

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



HUAWEI 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 section 7 "Warnings and Precautions."













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

Table of Contents

| | |
|---|-----------|
| 1 Getting to Know Your E960..... | 1 |
| Appearance | 1 |
| PC Configuration Requirements | 2 |
| 2 Quick Start..... | 3 |
| Gateway Mode..... | 3 |
| USB Modem Mode..... | 4 |
| 3 Use the Management Console | 6 |
| Login to the Management Console | 6 |
| Introduce the Management Page | 7 |
| Use the Quick Setup Wizard | 8 |
| Verify the PIN Code | 9 |
| View the Configuration Information | 9 |
| 4 Quick Setup..... | 10 |
| Configure PPP Profile | 10 |
| Select the Mode of PPP Connection..... | 11 |
| Configure SSID For WLAN..... | 11 |
| Configure the Security encryption | 12 |
| Validate Quick Setup | 14 |
| 5 Configuring Your Computer | 15 |
| Wireless Configuration | 15 |
| PC Network Configuration..... | 16 |
| 6 Introduce Advanced Setting | 19 |
| 7 System Management | 21 |
| Change the User password | 21 |
| Upgrade the Gateway | 22 |
| Restore Defaults | 23 |
| Reboot the Device | 23 |
| View the Version Information | 23 |
| 8 SIM Setting | 24 |

| | |
|--|-----------|
| Enable/Disable PIN Code..... | 24 |
| Unlock PIN code | 25 |
| Modify the PIN code | 25 |
| 9 UMTS Setting | 26 |
| Choose Preferred Mode and Band | 26 |
| Choose Searching Mode..... | 27 |
| 10 Dial-up Setting | 29 |
| Configure PPP Properties | 29 |
| Manage the Profile List | 30 |
| 11 IP Address Distribution | 32 |
| 12 WLAN Setting..... | 34 |
| Enable/Disable WLAN..... | 34 |
| Basic Settings for WLAN..... | 34 |
| Advanced Settings for WLAN | 36 |
| MAC Filter Setting | 40 |
| 13 Typical Networking Example | 41 |
| 14 Troubleshooting..... | 42 |
| 15 Warnings and Precautions | 46 |
| 16 Abbreviations | 49 |

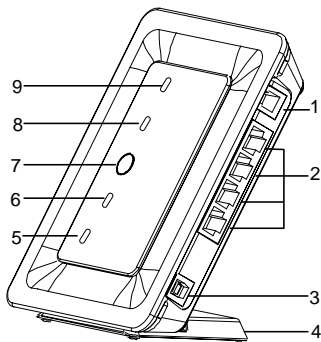
1

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
2. Ethernet Cable
3. Charger/USB Cable
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 in yellow, the charge is finished. |
| WLAN | If it is steady on and in yellow, the WLAN is enabled. If it is blinking, data is transmitting |
| Signal strength | <ul style="list-style-type: none">• Fast blinking in red: No SIM card or unverified PIN code• Steady on in red: Signal strength in level one (weak)• Steady on in yellow: Signal strength in level two or three (middle) |

| | |
|---------------|--|
| | <ul style="list-style-type: none"> Steady on in green: Signal strength in level four or five (strong) |
| Network mode | <ul style="list-style-type: none"> Double blinking in green: Searching the network Blinking in green: Normal 2G network Steady on and in green: GPRS/EDGE data service connected Fast blinking in green: Downloading the upgrade mode Blinking in blue: Normal WCDMA network Steady on in blue: WCDMA data service connected Steady on in cyan: HSDPA data service connected <p>Note: When the gateway is initialized, it is steady on in green for three seconds.</p> |
| Button | |
| ON/ OFF | Press and hold it to power on or off the E960 |

Interfaces

- Power adapter/USB cable:** 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:** Insert a Ethernet cable connected to the PC or other network equipments.
- Phone cable:** 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 Quick Start

Gateway Mode

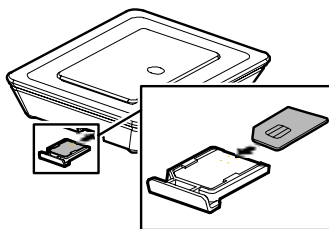
Step 1: Insert the SIM Card

1. Take out the card socket from the E960.
2. Insert the SIM card into the socket with the golden contact facing upward.
3. Insert the card socket into the E960.



Caution:

When inserting or removing the SIM card, you must disconnect the E960 with the power adapter.



Step 2: Connect the Power Adapter

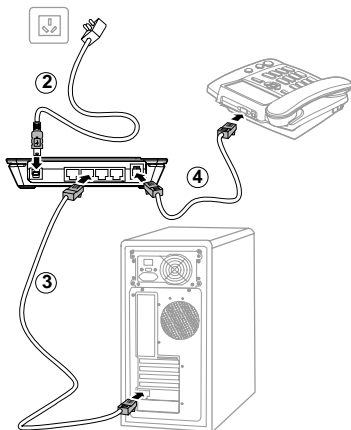
Please use the E960 compatible power adapter; otherwise, the E960 can be damaged.

Step 3: Connect to a PC

If the indicator of the Ethernet interface connecting with a network cable is on, the connection is successful. The Ethernet cable cannot be longer than 100 meters (328 feet). For better effect, please use the shielded cable.

Step 4: Connect to a telephone


To avoid the call effect from interfering by the wireless signal, place the telephone set one meter away from the E960.

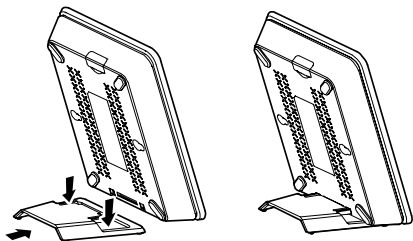


Step 5: Place the E960

The E960 can be placed horizontally on a table, hanging against wall, or leaning against the pedestal. Place the E960 on a higher place or near the window, so it can receive better signal strength.

Press the bayonet of the pedestal, and place the E960 into the pedestal as shown in the figure. Thus, the E960 can lean against the pedestal.


 **Caution:** To avoid electrical devices from interfering by the wireless signal, place electrical devices one meter away from the E960.

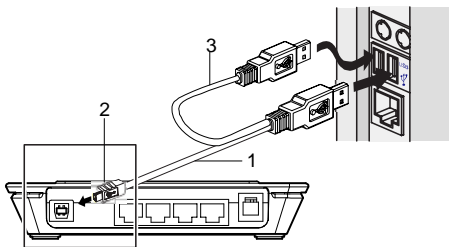




USB Modem Mode

In USB modem mode, you can use functions such as voice service, wireless accessing the Internet, SMS, and phone book only through connecting the PC with a USB data cable; however, the Ethernet interface and WLAN cannot be used to build LAN.

1. USB data cable
2. Auxiliary USB data cable
3. USB connector

 **Note:** The auxiliary USB data cable is for additional power supply. Ensure that all connectors are plugged in to the corresponding USB interfaces.



1. Insert the SIM card.
2. Connect the E960 and PC with a compatible USB data cable.
3. The system automatically recognizes the new hardware, and displays  on the lower right of the desktop. The E960 and PC are connected successfully.
4. If the E960 is connected with a telephone set, you can make calls when you hear the dial tone.
5. The Mobile Partner installation program of the E960 starts automatically. After the successful installation, the management program starts automatically, and the shortcut icon  is displayed on the desktop.

Note:

- If the program is not started, you can access the optical drive path of the E960, double-click the disk icon or right-click it, and then select **Open**. Double-click the **AutoRun.exe** file, the installation program starts.
 - Do not plug or unplug the E960 in the installation process.
6. Enter the Mobile Partner, and you can perform the applications such as wireless accessing the Internet, SMS, email, and phone book.

Making a Call

When the gateway is powered on, you can make a voice call with the telephone connected with E960. Pick up the handset and dial the number.

Using the E960 User Guide


The electrical version of the E960 user guide is compressed in the installation program of the Mobile Partner. In USB modem mode, you can copy the user guide to your PC as the following method.

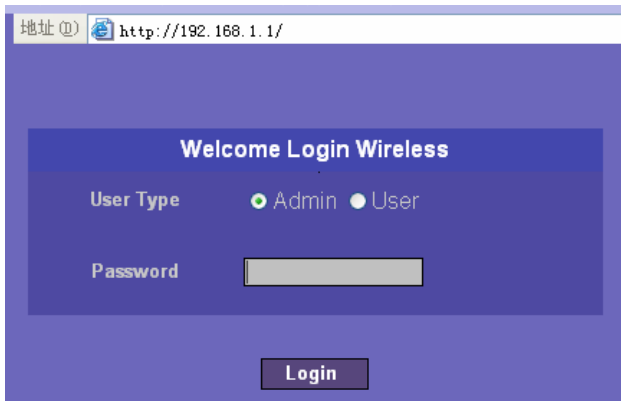
1. Access **My Computer**.
2. Right-click the drive icon of the Mobile Partner, and then select **Open** to access the drive document.
3. View and copy the *Huawei E960 HSDPA Wireless Gateway User Guide* and *Mobile Partner User Guide*.

3

Use the Management Console

Login to the Management Console

1. Open the Internet Explorer, and then enter the address `http://192.168.1.1`.
2. Select the **User Type**; enter the **Password**, and then click .



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

 **Note:**

Only one user can log in to the E960 management page once, which is to prevent the configuration conflict.

Introduce the Management Page



- **Operation navigation area:** Shows the main functions of the management console.
- **User operation area:** Shows detailed information about the gateway and set relevant parameters.
- **Status display area:** Shows the information about network connection and signal intensity in real time.









Functions Operation

The main gateway management console operations is shown in the following table.

| Click... | To... |
|-------------------|--|
| Basic Status | View the detailed information and relevant parameters about the gateway, refer to “View the status” |
| Quick Setup | Configure the gateway quick and easy by using the Quick Setup Wizard, refer to “Quick Setup” |
| Connection | Refresh the network connection status and connect to the network, refer to “Connect to the network” |
| Advanced Settings | Set the parameters about the LAN, WAN, user account, system upgrade, restoration, and reboot in the user work area, refer to “Advanced Settings” |
| Logout | Exit from the management Console |

Status Information

The following table shows the gateway status information.

| Item | Description | |
|-------|---|--|
| SIM |  The SIM card is valid |  The SIM card is invalid or unavailable |
| WAN |  The PPP dial access is successful |  The PPP dial access is failed |
| WCDMA |  WCDMA network connected |  No WCDMA network |
| |  Note: If the gateway connects to other network mode, the corresponding connection status is shown here. | |
| SIG | The signal intensity from weak to intensive is shown as follows:  | |

Use the Quick Setup Wizard

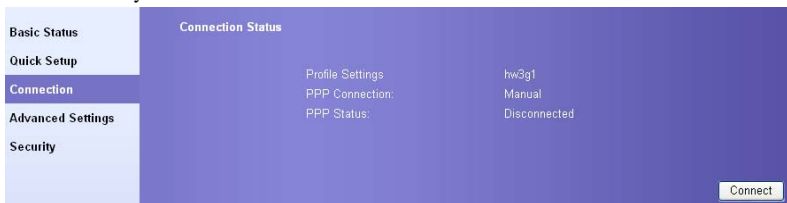
The Quick Setup Wizard guides you to the most important and basic configuration quick and easy.

For your first time use, the system will enter the quick setup wizard by default after Logging in. You can configure the basic parameters quickly following the interface prompts. For details, refer to “4 Quick Setup”.

Connect to the Internet

Enter the connection interface

- Click **Connection** in the operation navigation area.
- After you login in the management console over again, the connection interface displays automatically.



Connect to the Internet

1. If the PIN code protection is enabled, you are prompted to enter the PIN code. for details, refer to “Verify the PIN Code”.

2. If the PPP connection mode is **Auto** or **On Demand**, please refresh the interface to view the current connection status.
3. If the PPP connection mode is **Manual**, please click **Connect /Disconnect** button to .connect or disconnect the network connection,
4. Wait for a moment, interface displays connection successful, then you can open the Internet Browser and input the network site to surf the internet.


Verify the PIN Code

If the PIN code protection is enabled, you are prompted to enter the PIN code when you restart the gateway and login to the management console.

Note:

- The PIN code and PUK code are provided along with your SIM card. For details, contact your service provider.
- If you enter wrong PIN codes for three times, the PIN code id locked. For details about unlocking the PIN code, refer to “Unlock PIN code”.
- If verify PIN failed, you cannot use the management console and setup your gateway.



1. Input the correct PIN code, and then click .
2. After the page displays verifying PIN code successfully, please click **Continue** to enter the connection interface.

View the Configuration Information

On the page of configuration status, you can query the current status about gateway parameters and network connection status.

1. Click **Basic Status** in the operation navigation area.
2. Click **Advanced** on the right-hand side to view other configuration.
3. Click Refresh to view the current status on the advanced status page.

4 Quick Setup

You can use the Quick Setup Wizard to configure the main parameters of gateway quick and easy.

Click **Quick Setup** in the operation navigation to open the welcome interface of wizard, and then click **Next>** to enter the **PPP Profile Setting** page following the page prompts.

Configure PPP Profile

The interface shows as follow figure.

Configure PPP Profile Settings

- Profile Name : Type the name that you want to assign to the new profile.
- Dial-up Number | PPP User Name | PPP Password: These parameters are provided by your ISP. Dial-up Number is used for data service calls, PPP User Name and PPP Password are used to gain authentication of ISP when the call is established.
- APN | IP Address: If a fixed IP address or APN (Access Point Node) is given by your ISP, select Static, otherwise, select Dynamic, the router will automatically get these parameters.

Profile Name:

Dial-up Number:

PPP User Name:

PPP Password:

APN:
 Dynamic Static

IP Address:
 Dynamic Static

<Back Next> Cancel

- **Profile Name:** Input a character string as profile name when the textbox default is null.
- **Dial-up Number/PPP User Name/PPP Password:** Input the three parameters provided by network carrier. The dial-up number is used for PPP dialing, the user name and password is used for gaining the network service authorization.
- **APN/IP address:** Select the mode for obtaining the APN or IP address. When the setting is **Dynamic**, the network obtains the APN dynamically; when the setting is **Static**, and

you need to enter the APN manually. The two parameters are provided by the network carrier.

Select the Mode of PPP Connection

Configure PPP Dial-up Settings

- **PPP Connection**
Demand: The gateway will automatically dial-up when you attempt to send data via internet.
Auto : The gateway will automatically dial-up when the power is turned on.
Manual : The gateway will dial-up by clicking "connect" on the connection page of the management console.

PPP Connection:

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

- **Auto:** After a device is started, the system automatically creates a permanent connection, no matter whether there is data transfer.
- **On Demand:** The connection exists when there is data transfer, and disappears when there is no data transfer.
- **Manual:** Manually dial up to create a connection.

Configure SSID For WLAN

Configure Wlan Setting

- SSID(Service Set Identifier): Type a name up to 32 characters for your local wireless network(WLAN).
- SSID Broadcast: If you set the "Enabled" checkbox to broadcast then other devices can detect and connect to your network. Clear the checkbox to "Disable" broadcasting and hide the name of your network. This provides minimal security as other devices have to know the SSID to connect.

SSID:

SSID Broadcast: Enabled

SSID: Input a name for your WLAN

SSID is used to identify a WLAN. A wireless terminal (such as a PC) can communicate with the gateway only when they have the same SSID. To ensure the WLAN security, do not use the default SSID. SSID is case sensitive and at most 32 characters.

SSID Broadcast: Enable or disable the broadcast function

- **Enabled:** The gateway broadcasts the SSID of this WLAN, and users can easily access. Unauthorized users, however, can also easily access WLAN of this type. This type of WLAN has very low security level.
- **Disabled:** The E960 does not broadcast the SSID of this WLAN. Before accessing a WLAN of this type, the user must get the SSID of the WLAN. In this manner, the WLAN security is ensured.

Note:

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

Configure the Security encryption

To access the wireless network, you must set the wireless security key of your PC consistent with the security key 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. However, this option is not recommended in daily use for the security of the WLAN.

Configure Wlan Security

- Add encryption to your wireless network to prevent unauthorised traffic monitoring and access.
No encryption: Your wireless network is exposed to everyone without authentication and encryption, and this option is not recommended.
WEP: Wireless Equivalent Privacy is a 64-bit or 128-bit encryption method with user configurable fixed keys.
WPA: Wi-Fi Protected Access is a 256-bit encryption method with keys that change automatically over time.
WPA2: A more secure version of WPA with implementation of the 802.11i standard.
WPA Encryption algorithm: TKIP, AES, TKIP+AES
WPA Pre-Shared Key: Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.
Key Rotation Interval: Specify the key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.
Network Key: Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key, enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

Encryption mode:

<Back Next> Cancel

WPA-PSK /WPA2-PSK

- **WPA-PSK:** The Wi-Fi protected access and pre-shared key encryption method. It is a 256-bit encryption mode with keys changing automatically over time.
- **WPA2-PSK:** The higher security version of WPA-PSK encryption mode.
- **WPA Encryption:** It adopts the encryption algorithms of WPA. It has three encryption algorithms: TKIP, AES, and TKIP+AES.

- **WPA Pre-Shared Key:** It requires a WPA key consisting of 64 random hexadecimal key or 8–63 random ASCII characters. ASCII key contains all input characters through the keyboard of your PC, hexadecimal key contains numbers of 0~9 and characters of A~F.
- **Network Key Rotation Interval:** It is used to set how long a network key dynamically rotates. By default, the value is **0** second. To disable this function, you can set the value to **0** or **Null**.

Configure Wlan Security

- Add encryption to your wireless network to prevent unauthorised traffic monitoring and access.
 No encryption: You wireless network is exposed to everyone without authentication and encryption, and this option is not recommended.
 WEP: Wireless Equivalent Privacy is a 64-bit or 128-bit encryption method with user configurable fixed keys.
 WPA: Wi-Fi Protected Access is a 256-bit encryption method with keys that change automatically over time.
 WPA2: A more secure version of WPA with implementation of the 802.11i standard.
 WPA Encryption algorithm: TKIP, AES, TKIP+AES
 WPA Pre-Shared Key: Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.
 Key Rotation Interval: Specify the key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.
 Network Key :Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key,enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

Encryption mode:

WPA Encryption:

WPA Pre-Shared Key:

Network Key Rotation Interval:

WEP

Wireless Equivalent Privacy, a 64- 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 hex numerals to form a 64-bit key. You can also enter 13 ASCII characters or 26 hex numerals to form a 128-bit key.

Configure Wlan Security

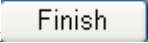
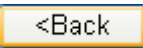
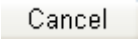
- Add encryption to your wireless network to prevent unauthorised traffic monitoring and access.
 No encryption: You wireless network is exposed to everyone without authentication and encryption, and this option is not recommended.
 WEP: Wireless Equivalent Privacy is a 64-bit or 128-bit encryption method with user configurable fixed keys.
 WPA: Wi-Fi Protected Access is a 256-bit encryption method with keys that change automatically over time.
 WPA2: A more secure version of WPA with implementation of the 802.11i standard.
 WPA Encryption algorithm: TKIP, AES, TKIP+AES
 WPA Pre-Shared Key: Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.
 Key Rotation Interval: Specify the key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.
 Network Key :Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key,enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

Encryption mode:

Network Key 1:




Validate Quick Setup

The last page displays the setting you have configured.

- To accept settings, click  to submit the information.
- To make changes, click  to return.
- Click  to quit the settings.

Quick Setup Wizard Step6 - Your Config as Follows

| | |
|---------------------|------------|
| Profile Name: | hw3g |
| Dial-up Number: | *99# |
| PPP User Name: | NULL |
| APN: | hw3g |
| IP Address: | Dynamic IP |
| PPP Connection: | Manual |
| <hr/> | |
| Network Name(SSID): | e960h |
| SSID Broadcast: | Enabled |
| Encryption mode: | WEP |

5

Configuring Your Computer

Window XP operating system is taken for an example hereinafter. For other operating systems, the configuration interface and configuration method may be slightly different. Please configure it according to the actual situation.

Wireless Configuration

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

Configuration Requirements

- To set up wireless network connection, your PC must have been configured with WLAN adapter that supports the IEEE 802.11 b/g protocol.
- If the encryption function is enabled, you need to ensure that the PCs' encryption parameters are identical with that of the E960.
- For the use of WLAN adapter, please refer to the WLAN adapter user guide provided by the manufacturer.

See For the convenience of the client accessing the WLAN, you can select Enabled for SSID Broadcast when you set up a WLAN. Once you finish setting up the WLAN, you can disable the SSID broadcast to enhance the security of the WLAN.

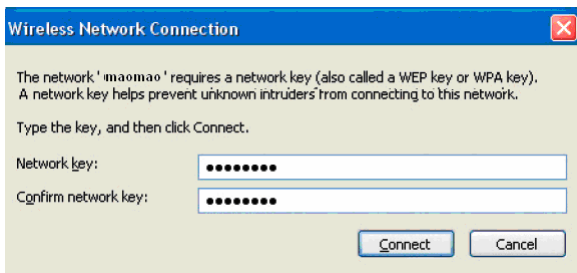
- for the encryption configuration of the E960.
- See Configure SSID For WLAN for SSID parameter configuration.

Configuration Operations

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 of whose SSID is consistent with that in the E960 WEB configuration, and click .



4. If encryption parameter is set for the E960, the **Wireless Network Connection** appears and requires the network key and confirmation. The value you entered must be identical with that in **WPA Pre-Shared Key** or **Network Key**.



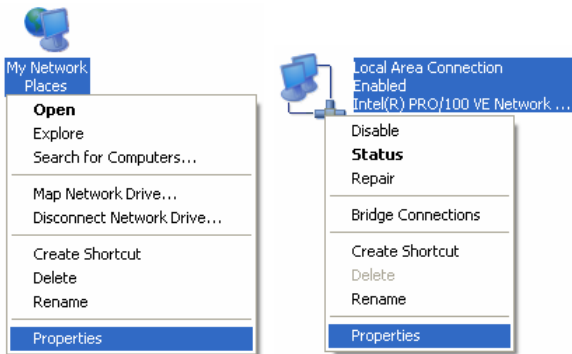
5. Wait a few minutes after you enter the correct value of the network key, the wireless connection icon displays in the status area in the lower right corner of the screen. Your PC can connect to the E960 automatically.



PC Network Configuration

E960 recommend configuring your LAN to obtain IP and DHCP server automatically.

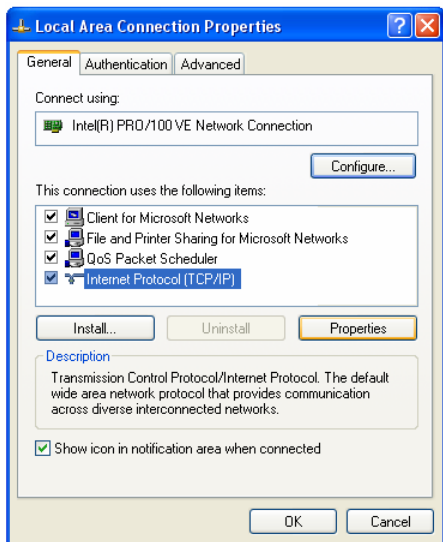
1. Right-click **My Network Places** and select **Properties** to display the **Local Area Connection** window.
2. Right-click **Local Area Connection** and select **Properties** form the shortcut menu.



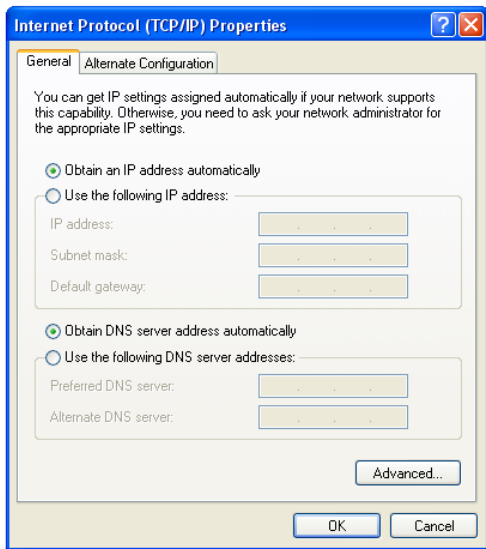
Note:

You should configure the available connections to E960, and take Local Area Connection as an example.

3. Select **Internet Protocol (TCP/IP)** in the **This connection uses the following items** list box and then click Properties.

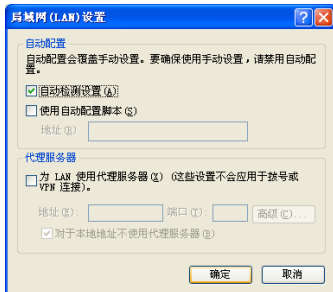


4. Select **Obtain an IP address automatically** and **Obtain DNS server address automatically** in the **Internet Protocol (TCP/IP) Properties** dialog box, and then click **OK**.



Disable Proxy Settings

1. Open the **Internet Explorer**, select **Tools>Internet Options**.
2. Choose **Connections** and then select **LAN Settings**.
3. Unpick the **Use a proxy server for your LAN**.

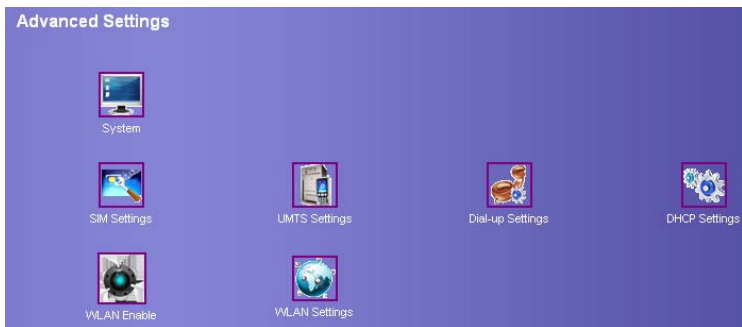


6





Introduce Advanced Setting

In the **Advance Settings** interface, you can not only configure the basic attributes of the gateway, but also configure the other more advanced parameters and perform the daily maintenance and management to the gateway.

In the operation navigation area, click **Advanced Settings** to enter the page as following figure.



The following table shows shortcut icons.

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



Open the DHCP setting interface to choose the mode of IP address assignment.



Open the interface to enable or disable WLAN.



Open the WLAN setting interface.

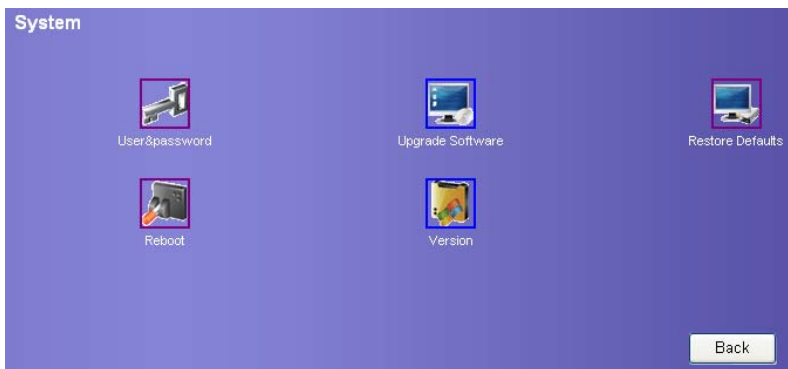


Open the interface to configure the MAC filter.

7 System Management

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

Click  to enter the system management page as following figure.




Change the User password

You can modify the entry password to prevent unauthorized users from logging on your management console.

Note:

- Administrators can modify only the administrator passwords. They cannot modify the passwords of common users.
- The common users cannot modify passwords.
- A password can contain the following characters: Uppercase letters, Lowercase letters, Numbers, Commonly used keyboard symbols, When special symbols are entered as the password, the system prompts error.

1. Click  to enter the page of modifying password.

Modify Password

- You can modify the login password on this page. The password cannot be null and should no more than 15 characters.


Current Password:

New Password:

Confirm Password:

- Input the current password, then input the new password and confirm.
- Click to save the setting.

Upgrade the Gateway

- Click . The system upgrading page is displayed.
- Input the path or click to select the software image files to be updated.
- Click . The system updates the software.

Upgrade Gateway

- Press the button "Browse" to specify the firmware to be upgrade.
Press the button "Upgrade" to update software of wireless gateway.


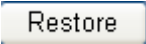


Caution:

- After the system is upgraded, the system automatically restarts.
The whole process takes about 2 minutes.
- The software programs used for upgrade must come from the official website of Huawei or the official website of the network carrier.
- The system upgrading could not affect the clients of your gateway at all.


Restore Defaults

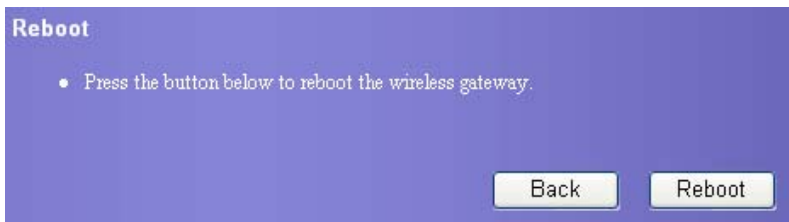
After the device is reset to factory defaults, you need to re-configure the gateway before accessing the network. If you need rebuild LAN or forget any parameters you can use this function.


Click  to open the restoring factory defaults page, and then click .




Reboot the Device

1. Click . The reboot page is displayed.



2. Click the  button, and you can reboot the gateway.

View the Version Information

Click  to display the version information page. You can view hardware version, software version, release time, boot loader version.

8


SIM Setting

You can perform setting and management on the SIM card and PIN code on the SIM setting page, consisting of enabling/disabling/modifying/unlocking PIN code.

Note:


- If you input the false PIN code over three times, the PIN code is locked. You need to input the PUK code to unlock.
- PIN code must be 4~8 digits.



Click  to enter the SIM setting pag.

Enable/Disable PIN Code

If the PIN code protection is enabled, you need to enter the correct PIN code when restart the device and log in to the management console; If the PIN code protection is disabled, You can log in without PIN code authentication

1. Select **enable/disable** in the **PIN Code Operation** list box.
2. Input correct PIN code.
3. Click , submit the setting.
4. The system prompts operation failed if the input PIN code is false.

PIN Code Operation

- PIN Code Operation:
Disabled: The PIN code protection function is cancelled and you need not authenticate SIM card when the power is turned on.
Enabled: The PIN code protection function is activated and you must authenticate SIM card every time when the power is turned on.
Validate: You can authenticate SIM card immediately.
Modify: You can modify your PIN code by filling in input fields.
- Personal Identification Number, 4-8 decimal digits.
- PIN unblock code, 8 decimal digits, is used to unblock PIN code when it is locked.

PIN Code Operation:


PIN Code:

Remaining times: 3

Unlock PIN code

When the PIN code is locked, you need to enter correct PUK code to unlock the PIN code,

Note:

- If you have forgotten the PUK code, please contact your carrier.
 - If you input the invalid PUK code over 10 times, the SIM card is locked. You need to please contact your carrier for help.
1. Input the correct PUK code.
 2. Input the new PIN code and confirm it.
 3. Click  to submit the setting.

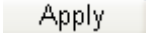


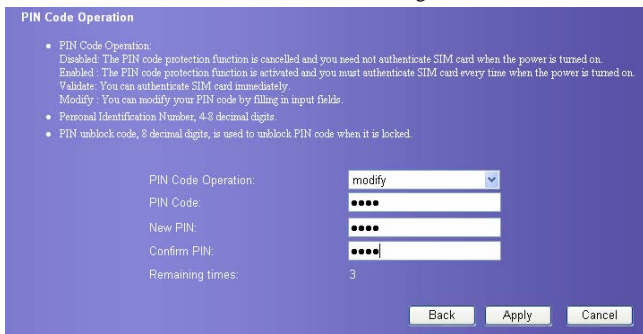
The screenshot shows a purple-themed screen titled "PUK Code Operation". It contains the following fields and controls:

- PUK Code: [Masked input field]
- New PIN: [Masked input field]
- Confirm PIN: [Masked input field]
- Remaining times: 10
- Buttons: Back, Apply, Cancel

Modify the PIN code

When the PIN code protection is enabled, you can modify 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  to submit the setting.




The screenshot shows a purple-themed screen titled "PIN Code Operation". It contains the following fields and controls:

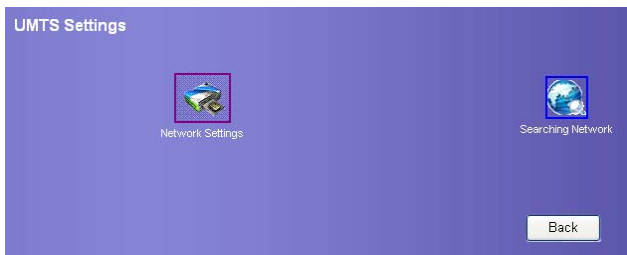
- PIN Code Operation:
 - Disabled: The PIN code protection function is cancelled and you need not authenticate SIM card when the power is turned on.
 - Enabled: The PIN code protection function is activated and you must authenticate SIM card every time when the power is turned on.
 - Validate: You can authenticate SIM card immediately.
 - Modify: You can modify your PIN code by filling in input fields.
- Personal Identification Number, 4-8 decimal digits.
- PIN unlock code, 8 decimal digits, is used to unlock PIN code when it is locked.
- PIN Code Operation: [Dropdown menu with "modify" selected]
- PIN Code: [Masked input field]
- New PIN: [Masked input field]
- Confirm PIN: [Masked input field]
- Remaining times: 3
- Buttons: Back, Apply, Cancel

9 UMTS Setting

On the UMTS setting page, you can set the preference of connection modes and bands in searching a network.




Click . The UMTS setting page displays as following figure.

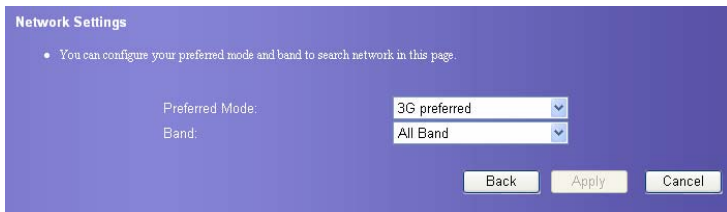


Choose Preferred Mode and Band

You can set the preference of connection modes and bands in searching a network.



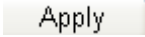
1. Click , enter the **Network Settings** page.



2. Select the preference of connection mode in the **Preferred Mode** list box. The following table lists the details of connection modes.

| Mode | Performance | Description |
|----------------|-------------------------------|---|
| 3G preferred | Maximum rate: 2.4 Mbit/s | The E960 automatically selects the data service mode according to the signal intensity of the network. The high-speed data service mode is preferred. |
| GPRS preferred | Maximum rate: 153.6 Kbit/s | The E960 automatically selects the data service mode according to the signal intensity of the network. The low-speed data service mode is preferred. |
| 3G only | Maximum rate: 2.4 Mbit/s | The E960 can only work in high-speed data service mode. |
| GPRS only | Maximum rate: 153.6 Kbit/s | The E960 can only work in voice mode and low-speed data service mode. |

Note:

- If carrier only provides GPRS service and **Preferred Mode** is configured as **3G Only**, you cannot use network service.
 - If carrier only provides 3G service and **Preferred Mode** is configured as **GPRS Only**, you cannot use network service.
 - If carrier neither provides GPRS or 3G service, you cannot use any network service.
3. Select the frequency of the chose connection mode in the **Band** list box. The available frequencies include: **Full frequency**, **GSM900/1800/WCDMA2100**, and **GSM1900**.
 4. Click  to submit setting.

Choose Searching Mode

You can set the mode for searching networks. The mode can be either **Auto** or **Manual**.

1. Click . The Searching Network page displays.

Searching Network

- Auto : The gateway will select a network and logon automatically in this mode.
- Manual: You should search a network and logon manually in this mode.

Mode:

2. Select the mode of searching network.
 - **Auto:** The gateway can automatically search a network and login.
 - **Manual:** You need search network and login manually.
3. Click to submit the setting.
4. If search network manually, please select searched network and click to login.


Network Setting

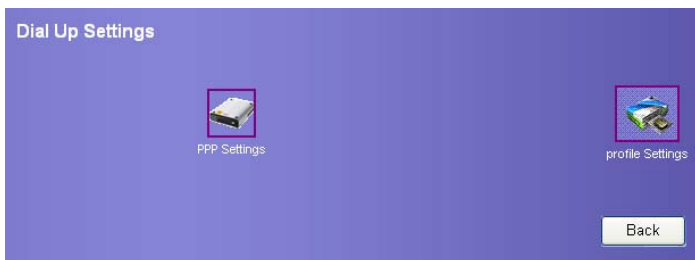
Mode:

Network:


10 Dial-up Setting

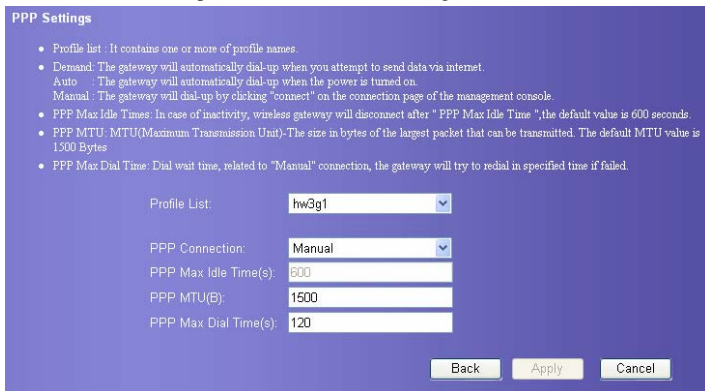
You can configure PPP parameters and manage the Profile list.

Click . The dial-up setting page displays as following figure.



Configure PPP Properties

1. Click  to open the interface as following.



2. Enter correct parameters.


- **Profile List:** It is used to select a Profile from an established dial access list. If the drop-down list is null, you need to create a Profile.
- **PPP Connection:** It is used to select the dial-up mode.

| Dial-up mode | description |
|--------------|---|
| Auto | After a device is started, the system automatically creates a permanent connection, no matter whether there is data transfer. |
| On Demand | The connection exists when there is data transfer, and disappears when there is no data transfer. |
| Manual | Manually dial up to create a connection. |

- **PPP Max Idle Time:** It refers to the lasting time of the PPP connection when no data is transferred. In **On Demand** mode, if no data is transferred during the set PPP max idle time, the PPP connection stops.
- **PPP MTU:** It is used to set the maximum number of bytes encapsulated in a single data frame. The default setting is **1500 bytes**.
- **PPP Max Dial Time:** It is used to set the longest waiting time during a dial access connection.

Manage the Profile List



Click . The **Profile Settings** page displays and you can create, edit, save and delete a profile.

Profile settings

- Profile list: It contains one or more of profile names.
- Profile Name: Type the name that you want to assign to the new profile.
- Dial-up Number | PPP User Name | PPP Password: These parameters are provided by your ISP. Dial-up Number is used for data service calls, PPP User Name and PPP Password are used to gain authentication of ISP when the call is established.
- If a fixed IP address or APN (Access Point Node) is given by your ISP, select "Static", otherwise, select "Dynamic", the gateway will automatically get these parameters.

Profile List:

Profile Name:

Dial-up Number:

PPP User Name:

PPP Password:

APN:
 Dynamic Static


IP Address:
 Dynamic Static

Introduce the Interface

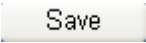
The following table shows details.

| Parameter | Description |
|----------------|--|
| Profile List | Include all profile name |
| Profile Name | Input the name of the selected or created profile |
| Dial-up Number | Input the character string for PPP dial-up. For details, refer to the carrier. |
| PPP User Name | The user name used in PPP communication. It is provided by the network carrier. |
| PPP Password | It refers to the password used in PPP communication. It is provided by the network carrier. |
| APN | Select the mode for obtaining the APN: <ul style="list-style-type: none">• Dynamic: Obtain the APN dynamically the network• Static: Enter the APN manually provided by the network carrier |
| IP Address | Select the mode for obtaining the IP address: <ul style="list-style-type: none">• Dynamic: Obtain the IP address dynamically the network• Static: Enter the IP address manually provided by the network carrier |


Create Profile

1. Input the profile information in the text box according to the interface prompts.
2. Click  to submit the new profile.

Modify Profile

1. Select the profile to be changed in the **Profile List** draw-down box. Relevant information is displayed in corresponding text box.
2. Input the Profile parameters.
3. Click  to submit the modified profile.


Delete Profile

1. Select the profile to be deleted in the **Profile List** draw-down box.
2. Click  to delete chosen profile.

11

IP Address Distribution

You can configure the IP address Distribution mode of LAN. Your gateway's DHCP server can allocate IP address for network devices automatically. If use DHCP server, ensure that the PC connected with the gateway is configured for obtaining IP address automatically also, refer to "PC Network Setting".

Click  to display the DHCP setting page.

LAN Basic Settings

- The gateway is set up by default as a DHCP (Dynamic Host Configuration Protocol) server, which provides IP address from "Start IP address" to "End IP address" for all the PCs that are connected to it on the LAN. If you disable the DHCP server, you must have another DHCP server within your network or else you must manually configure IP address of the computer.

| | |
|---------------------|---|
| IP Address: | <input type="text" value="192.168.1.1"/> |
| Subnet Mask: | <input type="text" value="255.255.255.0"/> |
| DHCP Server: | <input checked="" type="radio"/> Enabled <input type="radio"/> Disabled |
| Start IP Address: | <input type="text" value="192.168.1.100"/> |
| End IP Address: | <input type="text" value="192.168.1.200"/> |
| DHCP Lease Time(s): | <input type="text" value="86400"/> |

- IP Address:** The IP address of your gateway. By default, it is **192.168.1.1**.
- Subnet Mask:** It is used with the IP address to realize flexible subnetting. By default, the subnet mask is **255.255.255.0**.
- DHCP Server:** It refers to the Dynamic Host Configuration Protocol server. It is used to assign the IP addresses dynamically. If the setting is **Enabled**, the DHCP server can automatically assign IP addresses for the user PCs. In such case, users do not need to configure the IP addresses manually. The recommended setting is **Enabled**.
- Start IP Address & End IP Address:** It is used to define the IP address range for random selection during IP address assignment. That is, it is used to define the IP address range available for the hosts in the LAN. For example, within 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 IP address range is a single IP address.


- **DHCP Lease Time:** The DHCP server assigns a IP address to each device connected to the LAN for a this amount of time. When the lease expires, the DHCP server will check if the device has disconnected form the LAN. If it has, the server will reassign this IP address to a newly connected device. This way can avoid waster of IP address resource.

 **Note:**

- The **Start IP Address** must be smaller than the **End IP Address**.
- When the DHCP server is enabled, you can set **Start IP Address**, **End IP Address**, and **DHCP Lease Time**. Otherwise, you cannot set the preceding three parameters.

12 WLAN Setting

Enable/Disable WLAN

1. Click  to display The **WLAN Module Settings** page.

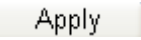


WLAN Module Settings


- Enabled: You can configure and use WLAN function.
- Disabled: WLAN is prohibited and can not be configured.

Wlan Module Enabled Disabled

Back Apply Cancel

2. Enable or disable the WLAN mode.
 - Enable: You can use WLAN function and configure relevant parameters.
 - Disable: You cannot use WLAN relevant function.
3. Click  to submit the setting.

Basic Settings for WLAN

- Click . You can perform basic settings on the WLAN.

WLAN Settings

- SSID(Service Set Identifier): Type a name up to 32 characters for your local wireless network(WLAN).
- SSID Broadcast
 - Enabled : The gateway will broadcast SSID and other devices can detect and connect to it.
 - Disabled: The gateway will disable broadcasting and hide the name of your network.
- AP Isolation
 - If you select "On", Stations can connect with the gateway, but can not visit each other,
 - If you select "Off", Stations can connect the gateway, and can visit each other.
- Country | Channel
 - IEEE 802.11g/b divided ISM band into multi-channels, and the total channel is not equivalent in different countries. You should set the same channel or select "auto" in channel field of WLAN devices in order to establish association.
- 802.11 Mode
 - 54g Auto for the widest compatibility.
 - 54g Performance: For the fastest performance among 54g certified equipment.
 - 54g LRS: For legacy 802.11b/g equipment.
 - 802.11b: Only 802.11b wireless devices can connect to the gateway.

| | | |
|---------------------|--------------------------|-------------|
| Wireless Interface: | e960h(00:90:4C:C0:85:5E) | |
| SSID: | e960h | |
| SSID Broadcast: | Enabled | |
| AP Isolation: | On | |
| Country: | AMERICAN SAMOA | Current: US |
| Channel: | Auto | Current: 11 |
| 802.11 Mode: | 54g Auto | |
| Rate: | Auto | |

Advanced...

Back

Apply

Cancel

Select Wireless Interface

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

Enter SSID

SSID: It refers to the server set ID used to identify a WLAN. A wireless terminal (such as a PC) can communicate with the E960 only when they have the same SSID. To ensure the WLAN security, please do not use the default SSID. You can enter a character string, such as MyHome, as the SSID.

Enable or Disable the SSID Broadcast

- **Enabled:** The WLAN is an open network. The gateway broadcasts the SSID of this WLAN. WLANs of this type are easy to access for users. Unauthorized users, however, can also easily access WLANs of this type. This type of WLANs has very low security level.
- **Disabled:** The WLAN is a closed network. The gateway does not broadcast the SSID of this WLAN. Before accessing a WLAN of this type, the user must configure the SSID of the WLAN on the wireless terminal (such as a PC). In this manner, the WLAN security is ensured.

Enable or Disable the AP Isolation

- **On:** The terminals accessing the gateway through the WLAN cannot communicate with each other.
- **Off:** The terminals accessing the gateway through the WLAN can communicate with each other.

Select the WLAN Channel.

- **Country:** It is used to identify the country. Different countries have different standards on channel usage. Each country defines a group of specific channels.
- **Channel:** It refers to the channel the gateway works with. According to the IEEE802.11 standard, the working frequency range for the wireless LAN based on the Direct Sequence Spread Spectrum (DSSS) technology is 2.4GHz to 2.4835GHz. The frequency occupation of each channel is 22MHz. The available channels vary with the selected country. The default setting is **11**. If you do not know which channel to select, please select **Auto** and gateway can search channel automatically.

Configure 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 gateway has some difficulty in communicating with devices conforming to the IEEE 802.11b standards, please select this mode. |
| 802.11b Only | The gateway can only work with data transfer rates defined by the 802.11b standard. |

Configure the Transfer Rate

Rate: It is used to set the WLAN transfer frequency of the E960. You can set the value to **Auto**, the gateway automatically search the rate. The highest data transfer rate of a WLAN supported by the gateway is 54Mbit/s.

Click to submit the setting. Click **Advanced** to configure WLAN advanced setting.

Advanced Settings for WLAN

You can configure the security and Network Bridge.

Configure Security Encryption

You can set a security key for your wireless network to prevent your wireless LAN from data attack. To access the wireless network, you must set the wireless security key of your PC consistent with the security key of the wireless gateway.

WLAN Advance Settings

- **802.11 Authentication**
Open System: Any WLAN client can join wireless network without authentication.
Shared key: Only those WLAN client having same WEP key with wireless gateway can authenticate successfully and access wireless network.
- **Encryption Mode**
No encryption: You wireless network is exposed to everyone without authentication and encryption, and this option is not recommended.
WEP: Wireless Equivalent Privacy is a 64-bit or 128-bit encryption method with user configurable fixed keys.
WPA: Wi-Fi Protected Access is a 128-bit encryption method with keys that change automatically over time.
WPA2: A more secure version of WPA with implementation of the 802.11i standard.
- **WPA Pre-Shared Key**
Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.
- **Key Rotation Interval**
Specify the key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.
- **Network Key**
Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key, enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

| | |
|------------------------|--------------------------|
| Wireless Interface: | e960h(00:90:4C:00:85:5E) |
| 802.11 Authentication: | Open |
| Encryption Mode: | WPA-PSK |
| WPA Encryption: | TKIP |
| WPA Pre-Shared Key: | |
| Key Rotation Interval: | 0 |

802.11 Authentication Mode

- **Open:** Open system authentication. The user accessing the WLAN can use **WEP**, **WPA-PSK**, **WPA2-PSK** to authenticate, or choose to non-authenticate.
- **Shared:** Shared key authentication. It is used only for **WEP** authentication. The user accessing the WLAN must use the WEP to authenticate.

Encryption Mode

There is three encryption mode: No Encryption, WPA-PSK, WPA2-PSK and WEP. For details, refer to “Configure the Security encryption”.

WLAN Advance Settings

- **802.11 Authentication**
Open System: Any WLAN client can join wireless network without authentication.
Shared key : Only those WLAN client having same WEP key with wireless gateway can authenticate successfully and access wireless network.
- **Encryption Mode**
No encryption: You wireless network is exposed to everyone without authentication and encryption, and this option is not recommended.
WEP : Wireless Equivalent Privacy is a 64-bit or 128-bit encryption method with user configurable fixed keys.
WPA : Wi-Fi Protected Access is a 128-bit encryption method with keys that change automatically over time.
WPA2: A more secure version of WPA with implementation of the 802.11i standard.
- **WPA Pre-Shared Key**
Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.
- **Key Rotation Interval**
Specify the key update interval in seconds. The value can be either 0 seconds or from 30 seconds and up, 1-29 seconds are not usable figures. Enter 0 to disable the update.
- **Network Key**
Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit key, enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

| | |
|------------------------|----------------------------|
| Wireless Interface: | e960h(00:90:4C:C0:85:5E) ▾ |
| 802.11 Authentication: | Open ▾ |
| Encryption Mode: | WPA-PSK ▾ |
| WPA Encryption: | TKIP ▾ |
| WPA Pre-Shared Key: | <input type="text"/> |
| Key Rotation Interval: | 0 <input type="text"/> |

Set Access Attributes of the Client

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

- **Preamble Type**
Long | Short. Set whether short or long preambles are used. Short preambles improve throughput but all clients in the wireless network must support this capability if selected.
- **Max Associations Limit**
Set the associations the wireless gateway supported, this value should be in the range of 1 to 32.
- **Mode**
Access Point : Access Point to enable access point functionality.
Wireless Bridge: Wireless Distribution System or WDS.
- **Bridge Restriction**
Enabled : Select "Enabled" to enable wireless bridge restriction. Only those bridges listed in Bridges will be granted access. Disabled: Select "Disabled" to disable wireless bridge restriction. Any wireless bridge (including the ones listed in Bridges) will be granted access.
Bridges : Enter the peer wireless MAC addresses of any wireless bridges that should be part of the wireless distribution system (WDS).

| | | |
|-------------------------|----------------------|----------------------|
| Preamble Type: | Long | |
| Max Associations Limit: | 128 | |
| Mode: | Access Point | |
| Bridge Restriction: | Enabled | |
| Bridges: | Peer MAC Address | Link Status |
| | <input type="text"/> | <input type="text"/> |
| | <input type="text"/> | <input type="text"/> |
| | <input type="text"/> | <input type="text"/> |
| | <input type="text"/> | <input type="text"/> |

- **Preamble Type:** It has two options: **Long** and **Short**. When clients (PCs) support the **Short** setting, the WLAN can have a better performance in **Short** mode.
- **MAX Associations Limit:** It refers to the maximum number of connections. It is used to set the upper threshold of WLAN clients connected to the gateway at the same time. A maximum of 128 clients can connect with the gateway in wireless mode.
- **Mode:** It refers to the WLAN access mode. The gateway has two work modes, as shown in the following table. The default setting is **Access Point**.

| Mode | Description |
|-----------------|---|
| Wireless Bridge | Two or more APs can connect with the gateway. |
| Access Point | Only APs and wireless terminals meeting the IEEE 802.11b/g standard can connect with the gateway. |

- **Bridge Restriction:** It refers to the limitation on the peer MAC addresses. When the setting is **Disabled**, the E960 can access all the remote bridges; when the setting is **Enabled**, the E960 can only access the remote bridges whose addresses are in the address list.
- **Bridges:** It refers to the physical address of the remote peer bridge. The gateway supports point-to-point bridge mode and can connect with 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 States:** **Up** shows connection successful and **Down** shows connection failed.

MAC Filter Setting



Click  to display the **WLAN MAC Filter Setting** interface. You can control and manage the clients accessing WLAN to enhance security level.

Wlan MAC Filter Settings

- **MAC Restrict Mode**
Disabled: Disable MAC Restrict function, any WLAN clients try to join the network will not be limited by MAC address.
Allow : Only those WLAN clients whose MAC listed in "Bridges" are allowed to access wireless gateway.
Deny : WLAN clients whose MAC addresses listed in "Bridges" are prohibited to access wireless gateway.
- **MAC Addresses**
The following list are allowed or denied clients with the specified MAC address which form is like XX:XX:XX:XX:XX:XX.

MAC Restrict Mode:

MAC Addresses:

| | |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |
| <input type="text"/> | <input type="text"/> |

MAC Restrict Mode

There are three parameter values, as shown in the following table.

| Value | Description |
|----------|--|
| Disabled | The MAC address restriction function is disabled. |
| Allow | The clients with addresses in the MAC Address columns are allowed to connect with the gateway through the WLAN. |
| Deny | The clients with addresses in the MAC Address columns are not allowed to connect with the gateway through the WLAN. |

MAC Addresses

Enter MAC address in the list. The gateway can perform access control on the clients whose addresses are in this list. The list can contain a maximum of 16 MAC addresses.

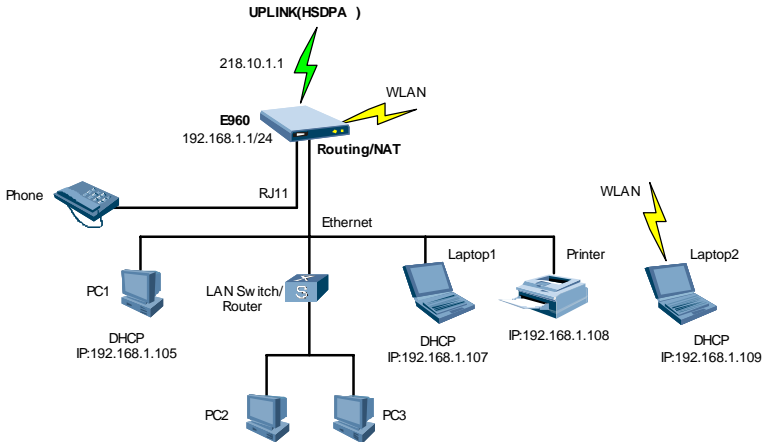
13

Typical Networking Example

Your gateway can form a WLAN through the WLAN interface, or can form a small-sized LAN through the four Ethernet interfaces connecting with a terminal device in small office or home office (SOHO).

Your gateway also supports external concentrator, Ethernet switch, or router. To form a LAN with multiple PCs, you can extend the Ethernet interfaces through the concentrator or Ethernet switch.

For example, your gateway forms a small-sized LAN with multiple PCs in the SOHO to access 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, 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 9 UMTS Setting 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 whether 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 Configure PPP Profile 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 PC Network Configuration.
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.

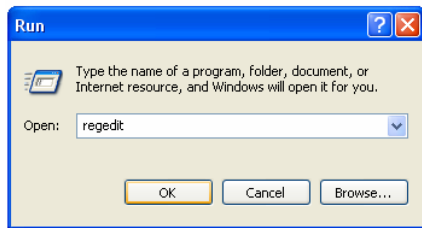
What to do if bridging between two EC506s is unsuccessful

1. Make sure that the two gateways work on the same channel. For details, see ” Choose Preferred Mode and Band ” .
2. Make sure that the MAC address of one gateway is in the peer MAC address list of another gateway. For details, see “MAC Addresses” .

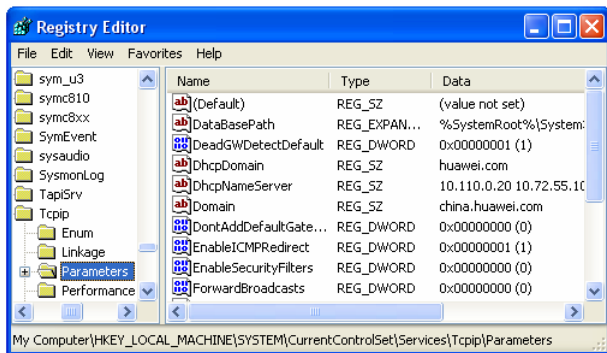
When the signal strength is normal, what to do if the downloading rate is much lower

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

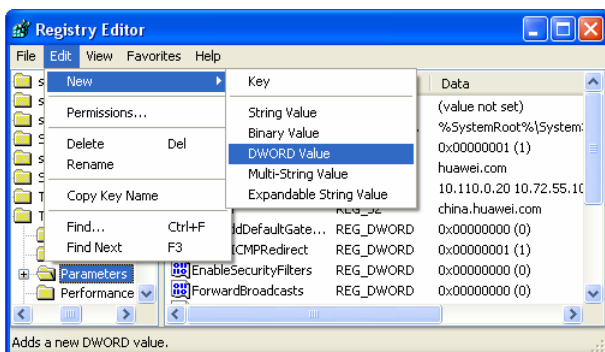
1. Click **start** and then select **Run**.
2. Type “regedit” in the **Open** text box and then click **OK**



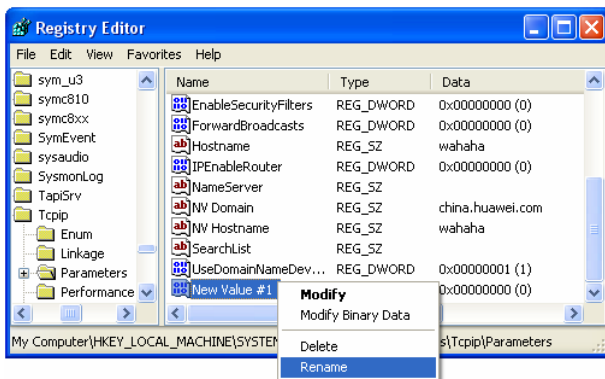
3. Select Parameters under the following directory:
\\HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\Tcpip.



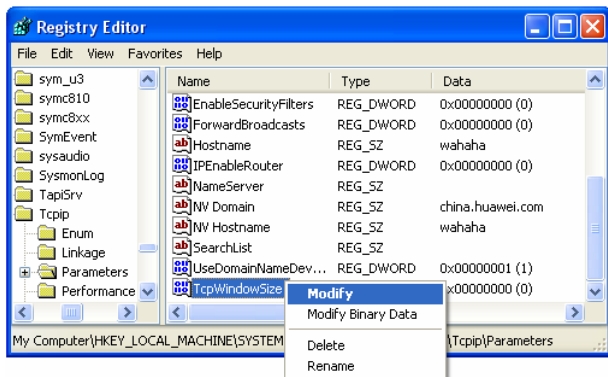
4. Select **Edit > New > DWORD Value**.



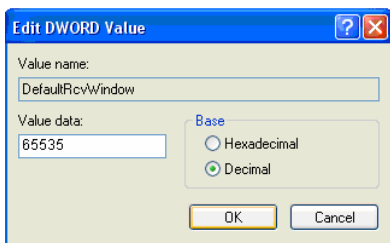
5. Rename “New Value #1” as “TcpWindowSize” .



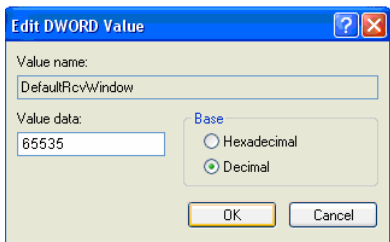
6. Right-click “TcpWindowSize” and then select **Modify** in the shortcut menu.



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 wireless 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 and take out the battery. 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, battery, or 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, battery, or charger 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, battery, and charger to serious collision or shock. Otherwise, battery leakage, 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, battery, and charger in places beyond the reach of children. Do not allow children to use the wireless device, battery, or charger without guidance.
- Do not allow children to put the battery in mouth, for electrolyte in the battery is poisonous.
- 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, battery, and charger are not water-resistant. Keep them dry. Protect the wireless device, battery and charge 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 one inch (2.5 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 of the battery or charger 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.

Statement

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20cm from all persons.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.
- Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning off and on the user is encouraged to try to correct the interference by one or more of the following measures.

16

Abbreviations

| | |
|----------|---|
| 3G | The Third Generation |
| A | |
| AC | Alternating Current |
| ARP | Address Resolution Protocol |
| AP | Access Preamble |
| 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 | |
| HSDPA | 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 |
|-------|-------------------|
