

MF23

3G Wireless Router

User Manual

ZTE CORPORATION
NO. 55, Hi-tech Road South, ShenZhen, P.R.China
Postcode: 518057
Tel: (86) 755 26779999
URL: <http://www.zte.com.cn>
E-mail: mobile@zte.com.cn

LEGAL INFORMATION

Copyright © 2010 ZTE CORPORATION.

All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without the prior written permission of ZTE Corporation.

The manual is published by ZTE Corporation. We reserve the right to make modifications on print errors or update specifications without prior notice.

Version No. : R1.0

Edition Time : Nov.2010

Manual No. :

Content

Welcome	1
General Information	1
Safety Precautions	1
Cleaning and Maintaining	1
Limited Warranty	2
Limitation of Liability	2
Emergency Call	2
Getting started	3
Parts Supplied	3
Appearance	3
LED Indicator	3
Interface Description	4
Installation	5
Inserting (U)SIM Card	5
Connecting to Phone	5
Connecting to Computer	5
Connecting with External Power	6
Switching on Your Device	6
Power Supply	6
About (U)SIM Card	6
Voice	7
Making a Call	7
Answering a Call	7
Internet Access	8
Preparation	8
Login	8
Settings	9
Quick Setup	9
WAN Connection	11
3G Settings	12
Router	13
Wi-Fi Settings	14
Firewall	20
SMS	24
Advanced	25
Disconnecting from the Internet	27
Logout	27
Troubleshooting	29
Technical Parameters	31
Glossary	32

Chapter 1

Welcome

Thank you for choosing ZTE MF23 3G Wireless Router (hereinafter referred to as “unit” or “router”). To get the most from your router and to keep it in the best condition, please read this manual carefully.

The pictures, symbols and contents in this manual are for your reference only. They might not be completely identical with your router. ZTE operates a policy of continuous development. We reserve the right to update the technical specifications in this manual at any time without prior notice.

General Information

Safety Precautions

- Some electronic devices may be susceptible to electromagnetic interference. Locate the router away from TV set, radio and other electronic equipment to avoid electromagnetic interference.
- The router may interfere with medical devices like hearing aids and pacemakers. Consult a physician or the manufacturer of the medical device before using the router.
- Please keep yourself at least 20 centimeters away from router.
- Do not use your router in dangerous environments such as oil terminals or chemical factories where there are explosive gases or explosive products being processed.
- Please use original accessories or accessories that are authorized by ZTE. Unauthorized accessories may affect the router performance, damage the router or cause danger to you.
- Do not attempt to dismantle the router. There are no user serviceable parts.
- Do not allow the router or accessories to come into contact with liquid or moisture at any time. Do not immerse the router in any liquid.
- Do not place objects on top of the router. This may lead to overheating of the device.
- The device must be placed in ventilation environment for use.
- Do not expose the router to direct sunlight or store it in hot areas. High temperature can shorten the life of electronic devices.
- Do not allow children to play with the router or charger.
- Keep the length of the cable between the router and the phone less than 10 meters.
- The router is for indoor use only. Do not use the router outside. Do not connect telephone extensions which run outside of the building. These can result in lightning damage to your unit.

Cleaning and Maintaining

- Use an antistatic cloth to clean the router. Do not use chemical or abrasive cleanser as these could damage the plastic case. Turn off your router before you clean it.
- Use the router within the temperature range of $-10^{\circ}\text{C} \sim +55^{\circ}\text{C}$, and the storage temperature range is $-20^{\circ}\text{C} \sim +65^{\circ}\text{C}$. The humidity range is 5%~95%.
- Do not use your router during a thunderstorm. Remove the mains power pack from the wall socket.
- Do not take out your (U)SIM card unnecessarily. The (U)SIM card may be easily lost or it can be damaged by static electricity.

Limited Warranty

- This warranty does not apply to defects or errors in the Product caused by:
 - i. Reasonable Router Appearance Disfiguration.
 - ii. End User's failure to follow ZTE's installation, operation or maintenance instructions or procedures.
 - iii. End User's mishandling, misuse, negligence, or improper installation, disassemble, storage, servicing or operation of the Product.
 - iv. Modifications or repairs not made by ZTE or a ZTE-certified individual.
 - v. Power failures, surges, fire, flood, accident, actions of third parties or other events outside ZTE's reasonable control.
 - vi. Usage of products of third Parties, or usage in conjunction with third party products provided that such defects is due to the combined usage.
 - vii. Any other cause beyond the range of normal usage for Products. End User shall have no right to reject, return, or receive a refund for any Product from ZTE under the above-mentioned situations.

- This warranty is end user's sole remedy and ZTE's sole liability for defective or nonconforming items, and is in lieu of all other warranties, expressed, implied or statutory, including but not limited to the implied warranties of merchantability and fitness for a particular purpose, unless otherwise required under the mandatory provisions of the law.

Limitation of Liability

ZTE shall not be liable for any loss of profits or indirect, special, incidental or consequential damages resulting from or arising out of or in connection with using of this product, whether or not ZTE had been advised, knew or should have known of the possibility of such damages, including, but not limited to lost profits, interruption of business, cost of capital, cost of substitute facilities or product, or any downtime cost.

Emergency Call

Do not rely on the 3G Wireless Router to provide emergency call in all situations.

Your 3G Wireless Router only supports emergency dialing when there is power and connection to the mobile network. If the power fails, the router can not work. If you have no network coverage you will not be able to make emergency calls. The 3G Wireless Router does not include a lifeline facility (wired access to the PSTN).

Chapter 2

Getting started

The router operates on the HSUPA/HSDPA/UMTS network and GSM/GPRS/EDGE network and supports voice and data service. And the router is only suitable for family user, not suitable for industry user.

Parts Supplied

Parts	Quantity
3G Wireless Router	1
External power adapter	1
User manual	1
Certificate of quality	1

Appearance



LED Indicator

Indicator	State	Description
POWER	ON	External power supply works normally.

Indicator	State	Description
	OFF	External power supply is disconnected or power off.
PHONE	Off	Not in use.
	Blinking	On Dialing, or there is an incoming call, the phone is ringing.
	On	In calling.
PPP	ON	Internet connected.
	Blinking	The router attempts to connect Internet.
	OFF	Internet disconnected and not attempt to connect.
3G	ON	RF signal is normal. Different color indicates different network. Red: GSM/GPRS/EDGE. Green: HSDPA/HSUPA/UMTS.
	Blinking	RF signal is poor.
	OFF	RF signal is not available.
WIFI	ON	WiFi works normally.
	Blinking	Data transmission.
	OFF	WiFi works abnormally, or this WiFi function is disabled.

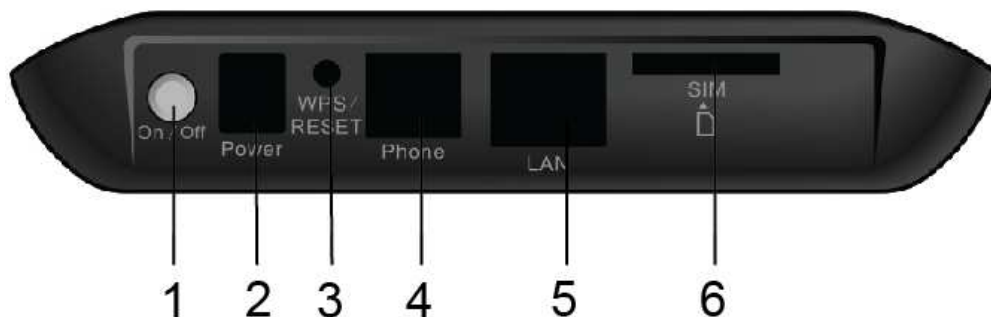


Notes:

The indicators (including PPP and 3G) are all blinking in green when:

- The (U)SIM card has not been installed.
- The PIN code or PUK code is required.
- The router can not work normally.

Interface Description



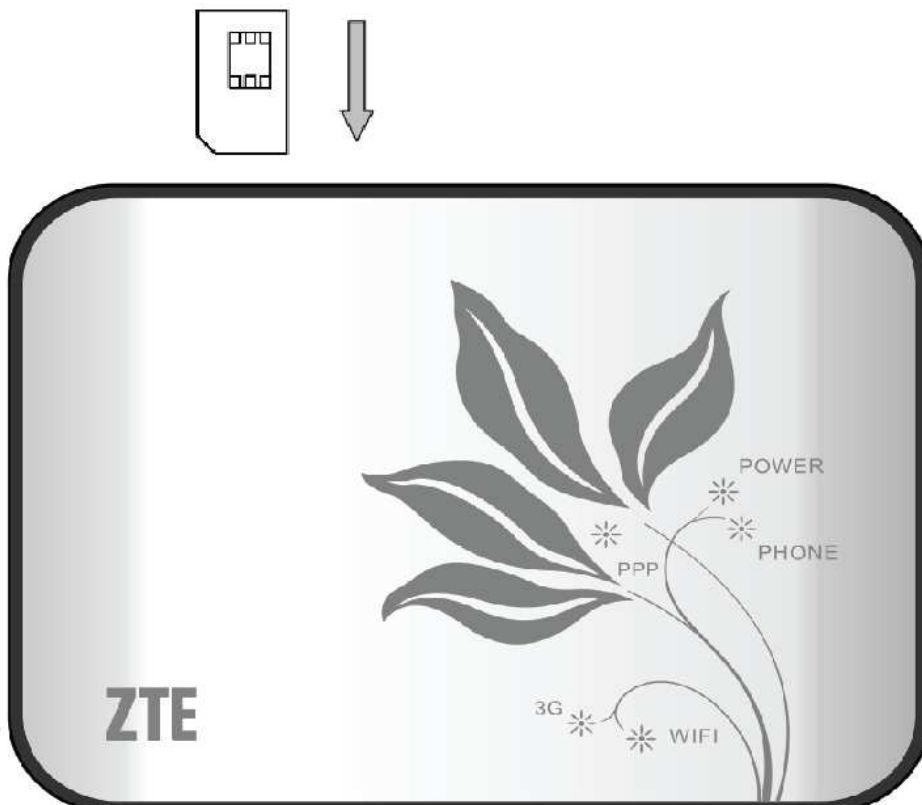
1. **POWER Switch:** Turn the router ON or OFF.
2. **POWER Socket:** Connection to the external power supply.

3. **WPS:** WPS button is used to start Wi-Fi Protected Setup authentication process.
4. **Phone:** Standard RJ11 connector for Telephone.
5. **LAN:** Ethernet connections to computer.
6. **SIM:** (U)SIM port for inserting (U)SIM card.

Installation

Inserting (U)SIM Card

Insert the (U)SIM card into the (U)SIM port.



Notes:

Please power off the router and remove the external power adapter before removing or inserting the (U)SIM card, if not, the router or (U)SIM card may be damaged.

Connecting to Phone

Connect the telephone to the **PHONE** interface with a phone cable(RJ11).

Connecting to Computer

Connect your computer to the **LAN** interface with an Ethernet cable (RJ45).



Notes:

The router will adapt the Ethernet cable style (crossover or straight) automatically.

Connecting with External Power

Connect the external power adaptor to a standard power outlet. Insert the plug into the socket at the rear of the router.

Switching on Your Device

1. Turn the power switch on to get started. Make sure that the phone is on hook before power on.



Notes:

Do not put anything on the top of the router. Do not lay routers to overlap each other when using.

2. Wait 1~2 minutes after turning the router on before you use the service. The 3G & POWER indicator should be lit on.



Notes:

When the router is turned off, an incoming caller will hear the prompt like “The number you have dialed is currently unavailable.”

If the 3G LED is blinking constantly, try to move the router to another location. The router takes 1~2 minutes to initialize, attach to the network and obtain an IP address.

Power Supply

For normal operation connect the router to the external power adapter. In case of power failure or when there is no available external power supply, the router can not work.

About (U)SIM Card

Avoid handling the (U)SIM card unnecessarily. Hold the card by the edges to prevent static damage. Keep the (U)SIM card away from electrical and magnetic appliances.

If you cannot get service, make sure that:

- You are in an area which has network coverage.
- You are using the correct (U)SIM card.

Chapter 3

Voice

Making a Call

Before making a call, make sure:

- The (U)SIM card is installed.
- The telephone cable (RJ11) is connected properly.
- The POWER light is on.
- The 3G light is on.

To make a call:

1. Pick up the handset.
2. Key in the telephone number.
3. You can either press # key on the telephone to send the call, or wait 4~8 seconds for the call to be connected automatically.
4. Call will be connected.



Notes:

If there is no 3G indication, the RF signal is unavailable. Change the location of the router and make sure nothing is blocking it.

Making a Trunk Call

If you are making a trunk call, add the area code as normal.

E.g. 03 9612 3456

Making an International Call

If you are making an international call, key in the international access code followed by the country code, area code and number.

E.g. 00 11 64 12 345678

Answering a Call

When the phone rings, pick up the handset to answer it. If the telephone has hands-free function you also can answer the call by pressing the **Hands-free** button. Press the **Hands-free** button again to end the call.

Chapter 4

Internet Access

The router does not require any drivers, and it supports all operating systems with Ethernet LAN capability, such as Windows 2000, XP, Vista, MAC OS X and Linux. The router supports two computers surfing on internet using Ethernet cable at the same time.

Note: All the parameter settings in this chapter are just for your reference. Please contact your service provider for detail.

Preparation

Before using the data service, make sure:

- The (U)SIM card is installed.
- The Ethernet cable is connected properly.
- The POWER light is on.
- The 3G light is on.
- The PPP light is on.

Web browser requirement:

It is suggested that you use one of these web browsers to connect to the internet.

- IE 6.0 or above
- Firefox 2.0
- Netscape version 9.0

Login

The router can be connected by RJ45 or by Wi-Fi (the SSID is “ZTE Wireless Network”). By either connection mode, you should set to obtain an IP address automatically in the attribution setting of Internet protocol(TCP/IP).

After your computer gets the IP address (like 192.168.0.100) from the router, open a web browser and type “ http://192.168.0.1” in the address bar. Input the username and password.

User name: admin

Password: admin

Welcome to ZTE MF23

goahead
WEBSERVER™

User Name :

Password :

Save

Login

Clear

Copyright © 2010.ZTE. All rights reserved.

Click **Login** to log in the router.



Notes:

If you click **Save** after you give user name and password, the router will save them, next time when you want to log in the router with the same user name and password, what you need to do is click **Login**.

Settings

Do not change any settings unless instructed by your service provider. If you want to make changes of settings, you need to disconnect the router from the network. After making changes, please reboot your router by turn off and on again.

Quick Setup

The **Quick Setup** helps you to quickly set the basic settings of your router. The following describe the steps and parameters of **Quick Setup**.

1. Read the guide carefully, and then click **Next**.

Quick Setup

•The wizard will show you how to set up your gateway in the safe way: Click "Next" to continue, click "Back" and "Next" to navigate, and click "Apply" to save the settings.

Notes:

Basic parameters can be set in this wizard. For advanced parameters, you need to set them in other menus.

Next

2. Set the **PPP Profile Configuration** and then click **Next**.

Quick Setup-->PPP Profile Configuration

- Profile Name: The default profile that you used currently.
- APN: If a fixed APN(Access Point Name) is given by your ISP, select "Manual APN"; otherwise, select "Auto APN", the gateway automatically obtains it.
- Dial No.:This parameter is provided by your ISP, Dial No. is used for data service connections.

Profile

Profile Name	ZTE
--------------	-----

APN

APN Setting	<input type="radio"/> Auto APN <input checked="" type="radio"/> Manual APN
APN	cmwap

Dial Setting

Dial No.	*99#
----------	------

Back Next

3. Set the **PPP Authentication** and then click **Next**.

Quick Setup-->PPP Authentication

•PPP Authentication

The authentication mode is provided by your Internet Service Provider(ISP).

Password Authentication Protocol(PAP): It provides a simple method without encryption for the peer to establish its identity using a 2-way handshake.

Challenge-Handshake Authentication Protocol(CHAP): It is used to periodically verify the identity of the peer PPP User Name and PPP Password are provided by your ISP and used to obtain authentication from the ISP when the connection is established.

PPP Authentication

Authentication	<input type="radio"/> CHAP <input checked="" type="radio"/> PAP
PPP User Name	
PPP Password	

Back Next

4. Set the **SSID Configuration** and then click **Next**.

Quick Setup -->SSID Configuration

•Name SSID(Service Set Identifier): Enter a character string up to 32 characters as the name for your wireless local area network (WLAN).

•SSID Broadcast

Enabled: The gateway broadcasts the SSID and other devices can detect and connect to it.

Disabled: The gateway disables broadcasting and hides the name of your network.

SSID

Name(SSID)	ZTE Wireless Network
------------	----------------------

SSID Broadcast

SSID Broadcast	Enabled
----------------	---------

Back Next

5. Set the **Security Configuration** and then click **Next**.

Quick Setup-->Security Configuration

•Add encryption to your wireless network to prevent unauthorized traffic monitoring and access.
 No Encryption: Your wireless network is open to everyone without authentication and encryption, and this option is not recommended.
 Wireless Equivalent Privacy(WEP): It is a 64-bit or 128-bit encryption method with user configurable fixed keys.
 Wi-Fi Protected Access(WPA): It is a 256-bit encryption method with keys changing automatically.
 WPA2: It is the securer 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. Enter 0 to disable the update function.(You'd better set more than 59)
 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

Encryption Mode	NO ENCRYPTION
-----------------	---------------

Back Next

6. Show all the configurations and then click **Apply** to complete. If you want to modify, please click **Back**. (The figure is only for your reference as shown below).

Quick Setup-->Configuration as Follows

Profile Name:	ZTE
Dial No.:	*99#
PPP User Name:	
API Setting:	manual
API:	cmwap
PPP Authentication:	pap
Name (SSID):	ZTE Wireless Network
SSID Broadcast:	enable
Encryption Mode:	NO ENCRYPTION

Back Apply

WAN Connection

Click **WAN Connection**, you can configure how to connect to the Internet.

WAN Connection

PPP Connection Mode

<input type="radio"/>	Auto Connect
<input type="radio"/>	On Demand Connect
<input checked="" type="radio"/>	Manual Connect <input type="text" value="Connect Internet"/>
PPP Connection Status	Disconnected

Apply

There are three connection modes:

- **Auto Connect:** The router will automatically connect to WAN when it is powered on.
- **On Demand Connect:** The connection will be established when data transmission is required. Router will disconnect from the Internet if there is no data traffic going through during the **Max Idle Time**.
- **Manual Connect:** Connect to Internet or disconnect from Internet manually.

Click **Apply** to confirm your configuration, and then the PPP connection status will be shown in the figure.

3G Settings

Wireless Info

Select **3G Settings > Wireless Info**, the 3G wireless information is shown in the following figure:

3G Settings-->Wireless Info

• Wireless Info • Network Select • APN Setting

3G Wireless Information

Network Provider	CMCC
Network Type	EDGE
Roam	OFF
RSSI	-49 dBm
RSCP	-0 dBm
Ec/Io	-0 dB
Cell ID	5054
LAC Code	37333

Refresh

Click **Refresh** to update the wireless information.

Network Select

Select **3G Settings > Network Select**, the band selection mode is shown in the following figure:

3G Settings-->Network Select

• Wireless Info • Network Select • APN Setting

Band Selection Mode

<input checked="" type="radio"/>	Automatic
<input type="radio"/>	WCDMA Only
<input type="radio"/>	GSM Only

Apply

- **Automatic**: Router searches for valid network according to the wireless network.
- **WCDMA Only**: Router searches for WCDMA network only.
- **GSM Only**: Router searches for GSM network only.

Click **Apply** to confirm your configuration.

APN Setting

Select **3G Settings > APN Setting**, the APN parameters are shown in the following figure:

3G Settings-->APN Setting

• Wireless Info • Network Select • **APN Setting**

APN Setting

Profile Selection	ZTE ▾
Profile Name	ZTE
APN Setting	<input type="radio"/> Auto APN <input checked="" type="radio"/> Manual APN
APN	cmwap
Dial No.	*99#
PDP Type	<input checked="" type="radio"/> IP <input type="radio"/> PPP
PDP Setting	<input checked="" type="radio"/> Auto PDP <input type="radio"/> Manual PDP
DNS	<input checked="" type="radio"/> Auto DNS <input type="radio"/> Manual DNS
Authentication	<input type="radio"/> CHAP <input checked="" type="radio"/> PAP
User Name	
Password	

Save Set default Add Delete

- **APN Setting:** APN address mode. If a fixed APN is provided by your service provider, select **Manual APN**. Otherwise select the **Auto APN**, and the router will automatically obtain this parameter.
- **APN:** APN string.
- **Dial No.:** This dial number is used for data service connections.
- **PDP Type:** Packet Data Protocol (PDP) Type. **IP** is recommended unless service provider instruct others.
- **PDP Setting:** PDP address mode. If a fixed IP address is given by your service provider, select **Manual PDP**. Otherwise select the **Auto PDP** and the router will automatically obtain this parameter.
- **DNS:** If a fixed IP address is given by your service provider, then choose **Manual DNS**. Otherwise choose **Auto DNS**. The router will automatically obtain parameters.
- **Authentication:** Password Authentication Protocol (PAP) provides a simple method without encryption for the peer to establish its identity using a 2-way handshake. Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake.
- **User Name:** User name is used to obtain authentication from the ISP when the connection is established
- **Password:** Password is used to obtain authentication from the ISP when the connection is established.

Click **Add** to define a new APN profile, and then click **Save** to save the profile. Click **Set default** to set the parameters to their default value. Select one profile and click **Delete** to delete it.



Notes:

You can not edit or delete the current default APN profile.

Router

LAN

Select **Router > LAN**, the LAN parameters are shown in the following figure:

Router-->LAN

LAN DHCP Clients

LAN Interface Setup

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
MAC Address	00:25:5E:F8:FE:64
DHCP Type	Server
DHCP Start IP	192.168.0.100
DHCP End IP	192.168.0.200
DHCP Lease Time	24 hour(s) (1-65535)
UPNP	Disable

Apply Cancel

- **IP Address:** IP address for LAN interface.
 - **Subnet Mask:** Subnet mask for the IP address.
 - **MAC Address:** MAC address for the LAN interface.
 - **DHCP Type:** Define the DHCP type. By default, router is set as DHCP server.
 - **DHCP Start IP:** Allocate start IP address for IP pool.
 - **DHCP End IP:** Allocate end IP address for IP pool. The DHCP End IP address should be larger than the DHCP Start IP address.
 - **DHCP Lease Time:** Define how long the leased IP address will be expired, and will relocate new IP address.
 - **UPNP:** Enable Universal Plug and Play(UPNP) function or not.
- Click **Apply** to confirm your configuration.

DHCP Clients

Select **Router > DHCP Clients**, the DHCP clients parameters are shown in the following figure:

Router-->DHCP Clients

LAN DHCP Clients

DHCP Clients

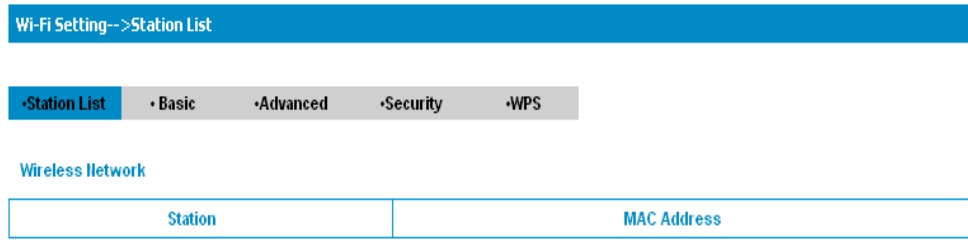
Host Name	MAC Address	IP Address	Expires in
Living	00:1E:90:4A:7C:B1	192.168.0.100	23:28:56

Refresh

Wi-Fi Settings

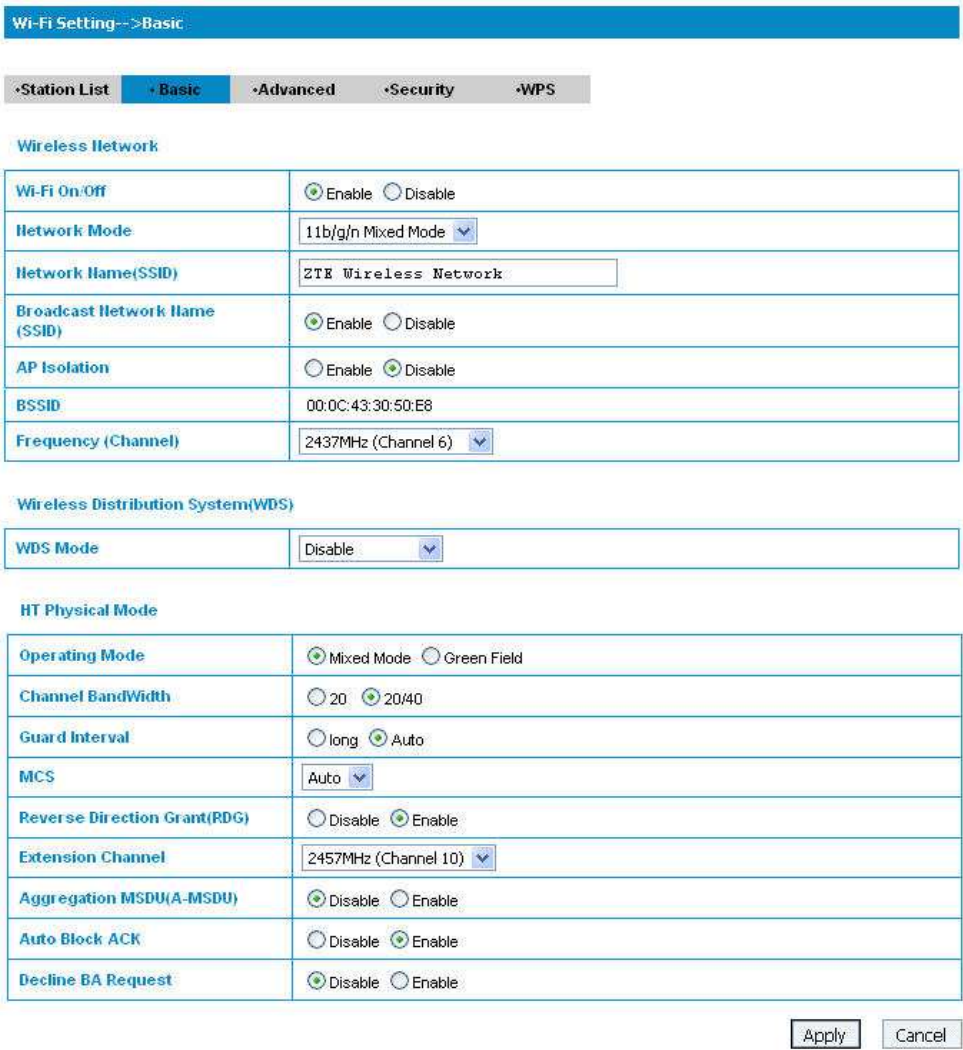
Station list

Select **Wi-Fi Setting > Station List**, the wireless network stations are shown in the following figure:



Basic

Select **Wi-Fi Setting > Basic**, the wireless network basic parameters are shown in the following figure:



- **Wi-Fi On/Off:** Enable Wi-Fi or not.
- **Network Mode:** If all of the wireless devices connect with this router in the same transmission mode, performance will be improved by choosing the appropriate wireless mode.
- **Network Name(SSID):** Service Set Identifier (SSID). Enter a string less than 32 characters as the name for your wireless local area network (WLAN).
- **Broadcast Network Name(SSID):** Disable or Enable (Default) this function. If **Enable** is selected, the router broadcasts the SSID, and other devices can detect and connect to it.

- **AP Isolation:** When **Enabled** is selected, each of your wireless clients will not be able to communicate with each other.
- **BSSID:** MAC address of the Wi-Fi.
- **Frequency(Channel):** Choose the appropriate channel to optimize the performance and coverage of your wireless network.
- **WDS Mode:** WDS enable router to communicate with other APs, WDS connection is two-way communication, APs should know each others wireless MAC address. And make sure that all APs share the same SSID and channel.

WDS configuration is shown below:

Step	Description
1.Set the same SSID and channel for APs	Manually set the SSID and channel is strongly recommended.
2.Select WDS mode: Disable, Lazy Mode, Bridge Mode or Repeater Mode	<p>If you select Disable, WDS is disabled.</p> <p>If you select Lazy Mode, WDS is enabled, and set wireless MAC address only on the peer APs.</p> <p>If you select Bridge Mode, WDS is enabled, and set the peer APs wireless MAC address on router. When you set Bridge Mode, your PC can not search SSID of AP after connected.</p> <p>If you select Repeater Mode, WDS is enabled, and set the peer APs wireless MAC address on router. When you set Repeater Mode, your PC can search SSID of AP after connected.</p>
3.Select Phy mode : CCK,OFDM, HTMIX or GREENFIELD	<p>CCK: 802.11b</p> <p>OFDM: 802.11g</p> <p>HTMIX: 802.11b/g/n Mixed Mode</p> <p>GREENFIELD: 802.11b/g Mixed Mode</p>
4.Select Encryp Type : WEP, TKIP, AES	If you select NONE , all the data transmitted without encryption, and other station can access router.
5.Set peer AP's wireless MAC address on router	Only Repeater Mode and Bridge Mode need this.

The HT physical Mode parameters are shown below:

- **Operating Mode:** In **Mixed Mode**, packets are transmitted with a preamble compatible with the legacy 802.11a/g, the rest of the packet has a new format. In **Green Field**, high throughput packets are transmitted without a legacy compatible part.
- **Channel Bandwidth:** Set the HT physical channel bandwidth.
- **Guard Interval:** Guard interval is to introduce immunity to propagation delays, echoes and reflections, to which digital data is normally very sensitive.
- **MCS:** The Modulation and Coding Scheme (MCS) is a value that determines the modulation, coding and number of spatial channels.
- **Reverse Direction Grant(RDG):** Enable **RDG** or not.
- **Extension Channel:** Set extension channel. Extension channel is also able to send and receive data.
- **Aggregation MSDU(A-MSDU) :**To enable Hyper Throughput TX Aggregate MAC Service Data Unit, select **Enable**.
- **Auto Block ACK:** Select to block ACK (Acknowledge Number) or not during data transferring.

- **Decline BA Request:** Select to reject peer BA-Request or not.

Click **Apply** to confirm your configuration.



Notes:

The maximum number of Wi-Fi users is 5.

Advanced

Select **Wi-Fi Setting > Advanced**, the advanced wireless network parameters are shown in the following figure:

Wi-Fi Setting-->Advanced

•Station List •Basic •Advanced •Security •WPS

Advanced Wireless

Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Short Preamble	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IEEE 802.11H Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable(only in A band)
Country Code	NONE

Wi-Fi Multimedia

WMM Capable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

Cancel

- **Beacon Interval:** The router broadcasts beacon message to announce that it has buffered frames to deliver. The default value is 100 (ms).Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. is recommended.
- **Data Beacon Rate(DTIM):** A Delivery Traffic Indication Message(DTIM) informs next clients to listen to broadcast and multicast messages.
- **Fragment Threshold:** This value should remain at its default value of 2346. If you experience a high packet error rate, you may slightly increase your fragment threshold. Setting the fragment threshold too low may result in poor performance.
- **RTS Threshold:** Request To Send (RTS) threshold should be remained as the value of 2347. If you encounter inconsistent data flow, only minor modifications are recommended.

- **TX Power:** Transmit power should be remained as the value of 100.
- **Short Preamble:** The length of CRC block in the frames during the wireless communication.
- **Shot Slot:** To indicate that 802.11g is using a shot time slot because there is no legacy station(802.11b) present.
- **Tx Burst:** Tx burst allows router to deliver better throughput in the same period and environment in order to increase speed.
- **Pkt_Aggregate:** Increase efficiency by aggregating multiple application packets data into a single transmission frame. In this way, 802.11n networks can send multiple data packets with the fixed overhead cost in just a single frame.
- **IEEE 802.11H Support:** Support IEEE 802.11H or not.

The Wi-Fi multimedia parameters are shown below:

- **WMM Capable:** When multimedia contents are transferred over wireless network, this function enhances data transfer performance.
- **APSD Capable:** Automatic Power Save Delivery (APSD),enable or disable data flow using APSD during transmitting for power saving.

Click **Apply** to confirm your configuration.

Security

Select **Wi-Fi Setting > Security**, the Security parameters are shown in the following figure:

Wi-Fi Setting-->Security

•Station List •Basic •Advanced •Security •WPS

Security Policy

Security Mode	OPEN
Encrypt Type	NO ENCRYPTION

Wireless MAC Filtering

Add MAC Filtering Rule	Wireless Disable
------------------------	------------------

Apply Cancel

Unless one of these encryption modes is selected, wireless transmissions to and from your wireless network can be easily intercepted and interpreted by unauthorized users.

The security modes are described below:

- **Open:** You can authenticate successfully with a SSID, whether it is valid or empty.
- **Shared:** The WLAN clients who have the same WEP key with wireless gateway can pass the authentication and access the wireless network.
- **WEPAUTO:** Select WEP security automatically.
- **WPA-PSK:** WPA Pre-Shared Key, Enter the Pre-Shared key as a plain text (ASCII) pass-phrase of at least 8 characters.
- **WPA2-PSK:** It is the securer version of WPA with implementation of the 802.11i standard.
- **WPA-PSK/WPA2-PSK:** Apply both the WPA-PSK and WPA2-PSK scheme.

If the Authentication type is **Open**, **Shared**, **WEPAUTO**, the bottom part of the configuration page displays parameters as shown.

- **WEP Keys:** At most four keys can be set in the blank. Choose the primary key index. The primary key is

the only key in use at a given time. Whatever keys you enter for an access point, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc. Select **Hex** if use 10 or 26 hexadecimal numbers (0~9, a~f or A~F). Select **ASCII** if use 5 or 13 ASCII characters (case-sensitive).

If the Authentication type is **WPA-PSK** , **WPA2-PSK** or **WPA-PSK/WPA2-PSK** , the bottom part of the configuration page displays WPA parameters.

- **WPA Algorithm:** TKIP, AES or AUTO.
- **Pass phrase:** You can input hexadecimal digits up to 64 characters or input ASCII characters choose a length of 63 characters or less.
- **Key Renewal Interval:** Define how long the key should be renew.

You can set **Wireless MAC Filtering**:

- **Wireless Disable:** If disabled, MAC address is not used to control network access.
- **Wireless Allow:** Set the MAC address that is allowed to access network.
- **Wireless Reject:** Set the MAC address that is not allowed to access network.

Click **Apply** to confirm your configuration.

WPS

Select **Wi-Fi Setting** > **WPS**, the WPS configuration is shown in the following figure:



Select **Enable**,click **Apply** ,the WPS settings are shown in the following figure:



WPS Summary, WPS Progress and WPS Status are all shown in the figure.

To set WPS, select WPS mode, the two modes are described below:

- **PIN**: There are two ways to use PIN mode, one is set PIN code on the client's wireless adapter(you can find the PIN code in **AP PIN** field of **WPS Summary**), the other way is set the client's PIN code in **Client PIN** field.
- **PBC**: Press the WPS button of the router or select PBC, and then click **Apply**. Press WPS button on the client wireless adapter within two minutes, and the negotiation process will be established.

Firewall

You may setup firewall rules to protect your network from virus, worm and malicious activity on the Internet.

NOTE
Notes:

You can set the maximum 10 filtering items for **MAC/IP/Port Filtering** and **URL Filtering**.

MAC/IP/Port Filtering

Select **Firewall > Mac/Ip/Port Filtering**, the Mac/IP/Port Filtering is shown in the following figure:

Firewall-->Mac/Ip/Port Filtering

• Mac/Ip/Port Filtering • URL Filtering • Port Forwarding • DMZ • System Security

Basic Settings

MAC/Ip/Port Filtering Disable ▾

Apply

If you select **Enable**, the filter settings will appear:

Firewall-->Mac/Ip/Port Filtering

• Mac/Ip/Port Filtering • URL Filtering • Port Forwarding • DMZ • System Security

Basic Settings

MAC/Ip/Port Filtering Enable ▾

Default Policy -- The packet that doesn't match with any rules would be: Dropped ▾

Apply

MAC/Ip/Port Filtering

MAC address	<input type="text"/> (XX:XX:XX:XX:XX:XX, eg:00:1E:90:FF:FF:FF)
Dest IP Address	<input type="text"/> (XXX.XXX.XXX.XXX, eg:192.168.5.101)
Source IP Address	<input type="text"/>
Protocol	None ▾
Dest Port Range	<input type="text"/> - <input type="text"/> (1~65535)
Source Port Range	<input type="text"/> - <input type="text"/>
Action	Accept ▾
Comment	<input type="text"/>

The maximum rule count is 10.

Apply Reset

Current MAC/Ip/Port filtering rules in system:

No.	MAC address	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment
Others would be dropped								

Delete Reset

• **Default Policy:** Set how to handle the packet if none of the rules matches.

- **MAC address:** Set the MAC address that will be filtered.
- **Dest IP Address:** Set the destination IP address that will be filtered.
- **Source IP Address:** Set the source IP address that will be filtered.
- **Protocol:** Set which protocol will be used for filtering.
- **Dest Port Range:** Set the destination port numbers that will be filtered
- **Source Port Range:** Set the source port numbers that will be filtered.
- **Action:** Set how to handle the packet if it matches with the rule.
- **Comment:** type comment for the filter settings.

Click **Apply** to confirm your configuration.

URL Filtering

You can setup content filter to restrict the improper content access. Select **Firewall > URL Filtering**, the URL Filtering is shown in the following figure:

The screenshot shows the 'URL Filtering' configuration page. At the top, there is a breadcrumb 'Firewall-->URL Filtering'. Below it is a navigation menu with options: 'Mac Ip/Port Filtering', 'URL Filtering' (selected), 'Port Forwarding', 'DMZ', and 'System Security'. The main content area is titled 'Current URL Filtering:' and contains a table with two columns: 'No.' and 'URL'. Below the table are 'Delete' and 'Reset' buttons. Underneath is the 'Add a URL filter:' section, which has a 'URL:' input field and a smaller input field for a comment (example: 'www.zte.com'). Below this is the text 'The maximum rule count is 10.' and 'Add' and 'Reset' buttons.

Type URL address, and then click **Add** to add the URL address into the filtering list. The new URL filtering item will be shown in the **Current Webs URL Filters:** field.

Port Forwarding

You can setup virtual servers to provide services on the Internet. Select **Firewall > Port Forwarding**, the virtual server settings is shown in the following figure:

The screenshot shows the 'Port Forwarding' configuration page. At the top, there is a breadcrumb 'Firewall-->Port Forwarding'. Below it is a navigation menu with options: 'Mac Ip/Port Filtering', 'URL Filtering', 'Port Forwarding' (selected), 'DMZ', and 'System Security'. The main content area is titled 'Virtual Server Settings' and contains a 'Virtual Server Settings' input field with a dropdown menu set to 'Disable'. Below this is an 'Apply' button.

If you select **Enable**, the Virtual Server Settings will appear:

Firewall-->Port Forwarding

- Mac/Ip/Port Filtering
- URL Filtering
- Port Forwarding
- DMZ
- System Security

Virtual Server Settings

Virtual Server Settings	Enable ▾
IP Address	<input type="text"/> (XXX.XXX.XXX.XXX, eg:192.168.5.101)
Port Range	<input type="text"/> - <input type="text"/> (1~65535)
Protocol	TCP&UDP ▾
Comment	<input type="text"/>

The maximum rule count is 10.

Apply

Current Virtual Servers in system:

No.	IP Address	Port Range	Protocol	Comment

Delete Reset

- **IP Address:** Set IP address for the virtual server.
- **Port Range:** Set port numbers for the virtual server.
- **Protocol:** Set protocol for the virtual server.
- **Comment:** Type comment for the virtual server settings.

Click **Apply** to confirm your configuration.

DMZ

You can setup a De-militarized Zone(DMZ) to separate internal network with the Internet. Select **Firewall > DMZ**, the DMZ setting is shown in the following figure:

Firewall-->DMZ

- Mac/Ip/Port Filtering
- URL Filtering
- Port Forwarding
- DMZ
- System Security

DMZ Settings

DMZ Settings	Disable ▾
--------------	-----------

Apply

If you select **Enable**, set the **DMZ IP Address**, and then click **Apply** to confirm your configuration.

Firewall-->DMZ

- Mac/Ip/Port Filtering
- URL Filtering
- Port Forwarding
- DMZ
- System Security

DMZ Settings

DMZ Settings	Enable ▾
DMZ IP Address	<input type="text"/> (XXX.XXX.XXX.XXX, eg:192.168.5.101)

Apply

System Security

You can configure system firewall to protect AP or router from being attacking. Select **Firewall > System Security**, the system security setting is shown in the following figure:

Firewall-->System Security

• Mac Ip/Port Filtering • URL Filtering • Port Forwarding • DMZ • **System Security**

Remote management
 Remote management (via WAN)

Ping from WAN
 Ping from WAN

Allow or **Deny** the remote management function and **Enable** or **Disable** ping from WAN filter on requirement, and then click **Apply**.

SMS

New Message

Select **SMS > New Message** to enter into New Message Interface.

SMS-->NEW Message

• **NEW Message** • Inbox • Outbox • Drafts

NEW Message

TO	<input type="text"/>
Content	<input style="height: 40px;" type="text"/>

Edit the new message. Click **Send** to send the message. Click **Save** to save the message to Drafts.

Inbox

Select **SMS > Inbox** to enter into Inbox Interface.

SMS-->Inbox

• NEW Message • **Inbox** • Outbox • Drafts

Inbox SMS Storage Status56/60

No	PhoneNumber	Date/Time	Status	Operations
1	95555	2010-01-11 16:16:27	Unread	<input checked="" type="radio"/>
2	95555	2010-08-10 13:05:45	Unread	<input type="radio"/>
3	10658309	2010-08-20 09:55:50	Unread	<input type="radio"/>
4	+8613371626172	2010-08-03 15:37:46	Unread	<input type="radio"/>

You can make the following operation: **View/Delete/Reply/Forward/Delete All**.

Outbox

Select **SMS > Outbox** to enter into Outbox Interface.

SMS-->Outbox

•NEW Message •Inbox •Outbox •Drafts

Outbox SMS Storage Status

No	Phonenumber	Content	Operations
1	1330000000		○

View Send Delete Forward Delete All

You can make the following operation: **View/Send/Delete/Forward/Delete All**.

Drafts

Select SMS > **Drafts** to enter into Drafts Interface.

SMS-->Drafts

•NEW Message •Inbox •Outbox •Drafts

Drafts SMS Storage Status59/60

No	Phonenumber	Content	Operations
1	133000000	Hi	⊙

View Send Delete Forward Delete All

You can make the following operation: **View/Send/Delete/Forward/Delete All**.

Advanced

Status

Select **Advanced** > **Status**, the system information is shown in the following figure:

Advanced-->Status

•Status •Statistics •Management •Upgrade •Restore •Reboot •PIII Manage

System Info

IMEI	0000000000000000
Wireless access module software version	BD_P678A1_GWV1.0.0B04
Control and route module software version	CR_MF23V1.0.0B02
Hardware version	PCBMF23V1.0.0
System Up Time	27 mins, 5 secs

Statistics

Select **Advanced** > **Statistics**, the system statistics information is shown in the following figure:

Advanced-->Statistics

•Status •Statistics •Management •Upgrade •Restore •Reboot •PIII Manage

Data

Data send	0 KB
Data rcv	0 KB

Management

Select **Advanced > Management**, the administrator settings information is shown in the following figure:

Advanced-->Management

•Status •Statistics •Management •Upgrade •Restore •Reboot •PIH Manage

Administrator Settings

Account	<input type="text" value="admin"/>
Password	<input type="password"/>
New Password	<input type="password"/>
Confirm New Password	<input type="password"/>

User Settings

Account	<input type="text" value="zte"/>
Password	<input type="password"/>
New Account	<input type="text"/>
New Password	<input type="password"/>
Confirm New Password	<input type="password"/>

To set new account, type new account and password, and then click **Apply** to confirm your configuration.

Upgrade

Select **Advanced > Upgrade** to upgrade the software version of the router.

Advanced-->Upgrade

•Status •Statistics •Management •Upgrade •Restore •Reboot •PIH Manage

Update Firmware

Location:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upgrade"/>
-----------	----------------------	--	--

Click **Browse...**, locate the latest software version, and then click **Upgrade**.



Notes:

Do not upgrade software unless necessary. Wrongly upgrade action may cause router malfunction or can not work.

Restore

Select **Advanced > Restore**, click **Restore** to set all the settings to their factory default values, and the device will be turned off.

Advanced-->Restore

•Status •Statistics •Management •Upgrade •Restore •Reboot •PIH Manage

Load Factory Defaults

Load Default Button	<input type="button" value="Restore"/>
---------------------	--

Reboot

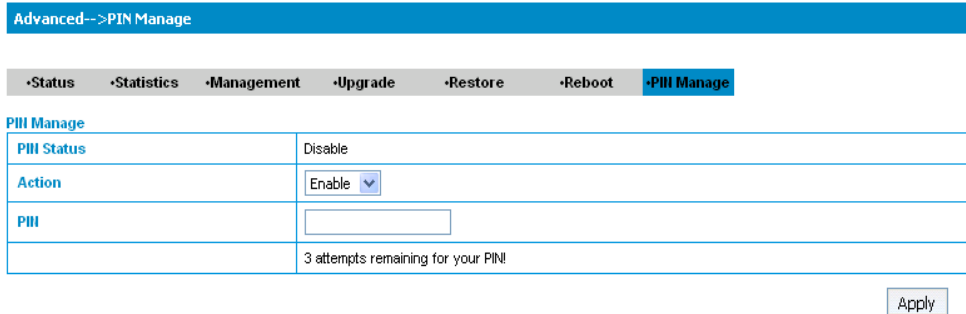
Select **Advanced > Reboot** link to access the following screen:



You can reboot the Home Gateway by webUI remotely, if the Gateway is not around you.

PIN Manage

Select **Advanced > PIN Manage**, the PIN manage is shown in the following figure:



If you select **Modify**, the modification parameters are shown in the following figure:

Type the old PIN code, and then type two times the new PIN code. Click **Apply** to confirm your configuration.



Notes:

Three time consecutive wrong PIN code entries will lock the (U)SIM card.

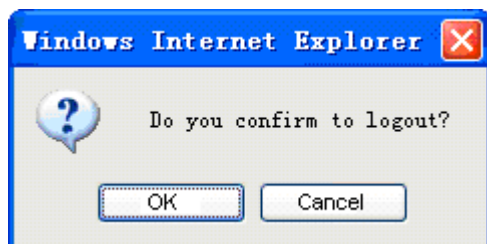
Disconnecting from the Internet

If you want to terminate your Internet connection, you can select **Disconnect Internet** from **WAN Connection** page, and click **Apply**.

Turn off the router can also terminate Internet connection.

Logout

Select **Logout**, a pop-up windows will appear as shown in the following figure :



Click **OK** to logout the router.

Chapter 5

Troubleshooting

- Make sure that the router is turned on and all the cables are connected correctly.
- Check the RSSI, PPP and PWR LED's are lit and NOT in a blinking state or off.

Voice Related Problems

Symptoms	Possible Problems/ Solutions
No Dial Tone.	Please wait for 1~2 minutes after the router is turned on. If 3G LED light is blinking, you have no good RF reception. Change the location of the router.
There is a prompt/ phone alert/ announcement as soon as I lift the phone off the hook.	Make sure your (U)SIM card is inserted correctly and the PIN number has been entered. If the PIN number has been entered incorrectly then you will need to enter the PUK code when prompted.
The line is noisy/ distorted when I lift the phone off the hook.	Remove any electrical appliance which is too close to the phone or router. The cable or phone set might be faulty.
I hear a rapid engaged tone as soon as I lift the phone off the hook.	Put the phone on hook and try again. If you are connected to the internet using the 2G (GSM) network, please disconnect this first.
After dialing the last digit I hear nothing /silence.	When you have finished dialing you can press the # key or wait 4-8 seconds to connect the call.
I can't make or receive a call when I am surfing on the net.	If you are connected using the 2G (GSM) network then you cannot surf the net and make a phone call simultaneously. Please disconnect the internet and wait 30 seconds to 1 minute before making a call.

Internet Related Problems

Symptoms	Possible Problems/ Solutions
I cannot access the internet at all.	Please check your configuration settings. Please wait 1~ 2 minutes for the router to initialize. Check your service indicator LED's.
The download or upload speeds are very slow.	The speed is dependent on signal strength. Check your signal strength and network type.

Others

Symptoms	Possible Problems/ Solutions
The RSSI signal indicator is always blinking or does not light.	This indicates poor reception. Try moving the router to another location near the window.

Chapter 6

Technical Parameters

Network & Frequency Band

EDGE/GPRS/GSM: 850/900/1800/1900MHz

HSUPA/HSDPA/UMTS: 850/1900/2100MHz

Power Adapter

Input: 100V~240V(AC), 50/60Hz

Output:+12V (DC), 700mA Max

Data Service

HSUPA 2Mbps UL

HSDPA 7.2Mbps DL

Dimensions (W×H×D)

138mm×102mm×27mm

Weight

About 400g

Chapter 7

Glossary

- AC: Alternating Current
- APN: Access Point Name
- DC: Direct Current
- DHCP: Dynamic Host Control Protocol
- DNS: Domain Name System (or Service or Server)
- DoS: Denial of Service
- EDGE: Enhanced Data GSM Evolution
- ESSID: Expanded Service Set Identifier
- Ethernet: A frame-based computer networking technology for local area networks (LANs)
- GSM: Global System for Mobile Communications
- GPRS: General Packet Radio Service
- HSDPA: High Speed Downlink Packet Access
- HSUPA: High Speed Uplink Packet Access
- IP: Internet Protocol
- LAN: Local Area Network
- LED: Light - emitting Diode
- MHz: Megahertz
- MTU: Maximum Transmission Unit
- PDP: Packet Data Protocol
- PIN: Personal Identification Number
- PPP: Point to Point Protocol
- PSTN: Public Switched Telephony Network
- PUK: PIN Unlocking Key
- RSSI: Radio Signal Strength Indicator
- RF: Radio Frequency
- SIP: Session Initiated Protocol
- UPnP: Universal Plug and Play
- (U)SIM: Subscriber Identification Module
- WCDMA: Wideband CDMA (Code-Division Multiple Access)
- WEP: Wired Equivalent Privacy
- WLAN: Wireless LAN
- WPA-PSK: Wi-Fi Protected Access–PreShared Key