

ZTE IX256

WiMAX MODEM

User Manual

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

There may be possibility of inconformity between the manual and new publishing documents, we promise a timely update. No prior notification for the updated materials but transfer into update version.

Copyright © 2010 by ZTE Corporation

All rights reserved.

TABLE OF CONTENTS

1	General	5
1.1	Welcome	5
1.2	Safety Precautions	5
1.3	Cleaning and Maintaining	6
1.4	Limited Warranty	6
1.5	Limitation of Liability	7
1.6	FCC Declaration	7
1.7	RF Declaration	7
2	Getting Started	9
2.1	Appearance	9
2.2	Parts Supplied	9
2.3	LED Indicator	10
2.4	Working Condition	11
2.5	Technical Parameters	11
2.6	Ports	12
3	Connecting MODEM	13
3.1	Application Structure	13
3.2	Hardware Installation	13
3.2.1	Connect to LAN	13
3.2.2	Connect to Phone	14
3.2.3	Connect Power Adapter	14
3.2.4	Power on MODEM	14
4	Preparation for Configuring MODEM	15
4.1	TCP/IP Installation and Configuration	15

4.2	Checking	16
4.2.1	Check LAN Connection	16
4.2.2	Cancel Proxy Server in Browser	17
4.2.3	Others	17
5	Ordinary Operation	18
5.1	Login	18
5.2	Router State	19
5.3	WAN Connection	21
5.3.1	WiMAX Connection	21
5.3.2	WiMAX Information	22
5.4	WIMAX Settings	23
5.4.1	Channel Settings	23
5.4.2	WiMAX Authentication	25
5.5	Router	27
5.5.1	LAN	27
5.5.2	DHCP Clients	29
5.6	Wi-Fi Settings	29
5.6.1	Station List	29
5.6.2	Basic	30
5.6.3	Advanced	33
5.6.4	Security	35
5.6.5	WPS	38
5.7	Firewall	40
5.7.1	Mac/Ip/Port Filtering	40
5.7.2	URL Filter	42

5.7.3	Time Filtering	43
5.7.4	Port Forwarding	44
5.7.5	DMZ	45
5.7.6	System Security	46
5.7.7	Advanced Settings	46
5.8	VPN	47
5.9	VoIP	48
5.9.1	User Details	48
5.9.2	Advanced	50
5.9.3	Supplementary	51
5.10	Advanced	52
5.10.1	Status	52
5.10.2	Statistics	52
5.10.3	Management	53
5.10.4	Time	54
5.10.5	Upgrade	55
5.10.6	Remote Upgrade	56
5.10.7	Restore	57
5.10.8	Reboot	57
5.10.9	DDNS Settings	57
5.10.10	System Log	58
5.11	Logout	59
6	Troubleshooting	60
7	Appendix Glossary	62

1 General

1.1 Welcome

Thanks for choosing the ZTE IX256 WiMAX MODEM (hereinafter referred to as “MODEM”). To get the most from your MODEM and to keep it in the best condition, please read this manual carefully.

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

1.2 Safety Precautions

Some electronic devices may be susceptible to electromagnetic interference. Locate the MODEM away from TV set, radio and other electronic equipment to avoid electromagnetic interference.

The MODEM may interfere with medical devices like hearing aids and pacemakers. Consult with a physician or the manufacturer of the medical device before using the MODEM.

Do not use your MODEM in dangerous environments such as oil or chemical factories where there are explosive gases or explosive products being processed.

Please use original accessories or accessories that are authorized by your Equipment Provider. Unauthorized accessories may affect the MODEM performance, damage the MODEM or cause danger to you.

Do not attempt to dismantle the MODEM. There are no user serviceable parts.

Do not immerse the MODEM in any liquid.

Do not place objects on top of the MODEM. This may lead to overheating of the device.

The MODEM must be placed in ventilation environment for use.

Do not expose the MODEM to direct sunlight or store it in hot areas. High temperature can shorten the life of electronic devices.

Do not touch the antenna while calling.

Do not allow children to play with the MODEM or charger.

Keep the length of the cable between the MODEM and the phone less than 33 feet.

The MODEM is for indoor use only. Do not use the MODEM outside. Do not connect telephone extensions which run outside of the building. These can result in lightning damage to your unit.

This device cannot be used with handheld PDA (personal digital assistants).

1.3 Cleaning and Maintaining

Use an antistatic cloth to clean the MODEM. Do not use chemical or abrasive cleanser as these could damage the plastic case. Turn off your MODEM before you clean it.

Do not use your MODEM during a thunderstorm. Remove the mains power pack from the wall socket.

Please do not touch the antenna with your hand during conversation. Covering the antenna may affect call quality, may cause the MODEM to operate at higher power level than needed.

1.4 Limited Warranty

This warranty does not apply to defects or errors in the Product caused by:

- (a) Reasonable MODEM Appearance Disfiguration.
- (b) End User's failure to follow ZTE's installation, operation or maintenance instructions or procedures.
- (c) End User's mishandling, misuse, negligence, or improper installation, disassemble, storage, servicing or operation of the Product.
- (d) Modifications or repairs not made by ZTE or a ZTE-certified individual.
- (e) Power failures, surges, fire, flood, accident, actions of third parties or other events outside ZTE's reasonable control.
- (f) Usage of products of third Parties, or usage in conjunction with third party products provided that such defects is due to the combined usage.
- (g) 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.

1.5 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.

1.6 FCC Declaration

We, ZTE Corporation, declared that:

The user is cautioned that changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the condition that this device does not cause harmful interference.

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 instructions, 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 the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/ TV technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

AMC Not supported.

BSCM250 does not support UL beamforming.

1.7 RF Declaration

Radio Frequency (RF) Energy

The device contains a transmitter and a receiver. When it is ON, it receives and transmits RF energy. When you communicate with your device, the system handling your connection controls the power level at which your device transmits.

Important safety information regarding radiofrequency radiation (RF) exposure. To ensure compliance with RF exposure guidelines the device must be used with a separation from the body. Failure to observe these instructions could result in your RF exposure exceeding the relevant guideline limits.

The transmitter is using external antenna that operate at 20cm or more from nearby persons. can be found under the Display Grant section of www.fcc.gov/oet/ea/fccid after searching on **FCC ID: Q78-ZTEIX256**.

2 Getting Started

2.1 Appearance



Figure 1 Front Panel

2.2 Parts Supplied

Parts	Quantity
MODEM	1
Power adapter	1
RJ-45 10/100 BaseT Ethernet cable	1
User Manual	1

Please contact with your provider as soon as possible if the parts have any damage or lost. If replacing product, please preserve the packing box and parts of the product.

2.3 LED Indicator

There are total six LEDs for the MODEM, detailed description as following table.



LED	Status	Description
1,2,3 WiMAX CINR	1,2,3 Leds On	Signals is strong: $CINR \geq 27$
	1,2 Leds On, 3 Led Off	Signals is medium: $13 \leq CINR \leq 27$
	1 Led On, 2,3 Leds Off	Signals is weak: $9 \leq CINR \leq 13$
	1,2,3 Leds Off	No Signal, $CINR < 9$
4 VoIP/FoIP Status	1 Led blinking	Connecting to WiMAX network
	Off	Hook on/Out of Service
	Blinking	Registering VoIP/FoIP service
5 WiFi Status	On	Registered VoIP/FoIP service
	Off	WiFi Off
	Blinking	WiFi On and data is transmitting
6 Power	On	WiFi On
	ON	Power Supply
	Off	Power Supply Failure

2.4 Working Condition

Working Condition for Host

Working temperature: 0°C ~ +55°C [32 °F ~ 131 °F]

Working humidity: 10% ~ 85%

Storage temperature: -40°C ~ +70°C [-40 °F ~ 158 °F]

Storage humidity: 5% ~ 95%

2.5 Technical Parameters

Mode of Access	WiMAX (Worldwide Interoperability for Microwave Access)
WiMAX Protocol	802.16e(IEEE 802.16-2005)
WiFi protocol	IEEE 802.11b/g/n
WiMAX Frequency Range	2496MHz~2690MHz
WiFi Frequency Range	2400MHz~2483.5MHz
Dimensions (W×H×D)	201.7mm*155.7mm*54.8mm
Weight	About 511 g

Please refer to the real objects for the related parameters about the charger.

2.6 Ports



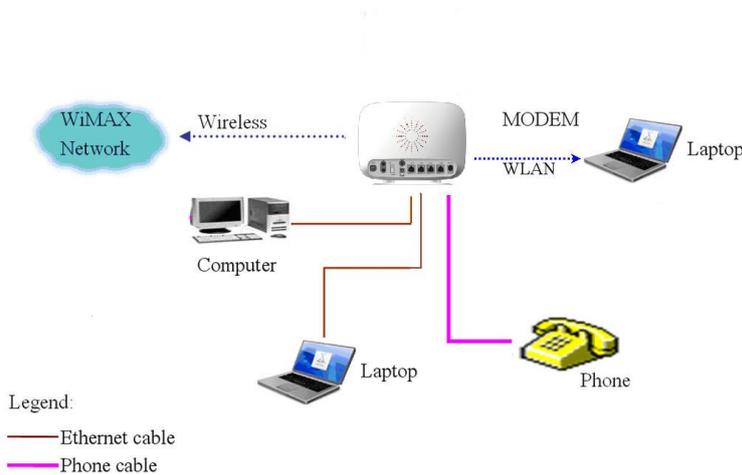
All ports are in back panel.

Port Indicator	Description
DC 12V 	External power socket
LAN1,LAN2,LAN3,LAN4	LAN port
PHONE	Phone port
Reset	Reset button
WPS	WPS button is used to start WiFi Protected Setup authentication process.
ON/OFF	WLAN button
ANT	Antenna connector

3 Connecting MODEM

3.1 Application Structure

Network connection is shown as follows:



3.2 Hardware Installation

Make sure that your MODEM is powered off.

You can turn on/off modem by connecting/disconnecting power cable.

3.2.1 Connect to LAN

1. Connect to LAN via Network Cable

2. Plug one end of an Ethernet network cable into LAN ports on the back of the MODEM, and plug the other end into an Ethernet port on a network device, for example, PCs or other network devices. The Ethernet cable can be crossover or straight.

3. Connect to LAN via WiFi

4. Enable the WiFi function and make sure that your PC has been installed wireless network card, and then use your PC to search for the SSID of MODEM to connect with it.

Note:

Don't insert phone cable into LAN ports.

3.2.2 Connect to Phone

Connect phone cable to **PHONE** port of MODEM.

3.2.3 Connect Power Adapter

Connect the included power adapter to the MODEM power port, and then plug the power adapter into an electrical outlet. The Power LED on the front panel will light up when the adapter is connected properly.

Note:

Make sure you use the power adapter that is supplied with the MODEM. Use of a different power adapter could damage the MODEM.

3.2.4 Power on MODEM

Turn on the modem.

4 Preparation for Configuring MODEM

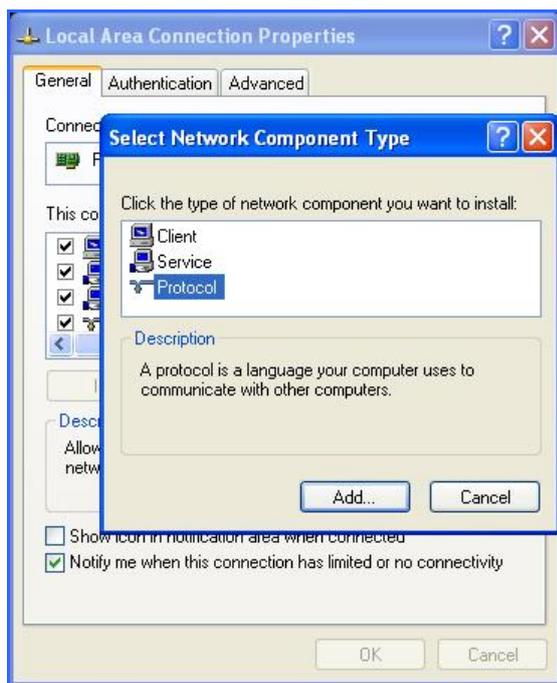
Usually, MODEM has been configured by service provider and you can use it directly. But in some instance, you need configure MODEM by yourself.

4.1 TCP/IP Installation and Configuration

Installation

If TCP/IP protocol is not installed, please install it first. Please refer to installation steps in Windows XP as follows (For classic start menu):

1. Select **Start** → **Settings** → **Control Panel** → **Network Connections**.
2. Double-click <**Local Area Connection**> and click <**Properties**>.
3. Click <**Install...**> and double-click <**Protocol**>.

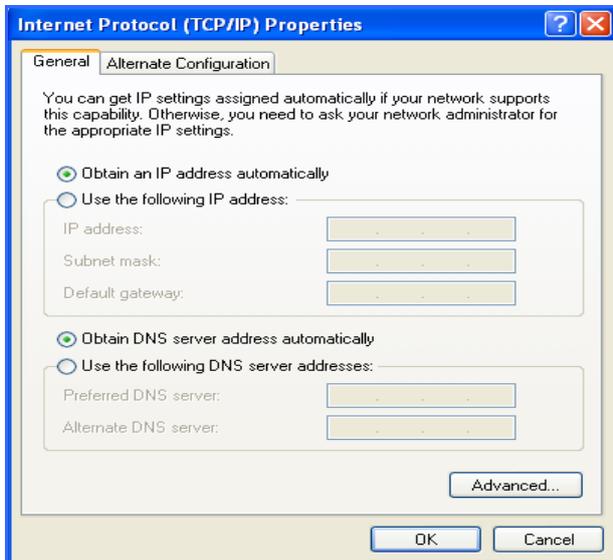


4. Select <**Internet Protocol (TCP/IP)**> and click <**OK**>.

Configuration (For classic start menu)

1. Click <**Start**> and select <**Settings**>, then click <**Network Connections**>.
2. Double-click <**Local Area Connection**> and click <**Properties**>.

3. Double-click **<Internet Protocol (TCP/IP)>** and select **<Obtain an IP address automatically>**, **<Obtain DNS server address automatically>**.



Note:

If the service provider provides DNS IP address, please select **<Use the following DNS server addresses>** and enter the specified IP address.

4.2 Checking

4.2.1 Check LAN Connection

1. Click **<Start>** and **<Run>**. In the *Open* field, enter **command**. Press the **Enter** key or click the **<OK>** button. In the command prompt, type **ping 192.168.0.1** and press the **Enter** key.

2. If you get a reply as follows, the LAN connection is ok.

```
C:\Documents and Settings\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
```

3. If you get a reply as follows, please check the LAN and TCP/IP configuration Refer to chapter 3.2 and chapter 4.1 in detail.

```
C:\Documents and Settings\Administrator>ping 192.168.0.1

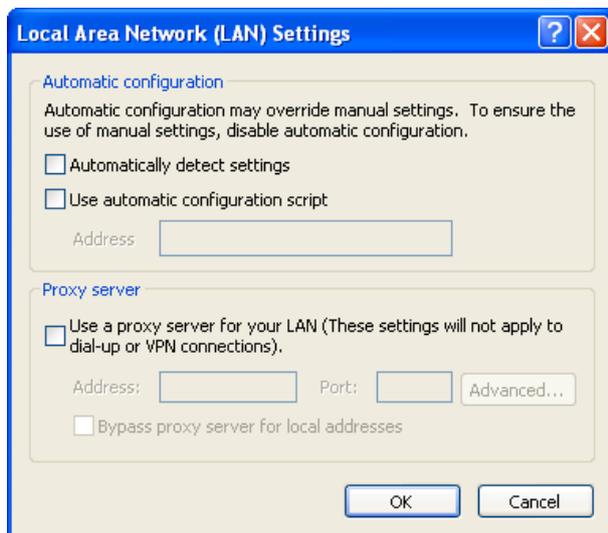
Pinging 192.168.0.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

4.2.2 Cancel Proxy Server in Browser

For classic start menu:

1. Select **Start** → **Settings** → **Control Panel** → **Internet Options**.
2. Select **<Connections>**.
3. Click the **<LAN Settings>** button and remove anything that is checked.



4. Click the **<Cancel>** button to go back to the previous screen.
5. Click the **<OK>** button to confirm canceling proxy server in browser.

4.2.3 Others

Sometimes you also need several parameters, please ask your service provider in detail.

5 Ordinary Operation

5.1 Login

To access the Web-based Utility of the MODEM, launch Internet Explorer and enter the MODEM's default IP address (192.168.0.1) in the address field, then press the **Enter** key. A screen will appear asking you for your **User Name** and **Password** (detail as following picture). Enter **admin** in the Username field and **admin** in the Password field. Then click the **<login>** button.

Welcome to ZTE IX256

goahead
WEB SERVER™

User Name :

Password :

Save

©1998-2010 ZTE Corporation. All rights reserved

Note: If you select **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>**.

When you access the MODEM setup page, the first screen you see as following:



The whole interface is divided into two parts, and related functions can be executed by operation in the related areas.

- **Index area:** Show configuration list for your router.
- **Content area:** Show the detail configuration.

5.2 Router State

After access MODEM setup page successfully, please click **Router State** link to access the following screen:

WiMAX Information

Network Provider	Unknown
Network Type	WiMAX

WAN Information

WiMAX Status	Connected
IP Address	10.12.1.11
Primary DNS	61.134.1.4
Secondary DNS	10.128.1.9

WLAN Current Status

SSID	ZTE Wireless Network
Channel	6
Security Level	Disable

LAN and WLAN Information

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.1
DHCP Server	Enable

WiMAX Information

- **Network Provider:** Network provider information.
- **Network Type:** The type of network.

WAN Information

- **WiMAX Status:** WiMAX network information
- **IP Address:** IP address for WAN connection. It is same IP address as the WiMAX address.
- **Primary DNS:** Primary DNS address.
- **Secondary DNS:** Secondary DNS address.

WLAN Current Status

- **SSID:** Service Set Identifier

- **Channel:** Channel information.
- **Security Level:** Security level of the router

LAN and WLAN Information

- **IP Address:** IP address for WAN connection. It is the same IP address as the WiMAX IP Address
- **Subnet Mask:** The subnet mask address
- **Default Gateway:** Default gateway.
- **DHCP Server:** DHCP server information.

5.3 WAN Connection

5.3.1 WiMAX Connection

After access MODEM setup page successfully, please click **WAN Connection** → **WiMAX Connection** link to access the following screen:

WAN Connection-->WiMAX Connection	
• WiMAX Connection	- WiMAX Information
WAN Status	Connected
WAN IP Address	10.12.1.11
WAN Netmask	255.255.255.255
WAN Gateway	10.12.1.11
Primary DNS	61.134.1.4
Secondary DNS	10.128.1.9

disconnect

- **WAN Status:** Wan current status
- **WAN IP Address:** IP address for WAN connection. It is the same IP address as the WiMAX IP Address

- **WAN Netmask:** Net mask assigned by DHCP server
- **WAN Gateway:** Gateway IP address
- **Primary DNS:** Primary DNS address
- **Secondary DNS:** Second DNS address

5.3.2 WiMAX Information

After access MODEM setup page successfully, please click **WAN Connection** → **WiMAX Information** link to access the following screen:

WAN Connection-->WiMAX Information	
• WiMAX Connection	• WiMAX Information
WAN IP Address	0.0.0.0
BSID	000457100001
Cell ID	57005
Frequency	2510000KHz
Tx Bytes	0
Rx Bytes	0
Connection Status	Ranging
Connection Duration	0 day 0 hour 0 minute
Connection RSSI	-90dBm
TX Power	26dBm
PER	0.010000
CIIR	6

WiMAX Information use to view WiMAX network information.

- **WAN IP address:** IP address for WAN connection. It is the same IP address as the WiMAX IP Address
- **BSID:** Base Station ID of the MODEM connected
- **Cell ID:** Cell ID of the MODEM connected

- **Frequency:** Frequency information
- **Tx Bytes:** Transmission flow statistic
- **Rx Bytes:** Receiver flow statistic
- **Connection Status:** Current connection status
- **Connection Duration:** Duration of time for connection
- **Connection RSSI:** Receive signal strength indicator
- **Tx Power:** Transmission power
- **PER:** Packet error ratio
- **CINR:** Carrier to interference and noise ratio

5.4 WIMAX Settings

5.4.1 Channel Settings

After access MODEM setup page successfully, please click **WiMAX Settings** → **Channel Settings** link to access the following screen:

WiMAX Settings-->Channel Settings

• Channel
Settings

• WiMAX
Authentication

WiMAX Bandwidths

Bandwidths	<input type="checkbox"/> 5M	<input type="checkbox"/> 7M	<input type="checkbox"/> 8.75M	<input checked="" type="checkbox"/> 10M
------------	-----------------------------	-----------------------------	--------------------------------	---

Center Frequencies

Search Mode	Frequency List <input type="button" value="v"/>
-------------	---

Frequency List Settings

Channel	Frequency(KHz)
1	<input type="text" value="2510000"/>
2	<input type="text" value="0"/>
3	<input type="text" value="0"/>
4	<input type="text" value="0"/>
5	<input type="text" value="0"/>
6	<input type="text" value="0"/>
7	<input type="text" value="0"/>
8	<input type="text" value="0"/>
9	<input type="text" value="0"/>
10	<input type="text" value="0"/>

Apply

- **Bandwidths:** Bandwidth lists can be selected.
- **Search Mode:** Select Frequency List or Frequency Band.
- **Channel:** Channel ID.
- **Frequency:** Frequency of the channel.

After finish the configuration, click <**Apply**> button to take effect.

5.4.2 WiMAX Authentication

After access MODEM setup page successfully, please click **WiMAX Settings** → **WiMAX Authentication** link to access the following screen:

1. EAP-MD5

WiMAX Settings-->WiMAX Authentication

• Channel Settings • WiMAX Authentication

Authentication Select	<input type="text" value="EAP-MD5"/>
Default Identity	<input type="text"/>
Default Password	<input type="password"/>
Re-enter To Confirm	<input type="password"/>
Anonymous Identity	<input type="text"/>

- **Default Identity:** Default Identity for EAP-MD5
- **Default Password:** Default Password for EAP-MD5
- **Re-enter To Confirm:** Enter user authentication password once again.
- **Anonymous Identity:** Anonymous identity for EAP-MD5

After finishing the related configuration, click <**Apply**> button to take effect.

2. EAP-TLS

WiMAX Settings-->WiMAX Authentication

• Channel Settings	• WiMAX Authentication
Authentication Select	EAP-TLS
Default Identity	<input type="text"/>
Device Private Key Password	••••••••••
Re-enter To Confirm	••••••••••

WiMAX Certificate Update

Device Private Key File	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="update"/>
Device Certificate File	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="update"/>
CA Certificate File	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="update"/>

- **Default Identity:** Default Identity for EAP-TLS
- **Device Private Key Password:** Device Private Key Password for EAP-TLS
- **Re-enter to Confirm:** Enter user authentication password once again.
- After finishing the above configuration, click **<Apply>** button to take effect.
- **Device Private Key File :** Click **<Browse...>** button to select device private key file in local disk, then click **<Update>** button to upload
- **Device Certificate File:** Click **<Browse...>** button to select device certificate file in local disk, then click **<Update>** button to upload
- **CA Certificate File:** Click **<Browse...>** button to select CA certificate file in local disk, then click **<Update>** button to upload

3. EAP-TTLS/MSCHAPv2

WiMAX Settings-->WiMAX Authentication

• Channel Settings • **WiMAX Authentication**

Authentication Select	EAP-TTLS/MSCHAPv2
Default Identity	<input type="text"/>
Default Password	••••••••••••••••
Re-enter To Confirm	••••••••~••••••••
Anonymous Identity	<input type="text"/>

Apply

WiMAX Certificate Update

CA Certificate File	<input type="text"/> Browse... update
---------------------	--

- **Default Identity:** default identity for EAP-TTLS/MSCHAPv2
- **Default Password:** default password for EAP-TTLS/MSCHAPv2
- **Re-enter to Confirm:** Enter user authentication password once again
- **Anonymous Identity:** anonymous identity for EAP-TTLS/MSCHAPv2
- After finishing the above configuration, click **<Apply>** button to take effect.
- **CA Certificate File:** Click **<Browse...>** button to select CA certificate file in local disk, then click **<Update>** button to upload

5.5 Router

5.5.1 LAN

After access MODEM setup page successfully, please click **Router** → **LAN** link to access the following screen:

LAN Interface Setup

IP Address	<input type="text" value="192.168.0.1"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
MAC Address	00:0C:43:30:50:77
DHCP Type	Server <input type="button" value="v"/>
DHCP Start IP	<input type="text" value="192.168.0.100"/>
DHCP End IP	<input type="text" value="192.168.0.200"/>
DHCP Lease Time	<input type="text" value="24"/> hour(s) (1-65535)
UPNP	Disable <input type="button" value="v"/>

- **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) or not.

Click <**Apply**> to confirm your configuration.

5.5.2 DHCP Clients

After access MODEM setup page successfully, please click **Router** → **DHCP Clients** link to access the following screen:

The screenshot shows a web interface for DHCP Clients. At the top, there is a blue header bar with the text "Router-->DHCP Clients". Below this, there are two tabs: "LAN" and "DHCP Clients", with "DHCP Clients" being the active tab. Underneath the tabs, the text "DHCP Clients" is displayed. A table with four columns is shown: "Host Name", "MAC Address", "IP Address", and "Expires in". The table contains one row with the following data: Host Name: Tom, MAC Address: 00:1E:90:4A:7C:B1, IP Address: 192.168.0.100, Expires in: 23:58:33. To the right of the table is a "Refresh" button.

Host Name	MAC Address	IP Address	Expires in
Tom	00:1E:90:4A:7C:B1	192.168.0.100	23:58:33

Refresh

- **MAC Address:** MAC address of DHCP client
- **IP Address:** IP address of DHCP client
- **Expires in:** The left time for lease, if this IP address is static bound, then demonstrated: Infinity
- Click <Refresh> button to refresh the information.

5.6 Wi-Fi Settings

5.6.1 Station List

After access MODEM setup page successfully, please click **Wi-Fi Settings** → **Station List** link to access the following screen:

The screenshot shows a web interface for the Station List. At the top, there is a blue header bar with the text "Wi-Fi Settings-->Station List". Below this, there are five tabs: "Station List", "Basic", "Advanced", "Security", and "WPS", with "Station List" being the active tab. Underneath the tabs, the text "Wireless Network" is displayed. A table with two columns is shown: "Station" and "MAC Address".

Station	MAC Address
---------	-------------

5.6.2 Basic

After access MODEM setup page successfully, please click **Wi-Fi Settings** → **Basic** link to access the following screen:

Wi-Fi Settings-->Basic

•Station List • **Basic** •Advanced •Security •WPS

Wireless Network

Wi-Fi On/Off	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Mode	11b/g/n Mixed Mode ▼
Network Name(SSID)	ZTE Wireless Network
Broadcast Network Name (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	02:1E:73:8A:E6:48
Frequency (Channel)	2437MHz (Channel 6) ▼

Wireless Distribution System(WDS)

WDS Mode	Disable ▼
----------	-----------

HT Physical Mode

Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40
Guard Interval	<input type="radio"/> long <input checked="" type="radio"/> Auto
MCS	Auto ▼
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Extension Channel	2457MHz (Channel 10) ▼
Aggregation MSDU (A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Apply Cancel

- **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 client 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 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. And select the known channel from channel 1 to channel 11.
2.Select WDS mode : Disable, Lazy Mode, Bridge Mode or Repeater Mode	<ul style="list-style-type: none"> -If you select Disable, WDS is disabled. -If you select Lazy Mode, WDS is enabled, and set wireless MAC address only on the peer APs. -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. -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.
3.Select Phy mode : CCK,OFDM,HTMIX or GREENFIELD	CCK : 802.11b OFDM : 802.11g HTMIX : 802.11b/g/n Mixed Mode GREENFIELD : 802.11n
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 AP 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 802.11b/g/n, 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.

5.6.3 Advanced

After access MODEM setup page successfully, please click **Wi-Fi Settings** → **Advanced** link to access the following screen:

Wi-Fi Settings-->Advanced

•Station List
• Basic
•Advanced
•Security
•WPS

Advanced Wireless

Beacon Interval	<input type="text" value="100"/> ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	<input type="text" value="1"/> ms (range 1 - 255, default 1)
Fragment Threshold	<input type="text" value="2346"/> (range 256 - 2346, default 2346)
RTS Threshold	<input type="text" value="2347"/> (range 1 - 2347, default 2347)
TX Power	<input type="text" value="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	<input type="text" value="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

- **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.
- **Short Slot:** To indicate that 802.11g is using a short 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.

5.6.4 Security

After access MODEM setup page successfully, please click **Wi-Fi Settings** → **Security** link to access the following screen:

Wi-Fi Settings-->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.

Wi-Fi Settings-->Security

•Station List •Basic •Advanced •**Security** •WPS

Security Policy

Security Mode	OPEN
Encrypt Type	WEP

Wire Equivalence Protection (WEP)

Default Key	Key 1	
WEP Keys	WEP Key 1 :	<input type="text"/> Hex
	WEP Key 2 :	<input type="text"/> Hex
	WEP Key 3 :	<input type="text"/> Hex
	WEP Key 4 :	<input type="text"/> Hex

Wireless MAC Filtering

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

Apply Cancel

- **Encrypt Type:** Select NO ENCRYPTION or WEP.
- **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, 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.

Wi-Fi Settings-->Security

•Station List •Basic •Advanced •Security •WPS

Security Policy

Security Mode	WPA-PSK/WPA2-PSK ▼
---------------	--------------------

WPA

WPA Algorithms	<input type="radio"/> TKIP <input type="radio"/> AES <input type="radio"/> AUTO
Pass Phrase	12345678
Key Renewal Interval	3600 seconds

Wireless MAC Filtering

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

Apply Cancel

- **WPA Algorithm:** TKIP, AES or AUTO.
- **Pass Phrase:** You can input a pass phrase encryption key format (8~64 bytes).
- **Key Renewal Interval:** Define how long the key should be renewed.

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.

5.6.5 WPS

After access MODEM setup page successfully, please click **Wi-Fi Settings** → **WPS** link to access the following screen:

The screenshot shows a web interface for configuring WPS. At the top, there is a blue header bar with the text "Wi-Fi Settings-->WPS". Below this is a navigation menu with five tabs: "•Station List", "•Basic", "•Advanced", "•Security", and "•WPS". The "•WPS" tab is currently selected and highlighted in blue. Underneath the tabs, the text "WPS Config" is displayed. Below this, there is a form with a label "WPS" and a dropdown menu currently set to "Disable". To the right of the form is an "Apply" button.

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

Wi-Fi Settings-->WPS

•Station List •Basic •Advanced •Security •WPS

WPS Config

WPS	Enable <input type="button" value="v"/>
-----	---

Apply

WPS Summary

WPS Current Status	Idle
WPS Configured	No
WPS SSID	ZTE Wireless Network
WPS Auth Mode	Open
WPS Encryp Type	None
WPS Default Key Index	1
WPS Key(ASCII)	
AP PIII	91029201 <input type="button" value="Generate"/>

Reset OOB

WPS Progress

WPS mode	<input checked="" type="radio"/> PIN <input type="radio"/> PBC
Client PIII	<input type="text"/>

Apply

WPS Status

WSC: Idle

This is used to setup security easily by choosing **PIN** (Pin Input Configuration) or **PBC** (Push Button Configuration) method to do Wi-Fi protected setup.

- **WPS Summary:** Shows the WPS function status.

- Click <Reset OOB> button to reset the settings.
- **WPS mode:** Select PBC or PIN WPS mode.
- **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**), and 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.
- **Client PIN:** Enter the PIN code from the registrar or enrollee.
- Click <Apply> to save and apply the current settings.
- **WPS Status:** Shows the current status of the WPS function.

Note:

When the security mode is **SHARED** or **Open**, you can not **use** WPS connection.

5.7 Firewall

5.7.1 Mac/Ip/Port Filtering

After access MODEM setup page successfully, please click **Firewall** → **Mac/Ip/Port Filtering** link to access the following screen:

Firewall-->MAC/IP/Port Filtering

• MAC/Ip/Port Filtering	•URL Filter	•Time Filtering	•Port Forwarding	•DMZ	•System Security	•Advanced Settings
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 Filter
- Time Filtering
- Port Forwarding
- DMZ
- System Security
- Advanced Settings

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.

Note: Filtering rules are matched one by one, if met this provision, it will not continue to match the rules listed below.

Click **<Apply>** to confirm your configuration. Click **<Delete>** to delete the rule which you selected. Click **<Reset>** to clear what you select or input.

To add a new rule:

- a) Select **Enable** and click **<Apply>** in the **Basic Settings** area.
- b) Input the detail information in the **Mac/Ip/Port Filtering** area.
- c) Click **<Apply>** in the **Mac/Ip/Port Filtering** area.

5.7.2URL Filter

After access MODEM setup page successfully, please click **Firewall** → **URL Filter** link to access the following screen:

Firewall-->URL Filter

• MAC/IP/Port Filtering • **URL Filter** • Time Filtering • Port Forwarding • DMZ • System Security • Advanced Settings

Current URL Filter:

No.	URL
-----	-----

Delete

Reset

Add a URL filter:

URL:	<input type="text"/> (eg: www.zte.com)
------	--

The maximum rule count is 10.

Add

Reset

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 URL Filter** field. Click <**Delete**> to delete the rule which you selected. Click <**Reset**> to clear what you select or input.

5.7.3 Time Filtering

After access MODEM setup page successfully, please click **Firewall** → **Time Filtering** link to access the following screen:

Firewall-->Time Filtering

• Mac/Ip/Port Filtering •URL Filter •Time Filtering •Port Forwarding •DMZ •System Security •Advanced Settings

Please Set

Days	<input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Time Range	From <input type="text" value="00:00"/> To <input type="text" value="00:00"/>

The maximum rule count is 10.

Apply

Current Time rules:

No.	Day	Time start	Time end
-----	-----	------------	----------

Delete Reset

Select the **Days** and **Time Range**, and then click **<Apply>** to add the Time filtering. The new Time filtering item will be shown in the **Current Time Rules** field. Click **<Delete>** to delete the rule which you selected. Click **<Reset>** to clear what you select or input.

5.7.4Fort Forwarding

After access MODEM setup page successfully, please click **Firewall → Port Forwarding** link to access the following screen:

Firewall-->Port Forwarding

• MAC/IP/Port Filtering •URL Filter •Time Filtering •Port Forwarding •DMZ •System Security •Advanced Settings

Virtual Server Settings

Virtual Server Settings	<input type="text" value="Disable"/>
--------------------------------	--------------------------------------

Apply

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

Firewall-->Port Forwarding

•MAC/IP/Port Filtering •URL Filter •Time Filtering •Port Forwarding •DMZ •System Security •Advanced Settings

Virtual Server Settings

Virtual Server Settings	<input type="text" value="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	<input type="text" value="TCP&UDP"/>
Comment	<input type="text"/>

The maximum rule count is 10.

Current Virtual Servers in system:

No.	IP Address	Port Range	Protocol	Comment
-----	------------	------------	----------	---------

- **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.

Select **Enable**, and input the detail information in the **Virtual Server Settings** area, and then click **<Apply>** to add a new rule. Click **<Delete>** to delete the rule which you selected. Click **<Reset>** to clear what you select or input.

5.7.5DMZ

After access MODEM setup page successfully, please click **Firewall** → **DMZ** link to access the following screen:

Firewall-->DMZ

• MAC/IP/Port Filtering • URL Filter • Time Filtering • Port Forwarding • **DMZ** • System Security • Advanced Settings

DMZ Settings

DMZ Settings

Apply

If you select **Enable**, set the DMZ IP address ,and then click **<Apply>** to confirm your configuration. You can setup a De-militarized Zone(DMZ) to separate internal network with the Internet.

5.7.6 System Security

After access MODEM setup page successfully, please click **Firewall** → **System Security** link to access the following screen:

Firewall-->System Security

• MAC/IP/Port Filtering • URL Filter • Time Filtering • Port Forwarding • DMZ • **System Security** • Advanced Settings

Remote management

Remote management (via WAN)

Ping from WAN

Ping from WAN

Apply Reset

Allow or **Deny** the remote management function and **Enable** or **Disable** ping from WAN on requirement, and then click **<Apply>**. Click **<Reset>** to restore the default value.

5.7.7 Advanced Settings

After access MODEM setup page successfully, please click **Firewall** → **Advanced Settings** link to access the following screen:

Firewall-->Advanced Settings

• Mac/Ip/Port Filtering •URL Filter •Time Filtering •Port Forwarding •DMZ •System Security •Advanced Settings

Advanced Settings

DNS Proxy	Enable ▾
NAT	Enable ▾

Apply

- **DNS Proxy:** Disable or enable to send this DNS request to high-level DNS server.
- **NAT:** Disable or enable the NAT in internal network.

Click <**Apply**> to confirm.

5.8 VPN

After access MODEM setup page successfully, please click **VPN** link to access the following screen:

VPN

VPN Connect Mode

Select Mode	PPTP ▼
-------------	--------

PPTP Mode

PPTP Server IP Address	<input type="text"/>
User Name	<input type="text"/>
Password	<input type="text"/>

Operation

Select Operation	Connect ▼
VPN Status	Disconnected

Apply

- **Select Mode:** Select **L2TP** or **PPTP**.
- **L2TP/PPTP Server IP Address:** Input server IP address.
- **User Name:** Input user Name
- **Password:** Input **password**.
- **Select Operation:** Select the operation, Connect or Disconnect.
- **VPN Status:** VPN current status.

Click **<Apply>** to confirm.

5.9 VoIP

5.9.1 User Details

After access MODEM setup page successfully, please click **VoIP** → **User Details** link to access the following screen:

SIP Server and Configuration

SIP Register Server	<input type="text"/>
SIP Domain	<input type="text"/>
SIP Realm	<input type="text"/>
SIP Port	<input type="text"/> [1024,65535]
SIP Proxy Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
T.38 FAX Ecoder	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Authorization

Display Name	<input type="text"/>
User Name	<input type="text"/>
Authorized User Name	<input type="text"/>
Authorized Password	<input type="text"/>
VoIP Register Status	Register Fail

Apply

- **SIP Register Server:** A server that accepts registration requests from users. If it is unspecified or blank, the **voice port** will not use a SIP registrar and will not send a REGISTER message. The value must specify the protocol.
- **SIP Domain:** A SIP Domain name or IP address, defined by customer.
- **SIP Realm:** This is a string value provided by the ITSP, such as AVSTW, or may be a domain name like www.zte.com.cn, defined by customer.
- **SIP Port:** The listening/binding port of the local User Agents for receiving and transmitting SIP messages. By default, it sets 5060.
- **SIP Proxy Mode:** Enable or disable the use of SIP proxy server config parameter.

- **T.38 FAX Ecoder:** T.38 Fax Mode for VoIP. Enable this item to ensure the successful of Fax.
- **Display Name:** Display name for using in the SIP URI.
- **User Name:** User name for using in the SIP URI for the respective appearance.
- **Authorized User Name:** This is for authentication with a registrar.
- **Authorization Password:** This is a password for authentication with a registrar.
- **VOIP Register Status:** Show the register status of SIP server.

Click <Apply> to confirm your choice.

5.9.2 Advanced

After access MODEM setup page successfully, please click **VoIP** → **Advanced** link to access the following screen:

VoIP-->Advanced

•User Details
•Advanced
•Supplementary

Topology

Outbound Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
STUN Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Reregister Every	<input type="text"/> Seconds
tel: format number	<input type="text"/>

Advanced Options

Appearance Displayname	<input type="text"/>
Encoder	G.711 u-Law ▼

- **Outbound Mode:** Enable or disable the use of SIP outbound server config parameter.
- **STUN Mode:** Enable or disable the use of STUN server to discover NAT mapping.
- **Reregister Every:** Expires value in seconds for a REGISTER request.
- **Appearance Displayname:** Be used in SIP REGISTER.
- **Encoder:** Used for SIP negotiation.

Click <**Apply**> to confirm your choice.

5.9.3 Supplementary

After access MODEM setup page successfully, please click **VoIP** → **Supplementary** link to access the following screen:

VoIP supplementary service	
Call Forwarding	Unconditional forwarding ▼
Forwarding URI	<input type="text"/>
Incoming Call Barring	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Outgoing Call Barring	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

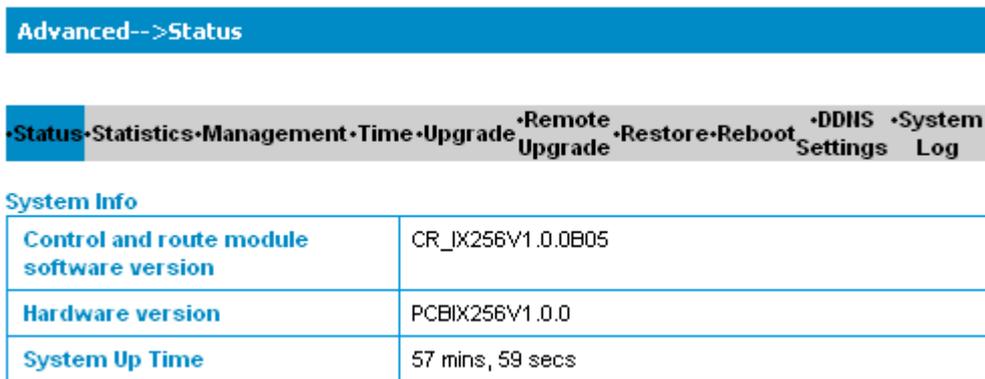
- **Call Forwarding:** Select call forwarding way,
- **Forwarding URI:** Call forwarding to URI.
- **Incoming Call Barring:** Enable or disable barring incoming call.
- **Outgoing Call Barring:** Enable or disable barring the outgoing call.

Click <**Apply**> to confirm your choice.

5.10 Advanced

5.10.1 Status

After access MODEM setup page successfully, please click **Advanced** → **Status** link to access the following screen:



The screenshot shows a web interface with a blue header bar containing the text "Advanced-->Status". Below the header is a navigation menu with the following items: Status (highlighted), Statistics, Management, Time, Upgrade, Remote Upgrade, Restore, Reboot, DDNS Settings, and System Log. The main content area is titled "System Info" and contains a table with the following data:

System Info	
Control and route module software version	CR_IX256V1.0.0B05
Hardware version	PCBIX256V1.0.0
System Up Time	57 mins, 59 secs

View software version, hardware version and system up time.

5.10.2 Statistics

After access MODEM setup page successfully, please click **Advanced** → **Statistics** link to access the following screen:

Advanced-->Statistics

•Status •Statistics •Management •Time •Upgrade •Remote Upgrade •Restore •Reboot •DDNS Settings •System Log

Memory

Memory total:	28536 kB
Memory left:	1040 kB

WAN/LAN

WAN Rx packets:	7319
WAN Rx bytes:	843852
WAN Tx packets:	8267
WAN Tx bytes:	4154276
LAN Rx packets:	7319
LAN Rx bytes:	843852
LAN Tx packets:	8267
LAN Tx bytes:	4154276

5.10.3 Management

After access MODEM setup page successfully, please click **Advanced** → **Management** link to access the following screen:

Advanced-->Management

•Status•Statistics•**Management**•Time•Upgrade•Remote Upgrade•Restore•Reboot•DDNS Settings•System Log

Administrator Settings

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

User Settings

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

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

5.10.4 Time

After access MODEM setup page successfully, please click **Advanced** → **Time** link to access the following screen:

Advanced-->Time

•Status•Statistics•Management•Time•Upgrade•Remote Upgrade•Restore•Reboot•DDIIS•System Settings Log

Current Local Time	2000-01-01 00:55:05 Saturday
--------------------	------------------------------

Time Set Mode	Manual Set Time
---------------	-----------------

Manual Set Time	Year 2000 Month 1 Day 1 Hour 0 Minute 0
-----------------	---

Apply

- **Time Set Mode:** Select the time set mode.
- **Manual Set Time:** Set the time manually.
- **SNTP Server IP:** Enter a SNTP server IP for time synchronization.

Click <Apply> to confirm your configuration to set the device time by manually, or by SNTP sever.

5.10.5 Upgrade

After access MODEM setup page successfully, please click **Advanced** → **Upgrade** link to access the following screen:

Advanced-->Upgrade

•Status•Statistics•Management•Time•Upgrade•Remote Upgrade•Restore•Reboot•DDIIS•System Settings Log

Update Firmware

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

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

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

5.10.6 Remote Upgrade

After access MODEM setup page successfully, please click **Advanced** → **Remote Upgrade** link to access the following screen:

Advanced-->Remote Upgrade

•Status •Statistics •Management •Time •Upgrade •Remote Upgrade •Restore •Reboot •DDNS Settings •System Log

Remote Upgrade

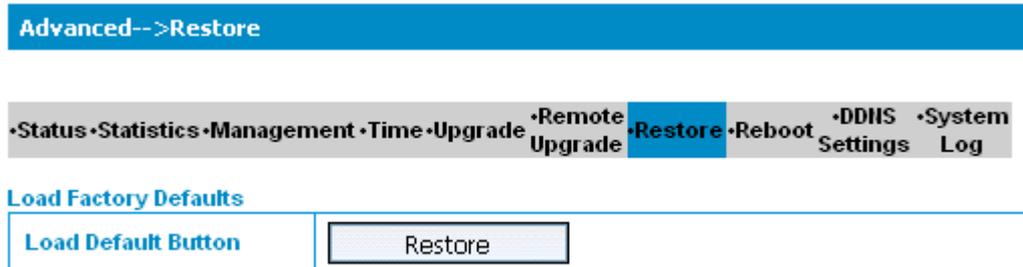
Upgrade Mode	FTP <input type="button" value="v"/>
Server Name	<input type="text"/> (XXX.XXX.XXX.XXX, eg: 192.232.33.10)
Server Port	<input type="text"/>
FTP Username	<input type="text"/>
FTP Password	<input type="text"/>
Remote Path/File Name	<input type="text"/>

- **Upgrade Mode:** Select upgrade mode. FTP or TFTP is available. If select TFTP, you don't need user authorization.
- **Server Name:** Remote FTP/TFTP server IP address.
- **Server Port:** The port of Remote FTP/TFTP server address.
- **FTP Username:** User name for the FTP server.
- **FTP Password:** Password for the FTP server.
- **Remote Path/File Name:** Locate upgrade file in FTP server. If TFTP is selected, you just need to type in file name.

Click <**Apply**> to confirm your configuration.

5.10.7 Restore

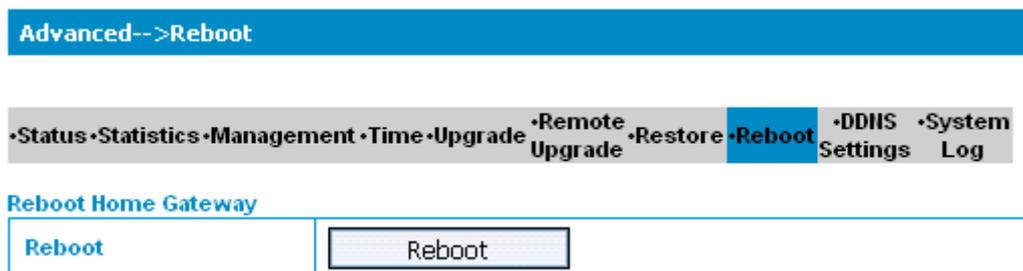
After access MODEM setup page successfully, please click **Advanced** → **Restore** link to access the following screen:



Restore to set all the settings to their factory default values, and the device will restart.

5.10.8 Reboot

After access MODEM setup page successfully, please click **Advanced** → **Reboot** link to access the following screen:



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

5.10.9 DDNS Settings

After access MODEM setup page successfully, please click **Advanced** → **DDNS Settings** link to access the following screen:

DDNS Settings

Dynamic DNS Provider	None <input type="button" value="v"/>
Account	<input type="text"/>
Password	<input type="text"/>
DDNS	<input type="text"/>

DDNS is a dynamic domain analysis system. After applying DDNS, a dynamic IP address to the mainframe also can provide domain name services. For example, the mainframe through dial-up or XDSL DHCP server gets IP address and domain names dynamically. Enable and configure DDNS so the host's IP address changes will not affect the users who visit through the domain name.

5.10.10 System Log

After access MODEM setup page successfully, please click **Advanced** → **System Log** link to access the following screen:

Advanced-->System Log

•Status •Statistics •Management •Time •Upgrade •Remote Upgrade •Restore •Reboot •DDNS Settings •System Log

```
Jan 1 00:00:22 (none) syslog.info syslogd started: BusyBox v1.12.1
Jan 1 00:00:22 (none) user.notice kernel: klogd started: BusyBox v1.12.1 (20
Jan 1 00:00:22 (none) user.notice kernel: Linux version 2.6.21 (root@localh
Jan 1 00:00:22 (none) user.warn kernel:
Jan 1 00:00:22 (none) user.warn kernel: The CPU feqenuce set to 384 MHz
Jan 1 00:00:22 (none) user.warn kernel: CPU revision is: 0001964c
Jan 1 00:00:22 (none) user.warn kernel: Determined physical RAM map:
Jan 1 00:00:22 (none) user.warn kernel: memory: 02000000 @ 00000000 (usabl
Jan 1 00:00:22 (none) user.debug kernel: On node 0 totalpages: 8192
Jan 1 00:00:22 (none) user.debug kernel: DMA zone: 64 pages used for memm
Jan 1 00:00:22 (none) user.debug kernel: DMA zone: 0 pages reserved
Jan 1 00:00:22 (none) user.debug kernel: DMA zone: 8128 pages, LIFO batch
Jan 1 00:00:22 (none) user.debug kernel: Normal zone: 0 pages used for me
Jan 1 00:00:22 (none) user.warn kernel: Built 1 zonelists. Total pages: 81
Jan 1 00:00:22 (none) user.notice kernel: Kernel command line: console=ttyS
Jan 1 00:00:22 (none) user.warn kernel: Primary instruction cache 32kB, phy
Jan 1 00:00:22 (none) user.warn kernel: Primary data cache 16kB, 4-way, lin
Jan 1 00:00:22 (none) user.info kernel: Synthesized TLB refill handler (20
Jan 1 00:00:22 (none) user.info kernel: Synthesized TLB load handler fastpa
Jan 1 00:00:22 (none) user.info kernel: Synthesized TLB store handler fastp
```

Refresh Export Clear

This page includes three buttons.

Refresh: Display the latest log items

Clear: Clear current log item

Export: Download the current log to the local specified directory

5.11 Logout

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



2. Click **OK** to log out.

6 Troubleshooting

This chapter lists some problems that you might encounter while installing or using MODEM, please read following relative information at first. If the problem still can not be solved, please contact with distributor or service provider.

Problem	Check Point
Indicator light	
After power on the MODEM, power LED is off.	<ol style="list-style-type: none"> 1. Make sure power adapter is original accessories. 2. Power adapter correctly connect with MODEM and wall socket/power.
After insert Ethernet cable, the LAN indicator light is off.	<ol style="list-style-type: none"> 1. Make sure Ethernet cable correctly connect with computer/HUB and MODEM. 2. Confirm computer/HUB is power on.
Access network failure	
Can not access the setup page of the MODEM	<ol style="list-style-type: none"> 1. Verify the LAN connection successful. 2. Checking your TCP/IP settings. Refer to Windows Help for details. Make sure Obtain IP address automatically is selected in the settings. 3. Using Ping command to make sure that your computer is properly connected to the MODEM. Please refer to chapter 4.2. <p>If it still does not work, please contact your service provider.</p>
Can not access Internet	<ol style="list-style-type: none"> 1. Please check your PC's settings and connection according to the above advices, make sure that your PC can access MODEM setup page. 2. If PC is configured correctly and only can access MODEM setup page, please check your MODEM. Detailed refer to chapter 5. <p>If MODEM configured correctly, but still not work, please contact your service provider.</p>

Others	
Call failure	<p>1. Please Confirm the connectivity of telephone.</p> <p>2. Make sure the telephones perfectly connect with MODEM.</p> <p>If the call still fails, please contact with your service provider.</p>
Web page configuration lost after restart the MODEM	<p>1. Make sure you have clicked <submit> button after modify the configuration every time.</p> <p>2. If you click <submit> button, but the problem still exist, please contact with your service provider.</p>

7 Appendix Glossary

AES

Advanced Encryption Standard

DNS

Domain Name Server: it can provide the service that network node name can be translated to network IP address in the internet.

DDNS

Dynamic Domain Name Server.

DHCP

Dynamic Host Configuration Protocol.

DMZ

Demilitarized Zone.

Internet

Global network, Use to exchange data, news and viewpoints within millions of computer.

IP Address

32 bit address, Use to identify one computer in TCP/IP.

ITSP

The sever of SIP network

Use to connect some communication equipment (computer, MODEM and printer) within one room, school or other limited region.

MAC Address

The Media Access Control (MAC) address is a unique number assigned by the manufacturer to any Ethernet networking device, such as a network adapter, that allows the network to identify it at the hardware level. For all practical purposes, this number is usually permanent. Unlike IP address, which can change every time a computer log in the network, the MAC address of a device stays the same, making it a valuable identifier for the network.

NAT

Network Address Translation.

Protocol

Communication protocol: it is a rule that network equipment must follow for mutual communicating to transfer, transmit and receive data.

SNTP

Simple Network Time Protocol.

SIP

Session Initiated Protocol

TCP/IP

Transmission Control Protocol/Internet Protocol: basic communication protocol of network communication, but TCP/IP defines one group of protocol, not only include TCP and IP.

TKIP

Temporal Key Integrity Protocol, a security protocol used in the IEEE 802.11 wireless networking standard..

UDP

User Data Protocol: packet exchanging communication protocol in internet, its default under layer protocol is IP, provide simple protocol mechanism when transfer information to another user.

WAN

Wide Area Network.

WEP

Wired Equivalent Privacy

WiMAX

Worldwide Interoperability for Microwave Access.