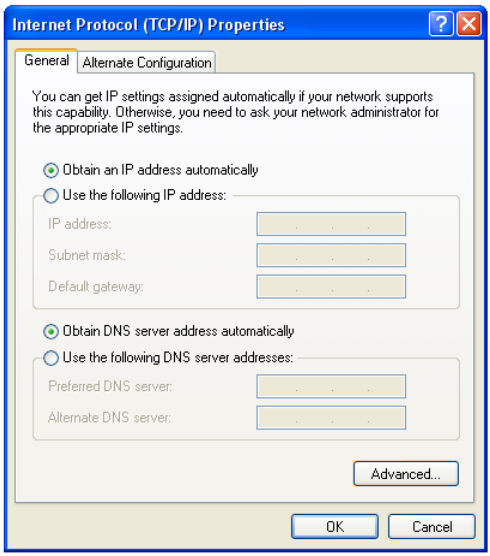
1. Select **My Network Places** > **Properties** > **Local Area Connection**.
2. Right-click the **Local Area Connection** icon and select **Properties** from the shortcut menu.



3. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)** in the **This connection uses the following items** list box, and then click **Properties**.



4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** in the **Internet Protocol (TCP/IP) Properties** dialog box, and then click **OK**.



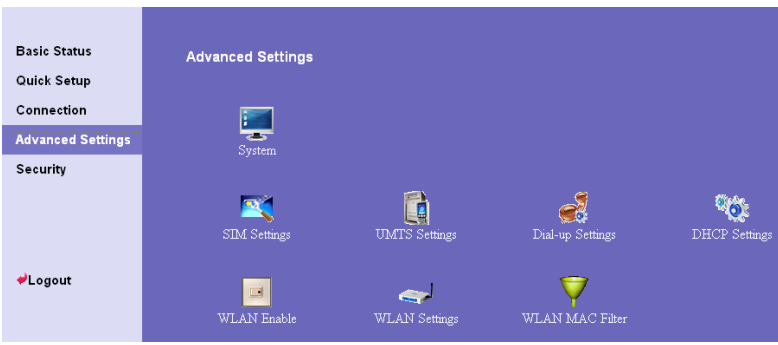
Disabling Proxy Settings

1. Start the IE browser, and then select **Tools > Internet Options**.
2. Select the **Connections** tab, and then click **LAN Settings**.
3. In the **LAN Settings** dialog box, deselect **Use a proxy server for your LAN**.

5 Describing Advanced Settings

In the **Advanced Settings** page, you can configure the basic attributes and advanced parameters of the gateway, and perform routine maintenance and management to the gateway.

In the operation navigation area, click **Advanced Settings** to access the page



The following table describes shortcut icons.

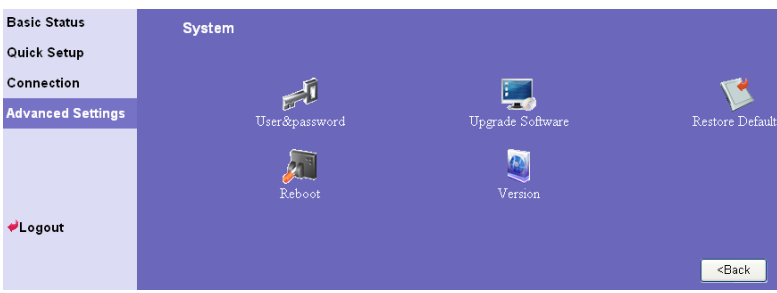
Icon	Description
	Open the system management interface to modify the password, upgrade software, restore the factory default, restart the device, and view the version information.
	Open the SIM card setting interface to manage the PIN code operation.
	Open the UMTS setting interface to configure the network search mode and band.
	Open the dial-up setting interface to configure PPP dial-up properties and manage the profile list.

Icon	Description
	Open the DHCP setting interface to choose the IP address assignment mode.
	Open the interface to enable or disable the WLAN.
	Open the WLAN setting interface.
	Open the MAC address filter setting window.

6 Managing the System

On the system management page, you can modify the password, upgrade the software, restore factory defaults, restart the device, and view the version information.

Click  to access the system management page, as shown in the following figure.



Modifying the Password

You can modify the login password to prevent unauthorized users from logging in to the management page.

1. Click  to open the **Modify Password** window.
2. Enter the current password, and then enter the new password and confirm it.
3. Click Modify to save the modification, click <Back to return to the previous page, and click Cancel to cancel the modification.

Upgrading the Gateway

1. Click  to open the **Upgrade Gateway** page.
2. Enter the path or click Browse... to select the software image file to be updated.

3. Click Upgrade to upgrade the system software.

Caution:

- After the system is upgraded, the system automatically restarts. The whole process takes two to three minutes.
- The software programs for upgrading must come from the official website of Huawei or the official website of the carrier.
- The system upgrading does not change the configuration of the client.

Restoring Factory Defaults

If you need to reconstruct the network or you forget the changes of some parameters, you can choose to restore factory defaults and reconfigure the gateway.

Click  to open the **Restore Defaults** window, and then click Restore.

Note:

After this operation, all configurations restore to the defaults.

Restarting the Device

1. Click  to open the **Reboot** window.
2. Click Reboot to restart the gateway.

Viewing the Version Information

Click  to display the **System Version** page. You can view the hardware version, software version, release time, and the hardware version and software version of the wireless module, as shown in the following figure.

7 Configuring SIM Card Settings

You can manage the PIN code on the SIM card settings window, including the following operations:

- Enabling the PIN code
- Disabling the PIN code
- Modifing the PIN code
- Unlocking the PIN code

🕮 **Note**:

- If you enter the wrong PIN code for three successive times, the PIN code is locked. You need to enter the PUK code to unlock it.
- The PIN code must be 4–8 numerals, and letters are not allowed.

Click  to open the SIM card setting window.

Enabling or Disabling the PIN Code

If the PIN code protection is enabled, you need to validate the PIN code each time when you restart the gateway and log in to the management page; if the PIN code protection is disabled, you do not need to validate the PIN code.

1. Select **enable/disable** in the **PIN Code Operation** list box.
2. Enter the correct PIN code.
3. Click Apply.
4. If the PIN code is wrong, the system prompts you to reset it.

Unlocking the PIN Code

If the PIN code is locked, you need to enter correct PUK code and set the new PIN code to unlock it.

🕮 **Note**:

- If you forgot the PUK code, consult your carrier.
- If you enter the wrong PUK code for successive 10 times, the SIM card is locked. You need to consult your carrier to unlock the SIM card.

1. Enter the correct PUK code.
2. Enter the new PIN code and confirm it.
3. Click Apply to submit the setting.

Modifying the PIN Code

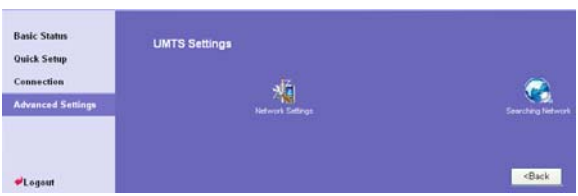
When the PIN code protection is enabled, you can reset the PIN code.

1. Select **modify** in the **PIN Code Operation** list box.
2. Enter the current PIN code.
3. Enter the new PIN code and confirm it.
4. Click Apply to submit the setting.

8 Configuring UMTS Settings

On the UMTS settings window, you can set the priority of connection modes and bands in searching a network.

Click  to open the **UMTS Settings** window, as shown in the following figure.



Choose the Preferred Mode and Band

1. Click  to open the **Network Settings** window.
2. Select the preference of connection mode in the **Preferred Mode** list box. The following table shows the details of connection modes.

Network Mode	Description
3G preferred	The E960 automatically selects the data service mode based on the network signal strength. The high-speed data service mode is preferred.
GPRS preferred	The E960 automatically selects the data service mode based on the network signal strength. The low-speed data service mode is preferred.
3G only	The E960 works only in high-speed data service mode.
GPRS only	The E960 works only in low-speed data service mode.

🕮 **Note**:

- If the carrier provides only the GPRS service and the **Preferred Mode** is configured as **3G only**, you cannot access the Internet.

- If the carrier only provides only the HSDPA service and **Preferred Mode** is configured as **GPRS only**, you cannot access the Internet.
- If the carrier provides neither the 3G nor GPRS service, you cannot access the Internet regardless of the **Preferred Mode**.

3. Select the band to search the network in the **Band** list box. You can select from the following:

- All Band
- GSM900/1800/WCDMA2100
- GSM1900
- GSM850

4. Click Apply to submit settings.

Configuring the Mode for Searching Network

1. Click  to open the **Searching Network** window.
2. Select the mode for searching network.

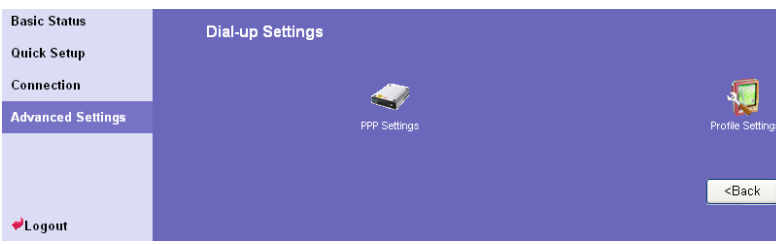
- **Auto**: The gateway automatically searches the network and registers with it.
- **Manual**: You need to manually search the network and register with it.

3. Click Apply to submit the setting.
4. In **Manual** mode, select the searched network and click Log on.

9 Configuring Dial-up Settings

In the **Dial Up Settings** window, you can configure PPP settings and manage profile settings.

Click  to open the **Dial Up Settings** window, as shown in the following figure.



Configuring PPP Settings

1. Click  to open the **PPP Settings** window, as shown in the following figure.
2. Enter the correct parameters.

- **Profile List**: Select a profile from the established dial-up connection list. If the drop-down list is null, you need to create a profile list.
- **PPP Connection:** Select the dial-up connection mode.

Dial-up Mode	Description
Auto	After the gateway is switched on, it automatically connects to the Internet and will not disconnect regardless of the data transmission.
On Demand	The gateway automatically connects to the Internet when there is data transmission. It automatically closes the connection when there is no data transmission.
Manual	Manual dial-up.

- **PPP Authentication:** The service is provided by your Internet Service Provider (ISP). For details, consult your ISP.

- **PPP Max Idle Time**: The duration of the idle PPP connection. In On **Demand** mode, if there is no data transmission beyond the duration, the PPP connection automatically closes.
- **PPP MTU**: The MTU of the PPP data transmission. It is used to set the maximum number of bytes encapsulated in a single data frame.
- **PPP Max Dial Time**: Set the maximum waiting time when connecting to the Internet.

Managing the Profile List

Click  to open the **Profile settings** window and you can create, edit, save, and delete a dial-up connection list.

Interface Description

Parameter	Description
Profile List	Include all created profile names.
Profile Name	Enter the name of the selected or created profile.
Dial-up Number	Enter the character string for PPP dial-up number. It is provided by the network carrier.
PPP User Name	The user name used in PPP communication. It is provided by the network carrier.
PPP Password	The password used in PPP communication. It is provided by the network carrier.
APN	Select the mode for obtaining the APN: • **Dynamic**: The network dynamically assigns the APN. • **Static**: Manually enter the APN provided by the network carrier.
IP Address	Select the mode for assigning IP addresses: • **Dynamic**: The network dynamically assigns the IP address. • **Static**: Manually enter the IP address provided by the network carrier.

Creating a Profile

1. Enter the profile information in the text box based on prompts.
2. Click Save to save the new profile.

Modifying a Profile

1. Select a profile to be modified in the **Profile List** drop-down list. Relevant information is displayed in the corresponding text box.

2. Enter the profile information.
3. Click Save to save the modified profile.

Deleting a Profile

1. Select a profile to be deleted in the **Profile List** drop-down list.
2. Click Delete to delete the selected profile.

10 Assigning IP Addresses

In the dynamic host configuration protocol (DHCP) settings page, you can set the mode for assigning IP addresses in a LAN. DHCP automatically assigns IP addresses to the network devices. If you are using the DHCP server, you need to do the following configurations on the PC connecting with the gateway. For details, refer to "Configuring the PC Network."

Click  to open the DHCP setting page.

- **IP Address**: The default IP address of the gateway is **192.168.1.1**.
- **Subnet Mask**: The combination of the subnet mask and IP address enables the flexible subnetting. By default, the subnet mask is **255.255.255.0**.
- **DHCP Server**: It is used to assign IP addresses dynamically. If the DHCP server is **Enabled**, it can automatically assign IP addresses for PCs. It is recommended to select **Disabled** for the DHCP server.
- **Start IP Address& End IP Address**: It is used to define the IP address range that the host can use during the IP address assignment. For example, in the network segment 192.168.1.0/24, the default IP address of the E960 is 192.168.1.1. The host IP address can range from 192.168.1.2 to 192.168.1.254. The minimum range is a single IP address.
- **DHCP Lease Time**: The DHCP server automatically assigns an IP address to each device connected to the network. When the leased time expires, the DHCP server checks whether the device is connected to the network. If the device is disconnected from the network, the server assigns the IP address to another device. Thus, the IP address is not wasted.

Note:

- The **Start IP Address** must be smaller than or equal to the **End IP Address**.
- If the **DHCP Server** is **Enabled**, the configurations of **Start IP Address**, **End IP address**, and **DHCP Lease Time** are valid; otherwise, you cannot configure them.

11 Configuring the WLAN

Enabling or Disabling the WLAN

1. Click  to open the **WLAN Module Settings** window, as shown in the following figure.
2. Enable or disable the WLAN module.

- **Enable**: Enable the WLAN module. You can use the WLAN function and configure relevant parameters.
- **Disable**: Disable the WLAN module. You cannot use the WLAN function and configure relevant parameters.

3. Click Apply to submit the setting.

Configuring WLAN Settings

Click  to open the **WLAN Settings** window, as shown in the following figure.

Selecting Interface IDs

Wireless Interface: It refers to the SSID and MAC address, and is used to identify the wireless gateway.

SSID

SSID: The service set identifier (SSID) is used to identify a WLAN. A wireless terminal (such as a PC) and the wireless gateway can perform normal data communication only when they have the same SSIDs. To ensure the WLAN security, do not use the default SSID. You can enter a character string as the SSID, such as **MyHome**.

Enabling or Disabling the SSID Broadcast

- **Enabled**: Enable the SSID broadcast. The E960 broadcasts the SSID of the WLAN, and users can easily access the WLAN. Unauthorized users, however, can also easily access the WLAN.
- **Disabled**: Disable the SSID broadcast. The E960 does not broadcast the SSID of the WLAN. Before accessing the WLAN, the user must obtain the SSID of the WLAN. Thus, the WLAN security is improved.

Enabling or Disabling the AP Isolation

- **On**: The terminals (PCs) connecting to the gateway through the WLAN cannot access each other.
- **Off:** The terminals (PCs) connecting to the gateway through the WLAN can access each other.

Selecting the WLAN Channel

- **Country:** It is used to identify the country. Different countries have different standards on channel usage.
- **Channel**: It refers to the channel that the gateway works with. According to the IEEE802.11 standard, the working frequency for the WLAN adopting the Direct Sequence Spread Spectrum (DSSS) technology ranges from 2.4 GHz to 2.4835 GHz. Each channel occupies a neighboring 22 MHz frequency band. The available channels vary with the selected country. If you do not know which channel to select, select **Auto** and the gateway can automatically search for the channel.

Configuring the 802.11 Mode

There are four available modes, as shown in the following table.

Mode	Description
54g Auto	The WLAN has the best compatibility in this mode.
54g Performance	The WLAN has the best performance in this mode.
54g LRS	If the E960 has difficulties in communicating with devices conforming to the IEEE 802.11b standards, select this mode.
802.11b Only	The E960 can only work in the low performance 802.11b standard network mode.

Configuring the Transmission Rate

1. Select **Auto**, the E960 automatically searches the transmission rate. The maximum WLAN transmission rate supported by the gateway is 54 Mbit/s.
2. Click Apply to submit the setting.
3. Click **Advanced** to configure the advanced WLAN setting.

Advanced WLAN Settings

You can configure the security and Network Bridge.

Configuring Security Key

A security key can protect your WLAN from illegal data attacking. The security key of your wireless gateway must be consistent with that of the PC.

Configuring the 802.11 Authentication

- **Open**: Open system authentication. A user accessing the WLAN can choose **WEP**, **WPA-PSK**, or **WPA2-PSK** key to pass the authentication or choose **No encrytion** to skip the authentication.
- **Shared:** Shared key authentication. It can use only **WEP**. The user accessing the WLAN must use the WEP to authenticate.

Configuring the Encryption Mode

There are four encryption modes: No Encryption, WPA-PSK, WPA2-PSK, and WEP. For details, refer to "Configuring the WLAN Encryption Mode."

Configuring Access Attributes of the Client

As shown in the following figure, you can set the **Preamble Type**, **Max Associations Limit**, **Mode**, and enable or disable the peer MAC address through the **Bridge Restriction**.

- **Preamble Type:** It has two options: **Long** and **Short**. In the case that the client (PC) supports the **Short** type, the WLAN can have a better performance if it is **Short**.
- **MAX Associations Limit:** It refers to the maximum number of connections. It is used to set the maximum number of concurrent WLAN users on the gateway. A maximum of 32 clients can connect with the gateway in wireless mode.
- **Mode:** It refers to the WLAN accessing mode. The gateway can work in two modes, as shown in the following table. The default value is **Access Point**.

Mode	Description
Wireless Bridge	It is used to connect two or more access points.
Access Point	The access points meeting the IEEE 802.11b/g standard or the wireless terminals can connect the wireless gateway.

- **Bridge Restriction:** It refers to the limitation to the peer MAC addresses. When it is **Disabled**, the E960 can access all the remote bridges; when it is **Enabled**, the E960 can only access the remote bridges that the addresses are in the address list.
- **Bridges:** It refers to the physical address of the remote peer bridge. The gateway supports the point-to-multipoint (PTM) bridge mode, and a wireless gateway can connect four remote peer bridges at the same time.
- **Peer MAC Address:** It refers to the physical address list of the remote peer bridges. It contains a maximum of four physical addresses.
- **Link Status: Up** shows the successful connection and **Down** shows the failed connection.

Configuring the MAC Filter

Click  to open the **Wlan MAC Filter Settings** window. You can control and manage the clients accessing the WLAN, and improve the WLAN security performance.

MAC Restrict Mode

The following table lists the MAC address filter modes:

Value	Description
Disabled	The MAC address filter function is disabled.
Allow	The clients with addresses in the **MAC Address** list are allowed to connect with the gateway through the WLAN.
Deny	The clients with addresses in the **MAC Address** list are not allowed to connect with the gateway through the WLAN.

MAC Addresses

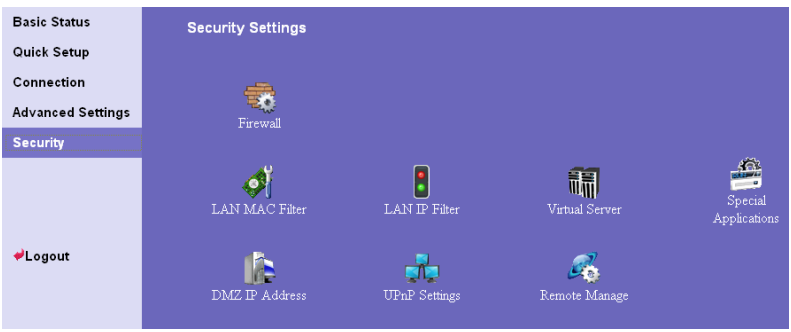
Enter MAC addresses in the list. The gateway can perform access control over the clients that MAC addresses are in the list. The list can contain a maximum of 16 MAC addresses.

12 Security Settings

In the **Security Settings** window, you can configure the advanced security settings.

In the operation navigation area, click **Security**.

The **Security Settings** window is displayed, as shown in the following figure.



Firewall Switch

Your gateway has a true firewall that controls the incoming and outgoing data flow and protects your computer from illegal intrusion.

1. Click  to access the **Firewall Switch** window.
2. Select the **Enable the firewall (main switch of the firewall)** check box to enable the firewall.

Note:

- Only when the **Enable the firewall** check box is selected, the other functions such as the IP address filter function, the MAC address filter function, and the WAN port ping function are available.
- When the **Enable LAN MAC address filter** check box is selected, the default filter rules are available.

3. Select other options as required, and then click Apply.

LAN MAC Filter

Your gateway supports MAC filtering based on a list of either denied or allowed computers. A common method to restricting network access is to specify the Media Access Control (MAC) address.

To locate the MAC address in Windows, choose **Start** > **Run**, and then enter **cmd**.

The command window is displayed, enter **ipconfig /all**, and then press **Enter**.

The MAC address is displayed as the **Physical Address**.

1. Click  to access the **LAN MAC Filter** window.
2. Select **MAC Filter Mode**.

Mode	Description
Disabled	It specifies that the MAC address filter function is disabled.
Allow	It specifies that the clients with addresses in the **MAC Address** list are allowed to connect with the gateway.
Deny	It specifies that the clients with addresses in the **MAC Address** list are denied to connect with the gateway.

3. Enter the MAC addresses of the clients and click 

LAN IP Filter

You can configure the gateway to block specific IP addresses from accessing the LAN.

Click  to access the **IP Address Filter** window.

Adding an IP Address

1. Select the protocol and status.
2. Enter the IP address and corresponding port to be blocked from accessing the LAN.
3. Click 

to add the IP address to the table.

Modifying an IP Address

1. Click  in the **Modification** column. The corresponding IP address filter is displayed.
2. Modify the contents as required.

3. Click Ok.

Deleting an IP Address

Click  in the **Modification** column.

The corresponding IP address filter is deleted.

Making an IP Filter Effective

1. Add a new IP address or select a record in the IP address filter table.
2. Select **On** for **Status**.
3. Click Ok.
4. Click Apply. The IP filter takes effect.

Virtual Server

Your gateway supports virtual server to enable external computers to access WWW, FTP, or other services provided by the LAN.

Click  to access the **Virtual Server** window.

Adding a Virtual Server

1. Select the protocol and status.
2. Enter values in the following textboxes:

- **Name**: Enter a name to the service provided by the LAN.
- **WAN Port**: Enter the WAN port of the LAN in which the computer provides services.
- **IP Address**: Specify a computer in the LAN to provide services.
- **LAN Port**: Enter the LAN port of the computer that provides services.

3. Click Ok to add the virtual server to the table.

Modifying a Virtual Server

1. Click  in the **Modification** column. The corresponding virtual server is displayed.
2. Modify the contents as required.
3. Click Ok.

Deleting a Virtual Server

Click  in the **Modification** column. The corresponding virtual server is deleted.

Making a Virtual Server Effective

1. Add a virtual server or select a record in the virtual server table.
2. Select **On** for **Enabled**.
3. Click Ok.
4. Click Apply.

Special Applications

Special applications refer to the interactive applications, such as online games and videoconferences.

You may want to expose your network to the Internet in certain limited and controlled ways, so that you can enable some applications (such as game, voice and chat) working from the LAN, and enable Internet access to servers in the home network. Your gateway supports both of these functions.

For example, to use a Transfer Control Protocol (TCP) application on one of your PCs, you can simply select **TCP** from the protocol list and enter the port of the used application. All TCP-related data arriving at your gateway from the Internet will be forwarded to the specified port.

Similarly, if you want to grant Internet users access to special application inside your home network, you must specify the application that you want to provide and the port that provides the application.

For example, if you want to share a UDP application inside the home network, you must select **UDP** from the protocol list and enter the port of the provided application. When an Internet user accesses the external IP address of your gateway, the gateway will forward the incoming UDP request to the port that provides the application.

Note:

- When setting a special application, ensure that the port is not in use by another application.

Click  to access the **Special Applications** window.

Adding an Interactive Application

Your gateway is equipped with a list of special applications; you can select one in **Common Port** and then click Ok to save it to the table. In addition, you can manually create an application with the following method.

1. Enter a name for the application.
2. Enter the trigger port that is accessed by other clients in the home network or Internet. The trigger port is single.
3. Select the trigger protocol that supports the interconnection and interplay between special applications and remote servers.
4. Enter the open port that will be using or providing the application service. The open port can be a single port or a range of ports.
5. Select the open protocol used by the special application.
6. Click Ok to add the special application server to the table.

Modifying an Interactive Application

1. Click  in the **Modification** column. The corresponding application is displayed.
2. Modify the contents as required.
3. Click Ok.

Deleting an Interactive Application

Click  in the **Modification** column. The corresponding application is deleted.

Making an Interactive Application Effective

1. Create an application or select one in the applications table.
2. Select **On** for **Status** to activate the application.
3. Click Ok.
4. Click Apply.

DMZ Service

The Demilitarized (DMZ) function allows a local computer to be exposed to the Internet. If you need to use an Internet service that is not in the special applications list or to expose your computer to all services without restriction, you can enable the DMZ function. However, the DMZ computer is not protected by the firewall. It is vulnerable to attack and may also put other computers in the home network at risk.

An incoming request for access to a service in the home network is filtered by the gateway. Your gateway forwards the request to the specified DMZ computer unless the service is

being provided by another PC in the home network (assigned in special application). In this case, that PC receives the request instead.

1. Click  to access the **DMZ** window.
2. Enter the local IP address of the computer that is specified as a DMZ host.
3. Select **Enabled** or **Disabled** for **DMZ Status** to enable or disable the DMZ service.
4. Click Apply.

🕮 **Note:**

Only one computer can be specified as a DMZ host at a time.

UPnP Setting

The Universal Plug and Play (UPnP) service allows other network users to control your gateway's network features to realize the intelligent interconnection.

1. Click  to access the **UPnP** window.
2. Select **Enabled** or **Disabled** for **UPnP Status** enable or disable the UPnP service.
3. Click Apply.

Remote Web Management

The remote web management allows the access and control of the gateway either from the home network or from the Internet.

When you are on a trip, you can maintain your gateway through the remote web management service. It also allows your ISP to help you solve gateway problems from a remote location.

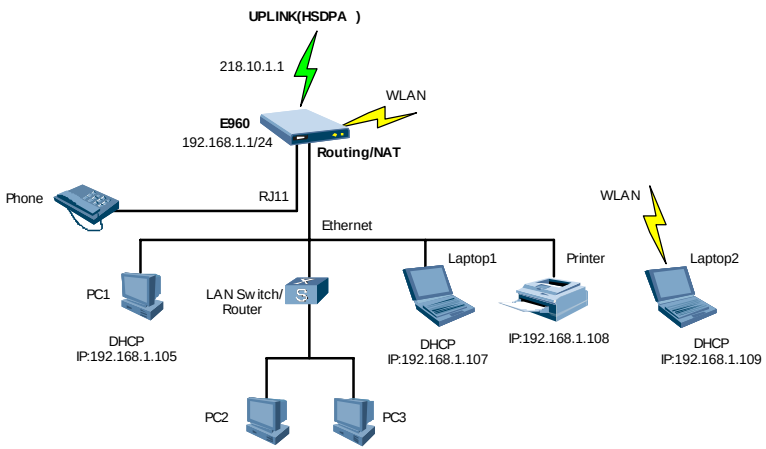
1. Click  to access the **Remote Web Management** window.
2. Select **Enabled** or **Disabled** for **Remote Status** to enable or disable the service.
3. Enter the IP address that can access and control your gateway.
4. Click Apply.

13 Typical Networking Example

You can construct a small LAN through the WLAN interface or four Ethernet interfaces of the gateway.

Your gateway also supports external hubs, Ethernet switches, or routers. To construct a LAN with multiple PCs, you can extend the Ethernet interfaces through a hub or Ethernet switch.

For example, the gateway constructs a small-sized LAN with multiple PCs in the SOHO to access the Internet wirelessly, and the networking diagram is as follows:



14 Troubleshooting

The PC in a LAN cannot access internet.

1. The power indicator is on, and the E960 is normally connected with the power adapter. If the power indicator is off, you need to check whether the power is normally connected.
2. There are five signal strength indicators on the E960 panel. The more green indicators are on, the stronger the signal strength. If all of the signal strength indicators are off, you need to check whether the area is covered by WLAN.
3. If the area is covered by WLAN, you need to check whether the network mode is right. See Chapter 9 "Configuring UMTS Settings" for information about network mode.
4. If the 1, 2, 3, 4 four indicators on the panel blinks, the corresponding Ethernet interfaces are normally connected. If the indicators are off, you need to check and ensure that the corresponding Ethernet connection is normal.
5. You must configure the correct PPP user name and PPP password when you access the internet through the E960. Check whether they are correct, and see "Configuring PPP Profile Settings" for details.
6. If the DHCP service is disabled and the PC obtains the IP address dynamically, the PC also cannot access the internet. You can change the mode to manually assign an IP address. See "Configuring the PC Network."
7. Check whether the driver of the network adapter is correctly installed.
8. If the preceding methods cannot solve the problem, you can reset the E960 to factory defaults.

The PC in a WLAN cannot access the WLAN.

1. If there are interferences or shields near the E960, you can adjust the position of the E960. When the signal strength is strong, you can move to the next step.
2. Check and record the following data on the PC's network adapter: SSID, WEP type, and key.
3. Check and record the following data on the E960: SSID, WEP type, and key.
4. Compare the data, the SSID on the network adapter should be ANY or be the same with that on the E960. The WEP type and key on the network adapter and E960 should be identical. Otherwise, you need to change the data on the network adapter.

What if I forgot the IP address of the LAN interface

If you forgot the IP address of the LAN interface, you can input http://e.home and login in the mode of PC obtaining IP address automatically.

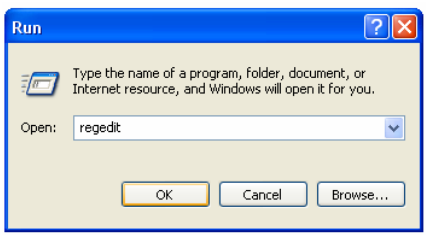
What to do if bridging between two EC506s is unsuccessful

1. Make sure that the two gateways work on the same channel. For details, see "Selecting the WLAN Channel."
2. Make sure that the MAC address of one gateway is in the peer MAC address list of another gateway. For details, see "Configuring Access Attributes of the Client."

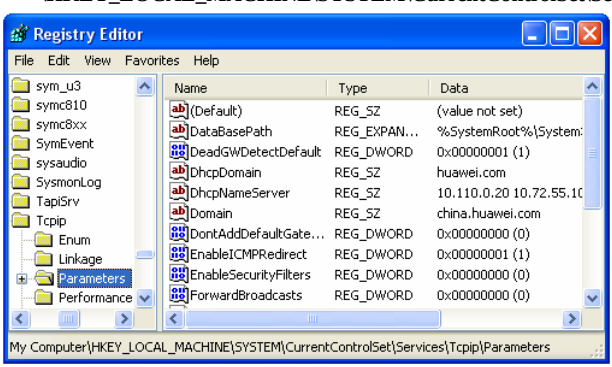
When the signal strength is normal, what to do if the downloading rate is much lower

In this case, you may need to set the value in registry as following procedure.

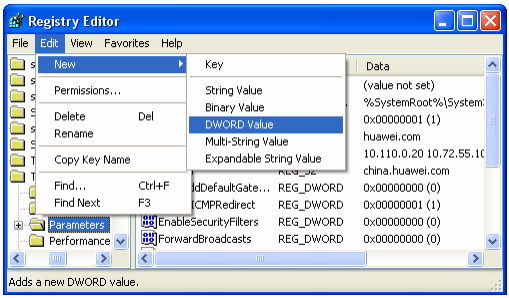
1. Click **Start** and then select **Run**.
2. Type **regedit** in the **Open** text box and then click **OK**.



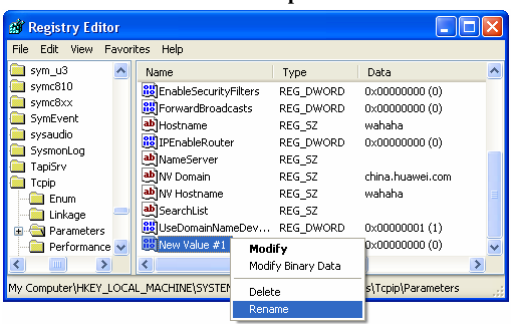
3. Select Parameters under the following directory: **\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip**.



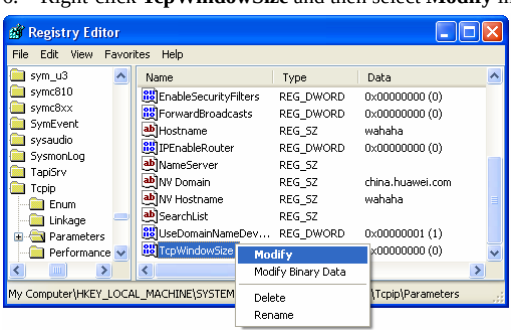
4. Select **Edit** > **New** > **DWORD** Value.



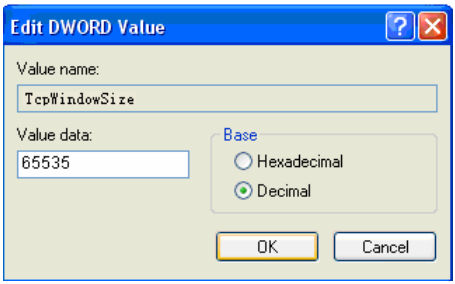
5. Rename **New Value #1** to **TcpWindowSize**.



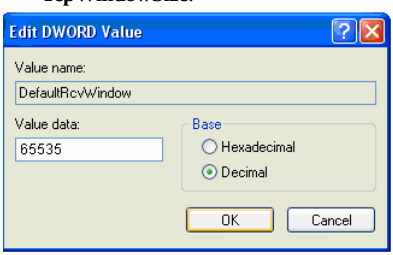
6. Right-click **TcpWindowSize** and then select **Modify** in the shortcut menu.



7. Select **Decimal** and enter **65535** in the **Value data** text box, and then click **OK**.



8. For the DWORD value of **DefaultRcvWindow**, do the same operations as that of **TcpWindowSize**.



15 Warnings and Precautions

Electronic Device

- Turn off your device near high-precision electronic devices. The wireless device may affect the performance of these devices.
- Such devices include hearing aids, pacemakers, fire alarm systems, automatic gates, and other automatic-control devices can be affected. If you are using an electronic medical device, consult the device manufacturer to confirm whether the radio wave affects the operation of this device.

Hospital

Pay attention to the following points in hospitals or health care facilities:

- Do not take your wireless device into the operating room (OR), intensive care unit (ICU), or coronary care unit (CCU).
- Do not use your wireless device at places for medical treatment where wireless device use is prohibited.
- When using your wireless device near someone who is suffering from a heart disease, turn down the ring tone volume or vibration properly so that it does not affect the person.

Traffic Safety

- Please observe local laws and regulations on wireless device use. Do not use your wireless device while driving to avoid traffic accident.
- Secure the wireless device on its holder. Do not place the wireless device on the seat or other places where it can get loose in a sudden stop or collision.
- Use the wireless device after the vehicle stops at a safe place.
- Do not place the wireless device over the air bag or in the air bag outspread area. Otherwise, the wireless device may hurt you owing to the strong force when the air bag inflates.
- Observe the rules and regulations of airline companies. When boarding or approaching a plane, turn off the wireless device. In areas where wireless device use is prohibited, turn off the wireless device. Otherwise, the radio signal of the wireless device may disturb the plane control signals. Turn off your wireless device before boarding an aircraft.

Storage Environment

- Do not place magnetic storage media such as magnetic cards and floppy disks near the wireless device. Radiation from the wireless device may erase the information stored on them.
- Do not put your wireless device, and other accessories in containers with strong magnetic field, such as an induction cooker and a microwave oven. Otherwise, circuit failure, fire, or explosion may occur.
- Do not leave your wireless device, and other accessories in a very hot or cold place. Otherwise, malfunction of the products, fire, or explosion may occur.
- Do not place sharp metal objects such as pins near the earpiece. The earpiece may attract these objects and hurt you when you are using the wireless device.
- Do not subject your wireless device, and other accessories to serious collision or shock. Otherwise, wireless device malfunction, overheat, fire, or explosion may occur.
- Do not put your wireless device in the back pocket of your trousers or skirt to avoid wireless device damage while seated.

Children Safety

- Put your wireless device, and other accessories in places beyond the reach of children. Do not allow children to use the wireless device, or other accessories without guidance.
- Do not allow children to touch the small fittings. Otherwise, suffocation or gullet jam can be caused if children swallow the small fittings.

Operating Environment

- The wireless device, and other accessories are not water-resistant. Keep them dry. Protect the wireless device, or other accessories from water or vapor. Do not touch the wireless device with a wet hand. Otherwise, short-circuit and malfunction of the product or electric shock may occur.
- Do not use the wireless device in dusty, damp and dirty places or places with magnetic field. Otherwise, malfunction of the circuit may occur.
- Do not turn on or off the wireless device when it is near your ears to avoid negative impact on your health.
- When carrying or using the wireless device, keep the antenna at least 20 centimeters away from your body, to avoid negative impact on your health caused by radio frequency leakage.
- If you feel uncomfortable (such as falling sick or qualm) after playing games on your wireless device for a long time, please go to see a doctor immediately.
- On a thunder stormy day, do not use your wireless device outdoors or when it is being charged.
- Do not touch the antenna when a call is going on. Touching the antenna may affect call quality and cause the wireless device to operate with more power. As a result, the talk time and standby time are shortened.
- The wireless device may interfere with nearby TV sets, radios and PCs.
- In accordance with international standards for radio frequency and radiation, use wireless device accessories approved by the manufacturer only.

Cleaning and Maintenance

- Before you clean or maintain the wireless device, turn off it and disconnect it from the charger. Otherwise, electric shock or short-circuit may occur.
- Do not use any chemical detergent, powder, or other chemical agent (such as alcohol and benzene) to clean the phone and the charge. Otherwise, part damage or a fire can be caused. You can clean the phone and the charger with a piece of soft antistatic cloth that is a little wet.
- Do not scratch the shell of the wireless device. Otherwise, the shed coating may cause skin allergy. Once it happens, stop using the phone at once and go to see a doctor.
- If the wireless device or any of its fittings does not work, turn to the local authorize service center for help.

16 Abbreviations

3G	The Third Generation
A	
AC	Alternating Current
ARP	Address Resolution Protocol
AP	Access Point
APN	Access Point Name
C	
CDMA	Code Division Multiple Access
D	
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DL	down link, downlink
E	
EDGE	Enhanced Data rates for GSM Evolution
G	
GSM	Global System for Mobile communications
GPRS	General Packet Radio Service
GGSN	Gateway GPRS Support Node
H	
HSPA	High Speed Packet Access
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access
HLR	Home Location Register

I	
IP	Internet Protocol
ICMP	Internet Control Message Protocol
L	
LAN	Local Area Network
LED	Light Emitting Diode
L2TP	Layer 2 Tunneling Protocol
M	
MSC	Mobile Switching Center
N	
NAT	Network Address Translation
P	
PCS	Personal communication systems
PSTN	Public Switched Telephone Network
POTS	Plain Old Telephone Service
PPTP	Point to Point Tunneling Protocol
R	
RTT	Radio Transmission Technology
S	
SOHO	Small Office Home Office
SCP	Service Control Point
SGSN	Serving GPRS Support Node
SDRAM	Synchronous Dynamic Random Access Memory
T	
TKIP	Temporal Key Integrity Protocol
U	
UMTS	Universal Mobile Telecommunications System
UL	up link, uplink
V	
VLR	Visitor Location Register

VPN	Virtual Private Network
W	
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WCDMA	Wideband CDMA
WI-FI	Wireless Fidelity