



ZXDSL 931WII

VDSL2 Modem

Operation manual

Version 2.0

ZTE CORPORATION
ZTE Plaza, Keji Road South,
Hi-Tech Industrial Park,
Nanshan District, Shenzhen,
P. R. China
518057
Tel: (86) 755 26771900
Fax: (86) 755 26770801
URL: <http://ensupport.zte.com.cn>
E-mail: support@zte.com.cn

LEGAL INFORMATION

Copyright © 2006 ZTE CORPORATION.

The contents of this document are protected by copyright laws and international treaties. Any reproduction or distribution of this document or any portion of this document, in any form by any means, without the prior written consent of ZTE CORPORATION is prohibited. Additionally, the contents of this document are protected by contractual confidentiality obligations.

All company, brand and product names are trade or service marks, or registered trade or service marks, of ZTE CORPORATION or of their respective owners.

This document is provided "as is", and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. ZTE CORPORATION and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

ZTE CORPORATION or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between ZTE CORPORATION and its licensee, the user of this document shall not acquire any license to the subject matter herein.

ZTE CORPORATION reserves the right to upgrade or make technical change to this product without further notice.

Users may visit ZTE technical support website <http://ensupport.zte.com.cn> to inquire related information.

The ultimate right to interpret this product resides in ZTE CORPORATION.

Revision History

Revision No.	Revision Date	Revision Reason
1.0	20090625	Initial transmittal

Serial Number:

content

Product Introduction	1
Application	1
Features.....	1
Wireless Specifications	2
Compliance Certificates	3
Standards Compatibility and Compliance	3
Supported Encapsulation	4
Environment Requirements	4
System Requirements	4
Packing List	9
Safety Precautions.....	10
LED Status and Interface Description	10
LED Status	10
Rear Panel	12
Hardware Installation	13
Choosing the Best Location for Wireless Operation	13
Connecting the Device.....	14
Factory Reset Button.....	15
Setting Up the Device	17
About the Device	17
Hardware Configuration of the Device and PC	
Configuration	18
Setting Up WAN and LAN Connections	18
PC Network Configuration	19
Device Information Configuration	21
Logging In to the Device.....	22
Device information	22
Device Information Summary	23
Statistics	24
LAN Statistics	24
WAN Statistics.....	25

xDSL Statistics	25
Route Table Information	27
ARP Table Information.....	28
WAN Interface Configuration	31
Configure ADSL EoA PPPoE WAN Connection	31
Configure ADSL EoA IPoE WAN Connection.....	37
Configure ADSL EoA Bridge WAN Connection	43
Configure ADSL PPPoA WAN Connection.....	47
Configure ADSL IPoA WAN Connection.....	53
Configure VDSL2 EoA WAN Connection	58
Configure VDSL2 Bridge WAN Connection	64
Configure VDSL2 IPoE WAN Connection	67
LAN Configuration	75
VLAN Trunking Configuration	79
NAT Configuration	83
Overview.....	83
Virtual Servers Setup	84
Port Triggering	87
DMZ Host	89
Security Configuration.....	93
Configure MAC Filtering Policy	93
Configure MAC Filtering Rule	95
MAC Filtering - Global Policy FORWARDED.....	96
MAC Filtering - Global Policy BLOCKED	97
QoS Configuration	99
Enable QoS.....	100
QoS-Queue Config	100
QoS-QoS Classification	103
QoS - DSCP Setting	106
Routing Configuration	109
Routing – Default Gateway	109
Static Routes	110
Policy Routing	111
RIP.....	113
DNS.....	115
DNS Server	115
Dynamic DNS.....	116
DSL Configuration	119

IPSec.....	121
VPN	121
ISAKMP.....	122
IKE.....	123
Parental Control	125
Time Restriction	125
URL Filter	126
UPNP Configuration.....	129
Certificate Configuration	131
Create New Local Certificate	132
Import An Existing Local Certificate.....	134
Import Trusted CA Certificates.....	135
Wireless Configuration	137
Overview.....	137
Wireless Network.....	137
About the Guw5.5Z66-5	138
Wireless LAN Basics	139
Basic terms	139
Wireless Standard	140
Wireless Security.....	144
Wireless Client requirements.....	146
Wireless Distribution System.....	147
Configure Wireless Connection	147
Wireless - Basic.....	147
Wireless–Security	149
No Encryption.....	150
64-bit WEP.....	151
128-bit WEP	152
802.1x Authentication	153
WPA Authentication	155
WPA2 Authentication	156
WPA-PSK Authentication	158
WPA2-PSK Authentication	159
Mixed WPA2/WPA-PSK Authentication	161
Mixed WPA2/WPA Authentication.....	162
Wireless - Advanced.....	164
Wireless - Station Info	169
Diagnostics Configuration	171
Management Configuration	173

Settings	173
Setting Backup.....	173
Setting Update.....	174
Setting Restore Default	174
System Log	175
SNMP Agent.....	177
TR-069 Client Management.....	178
Protocol Components	178
Protocol Application	179
TR-069 Client Configuration	180
Internet Time.....	181
Access Control	182
Update Software	183
Reboot	184
Figures	185
Tables	191

Chapter 1

Product Introduction

The ZXDSL 931WII is a [VDSL2](#) access device, which supports multiple line transmission mode. It provides four 10/100Base-T Ethernet interfaces and wireless user access function according to the [IEEE 802.11b/g](#) standard. In addition, ZXDSL 931WII provides the broadband Internet service or enterprise network access service via high-speed [ADSL](#) access.

Table of Contents

Application	1
Features.....	1
Wireless Specifications	2
Compliance Certificates	3
Standards Compatibility and Compliance	3
Supported Encapsulation	4
Environment Requirements	4
System Requirements	4
Packing List	9
Safety Precautions.....	10
LED Status and Interface Description	10

Application

- Home gateway
- SOHOs
- Small enterprises
- TV over IP (IPTV)
- Higher data rate broadband sharing
- Shared broadband Internet access
- Audio and video streaming and transfer
- PC file and application sharing
- Network and online gaming

Features

- 4 x 10/100 Ethernet ports

- User-friendly GUI for web configuration
- Supports IPSec for virtual private network (VPN)
- Several pre-configured popular games. Just enable the game and the port settings are automatically configured.
- Configurable as a DHCP server in the network
- Compatible with all standard Internet applications
- Industry standard and interoperable DSL interface
- Support virtual server, IP filter, and demilitarized military zone (DMZ) host
- Simple web-based status page displays a snapshot of system configuration and links to the configuration pages
- Downloadable flash software upgrades
- For ADSL and VDSL2, each supports up to 8 PPPoE sessions
- Supports SNMP v2, RIP v1 & RIP v2, NAT
- WLAN with high-speed data transfer rates of up to 54 Mbps, compatible with IEEE 802.11b/g, 2.4 GHz compliant equipment

Wireless Specifications

TABLE 1 WIRELESS SPECIFICATIONS

Network Standard	IEEE 802.11b,	
	IEEE 802.11g	
Frequency Range	2.40 GHz~2.4835 GHz, ISM Band	
Modulation	802.11b: DBPSK, DQPSK, CCK	
	802.11g: BPSK, QPSK, 16 QAM, 64 QAM	
RF Power	Max.: 20 dBm	
	802.11b: Typ. 18 dBm@Normal Temp Range	
	802.11g: Typ. 15 dBm@Normal Temp Range	
AP Capacity	Access user quantity	50~80Pcs/AP
	Number of channels	US and Canada: 11
		Europe and China: 13
		Japan: 14
Auto-sensing data rate	802.11.b: 1 Mbps, 2 Mbps, 5.5 Mbps, 11 Mbps	
	802.11g: 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps	

		Mbps, 48 Mbps, 54 Mbps
Payload Rate	1 Mbps	DBPSK@0.81 Mbps
	2 Mbps	DQPSK@1.58 Mbps
	5.5 Mbps	CCK@4.07 Mbps
	6 Mbps	BPSK@4.64 Mbps
	9 Mbps	BPSK@6.55 Mbps
	11 Mbps	CCK@7.18 Mbps
	12 Mbps	BPSK@8.31 Mbps
	18 Mbps	QPSK@11.5 Mbps
	24 Mbps	6QAM@14.18 Mbps
	36 Mbps	16QAM@18.31 Mbps
	48 Mbps	64QAM@23.25 Mbps
	54 Mbps	64QAM @26.12 Mbps
Security	64-bit/128-bit WEP, 802.1x, WPA, WPA2	
User Isolation	MAC level	
Authentication	DHCP Client & Static IP	Support
	802.1X and Radius Client	Support
	DHCP Server	Support
Radio Cover Rage (m)	Outdoor	100~150
	Indoor	35~100
Antenna Type	Internal diversity with connector. 2 dBi	

Compliance Certificates

CE Mark

Standards Compatibility and Compliance

- RFC2516 PPP Over Ethernet (PPPoE)

- RFC 1662 PPP in HDLC-like Framing
- RFC1332 PPP Internet Protocol Control Protocol
- RFC1483R
- RFC894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
- RFC1042 A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
- IPoE (IP over Ethernet)
- Supports ALG (Application Level Gateway)
- IEEE802.3
- IEEE802.3u
- IEEE 802.11b
- IEEE 802.11g

Supported Encapsulation

- RFC 1483 bridge
- RFC 1483 router
- PPP over Ethernet (RFC 2516)

Environment Requirements

- Operating temperature: 0 °C - 40 °C (32 °F - 104°F)
- Storage temperature: 20 °C - 70 °C (-4 °F - 158 °F)
- Operating humidity: 20 % - 90 %, non-condensing
- Storage humidity: 5 % - 95 %, non-condensing

System Requirements

Recommended system requirements are as follows:

- Pentium 233 MHz or higher
- Memory: 64 MB or higher
- 10M Base-T Ethernet or higher
- Windows 9x, Windows 2000, Windows XP, Windows ME, Windows NT
- Ethernet network interface card

The following information in [Table 2](#) is very helpful for your [VDSL2](#) configuration. You can collect it from your VDSL2 service provider:

TABLE 2 VDSL2 SERVICE INFORMATION REQUIREMENT

Item	Description	Enter Information in This Column
PTM	Most users are not required to change this setting. The Packet Transfer Mode (PTM) interface is used to identify the data path between the network of your VDSL2 service provider and your computer. If you are setting up the 931WII for multiple connections, you need to configure the PTM interface as instructed by your VDSL2 service provider for additional connections. You can change this setting by accessing the layer-2 configuration and WAN menu of the web management interface.	
Username	This is the user name used to log in to the network of your VDSL2 service provider. It is usually in the form of user@isp.com. Your VDSL2 service provider uses this to identify your account.	
Password	This is the password used, in conjunction with the user name previously mentioned, to log in to the network of your VDSL2 service provider. It is used to verify the identity of your account.	

The following information in [Table 3](#) is very helpful for your [ADSL](#) configuration. You can collect it from your ADSL service provider:

TABLE 3 ADSL SERVICE INFORMATION REQUIREMENT

Item	Description	Enter Information in This Column
VPI	<p>Most users are not required to change this setting. The virtual path identifier (VPI) is used in conjunction with the virtual channel identifier (VCI) to identify the data path between the network of your ADSL service provider and your computer. If you are setting up the 931WII for multiple virtual connections, you need to configure the VPI and VCI as instructed by your ADSL service provider for additional connections. You can change this setting by accessing the layer-2 configuration and WAN menu of the web management interface.</p>	
VCI	<p>Most users are not required to change this setting. The VCI is used in conjunction with the VPI to identify the data path between the network of your ADSL service provider and your computer. If you are setting up the 931WII for multiple virtual connections, you need to configure the VPI and VCI as instructed by your ADSL service provider for additional connections. You can change this setting by accessing the layer-2 configuration and WAN menu of the web management interface.</p>	

Item	Description	Enter Information in This Column
Connection and Encapsulation Type	This is the method your ADSL service provider uses to transmit data between the Internet and your computer. Most users use the default PPPoE connection type. The Setup Wizard can be used to configure a PPPoE connection type. You may need to specify one of the following connection types: PPPoE, LLC. Other available connections and encapsulation combinations must be configured by using the Web manager. These include the Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC-MUX), Static IP (Bridged IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP LLC, 1483 Routed IP VC-MUX), etc.	
Username	This is the user name used to log in to the network of your VDSL service provider. It is usually in the form of user@isp.com. Your ADSL service provider uses this to identify your account.	
Password	This is the password used, in conjunction with the user name previously mentioned, to log in to the network of your ADSL service provider. It is used to verify the identity of your account.	

Necessary information about your 931WII is as follows in [Table 4](#).

TABLE 4 DEVICE INFORMATION REQUIREMENT

Item	Description	Enter Information in This Column
LAN IP addresses	This is the IP address you enter in the Address field in the Web browser to access the configuration graphical user interface (GUI) of the gateway. The default IP address is 192.168.1.1 and it is referred to as the Management IP address in this User Manual. You can change this to suit any desired IP address scheme. This address is the basic IP address used for DHCP service on the LAN when DHCP is enabled.	
LAN Subnet Mask	This is the subnet mask used by the 931WII, and is used throughout your LAN. The default subnet mask is 255.255.255.0. You can change it later.	
Username	This is the user name used to access the management interface of the gateway, when you attempt to connect to the device through a web browser. The default username of the 931WII is admin. It cannot be changed.	
Password	This is the password required when you access the management interface of the gateway. The default password is admin. It cannot be changed.	

Necessary information about your LAN or computer is as follows in [Table 5](#).

TABLE 5 PC INFORMATION REQUIREMENT

Item	Description	Enter Information in This Column
Ethernet NIC	If your computer has an Ethernet NIC, you can connect the 931WII to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the 931WII to connect to other computers or Ethernet devices.	
DHCP Client status	By default, your 931WII residential gateway is configured as a DHCP server. This means that it can assign an IP address, a subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses that the 931WII assigns is from 192.168.1.2 to 192.168.1.254. You need to set your computer (or computers) to Obtain an IP address automatically (that is, to set computers as DHCP clients.)	

Packing List

- 1 x ZXDSL 931WII
- 1 x external splitter
- 1 x power adapter
- 1 x Ethernet cable (RJ-45)
- 2 x Phone cable (RJ-11)
- 1 x User Manual (optional)
- 1 x quality guarantee card (optional)
- 1 x certificate of quality (optional)

Safety Precautions

Follow the instructions to protect the device from risks and damage caused by fire and electric power:

- Use volume labels to mark the type of power.
- Use the power adapter that is packed within the device package.
- Pay attention to the power load of the outlet or prolonged lines. An overburden power outlet or damaged lines and plugs may cause electric shock or fire accident. Check the power cords regularly. If you find any damage, replace it at once.
- Proper space left for heat dissipation is necessary to avoid any damage caused by overheating to the device. The long and thin holes on the device are designed for heat dissipation to ensure that the device works normally. Do not cover these heat dissipation holes.
- Do not place this device close to a place where a heat source exits or high temperature occurs. Avoid the device from direct sunshine.
- Do not place this device close to a dampened place.
- Do not spill any fluid on this device.
- Do not connect this device to any PC or electronic product, unless our customer engineer or your broadband provider instructs you to do this, because any incorrect connection may cause power or fire risk.
- Do not place this device on an unstable surface or support.

LED Status and Interface Description

LED Status

FIGURE 1 FRONT PANEL LED DIAGRAM

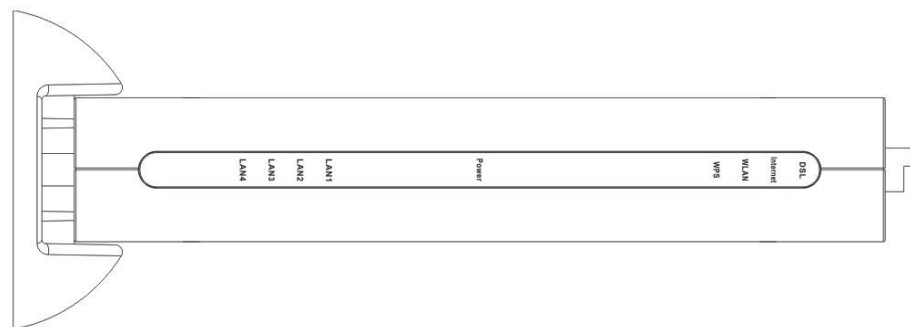


TABLE 6 FRONT PANEL LED STATUS

Indicator	Color	Status	Description
Power	Blue/Red	OFF	Power OFF
		Red	Power ON, HW Testing
		Blue	Power ON, HW Test ok
DSL	Green	OFF	The modem is in the non-communication state
		Flash	The modem is in training state
		ON	The modem is in the communication state
Internet	Green	OFF	No detected data
		Flash	WAN port is receiving or sending data
		ON	WAN port is in communication status
WLAN	Green	OFF	No detected radio signal
		Flash	WLAN port is receiving or sending data
		ON	WLAN interface is ready to work
WPS	Green	OFF	WPS function is OFF
		Flash	WLAN port is in negotiation status
		ON	WPS function is ON
	Red	Flash	WLAN port negotiation is failure

Indicator	Color	Status	Description
LAN 1 - LAN 4	Green	OFF	The Ethernet port is in the non-communication state
		ON	The Ethernet port is in the communication state
		Flash	Ethernet interface is receiving or sending data

Rear Panel

FIGURE 2 REAR PANEL INTERFACE DIAGRAM



Interface	Description
DSL	RJ-11port: Use the telephone line to connect the modem with the VDSL2 cable or splitter
LAN 1-LAN 4	RJ-45 port: It is used to connect the modem to computer or other network devices
WPS	WLAN Protected Setup
Reset	During power ON period, hold on this button for more than 3 seconds to reset the current settings to the factory default setting, and then the system restarts automatically
Power	Power supply port: It is connected to the power adapter
ON/OFF	Power switch

Chapter 2

Hardware Installation

The 931WII has three separate interfaces, an Ethernet LAN, a wireless LAN and a VDSL2 (WAN) interface. Place the 931WII in a location where it can be connected to the various devices as well as to a power source. The 931WII should not be placed where it is exposed to moisture or excessive heat. Ensure the cables and power cord are placed safely to avoid tripping hazard. As with any electrical appliance, observe common safety procedures.

The 931WII can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, if you may need to view them for troubleshooting.

Table of Contents

Choosing the Best Location for Wireless Operation	13
Connecting the Device	14
Factory Reset Button.....	15

Choosing the Best Location for Wireless Operation

Many environmental factors may effect the wireless function of the 931WII. If this is the first time that you set up a wireless network device, read the following information.

The device can be placed on a shelf or desktop, ideally you should be able to see the LED indicators in the front, if you may need to view them for troubleshooting.

Designed to go up to 100 meters indoors and up to 300 meters outdoors, WLAN lets you access your network from anywhere you want. However, the numbers of walls, ceilings, or other objects that the wireless signals must pass through limit signal range. Typical ranges vary depending on types of materials and background RF noise in your home or business.

For optimum range and signal strength, use these basic guidelines:

- Keep the numbers of walls and ceilings to the minimum.

The signal emitted from wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range of wireless LAN devices from 1 to 30 M. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.

- Consider the direct line between access points and workstations.

A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it appears over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90° angle) a wall or ceiling for better reception.

- Building materials make a difference.

Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signals can pass through drywall or open doorways. Avoid positioning them in the way that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.

- Position the antenna for best reception.

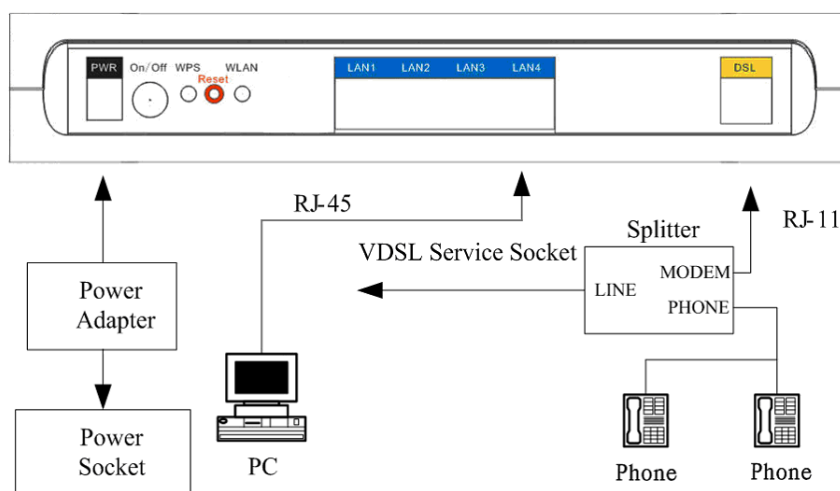
Direct the antenna position to check if signal strength improves. Some adapters or access points allow you to judge the strength of the signal.

- Keep the device away (at least 1 - 2 meters) from electrical devices.

Keep wireless devices away from electrical devices that generate RF noise, such as microwave ovens, monitors, and electric motors.

Connecting the Device

Context FIGURE 3 CONNECTION OF MODEM, PC AND TELEPHONES



- Steps** 1. Connect the **DSL** port of the 931WII with a telephone cable.

2. Connect the **LAN** port of the 931WII to the network card of the PC with an Ethernet line.
3. Plug one end of the power adapter to the wall outlet and connect the other end to the **PWR** port of the 931WII.

END OF STEPS

Factory Reset Button

The 931WII may be reset to the original factory default settings by pressing the reset button for a few seconds while the device is powered ON. Use a ballpoint or paperclip to gently push down the reset button.

Remember that this wipes out any settings stored in the flash memory, including user account information and LAN IP settings. The device settings are restored to the following factory defaults: the IP address is 192.168.1.1, subnet mask is 255.255.255.0, user name for management is `admin`, and password is `admin`.

This page is intentionally blank.

Setting Up the Device

Table of Contents

About the Device	17
Hardware Configuration of the Device and PC Configuration	18

About the Device

The 931WII provides a wide range of compelling broadband-based applications and services and includes an operating system, drivers and remote management capabilities. 931WII delivers a set of highly integrated solutions, required for the home and small company, such as:

- Optimized Linux 2.6 operating system
- IP routing and bridging
- Point-to-point protocol (PPP)
- Network/port address translation (NAT/PAT)
- Quality of service (QoS)
- Wireless LAN security: WPA, 802.1x, RADIUS client
- VPN: IPSec
- Secure Socket Layer (SSL) VPN
- Universal plug-and-play
- File server for network attached storage (NAS) devices
- Print server
- Web filtering
- Management and Control:
 - ▶ Web-based management (WBM)
 - ▶ Simple network management protocol (SNMP)
 - ▶ Command line interface (CLI)
 - ▶ TR-069 WAN management protocol
- Remote update
- System statistics and monitoring

- Oriented to the following platforms: DSL modems, wireless access points and bridge.

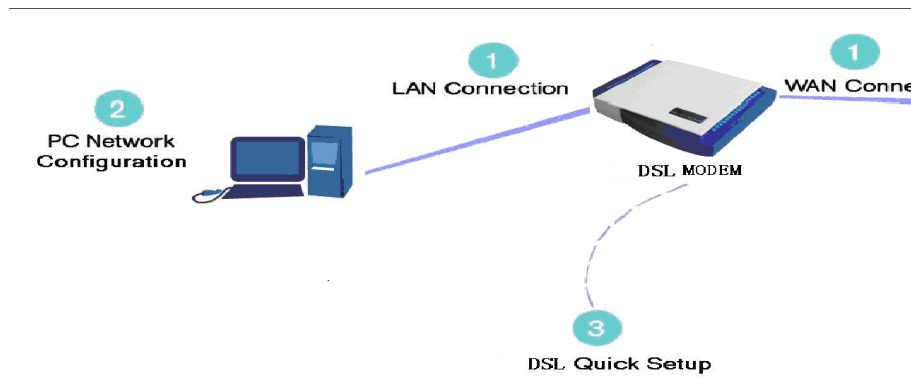
Hardware Configuration of the Device and PC Configuration

Connecting your computer or home network to the 931WII is a simple procedure, varying slightly depending on the operating system. This chapter guides you to seamlessly integrate the 931WII with your computer or home network. The Windows default network settings dictate that in most cases the setup procedure described as follows is unnecessary. For example, the default DHCP setting in Windows 2000 is 'client', requiring no further modification. However, it is advised to follow the setup procedure described as follows to verify that all communication parameters are valid and that the physical cable connections are correct.

The setup procedure consists of three consecutive configuration stages:

1. Set up WAN and LAN connections.
2. Perform PC network configuration.
3. Configure the 931WII through the Web-based management page.

FIGURE 4 HARDWARE CONFIGURATION



Setting Up WAN and LAN Connections

WAN Connection Your connection to the Internet by DSL modem connects its DSL socket to the wall socket by using a telephone cable. If it has an Ethernet socket for the wide area network (WAN), connect it to the external modem you have, or to the Ethernet socket you might have, by using an Ethernet cable.

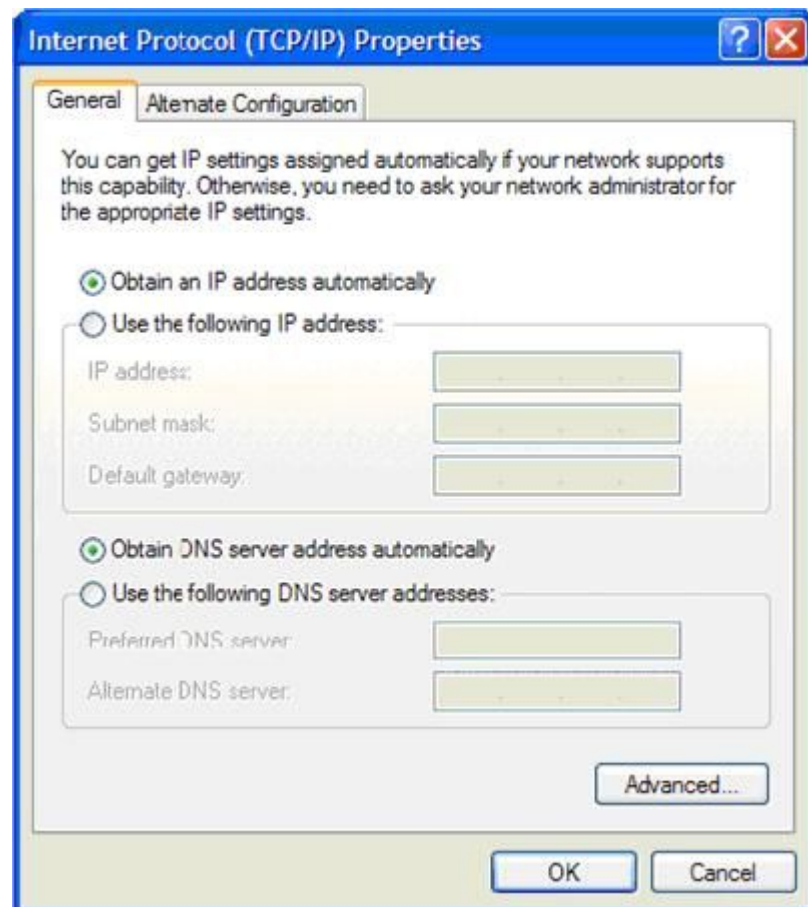
LAN Connection Your computer can connect to the gateway in various ways (such as Ethernet and wireless), each requiring a different physical connection, if any in case of wireless. The most common type of connection is Ethernet, with most platforms featuring four such ports. Use an Ethernet cable to connect an Ethernet port on the 931WII and the network card of your computer. For additional information, refer to the accompanying Installation Guide.

PC Network Configuration

Each network interface on the PC should either be configured with a statically defined IP address and DNS address, or be instructed to automatically obtain an IP address using the network DHCP server. The 931WII provides a DHCP server on its LAN and it is recommended to configure your LAN to automatically obtain its IP address and DNS server IP address. The configuration principle is identical but should be carried out differently on each operating system.

[Figure 5](#) displays the **TCP/IP Properties** dialog box as it appears on Windows XP.

FIGURE 5 IP AND DNS CONFIGURATION



- Windows XP**
1. Choose **Start > Control Panel** to open the control panel. Open **Network Connection** from the **control panel**.
 2. Right-click the **Ethernet connection** icon and choose **Properties**.
 3. On the **General** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**. The **Internet Protocol (TCP/IP) Properties** window appears.
 4. Select the **Obtain an IP address automatically** radio button.
 5. Select the **Obtain DNS server address automatically** radio button.
 6. Click **OK** to save the settings.
- Windows 2000/98/Me**
1. Choose **Start > Control Panel > Network and Dialing Connections** from the desktop.
 2. Right-click the **Ethernet connection** icon and choose **Properties**.
 3. Select the **Internet Protocol (TCP/IP)** component and click **Properties**. The **Internet Protocol (TCP/IP) Properties** window appears.
 4. Select the **Obtain an IP address automatically** radio button.
 5. Select the **Obtain DNS server address automatically** radio button.
 6. Click **OK** to save the settings.
- Windows NT**
1. Choose **Start > Control Panel > Network** from the desktop.
 2. On the **Protocol** tab, select the **Internet Protocol (TCP/IP)** component and click **Properties**.
 3. On the **IP Address** tab, select the **Obtain an IP address automatically** radio button.
 4. On the **DNS** tab, verify that no DNS server is defined in the **DNS Service Search Order** box and no suffix is defined in the **Domain Suffix Search Order** box.
- Linux**
1. Enter `su` at the prompt to log in to the system as a super user.
 2. Enter `ifconfig` to display the network devices and allocated IP addresses.
 3. Enter `pump -i <dev>`, where `<dev>` is the network device name.
 4. Enter `ifconfig` again to view the newly allocated IP address.
 5. Ensure that no firewall is active on device `<dev>`.

Chapter 4

Device Information Configuration

This chapter describes how to use Web-based management (WBM) of the 931WII, which allows you to configure and control all of the 931WII features and system parameters in a user-friendly GUI. This user-friendly approach is also implemented in the WBM documentation structure, which is directly based on the WBM structure. It is easy to navigate through both the WBM and its documentation.

FIGURE 6 WEB-BASED MANAGEMENT - HOME PAGE

The screenshot shows the ZTE 931WII Web-based Management (WBM) Home Page. The page has a blue header with the ZTE logo and a navigation menu on the left. The main content area displays 'Device Info' with a table of system parameters and a section for DSL connection status.

Device Info	
Board ID:	96368MVWG
Software Version:	ZXDSL 931WII V1.2.0c_Z31_OV
Bootloader (CFE) Version:	1.0.37-102.6
Wireless Driver Version:	4.174.64.19.cpe4.402

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS server:	
Secondary DNS server:	

Table of Contents

Logging In to the Device.....	22
Device information	22

Logging In to the Device

The following description is a detailed “How-To” user guide and is prepared for first time users. When you log in to the 931WII for the first time, the login wizard appears.

1. Open a Web browser on your computer.
2. Enter `http://192.168.1.1` (default IP address of the 931WII) in the address bar. The login page is as shown in [Figure 7](#).

FIGURE 7 WEB-BASED MANAGEMENT - LOGIN AUTHENTICATION PAGE



3. Enter the user name and the password. The default username and password of the super user are `admin` and `admin`. The username and password of the common user are `user` and `user`. You need not enter the username and password again if you select the option **Remember my password**. It is recommended to change these default values after logging in to the 931WII for the first time.
4. Click **OK** to log in or click **Cancel** to exit the login page.

After logging in to the 931WII as a super user, you can query, configure, and modify all configurations, and diagnose the system.

You need to reboot the 931WII to enable your modification or configuration effective in some cases, for example, after you modify the [PVC](#) configuration. Some modification, such as adding a static route, takes effect at once, and does not require modem reboot.

Device information

Click **Device Info** and you can view the following information:

- Summary

- WAN
- Statistics
- Route
- ARP

FIGURE 8 DEVICE INFO MENU



Device Information Summary

Click **Device Info > Summary** to display the interface as shown in [Figure 9](#) .

FIGURE 9 DEVICE INFORMATION SUMMARY

Board ID:	96368MVWG
Software Version:	ZXDSL 931WII V1.2.0c_Z31_OV
Bootloader (CFE) Version:	1.0.37-102.6
Wireless Driver Version:	4.174.64.19.cpe4.402

This information reflects the current status of your DSL connection.

Line Rate - Upstream (Kbps):	
Line Rate - Downstream (Kbps):	
LAN IPv4 Address:	192.168.1.1
Default Gateway:	
Primary DNS server:	
Secondary DNS server:	

- Board ID
- Software Version
- Bootloader Version
- Wireless Driver Version
- Upstream Line Rate
- Downstream Line Rate

- **LAN IP Address:** The management IP address
- **Default Gateway:** In the bridging mode there is no gateway. In other modes, it is the address of the uplink equipment, for example, PPPoE/PPPoA.
- **DNS Server address:** In the PPPoE/PPPoA mode, it is obtained from the uplink equipment. In the bridging mode, there is no DNS server address and you can manually enter the information.

Statistics

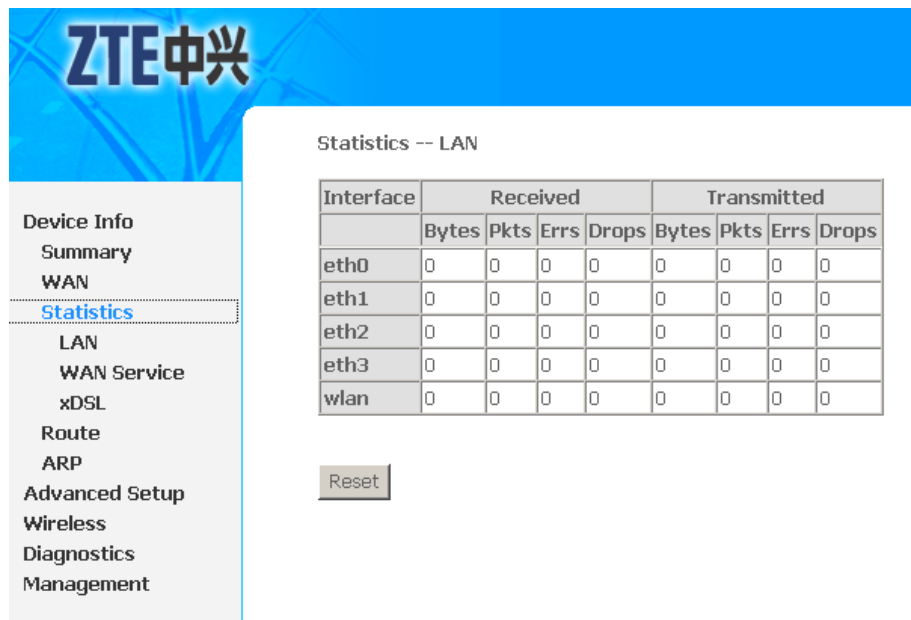
This page includes following three parts:

- LAN statistics
- WAN statistics
- xDSL statistics

LAN Statistics

Click **Device Info > Statistics > LAN** to display the interface as shown in [Figure 10](#).

FIGURE 10 LAN STATISTICS



You can query information of packets received at the Ethernet, and wireless interfaces. Click **Reset** to restore the values to zero and recount them.

The LAN side interface includes Ethernet and wireless device. You can view the following information of each device:

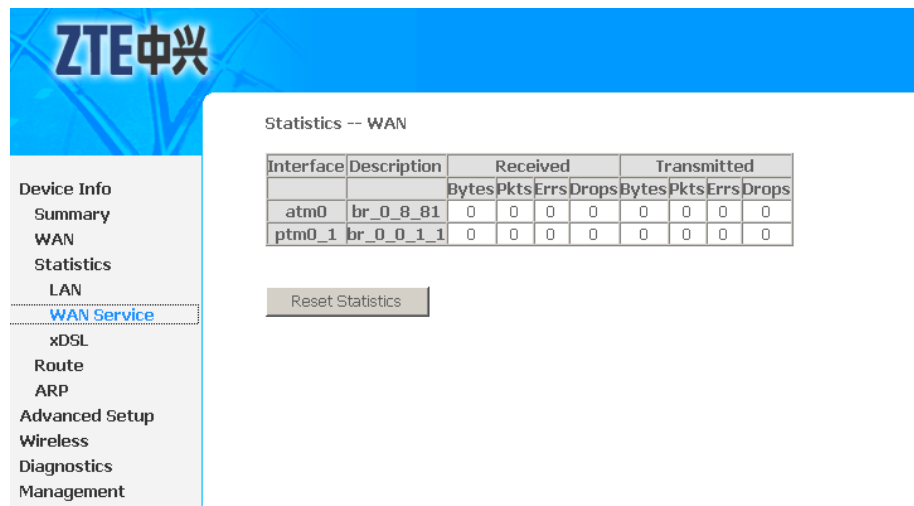
- Interface

- Received
 - ▶ Bytes: received bytes
 - ▶ Pkts: received packets
 - ▶ Errs: errors packets received
 - ▶ Drops: received dropped packets
- Transmitted
 - ▶ Bytes: transmitted bytes
 - ▶ Pkts: transmitted packtes
 - ▶ Errs: error packets transmitted
 - ▶ Drops: dropped packets transmitted

WAN Statistics

Click **Device Info > Statistics > WAN** to display the interface as shown in [Figure 11](#).

FIGURE 11 WAN STATISTICS

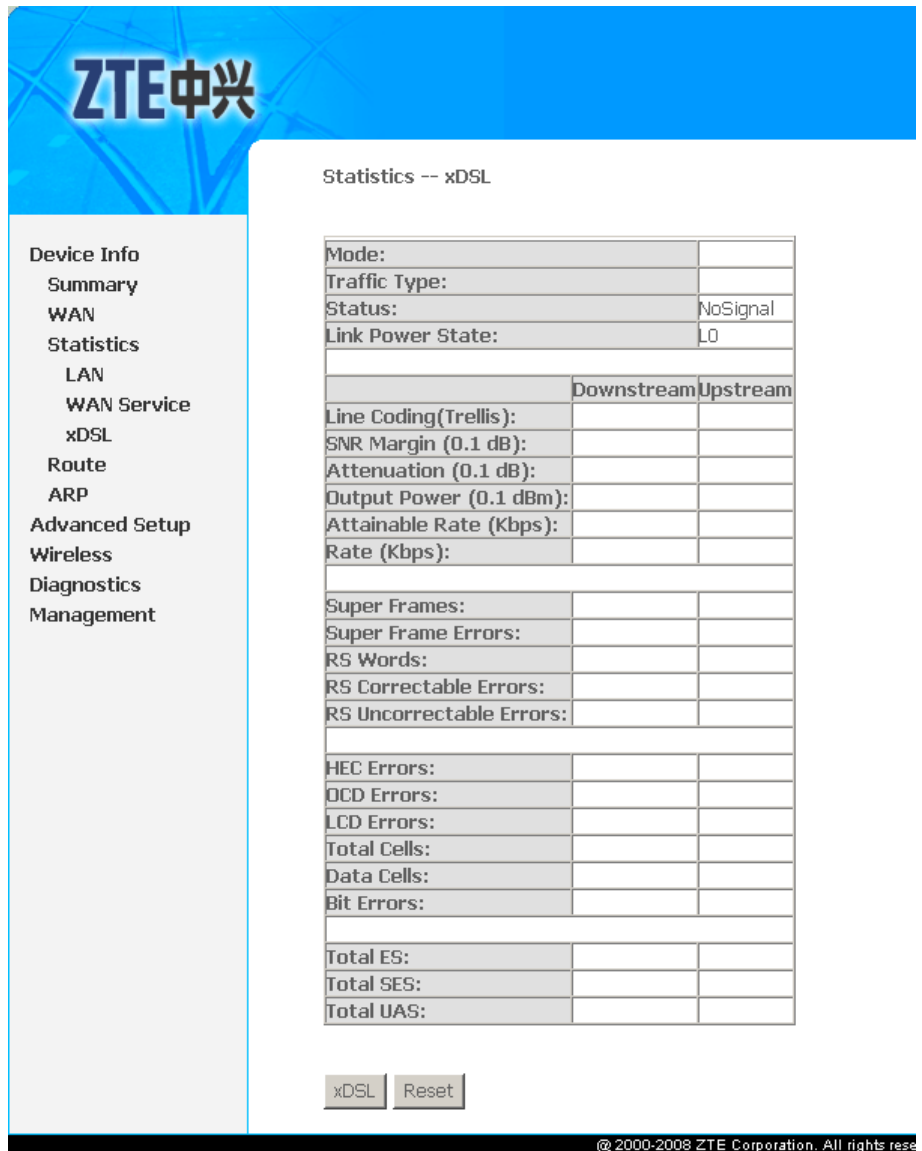


You can query information of packets received at the [WAN](#) interfaces. The WAN side interface includes [ADSL PVC](#) and [VDSL2 PTM](#) interface. Click **Reset Statistics** to restore the values to zero and recount them.

xDSL Statistics

1. Click **Device Info > Statistics > xDSL** to display the interface as shown in [Figure 12](#).

FIGURE 12 xDSL STATISTICS



2. You can query information of packets received at the xDSL interfaces. Click **Reset** to restore the values to zero and recount them.
3. Click **xDSL** to start ADSL BER test. The interface is as shown in [Figure 13](#)

FIGURE 13 ADSL BER TEST



4. Select the test duration in **Test Time(sec)** drop-down menu.
5. Click **Start** to start the ADSL BER test, and the test result is as shown in [Figure 14](#).

FIGURE 14 ADSL BER TEST RESULT



Route Table Information

Click **Device Info > Route** to display the interface as shown in [Figure 15](#).

FIGURE 15 ROUTE TABLE

Device Info -- Route

Flags: U - up, I - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

You can view the following information of each route in the route table:

- Destination
- Gateway
- Subnet Mask
- Flag
- Metric
- Service
- Interface

ARP Table Information

Click **Device Info > ARP** to display the interface as shown in [Figure 16](#).

FIGURE 16 ARP TABLE



The screenshot shows the ZTE web interface. At the top left is the ZTE logo. A navigation menu on the left lists: Device Info, Summary, WAN, Statistics, Route, ARP (highlighted), Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info -- ARP" and contains a table with the following data:

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:1E:90:3F:5B:B5	br0

You can query the MAC and IP address information of the equipment attached to the modem and the information includes the following:

- IP address
- Flags
- HW address
- Device

This page is intentionally blank.

Chapter 5

WAN Interface Configuration

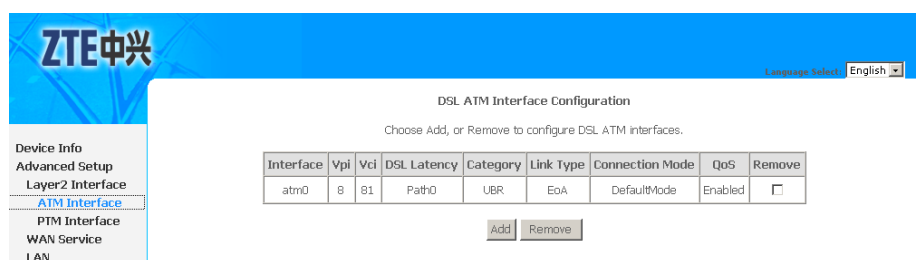
Table of Contents

Configure ADSL EoA PPPoE WAN Connection	31
Configure ADSL EoA IPoE WAN Connection.....	37
Configure ADSL EoA Bridge WAN Connection	43
Configure ADSL PPPoA WAN Connection.....	47
Configure ADSL IPoA WAN Connection.....	53
Configure VDSL2 EoA WAN Connection	58
Configure VDSL2 Bridge WAN Connection	64
Configure VDSL2 IPoE WAN Connection	67

Configure ADSL EoA PPPoE WAN Connection

1. Select **Advanced Setup > Layer2 Interface > ATM Interface** to display the interface as shown in [Figure 17](#).

FIGURE 17 ADSL PVC CONFIGURATION OVERVIEW



By default, system preset **ADSL ATM PVC** is **atm0**, vpi/vci is 8/81.

2. Click **Add** to display the interface as shown in [Figure 18](#).

FIGURE 18 ADDING EOA PVC

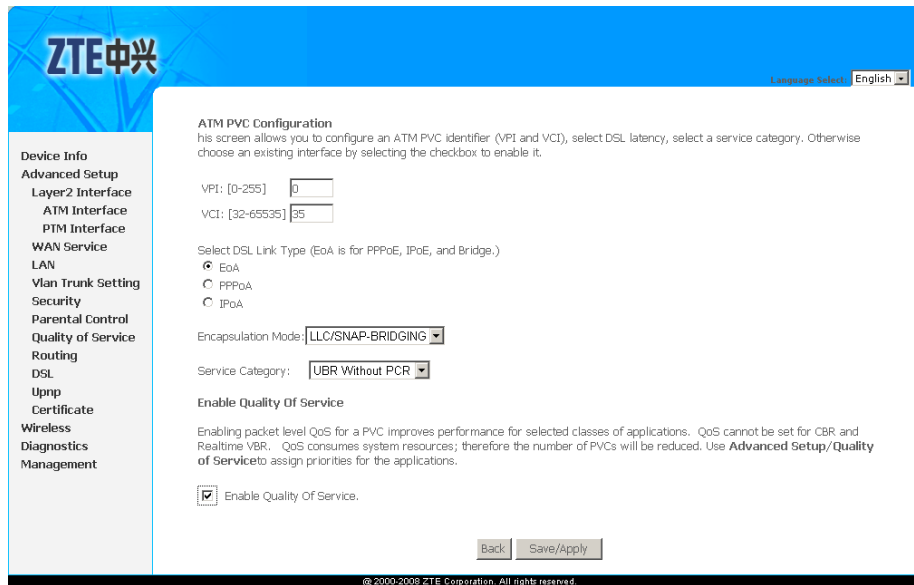


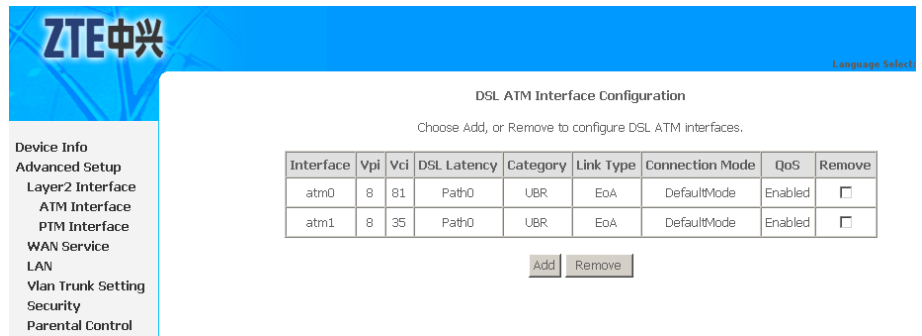
Table 8 is a description of the different options.

TABLE 8 EOA PVC CONFIGURATION OPTIONS

Field	Description
VPI/VCI	Enter VPI and VCI value.
Select DSL Link Type	Select EOA , EoA is for PPPoE, IPoE, and Bridge.
Encapsulation Mode	The value can be LLC/SNAP-BRIDGING, VC/MUX .
Service Category	The value can be UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR .
Enable Quality Of Service	Select the checkbox to enable the QoS function.

3. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 19](#).

FIGURE 19 EOA PVC CONFIGURATION COMPLETED



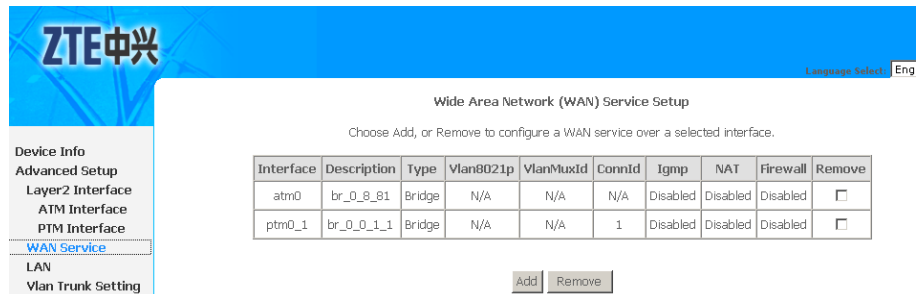
- To delete the ATM PVC, select the **Remove** check box in the table and click **Remove** to apply the settings.

Note:

If the ATM PVC is used to be WAN interface, you need to remove the ATM PVC from WAN interface.

- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 20](#).

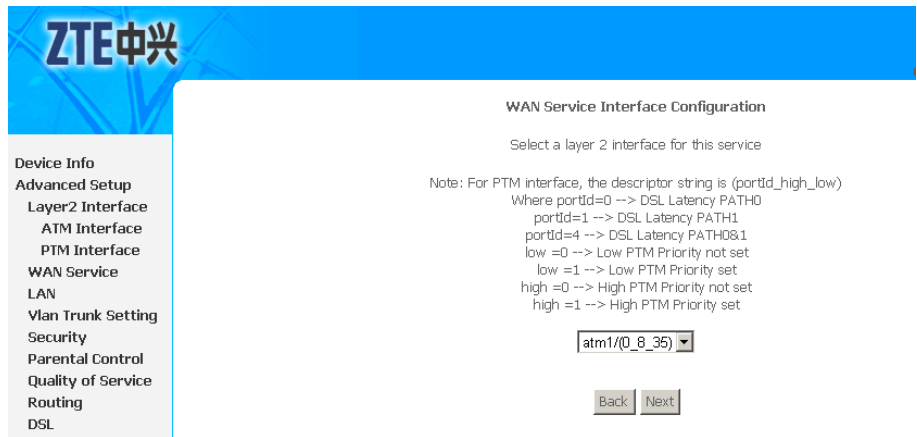
FIGURE 20 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

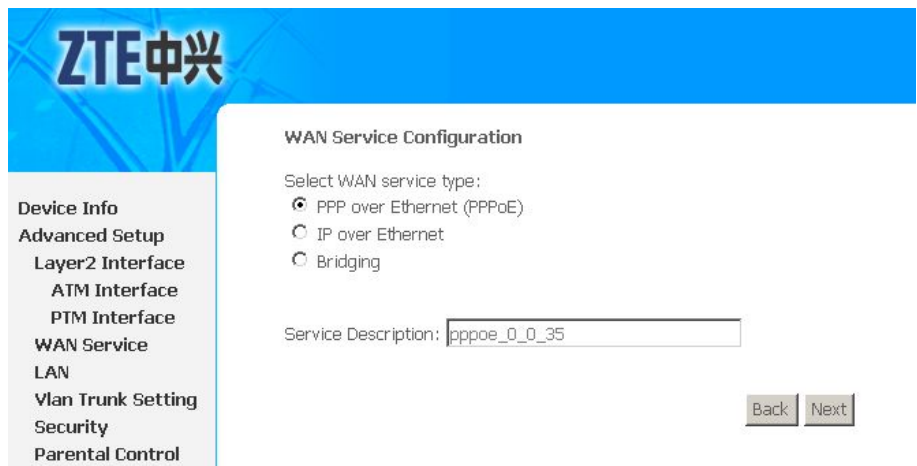
- Click **Add** to display the interface as shown in [Figure 21](#), and select the Layer 2 interface.

FIGURE 21 SELECT LAYER2 INTERFACE



7. Click **Next** to enter the interface as shown in [Figure 22](#).

FIGURE 22 SELECT WAN SERVICE TYPE



8. Select **PPP over Ethernet (PPPoE)**.
9. Click **Next** to enter the interface as shown in [Figure 23](#).

FIGURE 23 PPPoE CONFIGURATION

PPP Username and Password

PPP usually requires that you have a user name and password to establish your connection. In the boxes below, enter the user name and password that your ISP has provided to you.

PPP Username:

PPP Password:

PPPoE Service Name:

Authentication Method:

PPP IP extension

Enable NAT

Use Static IPv4 Address

IGMP Multicast

Enable IGMP Multicast

[Back](#) [Next](#)

[Table 9](#) is a description of the different options.

TABLE 9 PPPoE CONFIGURATION OPTIONS

Field	Description
PPP Username	The user name that your ISP provides to you.
PPP Password	The password that your ISP provides to you.
PPPoE Service Name	If your ISP provides it to you, enter it. If not, do not enter any information.
Authentication Method	The value can be AUTO , PAP , CHAP , or MSCHAP . Usually, you can select AUTO .
Enable NAT	Select it to enable the NAT functions of the modem. If you do not want to enable NAT and wish the modem user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.
Use Static IPv4 Address	The static IP address that your ISP provides to you.
Enable IGMP Multicast	IGMP proxy. For example, if you want the PPPoE mode to support IPTV, enable this function.

10. Click **Next** to enter the interface as shown in [Figure 24](#).

FIGURE 24 DEFAULT GATEWAY CONFIGURATION

The screenshot shows the ZTE web interface for the 'Default Gateway' configuration. The page title is 'Routing -- Default Gateway'. Below the title, there is a instruction: 'Select a preferred wan interface as the system default gateway.' A dropdown menu labeled 'Selected WAN Interface' is set to 'pppoe_0_8_35/ppp0'. On the right side, there are 'Back' and 'Next' buttons. On the left side, there is a navigation menu with the following items: Device Info, Advanced Setup (selected), Layer2 Interface, ATM Interface, PTM Interface, WAN Service, LAN, Vlan Trunk Setting, Security, Parental Control, Quality of Service, and Routing.

11. Click **Next** to enter the interface as shown in [Figure 25](#).

FIGURE 25 DNS CONFIGURATION

The screenshot shows the ZTE web interface for the 'DNS Server Configuration' page. The page title is 'DNS Server Configuration'. Below the title, there is a instruction: 'Get DNS server information from the selected WAN interface OR enter static DNS server IP addresses. If only a single PVC with IPoA or static MER protocol is configured, you must enter static DNS server IP addresses.' There are two radio button options: 'Obtain DNS info from a WAN interface:' (selected) and 'Use the following Static DNS IP address:'. Under the selected option, there is a dropdown menu labeled 'WAN Interface selected:' set to 'pppoe_0_8_35/ppp0'. Under the unselected option, there are two input fields for 'Primary DNS server:' and 'Secondary DNS server:'. On the right side, there is a 'Language Select: En' button. On the left side, there is a navigation menu with the following items: Device Info, Advanced Setup (selected), Layer2 Interface, ATM Interface, PTM Interface, WAN Service, LAN, Vlan Trunk Setting, Security, Parental Control, and Quality of Service.

If **Obtain DNS info from a WAN interface** is selected, device accepts the first received DNS assignment from WAN connection.

If **Use the following Static DNS IP address** is selected, enter the **Primary DNS server** and **Secondary DNS server**.

12. Click **Next** to enter the interface as shown in [Figure 26](#).

FIGURE 26 EOA PPPoE WAN CONNECTION SETUP SUMMARY

ZTE中兴

WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
Service Name:	pppoe_0_8_35
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Enabled
Quality Of Service:	Enabled

Click Apply/Save to have this interface to be effective. Click Back to make any modifications.

[Back](#) [Save/Apply](#)

- Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 27](#).

FIGURE 27 EOA PPPoE WAN CONNECTION CONFIGURATION COMPLETED

ZTE中兴

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
atm0	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>
ppp0	pppoe_0_8_35	PPPoE	N/A	N/A	N/A	Enabled	Enabled	Enabled	<input type="checkbox"/>
ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	<input type="checkbox"/>

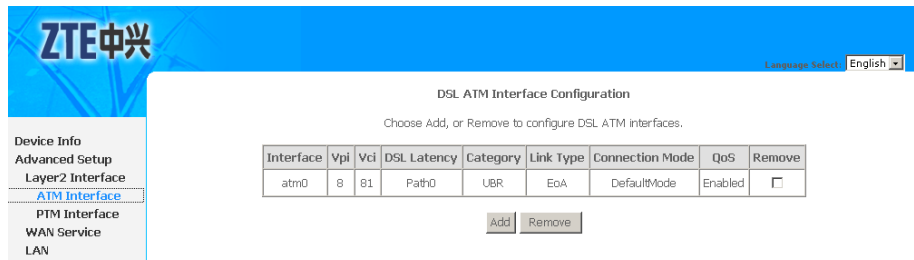
[Add](#) [Remove](#)

- To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

Configure ADSL EoA IPoE WAN Connection

- Select **Advanced Setup > Layer2 Interface > ATM Interface** to display the interface as shown in [Figure 28](#).

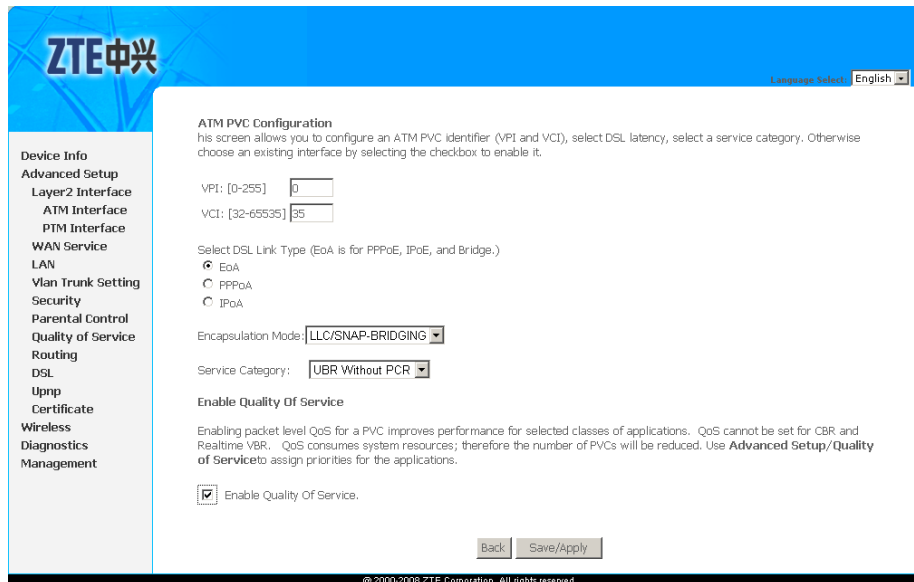
FIGURE 28 ADSL PVC CONFIGURATION OVERVIEW



By default, system preset ADSL ATM PVC is **atm0**, vpi/vci is 8/81.

2. Click **Add** to display the interface as shown in [Figure 29](#).

FIGURE 29 ADDING EOA PVC



[Table 10](#) is a description of the different options.

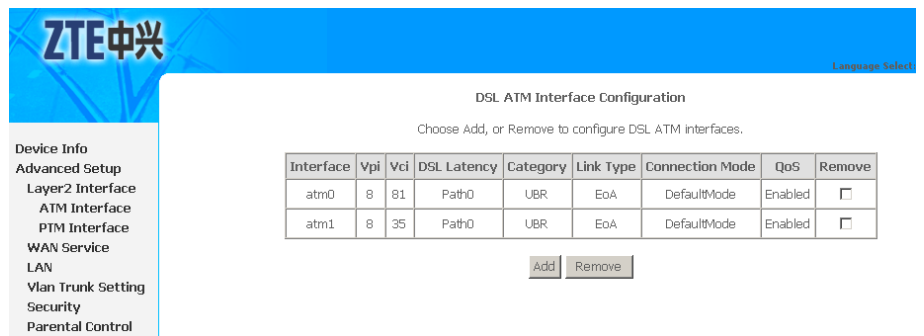
TABLE 10 EOA PVC CONFIGURATION OPTIONS

Field	Description
VPI/VCI	Enter VPI and VCI value.
Select DSL Link Type	Select EOA , EoA is for PPPoE, IPoE, and Bridge.
Encapsulation Mode	The value can be LLC/SNAP-BRIDGING, VC/MUX.
Service Category	The value can be UBR Without PCR, UBR With PCR, CBR,

Field	Description
	Non Realtime VBR, Realtime VBR.
Enable Quality Of Service	Select the checkbox to enable the QoS function.

- Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 30](#).

FIGURE 30 EOA PVC CONFIGURATION COMPLETED



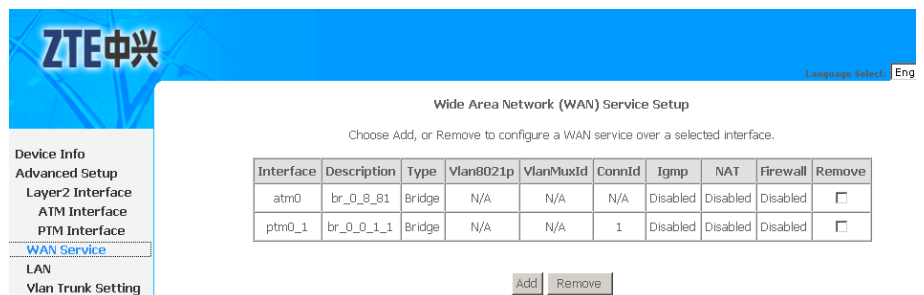
- To delete the ATM PVC, select the **Remove** check box in the table and click **Remove** to apply the settings.

Note:

If the ATM PVC is used to be WAN interface, you need to remove the ATM PVC from WAN interface.

- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 31](#).

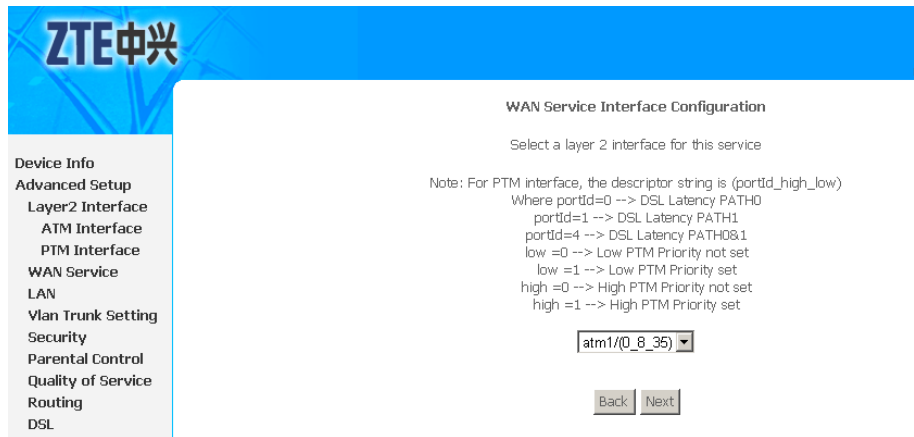
FIGURE 31 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

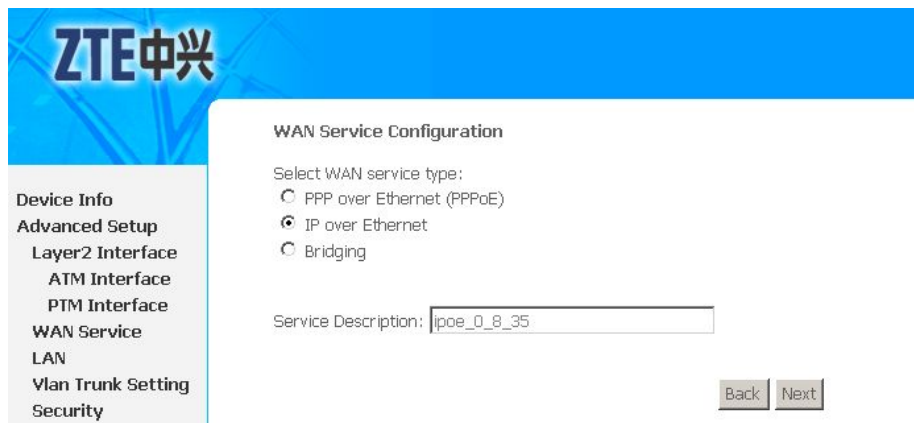
- Click **Add** to display the interface as shown in [Figure 32](#), and select the Layer 2 interface.

FIGURE 32 SELECT LAYER2 INTERFACE



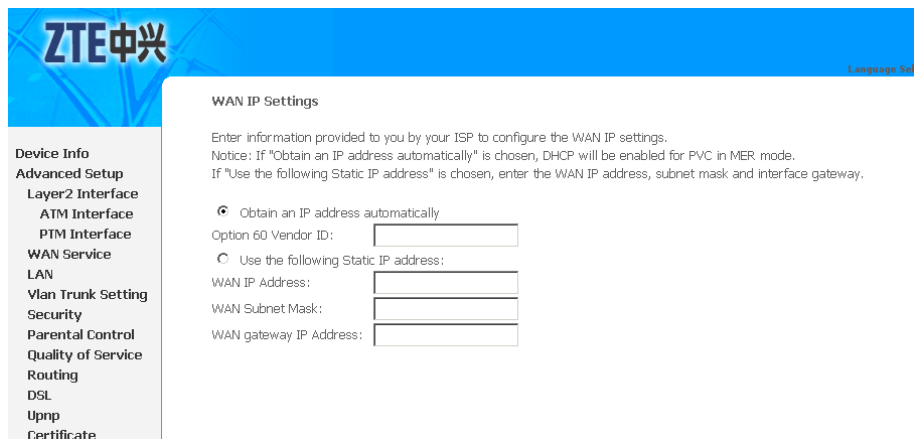
7. Click **Next** to enter the interface as shown in [Figure 33](#).

FIGURE 33 SELECT WAN SERVICE TYPE



8. Select **IP over Ethernet**.
9. Click **Next** to enter the interface as shown in [Figure 34](#).

FIGURE 34 WAN IP CONFIGURATION

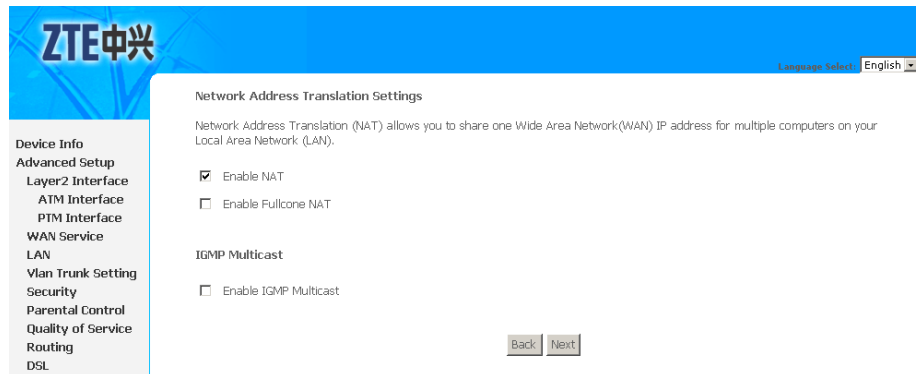


If **Obtain an IP address automatically** is selected, input the **Option 60 Vendor ID**.

If **Use the following Static IP address** is selected, enter the **WAN IP Address, WAN Subnet Mask** and **WAN gateway IP Address**.

10. Click **Next** to enter the interface as shown in [Figure 35](#).

FIGURE 35 NAT CONFIGURATION



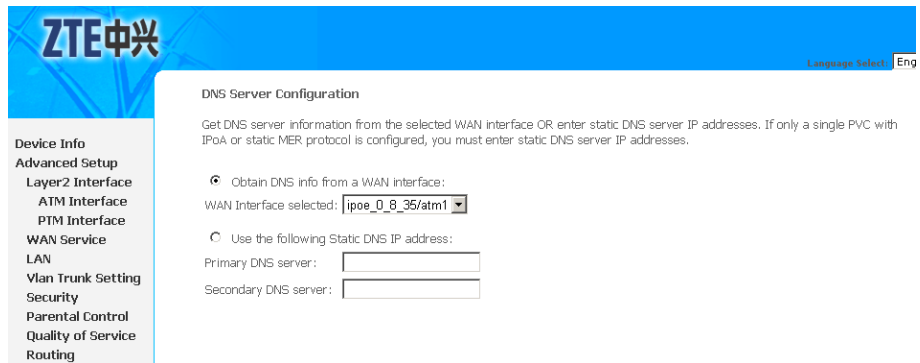
11. Click **Next** to enter the interface as shown in [Figure 36](#).

FIGURE 36 DEFAULT GATEWAY CONFIGURATION



12. Click **Next** to enter the interface as shown in [Figure 37](#).

FIGURE 37 DNS CONFIGURATION

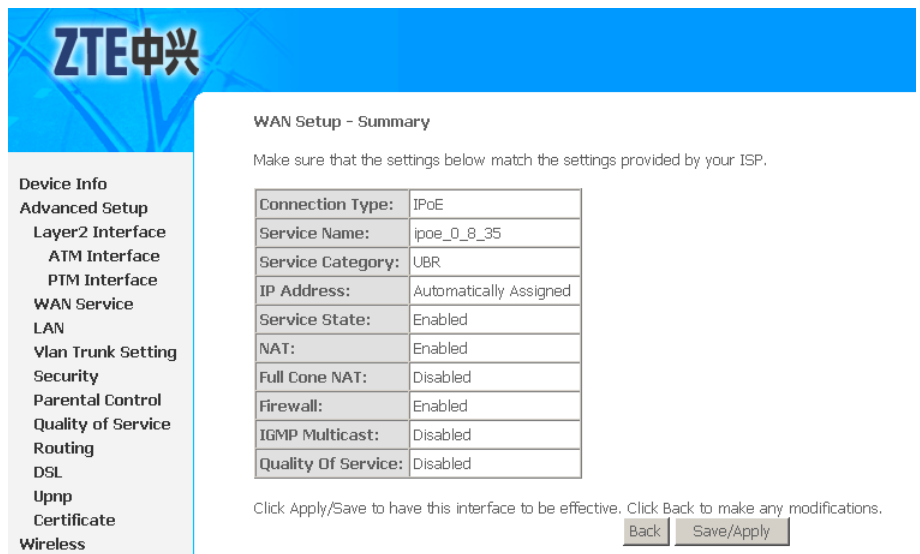


If **Obtain DNS info from a WAN interface** is selected, device accepts the first received DNS assignment from WAN connection.

If **Use the following Static DNS IP address** is selected, enter the **Primary DNS server** and **Secondary DNS server**.

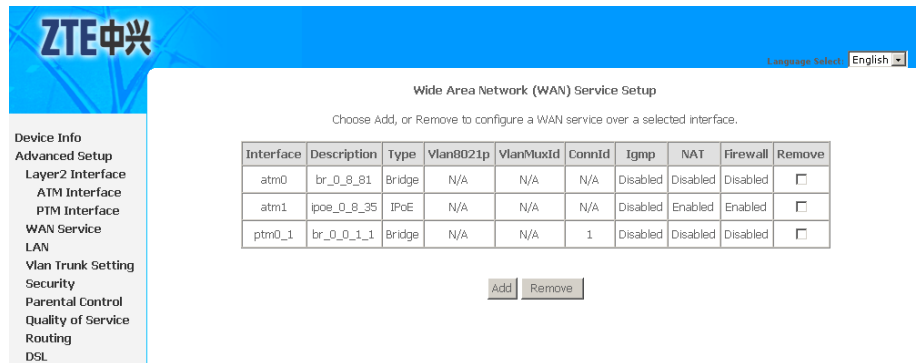
13. Click **Next** to enter the interface as shown in [Figure 38](#).

FIGURE 38 EOA IPoE WAN CONNECTION SETUP SUMMARY



14. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 39](#).

FIGURE 39 EOA IPoE WAN CONNECTION CONFIGURATION COMPLETED

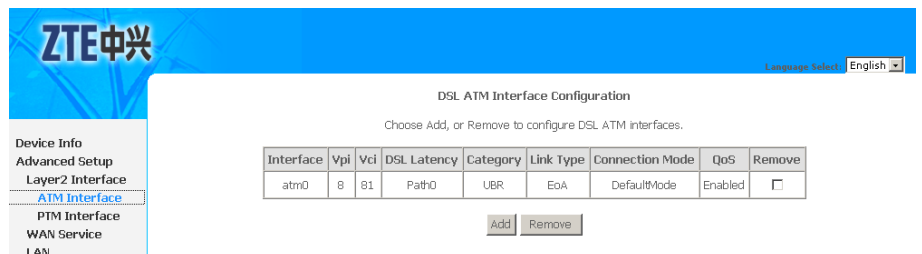


- To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

Configure ADSL EoA Bridge WAN Connection

- Select **Advanced Setup > Layer2 Interface > ATM Interface** to display the interface as shown in [Figure 40](#).

FIGURE 40 ADSL PVC CONFIGURATION OVERVIEW



By default, system preset **ADSL ATM PVC** is **atm0**, vpi/vci is 8/81.

- Click **Add** to display the interface as shown in [Figure 41](#).

FIGURE 41 ADDING EOA PVC

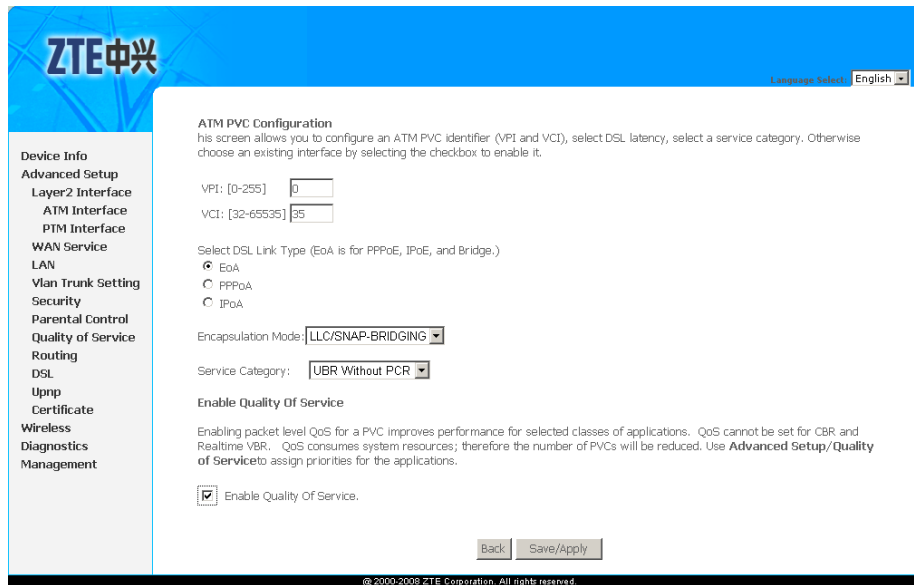


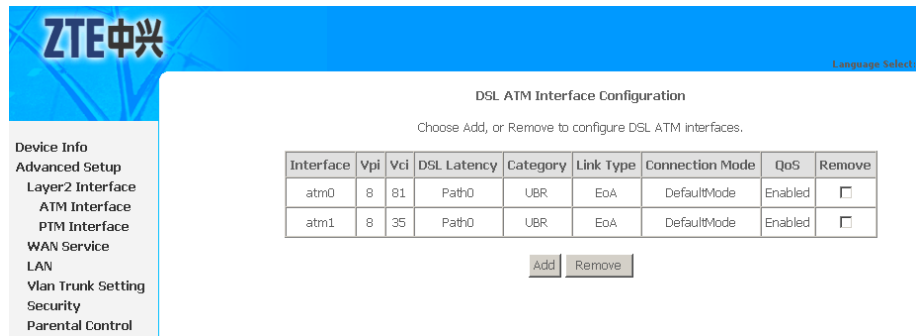
Table 11 is a description of the different options.

TABLE 11 EOA PVC CONFIGURATION OPTIONS

Field	Description
VPI/VCI	Enter VPI and VCI value.
Select DSL Link Type	Select EOA , EoA is for PPPoE, IPoE, and Bridge.
Encapsulation Mode	The value can be LLC/SNAP-BRIDGING, VC/MUX .
Service Category	The value can be UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR .
Enable Quality Of Service	Select the checkbox to enable the QoS function.

3. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 42](#).

FIGURE 42 EOA PVC CONFIGURATION COMPLETED



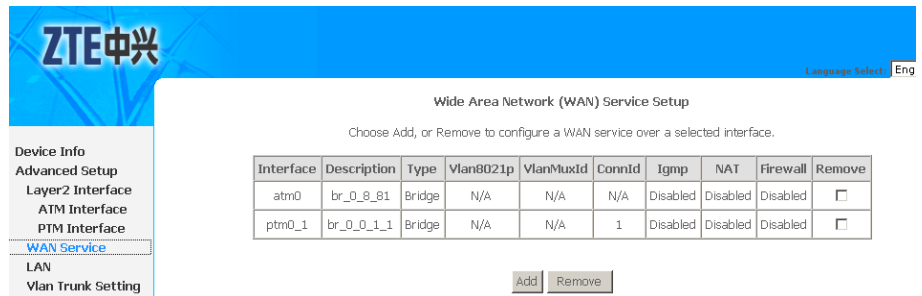
- To delete the ATM PVC, select the **Remove** check box in the table and click **Remove** to apply the settings.

**Note:**

If the ATM PVC is used to be WAN interface, you need to remove the ATM PVC from WAN interface.

- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 43](#).

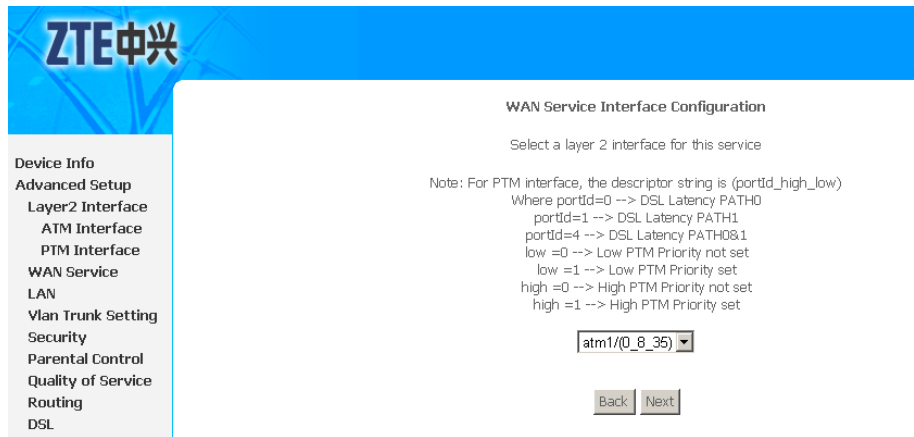
FIGURE 43 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

- Click **Add** to display the interface as shown in [Figure 44](#), and select the Layer 2 interface.

FIGURE 44 SELECT LAYER2 INTERFACE



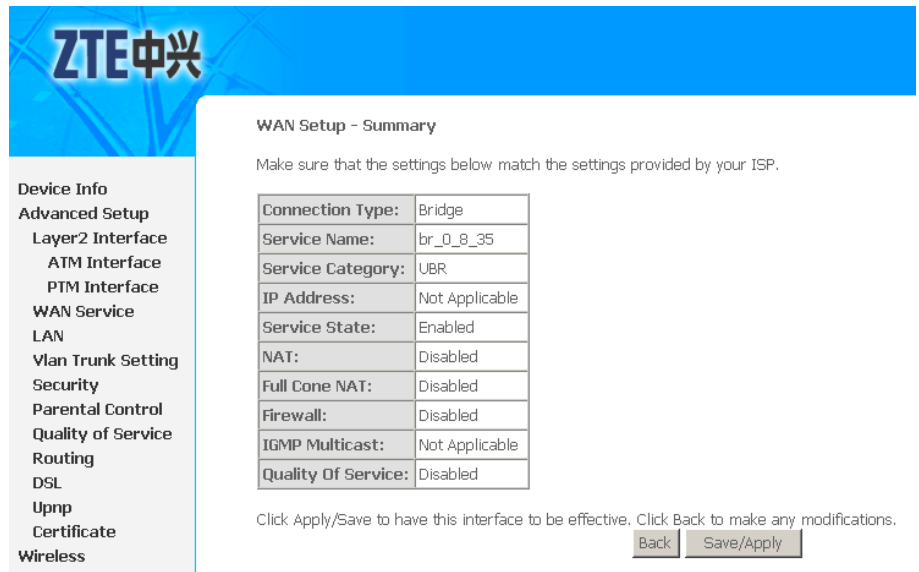
7. Click **Next** to enter the interface as shown in [Figure 45](#).

FIGURE 45 SELECT WAN SERVICE TYPE



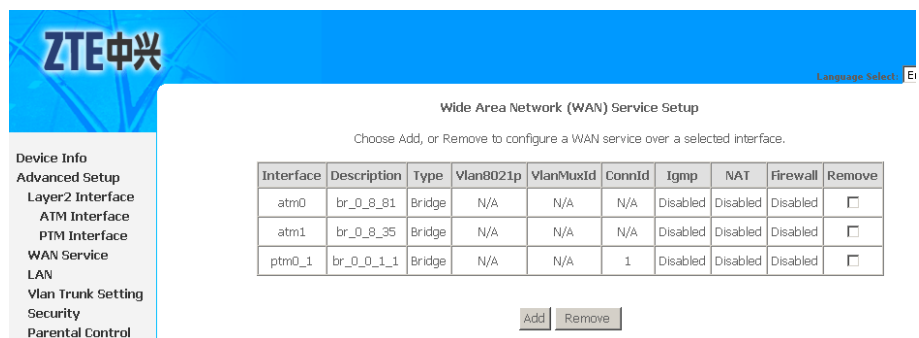
8. Select **Bridging** .
9. Click **Next** to enter the interface as shown in [Figure 46](#).

FIGURE 46 EOA BRIDGE WAN CONNECTION SETUP SUMMARY



10. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 47](#).

FIGURE 47 EOA BRIDGE WAN CONNECTION CONFIGURATION COMPLETED

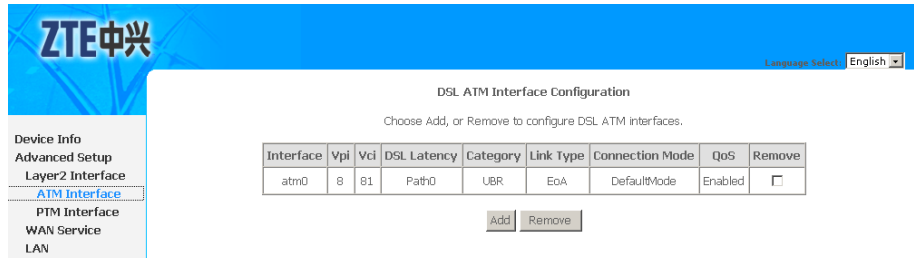


11. To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

Configure ADSL PPPoA WAN Connection

1. Select **Advanced Setup > Layer2 Interface > ATM Interface** to display the interface as shown in [Figure 48](#).

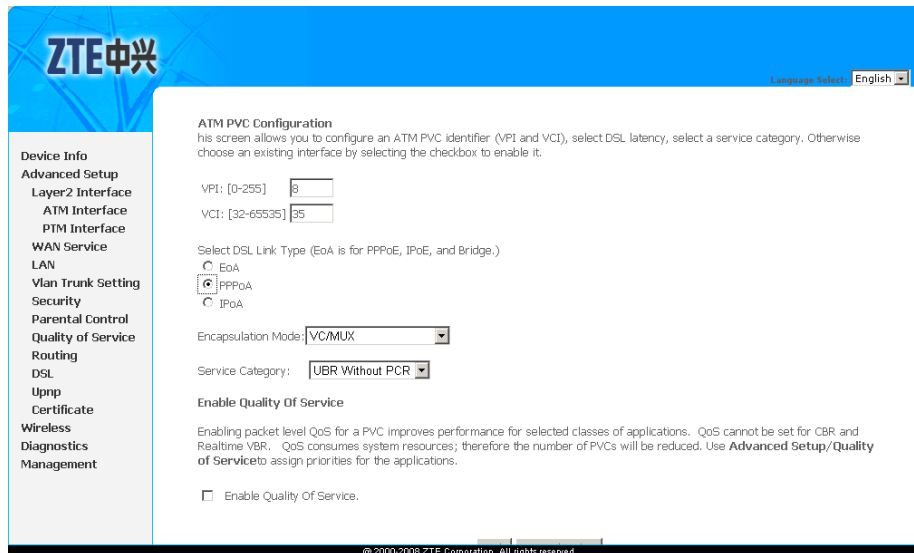
FIGURE 48 ADSL PVC CONFIGURATION OVERVIEW



By default, system preset **ADSL ATM PVC** is **atm0**, vpi/vci is 8/81.

- To add **PPPoA** PVC, click **Add** to display the interface as shown in [Figure 49](#).

FIGURE 49 ADDING PPPoA PVC



[Table 12](#) is a description of the different options.

TABLE 12 PPPoA PVC CONFIGURATION OPTIONS

Field	Description
VPI/VCI	Enter VPI and VCI value.
Select DSL Link Type	Select PPPoA .
Encapsulation Mode	The value can be LLC/SNAP-BRIDGING, VC/MUX .
Service Category	The value can be UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR .
Enable Quality Of Service	Select the checkbox to enable the QoS function.

- Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 50](#).

FIGURE 50 PPPoA PVC CONFIGURATION COMPLETED

The screenshot shows the 'DSL ATM Interface Configuration' page. On the left is a navigation menu with 'WAN Service' selected. The main area contains a table of DSL ATM interfaces. Below the table are 'Add' and 'Remove' buttons.

Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
atm0	8	81	Path0	UBR	EoA	DefaultMode	Enabled	<input type="checkbox"/>
atm1	8	35	Path0	UBR	PPPoA	DefaultMode	Disabled	<input checked="" type="checkbox"/>

- To delete the ATM PVC, select the **Remove** check box in the table and click **Remove** to apply the settings.



Note:

If the ATM PVC is used to be WAN interface, you need to remove the ATM PVC from WAN interface.

- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 51](#).

FIGURE 51 WAN SERVICE OVERVIEW

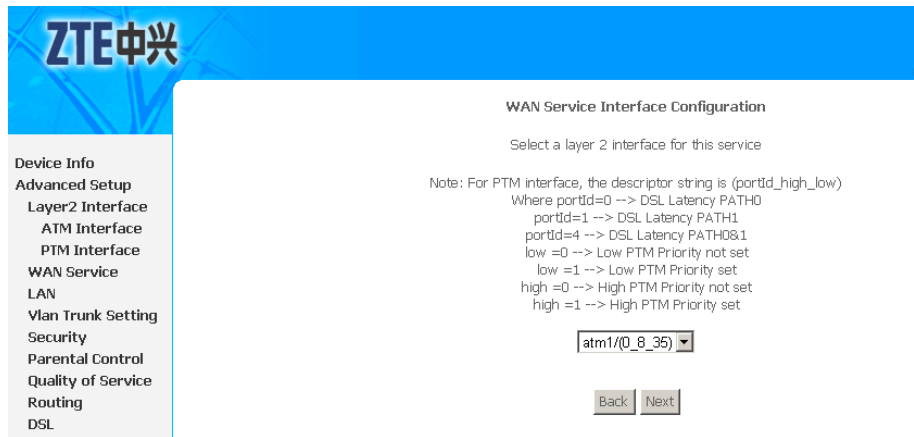
The screenshot shows the 'Wide Area Network (WAN) Service Setup' page. On the left is a navigation menu with 'WAN Service' selected. The main area contains a table of WAN services. Below the table are 'Add' and 'Remove' buttons.

Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
atm0	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	<input type="checkbox"/>
ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	<input type="checkbox"/>

By default, system preset WAN Interface is **atm0** and **ptm0_1**.

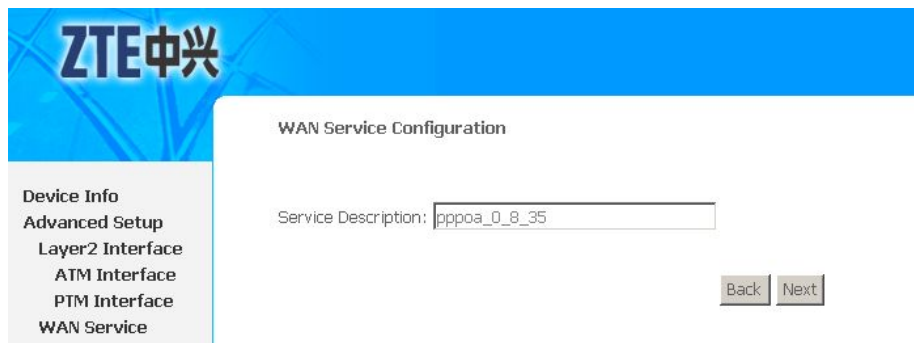
- Click **Add** to display the interface as shown in [Figure 52](#), and select the Layer 2 interface.

FIGURE 52 SELECT LAYER2 INTERFACE



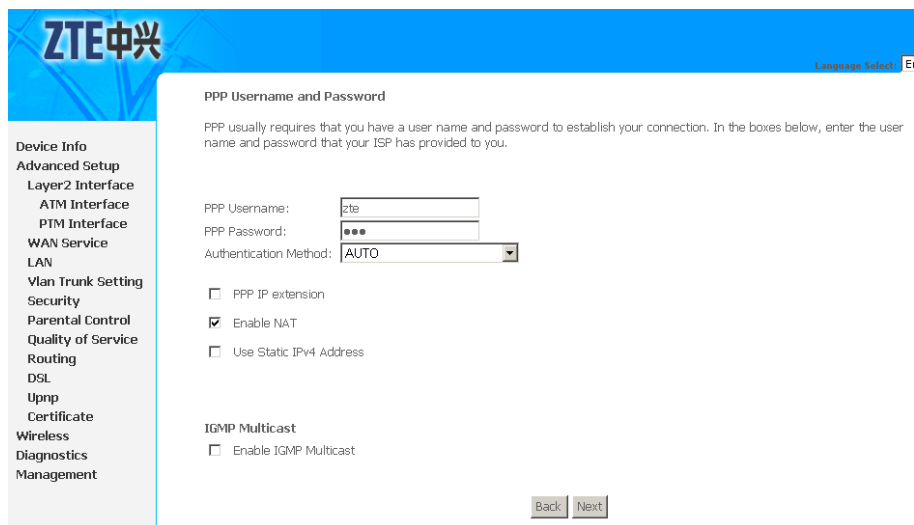
7. Click **Next** to enter the interface as shown in [Figure 53](#).

FIGURE 53 WAN SERVICE CONFIGURATION



8. Click **Next** to enter the interface as shown in [Figure 54](#).

FIGURE 54 PPPoA CONFIGURATION



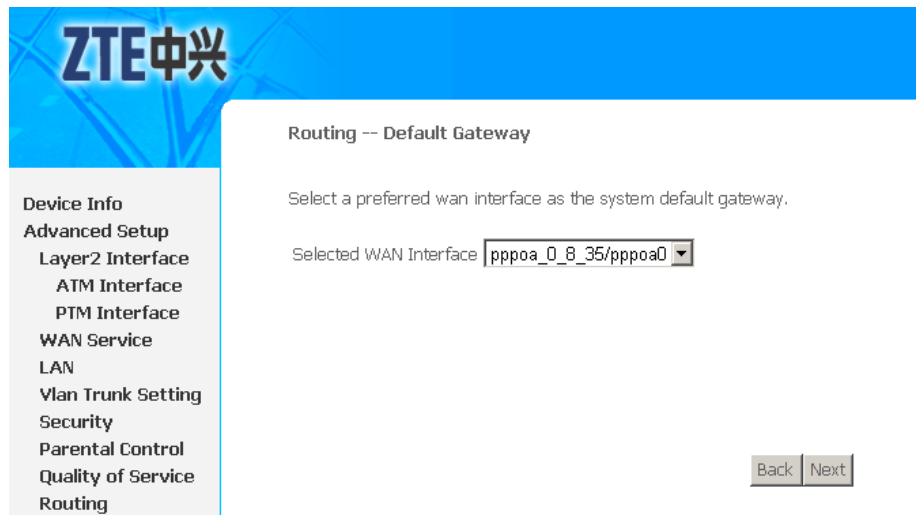
[Table 13](#) is a description of the different options.

TABLE 13 PPPoA CONFIGURATION OPTIONS

Field	Description
PPP Username	The user name that your ISP provides to you.
PPP Password	The password that your ISP provides to you.
Authentication Method	The value can be AUTO , PAP , CHAP , or MSCHAP . Usually, you can select AUTO .
Enable NAT	Select it to enable the NAT functions of the modem. If you do not want to enable NAT and wish the modem user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.
Use Static IPv4 Address	The static IP address that your ISP provides to you.
Enable IGMP Multicast	IGMP proxy. For example, if you want the PPPoE mode to support IPTV, enable this function.

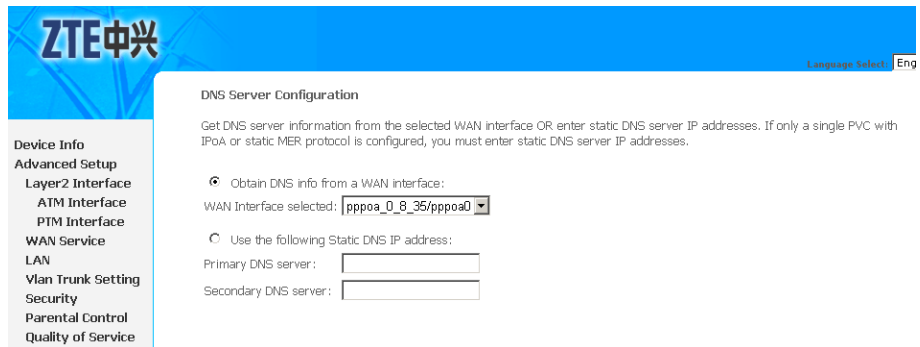
9. Click **Next** to enter the interface as shown in [Figure 55](#).

FIGURE 55 DEFAULT GATEWAY CONFIGURATION



10. Click **Next** to enter the interface as shown in [Figure 56](#).

FIGURE 56 DNS CONFIGURATION

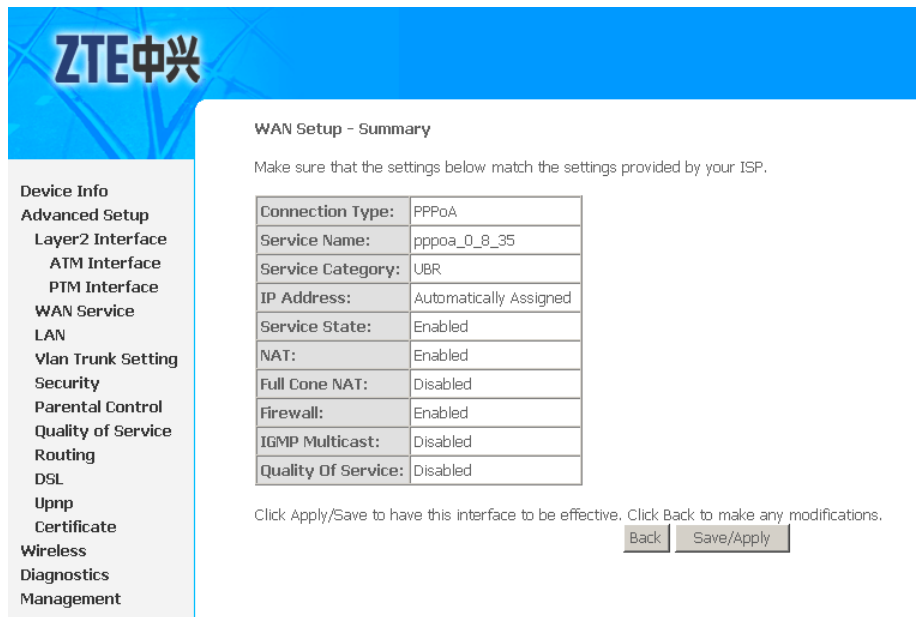


If **Obtain DNS info from a WAN interface** is selected, device accepts the first received DNS assignment from WAN connection.

If **Use the following Static DNS IP address** is selected, enter the **Primary DNS server** and **Secondary DNS server**.

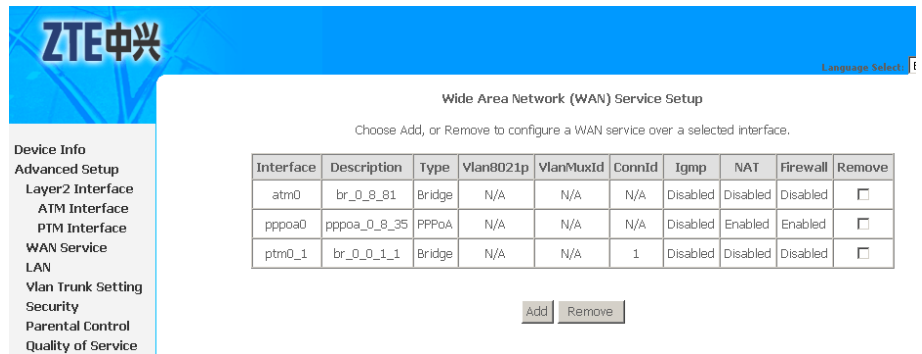
11. Click **Next** to enter the interface as shown in [Figure 57](#).

FIGURE 57 PPPoA WAN CONNECTION SETUP SUMMARY



12. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 58](#).

FIGURE 58 PPPoA WAN CONNECTION CONFIGURATION COMPLETED

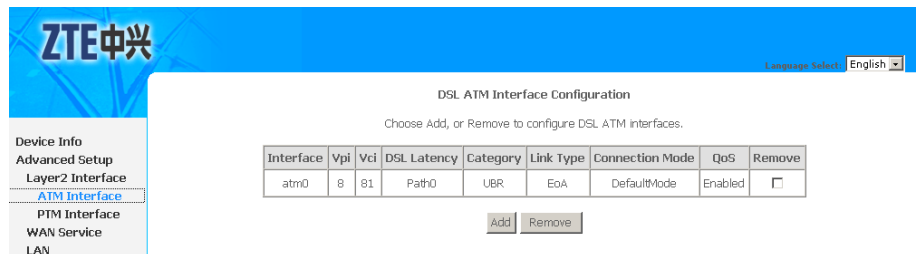


13. To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

Configure ADSL IPoA WAN Connection

1. Select **Advanced Setup > Layer2 Interface > ATM Interface** to display the interface as shown in [Figure 59](#).

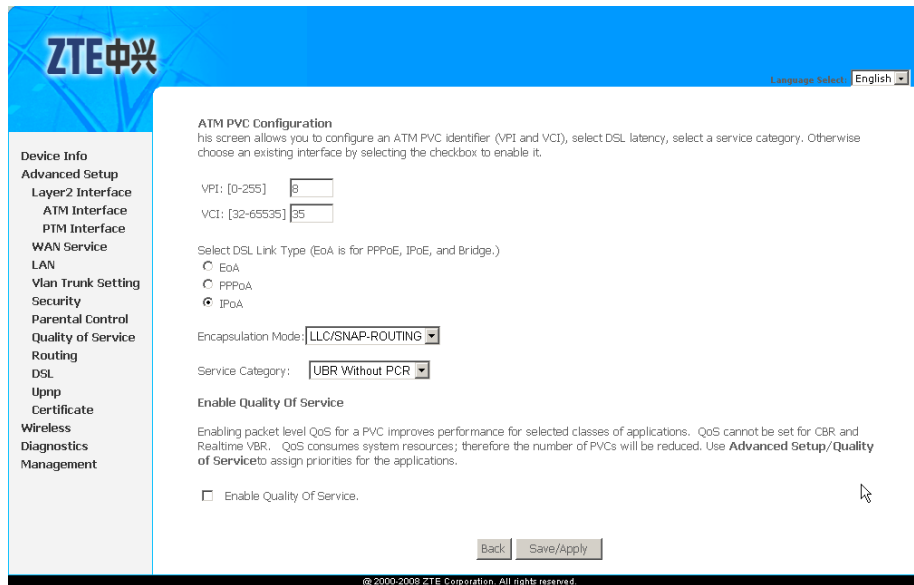
FIGURE 59 ADSL PVC CONFIGURATION OVERVIEW



By default, system preset **ADSL ATM PVC** is **atm0**, vpi/vci is 8/81.

2. To add **IPoA** PVC, click **Add** to display the interface as shown in [Figure 60](#).

FIGURE 60 ADDING IPoA PVC



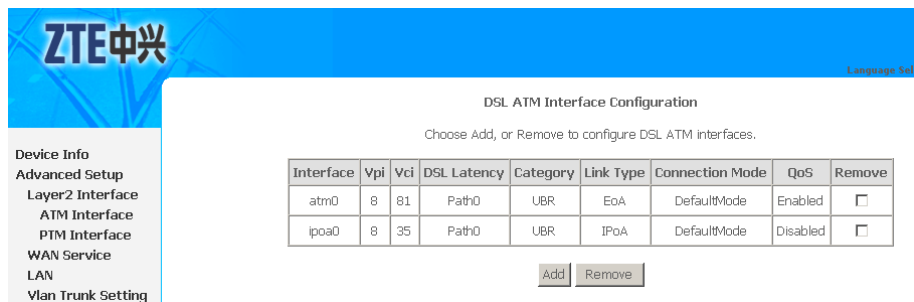
[Table 14](#) is a description of the different options.

TABLE 14 IPoA PVC CONFIGURATION OPTIONS

Field	Description
VPI/VCI	Enter VPI and VCI value.
Select DSL Link Type	Select IPoA .
Encapsulation Mode	The value can be LLC/SNAP-BRIDGING, VC/MUX .
Service Category	The value can be UBR Without PCR, UBR With PCR, CBR, Non Realtime VBR, Realtime VBR .
Enable Quality Of Service	Select the checkbox to enable the QoS function.

- Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 61](#).

FIGURE 61 IPoA PVC CONFIGURATION COMPLETED



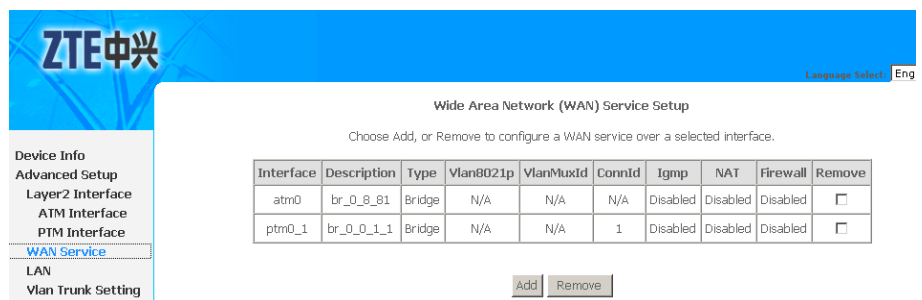
- To delete the ATM PVC, select the **Remove** check box in the table and click **Remove** to apply the settings.

Note:

If the ATM PVC is used to be WAN interface, you need to remove the ATM PVC from WAN interface.

- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 62](#).

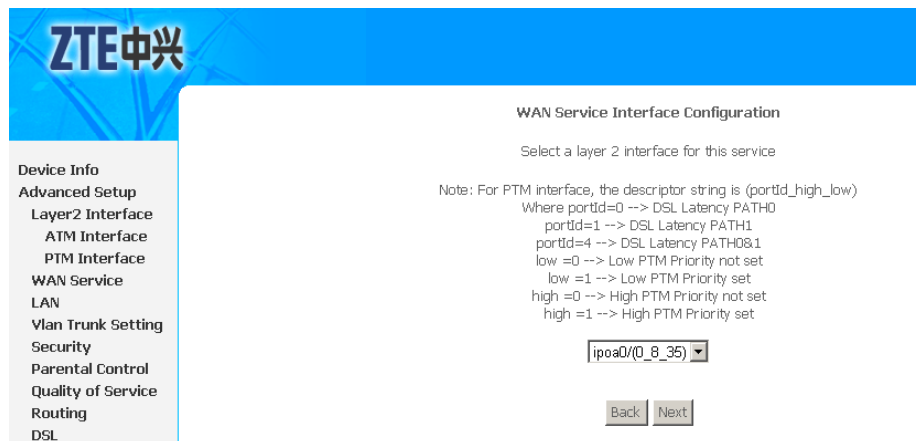
FIGURE 62 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

- Click **Add** to display the interface as shown in [Figure 63](#), and select the Layer 2 interface.

FIGURE 63 SELECT LAYER2 INTERFACE



- Click **Next** to enter the interface as shown in [Figure 64](#).

FIGURE 64 WAN SERVICE CONFIGURATION

ZTE中兴

WAN Service Configuration

Service Description:

Back Next

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
WAN Service
LAN
Vlan Trunk Setting

8. Click **Next** to enter the interface as shown in [Figure 65](#).

FIGURE 65 WAN IP CONFIGURATION

ZTE中兴

WAN IP Settings

Enter information provided to you by your ISP to configure the WAN IP settings.

WAN IP Address:

WAN Subnet Mask:

Back Next

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
WAN Service
LAN

9. Click **Next** to enter the interface as shown in [Figure 66](#).

FIGURE 66 NAT CONFIGURATION

ZTE中兴 Language Selected: English

Network Address Translation Settings

Network Address Translation (NAT) allows you to share one Wide Area Network(WAN) IP address for multiple computers on your Local Area Network (LAN).

Enable NAT
 Enable Fullcone NAT

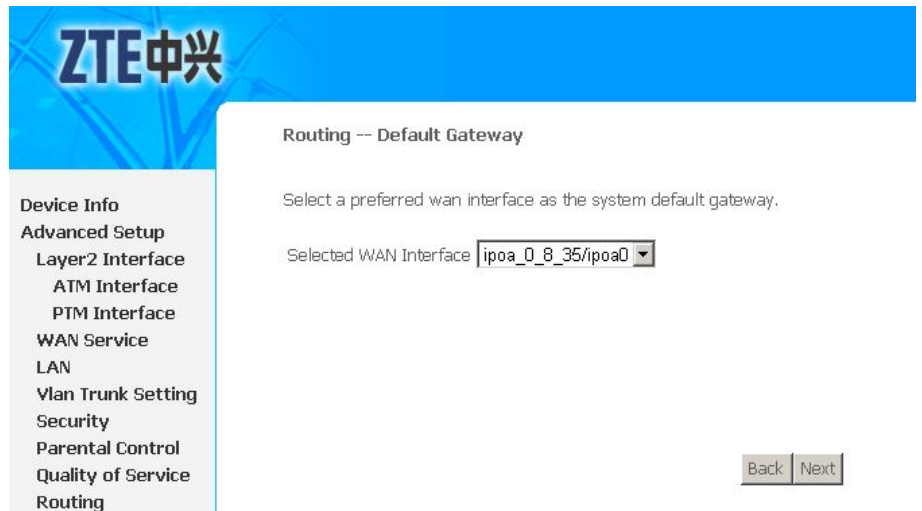
IGMP Multicast
 Enable IGMP Multicast

Back Next

Device Info
Advanced Setup
Layer2 Interface
ATM Interface
PTM Interface
WAN Service
LAN
Vlan Trunk Setting
Security
Parental Control
Quality of Service
Routing
DSL

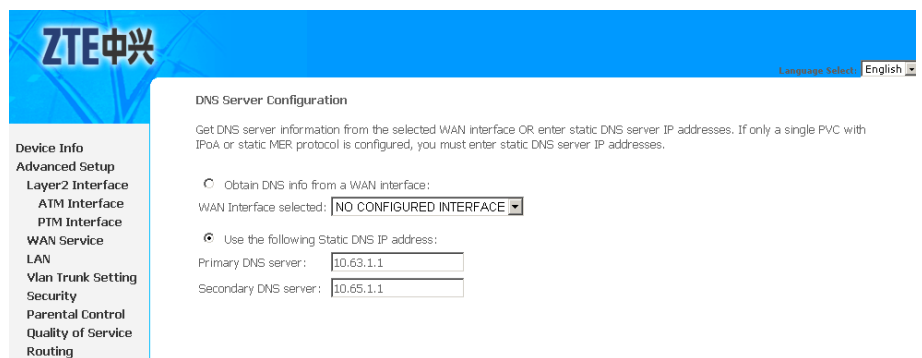
10. Click **Next** to enter the interface as shown in [Figure 67](#).

FIGURE 67 DEFAULT GATEWAY CONFIGURATION



11. Click **Next** to enter the interface as shown in [Figure 68](#).

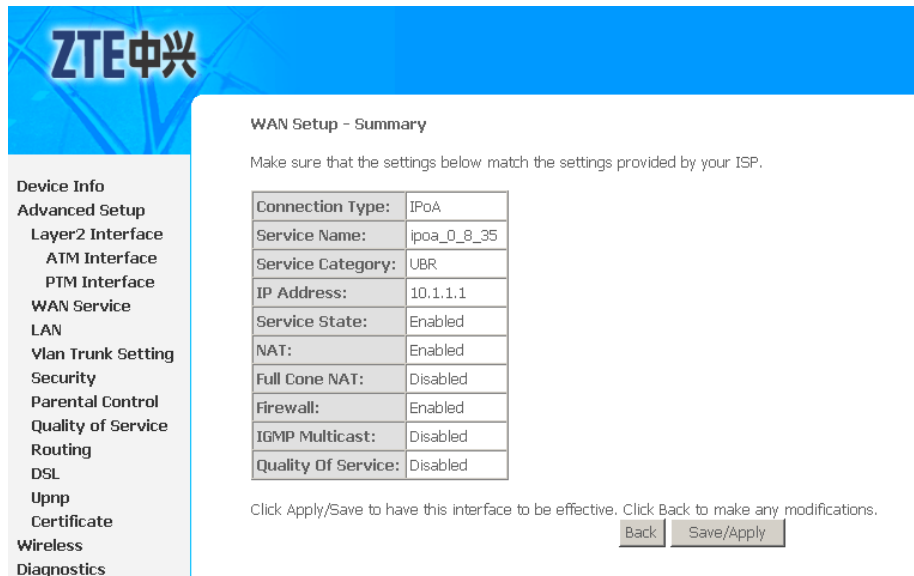
FIGURE 68 DNS CONFIGURATION



You must select the **Use the following Static DNS IP address** and enter the **Primary DNS server** and **Secondary DNS server**.

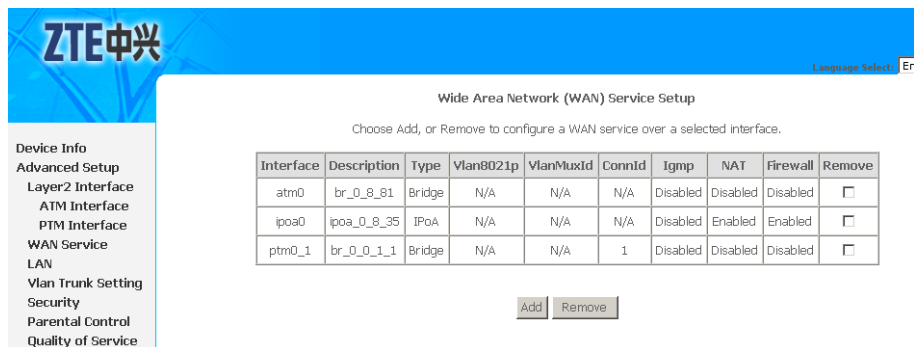
12. Click **Next** to enter the interface as shown in [Figure 69](#).

FIGURE 69 IPoA WAN CONNECTION SETUP SUMMARY



- Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 70](#).

FIGURE 70 IPoA WAN CONNECTION CONFIGURATION COMPLETED

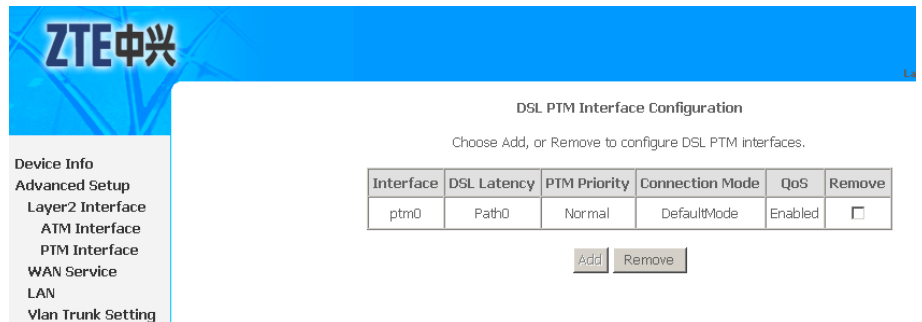


- To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

Configure VDSL2 EoA WAN Connection

- Select **Advanced Setup > Layer2 Interface > PTM Interface** to display the interface as shown in [Figure 71](#).

FIGURE 71 VDSL2 PTM INTERFACE CONFIGURATION OVERVIEW



By default, system preset VDSL2 PTM interface is **ptm0**.

Note:

The 931WII can only support 1 PTM interface, so that if you want to add or modify the PTM interface, you need to remove the default PTM interface first.

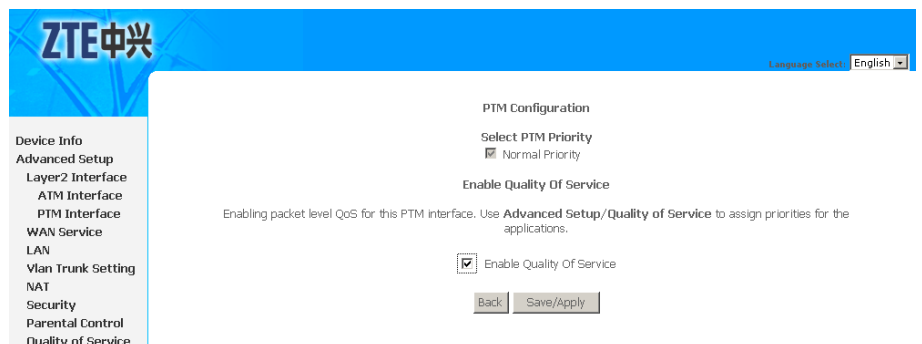
- To delete the PTM interface, select the **Remove** check box in the table and click **Remove** to apply the settings.

Note:

If the PTM interface is used to be WAN interface, you need to remove the PTM interface from WAN interface.

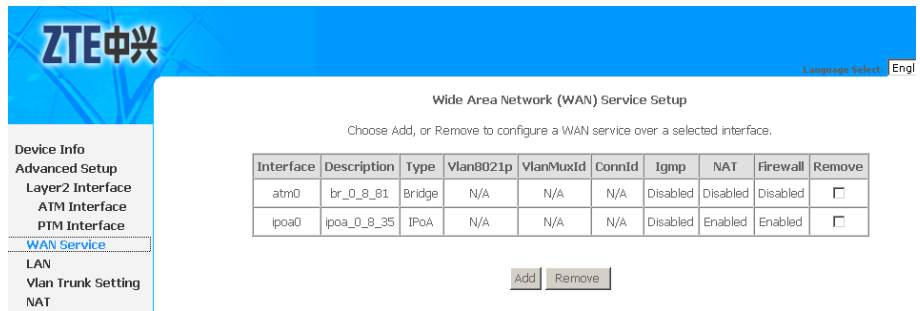
- To add new PTM interface, click **Add** to display the interface as shown in [Figure 72](#).

FIGURE 72 ADDING PTM INTERFACE



- Click **Save/Apply** to save the configuration so that the changes can take effect.
- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 73](#).

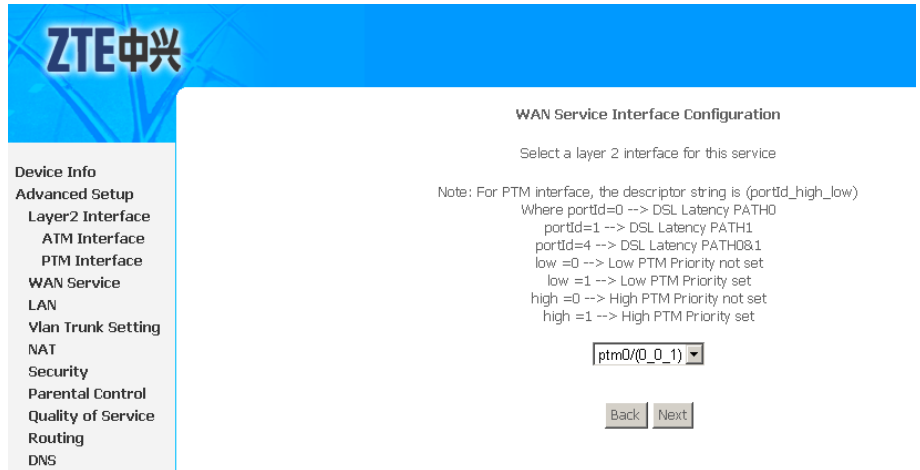
FIGURE 73 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

6. Click **Add** to display the interface as shown in [Figure 74](#), and select the Layer 2 interface.

FIGURE 74 SELECT LAYER2 INTERFACE



7. Click **Next** to enter the interface as shown in [Figure 75](#).

FIGURE 75 SELECT WAN SERVICE TYPE

8. Select **PPP over Ethernet (PPPoE)**.
9. If **Enable VLAN Mux** is selected, enter the value of the 802.1q VLAN tag and priority.
10. Click **Next** to enter the interface as shown in [Figure 76](#).

FIGURE 76 PPPoE CONFIGURATION

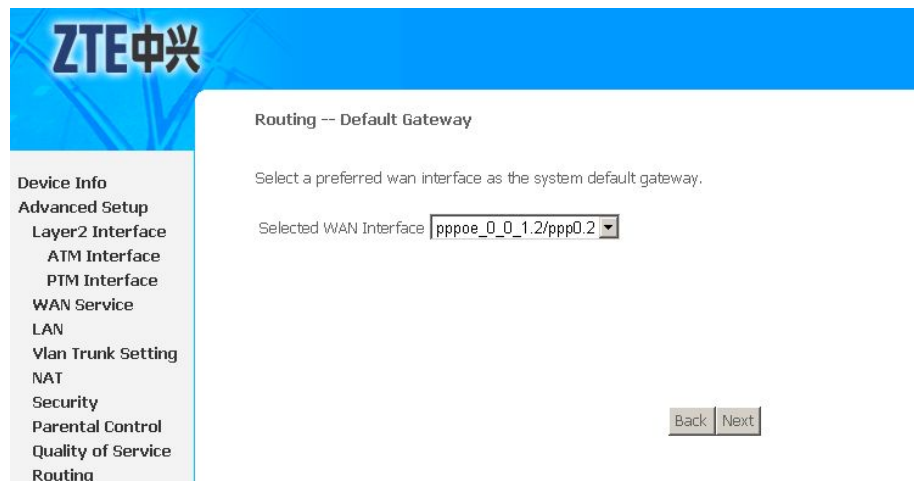
[Table 15](#) is a description of the different options.

TABLE 15 PPPoE CONFIGURATION OPTIONS

Field	Description
PPP Username	The user name that your ISP provides to you.
PPP Password	The password that your ISP provides to you.
PPPoE Service Name	If your ISP provides it to you, enter it. If not, do not enter any information.
Authentication Method	The value can be AUTO , PAP , CHAP , or MSCHAP . Usually, you can select AUTO .
Enable NAT	Select it to enable the NAT functions of the modem. If you do not want to enable NAT and wish the modem user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.
Use Static IPv4 Address	The static IP address that your ISP provides to you.
Enable IGMP Multicast	IGMP proxy. For example, if you want the PPPoE mode to support IPTV, enable this function.

11. Click **Next** to enter the interface as shown in [Figure 77](#).

FIGURE 77 DEFAULT GATEWAY CONFIGURATION



12. Click **Next** to enter the interface as shown in [Figure 78](#).

FIGURE 78 DNS CONFIGURATION

If **Obtain DNS info from a WAN interface** is selected, device accepts the first received DNS assignment from WAN connection.

If **Use the following Static DNS IP address** is selected, enter the **Primary DNS server** and **Secondary DNS server**.

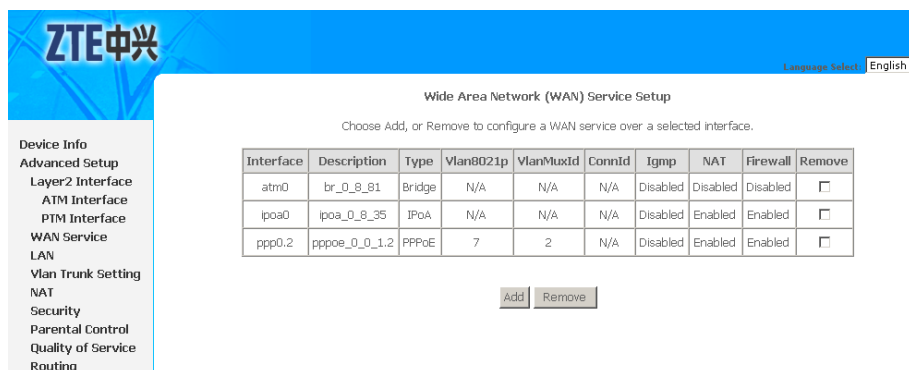
- Click **Next** to enter the interface as shown in [Figure 79](#).

FIGURE 79 PTM INTERFACE PPPoE WAN CONNECTION SETUP SUMMARY

Connection Type:	PPPoE
Service Name:	pppoe_0_0_1.2
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast:	Disabled
Quality Of Service:	Enabled

- Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 80](#).

FIGURE 80 PTM INTERFACE PPPoE WAN CONNECTION CONFIGURATION COMPLETED

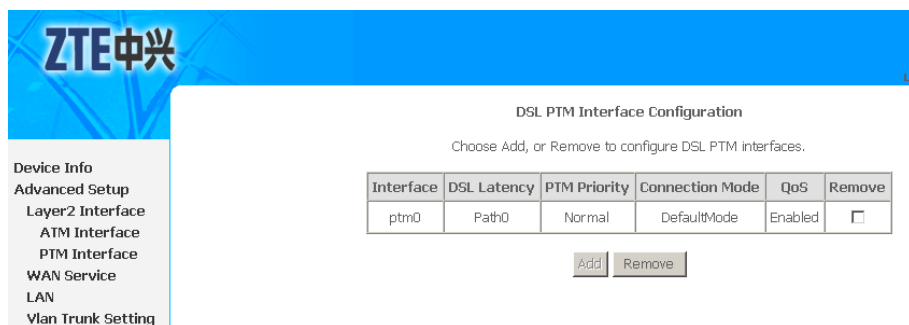


15. To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

Configure VDSL2 Bridge WAN Connection

1. Select **Advanced Setup > Layer2 Interface > PTM Interface** to display the interface as shown in [Figure 81](#).

FIGURE 81 VDSL2 PTM INTERFACE CONFIGURATION OVERVIEW



By default, system preset **VDSL2 PTM** interface is **ptm0**.

Note:

The 931WII can only support 1 PTM interface, so that if you want to add or modify the PTM interface, you need to remove the default PTM interface first.

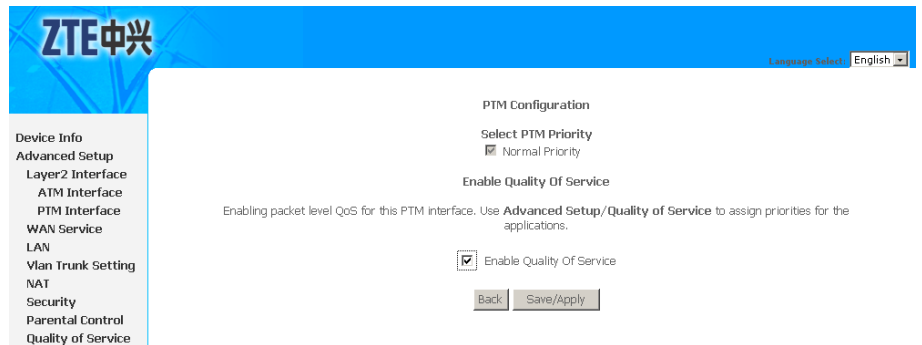
2. To delete the PTM interface, select the **Remove** check box in the table and click **Remove** to apply the settings.

 **Note:**

If the PTM interface is used to be WAN interface, you need to remove the PTM interface from WAN interface.

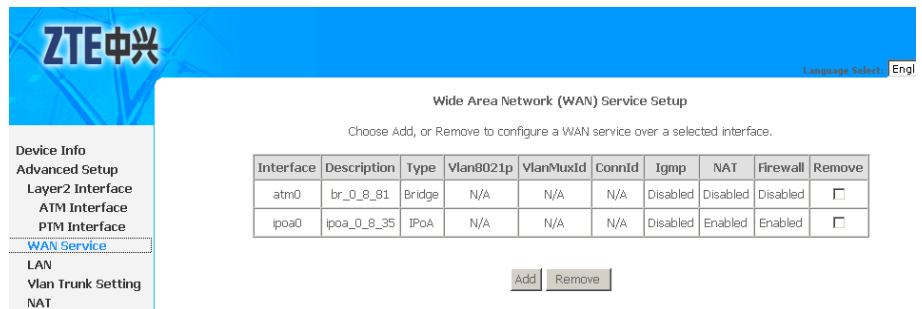
- To add new PTM interface, click **Add** to display the interface as shown in [Figure 82](#).

FIGURE 82 ADDING PTM INTERFACE



- Click **Save/Apply** to save the configuration so that the changes can take effect.
- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 83](#).

FIGURE 83 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

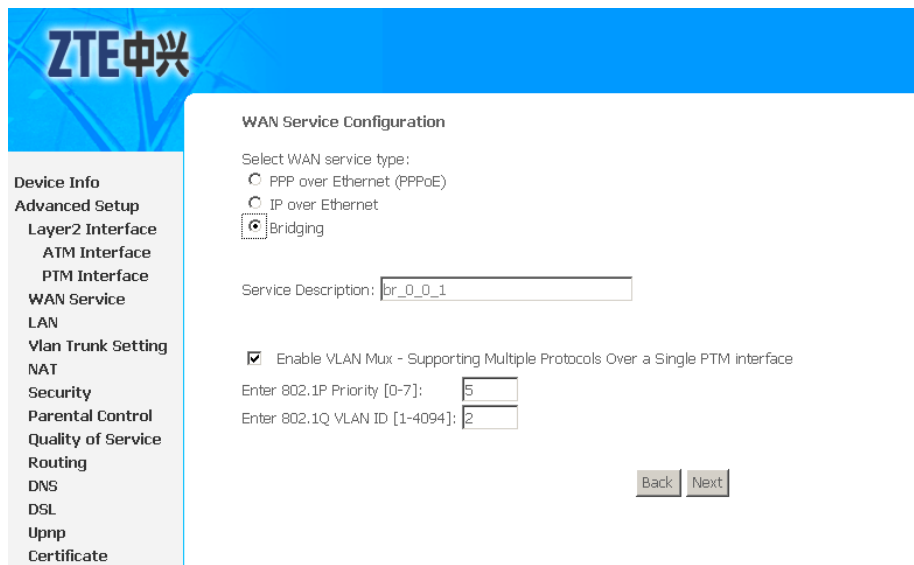
- Click **Add** to display the interface as shown in [Figure 84](#), and select the Layer 2 interface.

FIGURE 84 SELECT LAYER2 INTERFACE



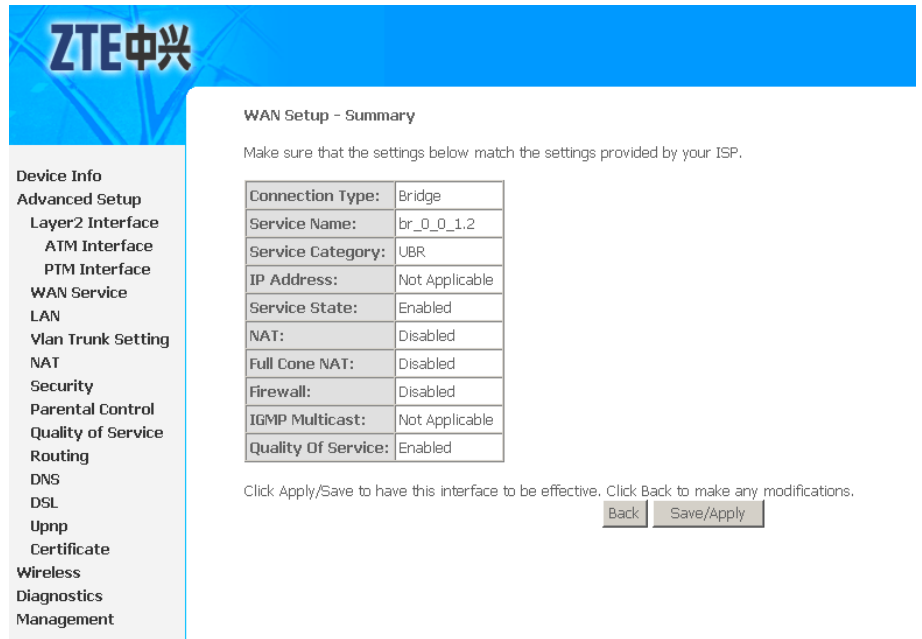
7. Click **Next** to enter the interface as shown in [Figure 85](#).

FIGURE 85 SELECT WAN SERVICE TYPE



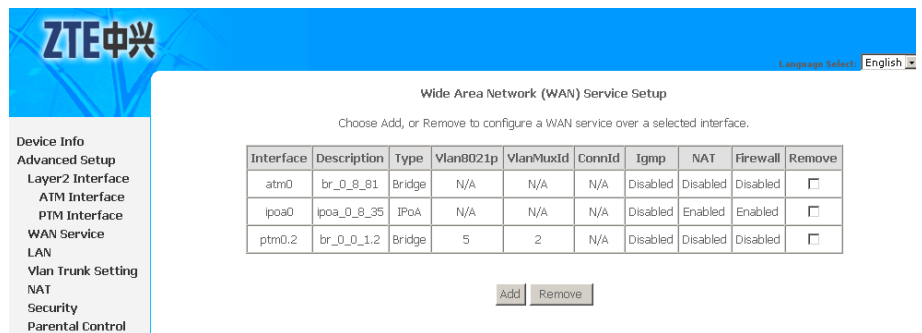
8. Select **Bridging**.
9. If **Enable VLAN Mux** is selected, enter the value of the 802.1q VLAN tag and priority.
10. Click **Next** to enter the interface as shown in [Figure 86](#).

FIGURE 86 PTM INTERFACE BRIDGE WAN CONNECTION SETUP SUMMARY



11. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 87](#).

FIGURE 87 PTM INTERFACE BRIDGE WAN CONNECTION CONFIGURATION COMPLETED

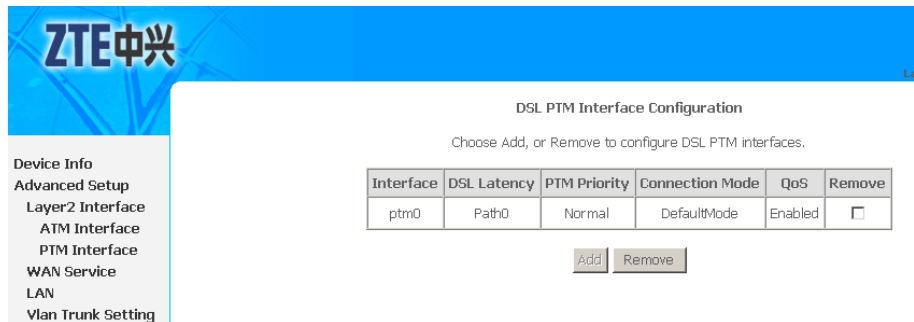


12. To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

Configure VDSL2 IPoE WAN Connection

1. Select **Advanced Setup > Layer2 Interface > PTM Interface** to display the interface as shown in [Figure 88](#).

FIGURE 88 VDSL2 PTM INTERFACE CONFIGURATION OVERVIEW



By default, system preset **VDSL2 PTM** interface is **ptm0**.

Note:

The 931WII can only support 1 PTM interface, so that if you want to add or modify the PTM interface, you need to remove the default PTM interface first.

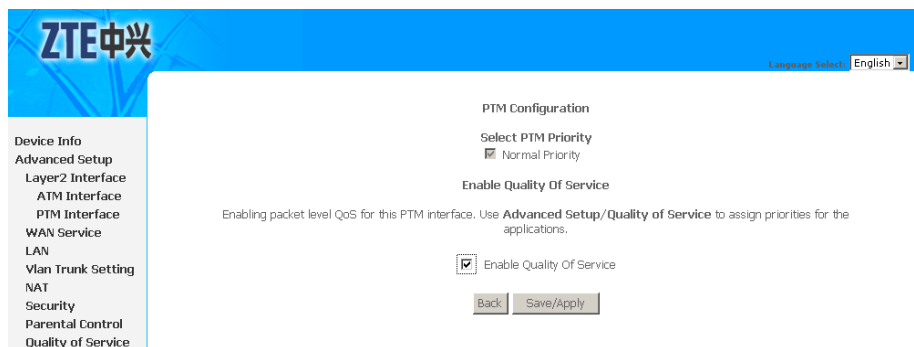
- To delete the PTM interface, select the **Remove** check box in the table and click **Remove** to apply the settings.

Note:

If the PTM interface is used to be WAN interface, you need to remove the PTM interface from WAN interface.

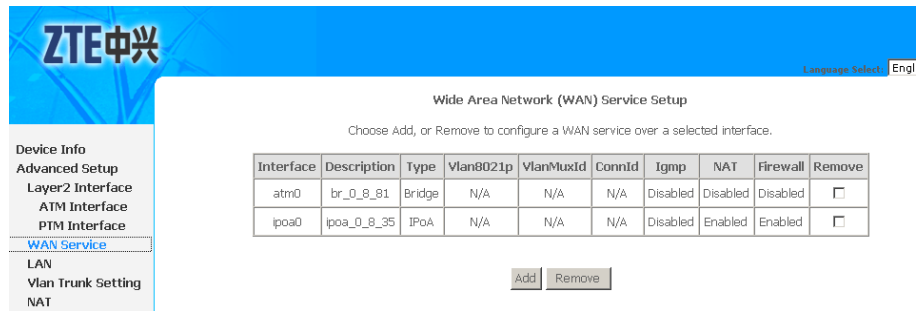
- To add new PTM interface, click **Add** to display the interface as shown in [Figure 89](#).

FIGURE 89 ADDING PTM INTERFACE



- Click **Save/Apply** to save the configuration so that the changes can take effect.
- Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 90](#).

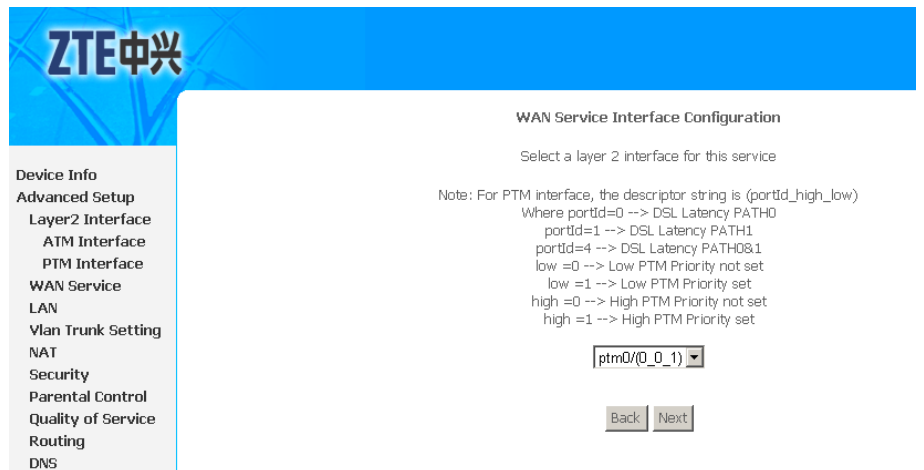
FIGURE 90 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

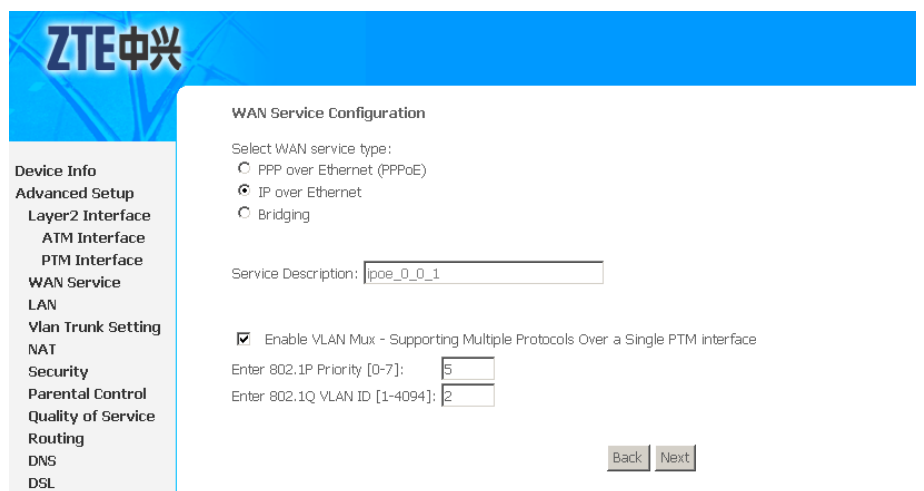
- Click **Add** to display the interface as shown in [Figure 91](#), and select the Layer 2 interface.

FIGURE 91 SELECT LAYER2 INTERFACE



- Click **Next** to enter the interface as shown in [Figure 92](#).

FIGURE 92 SELECT WAN SERVICE TYPE



8. Select **IP over Ethernet**.
9. If **Enable VLAN Mux** is selected, enter the value of the 802.1q VLAN tag and priority.
10. Click **Next** to enter the interface as shown in [Figure 93](#).

FIGURE 93 WAN IP CONFIGURATION

If **Obtain an IP address automatically** is selected, input the **Option 60 Vendor ID**.

If **Use the following Static IP address** is selected, enter the **WAN IP Address**, **WAN Subnet Mask** and **WAN gateway IP Address**.

11. Click **Next** to enter the interface as shown in [Figure 94](#).

FIGURE 94 DEFAULT GATEWAY CONFIGURATION

12. Click **Next** to enter the interface as shown in [Figure 95](#).

FIGURE 95 DNS CONFIGURATION

If **Obtain DNS info from a WAN interface** is selected, device accepts the first received DNS assignment from WAN connection.

If **Use the following Static DNS IP address** is selected, enter the **Primary DNS server** and **Secondary DNS server**.

- Click **Next** to enter the interface as shown in [Figure 96](#).

FIGURE 96 NAT CONFIGURATION

- Click **Next** to enter the interface as shown in [Figure 94](#).

FIGURE 97 DEFAULT GATEWAY CONFIGURATION

15. Click **Next** to enter the interface as shown in [Figure 95](#).

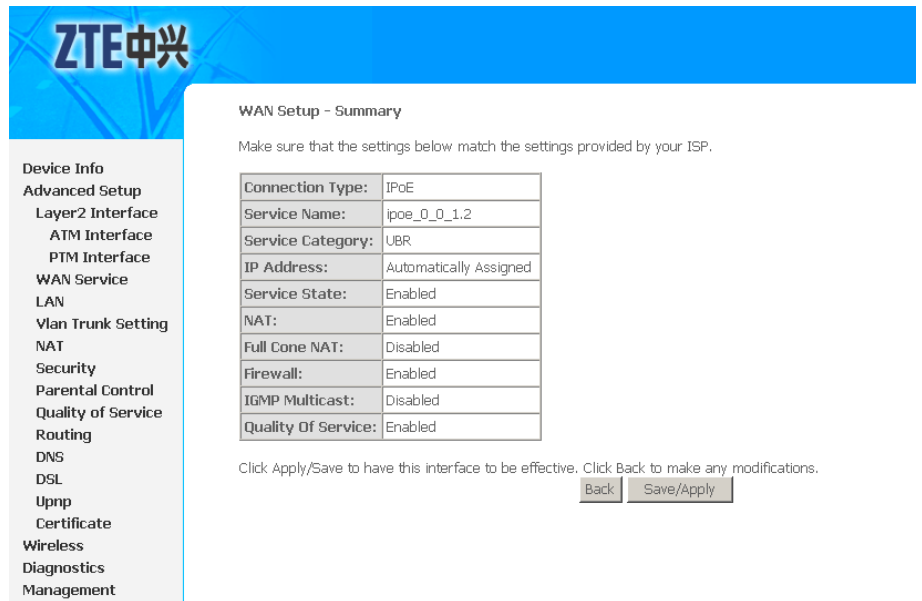
FIGURE 98 DNS CONFIGURATION

If **Obtain DNS info from a WAN interface** is selected, device accepts the first received DNS assignment from WAN connection.

If **Use the following Static DNS IP address** is selected, enter the **Primary DNS server** and **Secondary DNS server**.

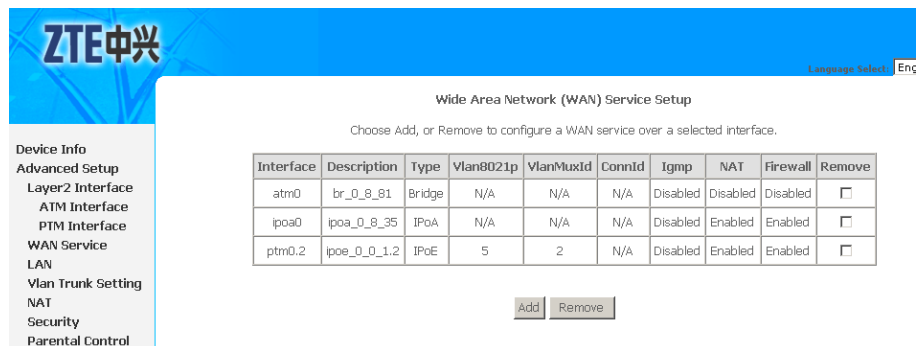
16. Click **Next** to enter the interface as shown in [Figure 99](#).

FIGURE 99 PTM INTERFACE IPOE WAN CONNECTION SETUP SUMMARY



17. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 100](#).

FIGURE 100 PTM INTERFACE IPOE WAN CONNECTION CONFIGURATION COMPLETED



18. To delete the WAN connection, select the **Remove** check box in the table and click **Remove** to apply the settings.

This page is intentionally blank.

Chapter 6

LAN Configuration

1. Select **Advanced Setup** > **LAN** to display the interface as shown in [Figure 101](#).

FIGURE 101 LAN CONFIGURATION OVERVIEW

ZTE中兴

Local Area Network Setup

Configure the DSL Router IP Address and Subnet Mask for LAN Interface.

IP Address:

Subnet Mask:

Enable IGMP Snooping

Disable DHCP Server

Enable DHCP Server

Start IP Address:

End IP Address:

Leased Time(hour):

Static IP Lease List: (A maximum 10 entries can be configured)

MAC Address	IP Address	Remove
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

Configure the second IP Address and Subnet Mask for LAN interface

2. In this interface, you can change the IP address of the device. The preset IP address is 192.168.1.1. This is the private IP address of the 931WII, under which the device can be reached in the local network.

Note:

New settings can only be made after the 931WII has been re-booted. If necessary, reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration.

3. [Table 16](#) is a description of the different options.

TABLE 16 LAN CONFIGURATION OPTIONS

Field	Description
IP Address	If you want to assign a different IP address to the 931WII, enter new IP address in this fields.
Subnet Mask	Adjust the subnet mask if necessary
Enable IGMP Snooping	Select the checkbox to enable the IGMP function.
Disable DHCP Server/Enable DHCP Server	Enable or disable the DHCP Server function.

4. If the **DHCP** server is activated, extra configuration is as following:
 - i. Configure the network setting on the PC so that the option **Obtain an IP address automatically** is set up.
 - ii. Define the range of IP addresses, **Start IP Address**, **End IP Address**, and **Lease Time(Hour)**.
 - iii. If the DHCP server is active, 931WII supports 10 static IP addresses. Click **Add** to display the interface as shown in [Figure 102](#).

FIGURE 102 ADDING DHCP STATIC IP LEASE

DHCP Static IP Lease

Enter the Mac address and Static IP address then click .

MAC Address: (e.g 00:19:5B:74:32:72)

IP Address: (e.g 192.168.1.100)

- iv. Click **Save** to save the configuration so that the changes can take effect.
5. If you deactivate the DHCP server, you need to assign a static IP address for the PCs that use the network settings.
6. Select the **Configure the second IP Address and Subnet Mask for LAN interface** to enable the function and configure the second IP address for the device, as shown in .

FIGURE 103 CONFIGURE SECOND IP ADDRESS

Configure the second IP Address and Subnet Mask for LAN interface

IP Address:

Subnet Mask:

7. Click **Save/Reboot** to save the configuration so that the changes can take effect.

**Caution:**

All application will take effect after click the button of Apply/Reboot , then MODEM will reboot . Please wait for 2 minutes before reopening your web browser.

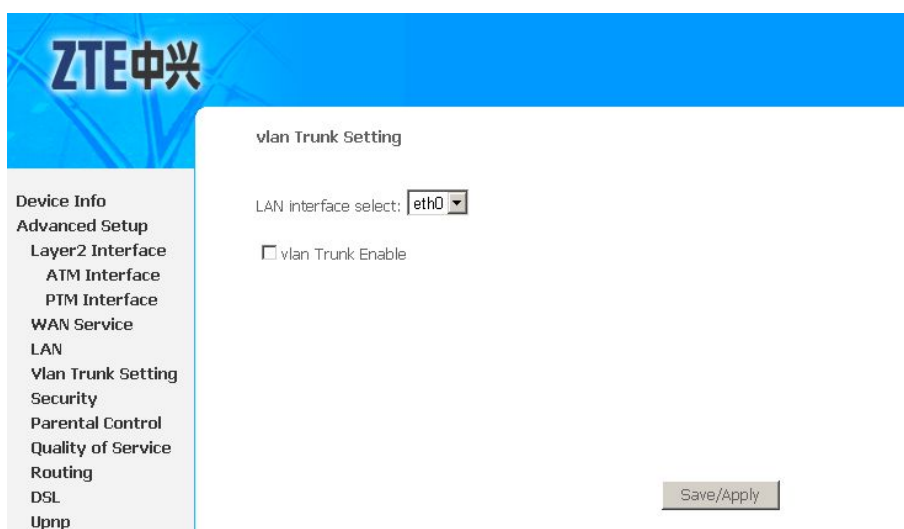
This page is intentionally blank.

Chapter 7

VLAN Trunking Configuration

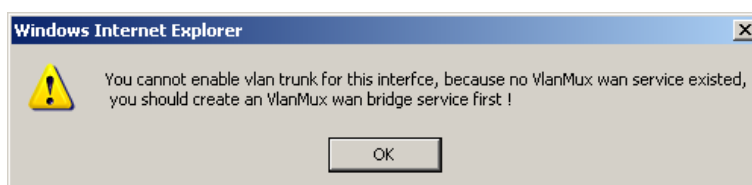
1. Select **Advanced Setup > Vlan Trunk Setting** to display the interface as shown in [Figure 104](#).

FIGURE 104 VLAN TRUNKING OVERVIEW



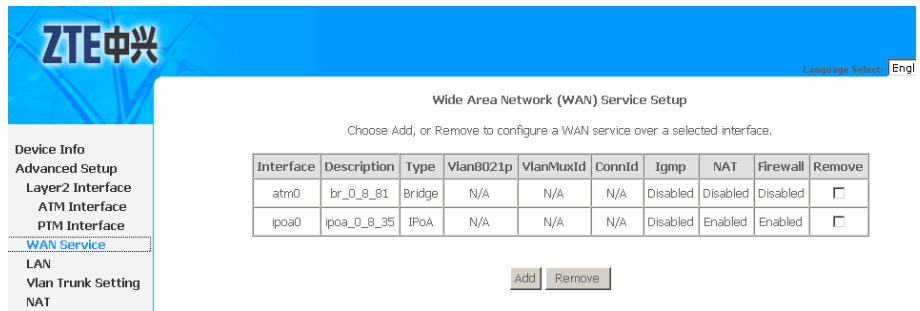
2. Select the **LAN interface select** and **vlan Trunk Enable** checkbox.
3. If system pops up the notices as shown in [Figure 105](#), you need to follow the next steps to create **VLAN MUX PTM interface WAN** bridge connection.

FIGURE 105 VLAN TRUNKING NOTICE



4. Select **Advanced Setup > WAN Service** to display the interface as shown in [Figure 106](#).

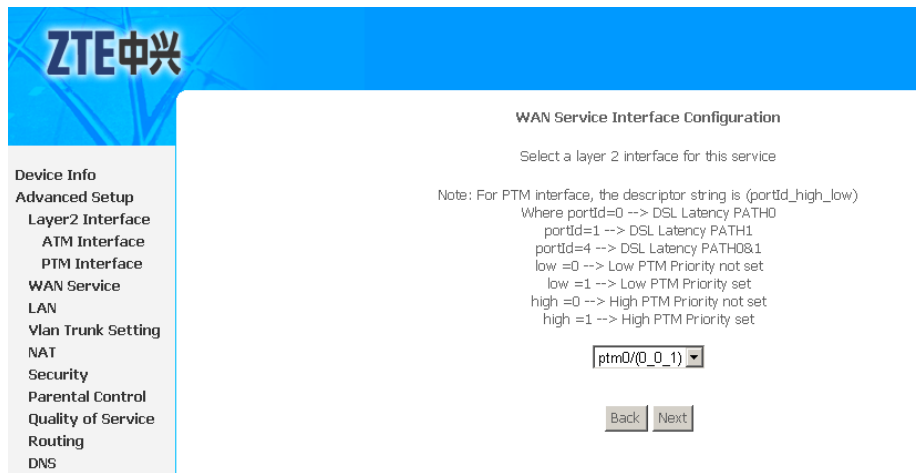
FIGURE 106 WAN SERVICE OVERVIEW



By default, system preset WAN Interface is **atm0** and **ptm0_1**.

5. Click **Add** to display the interface as shown in [Figure 107](#), and select PTM interface the Layer 2 interface.

FIGURE 107 SELECT LAYER2 INTERFACE



6. Click **Next** to enter the interface as shown in [Figure 108](#).

FIGURE 108 SELECT WAN SERVICE TYPE

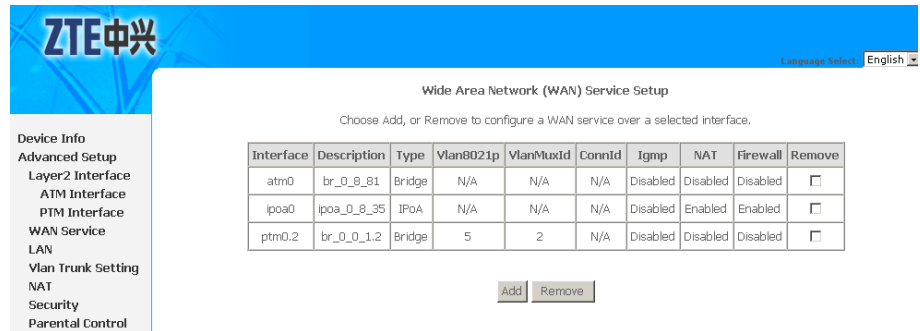
7. Select **Bridging**.
8. Select the **Enable VLAN Mux** checkbox and enter the value of the 802.1q VLAN tag and priority.
9. Click **Next** to enter the interface as shown in [Figure 109](#).

FIGURE 109 PTM INTERFACE BRIDGE WAN CONNECTION SETUP SUMMARY

Connection Type:	Bridge
Service Name:	br_0_0_1.2
Service Category:	UBR
IP Address:	Not Applicable
Service State:	Enabled
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Not Applicable
Quality Of Service:	Enabled

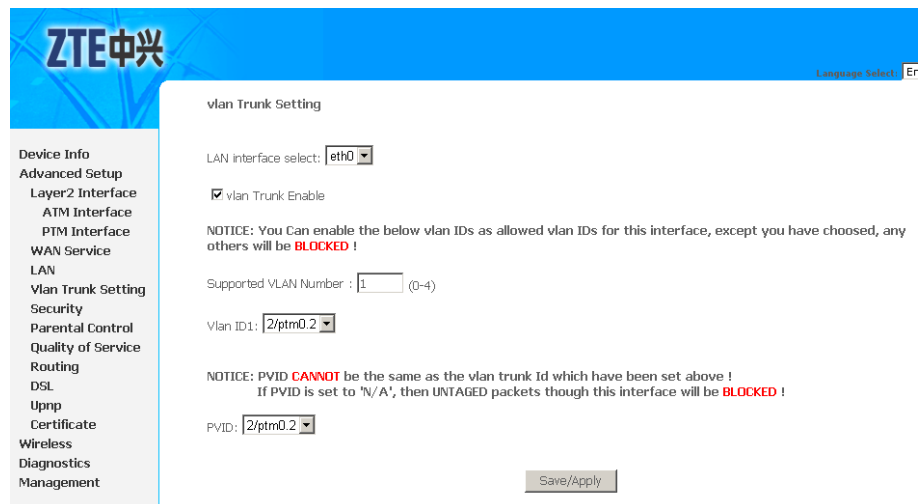
10. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 110](#).

FIGURE 110 PTM INTERFACE BRIDGE WAN CONNECTION CONFIGURATION COMPLETED



11. Go back to **vlan Trunk Setting** interface, select the **LAN interface select** and **vlan Trunk Enable** checkbox to display the interface as shown in [Figure 111](#).

FIGURE 111 VLAN TRUNKING CONFIGURATION



12. Enter the **Supported VLAN Number, Vlan ID** and **PVID** .



Note:

- ▶ PVID **CANNOT** be the same as the VLAN trunk Id.
- ▶ If PVID is set to 'N/A', then UNTAGED packets though this interface will be **BLOCKED**.

13. Click **Save/Apply** to save the configuration so that the changes can take effect.

NAT Configuration

Table of Contents

Overview.....	83
Virtual Servers Setup.....	84
Port Triggering.....	87
DMZ Host.....	89

Overview

Setting up the NAT function

The 931WII is equipped with the [NAT](#) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the public IP address of the 931WII by default.

One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it is explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the 931WII allows the data to pass through. The 931WII opens one specific port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network. Communicating via a port is subject to the rules of a particular protocol ([TCP](#) or [UDP](#)).

If an external application tries to send a call to a PC in the local network, the 931WII blocks it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links (that is, several ports), so that players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot be run if NAT is activated.

Using port forwarding (the forwarding of requests to particular ports) the 931WII is forced to send requests from the Internet for a certain service, for example, a game, to the appropriate port(s) on the PC on which the game is running. Port triggering is a special variant of port forwarding. Unlike port forwarding, the 931WII forwards the data from the port block to the PC which has previously sent data to the Internet via a certain port (trigger port). This means that approval for the data transfer is not tied to one specific PC in the network, but rather to the port numbers of the required Internet service.

Configuring Port Triggering

Define a trigger port for the application and the protocol (TCP or UDP) that this port uses. You then assign the public ports that are to be opened for the application to this trigger port.

The 931WII checks all outgoing data for the port number and protocol. If it identifies a match of port and protocol for a defined trigger port, then it opens the assigned public ports and notes the IP address of the PC that sent the data. If data comes back from the Internet via one of these public ports, the 931WII allows it to pass through and directs it to the appropriate PC. A trigger event always comes from a PC within the local network. If a trigger port is addressed from outside, the 931WII simply ignores it.

**Note:**

- An application that is configured for port triggering can only be run by one user in the local network at a time.
- After public ports are open, they can be used by unauthorized persons to gain access to a PC in the local network.
- When the 931WII is supplied, the NAT is activated, i.e. all IP addresses of PCs in the local network are converted to the public IP address of the 931WII when accessing the Internet.
- IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the 931WII, you must select Never expires as the settings in the local network menu entry for the lease time or assign static IP addresses for the PCs.

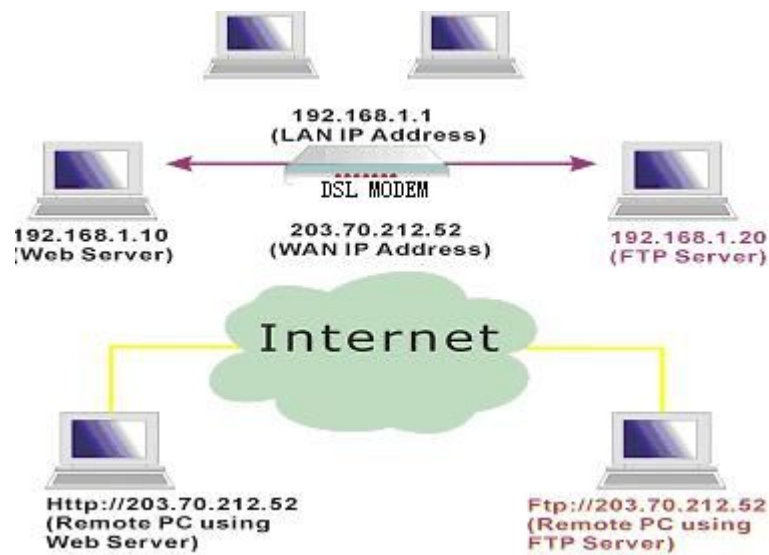
You can activate or deactivate the NAT function. By default, the NAT function is activated.

Virtual Servers Setup

Background

By default, the 931WII blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude on the network and damage it, as shown in [Figure 112](#).

FIGURE 112 VIRTUAL SERVER



However, you may want to expose your network to the Internet in limited and controlled ways in order to enable some applications to work from the LAN (for example, game, voice, and chat applications) and to enable Internet access to servers in the home network. The port forwarding feature supports both functionality. This topic is also referred to as Local Servers.

The port forwarding page is used to define applications that require special handling by the 931WII. All you need to do is to select the application protocol and the local IP address of the computer that is using or providing the service. You can also add new protocols, besides the most common ones provided by the 931WII.

For example, if you want to use a File Transfer Protocol (FTP) application on one of your PCs, simply select FTP from the list and enter the local IP address or host name of the designated computer. All FTP-related data arriving at the 931WII from the Internet henceforth is forwarded to the specific computer.

Similarly, you can grant Internet users access to servers inside your home network, by identifying each service and the PC that provides it. This is useful, for example, if you want to host a Web server inside your home network.

When an Internet user points his/her browser to 931WII external IP address, the gateway forwards the incoming HTTP request to your web server. With one external IP address (the 931WII main IP address), different applications can be assigned to your LAN computers, however, each type of application is limited to use one computer.

For example, you can define that FTP uses address X to reach computer A and Telnet also uses address X to reach computer A. But attempting to define FTP to use address X to reach both computer A and B fails. The 931WII, therefore, provides the ability to add additional public IP addresses to port forwarding rules, which you must obtain from your ISP, and enter into the IP addresses pool. Then, you can define FTP to use address X to reach computer A and address Y to reach computer B.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. For example, if you have a Web server running on your PC on port 8080 and you want to grant access to this server to any one who accesses the 931WII via HTTP, do as follows:

1. Define a port forwarding rule for the HTTP service, with the PC IP or host name.
2. Specify 8080 in the Forward to Port' field.

All incoming HTTP traffic is forwarded to the PC running the web server on port 8080. When setting a port forwarding service, ensure that the port is not already used by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP, the port used by the gateway VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.

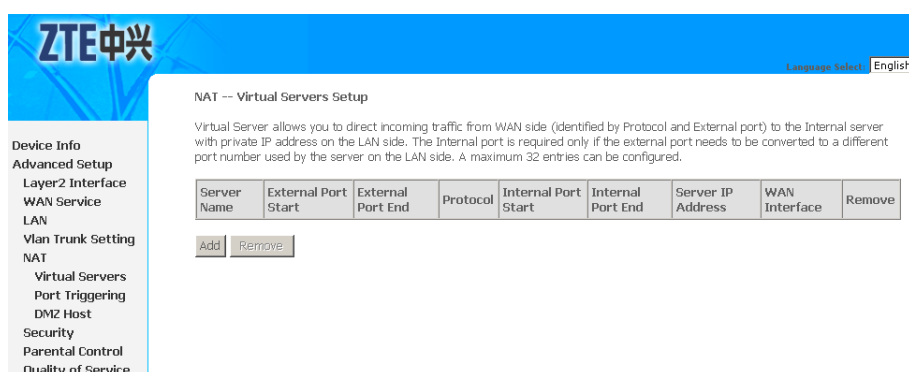
Note:

Some applications, such as FTP, TFTP, PPTP, and H323, require the support of special specific ALG modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. The 931WII is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network. The ALG is automatically assigned based on the destination port.

Adding Port Forwarding

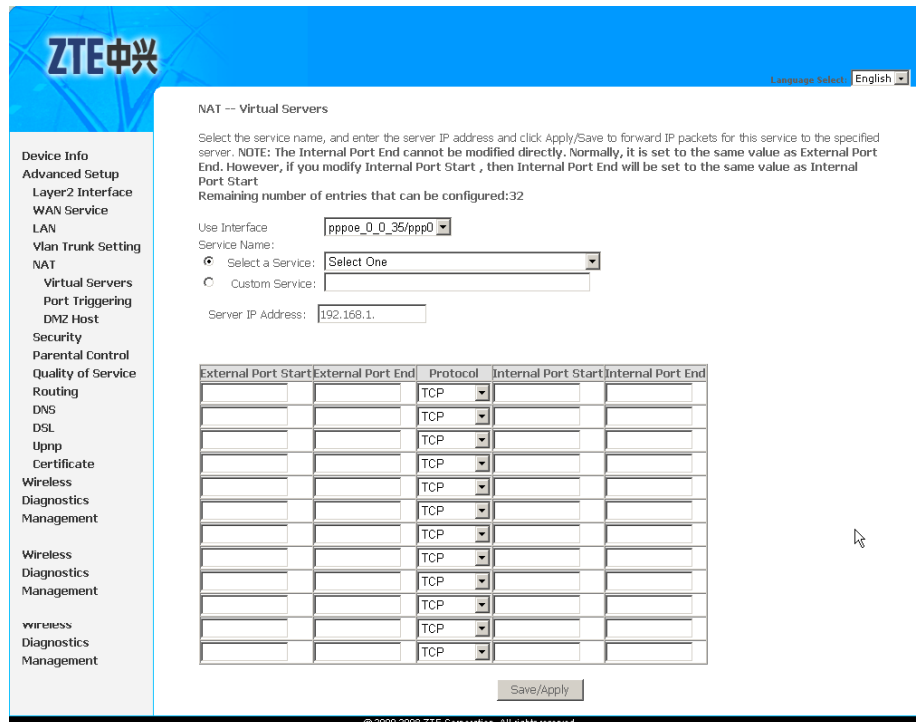
1. Select **Advanced Setup > NAT > Virtual Servers** to display the interface as shown in [Figure 113](#).

FIGURE 113 VIRTUAL SERVERS OVERVIEW



2. Click **Add** to display the interface as shown in [Figure 114](#).

FIGURE 114 ADDING VIRTUAL SERVERS



3. Select the dedicated WAN interface to be **Use Interface**.
4. Select a service or enter a custom server.
5. Enter the **Server IP Address** of the computer that provides the service (the server in the Local Host field).

Note:

Note that unless an additional external IP address is added, only one LAN computer can be assigned to provide a specific service or application.

6. Set External Port Start and External Port End.
7. Select Protocol.
8. Set Internal Port Start and Internal Port End.
9. Click **Save/Apply** to save the configuration so that the changes can take effect.

Deleting Port Forwarding

Select the **Remove** check box in the table and click **Remove** to apply the settings.

Port Triggering

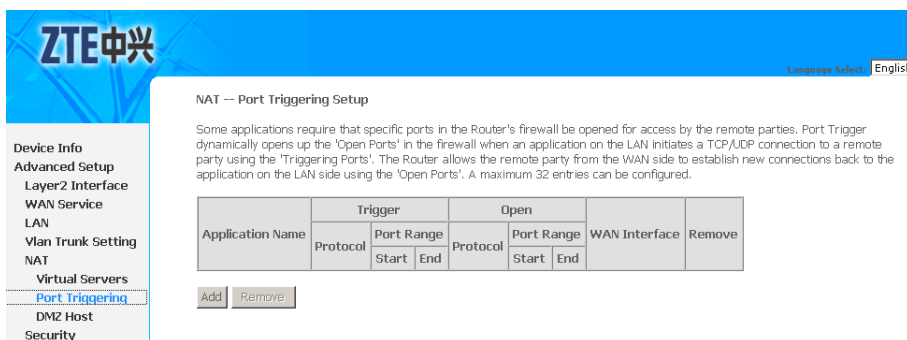
If you configure port triggering for a certain application, you need to determine a trigger port and the protocol (**TCP** or **UDP**) that this port uses. You then assign the public ports that are to be opened

for the application to this trigger port. You can select known Internet services or assign ports or port blocks manually.

Add port Triggering

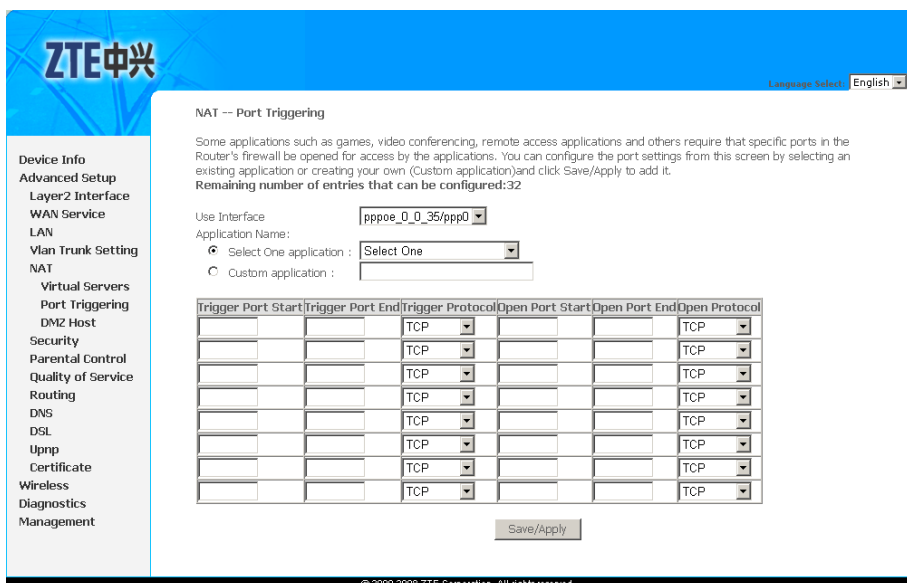
1. Select **Advanced Setup > NAT > Port Triggering** to display the interface as shown in [Figure 115](#).

FIGURE 115 PORT TRIGGERING OVERVIEW



2. Click **Add** to display the interface as shown in [Figure 116](#).

FIGURE 116 ADDING PORT TRIGGERING



3. Select the dedicated WAN interface to be **Use Interface**.
4. Select the required application from the **Select One Application** drop-down list.
5. You can also manually enter the information in the **Custom application** field.
6. [Table 17](#) is a description of the different options.

TABLE 17 CUSTOM PORT TRIGGERING CONFIGURATION OPTIONS

Field	Description
Trigger Port Start/Trigger Port End	Enter the port that is to be monitored for outgoing data traffic.
Trigger Protocol	Select the protocol that is to be monitored for outgoing data traffic.
Open Protocol	Select the protocol that is to be allowed for incoming data traffic.
Open Port Start and Open Port End	Enter the port that is to be opened for incoming traffic.

**Note:**

You can use a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these, for example 80, 90-140, 180.

- Click **Save/Apply** to save the configuration so that the changes can take effect.

Removing Port Triggering

Select the **Remove** check box in the table and click **Remove** to apply the settings.

DMZ Host

The **DMZ** host feature allows one local computer to be exposed to the Internet. This function is applicable for:

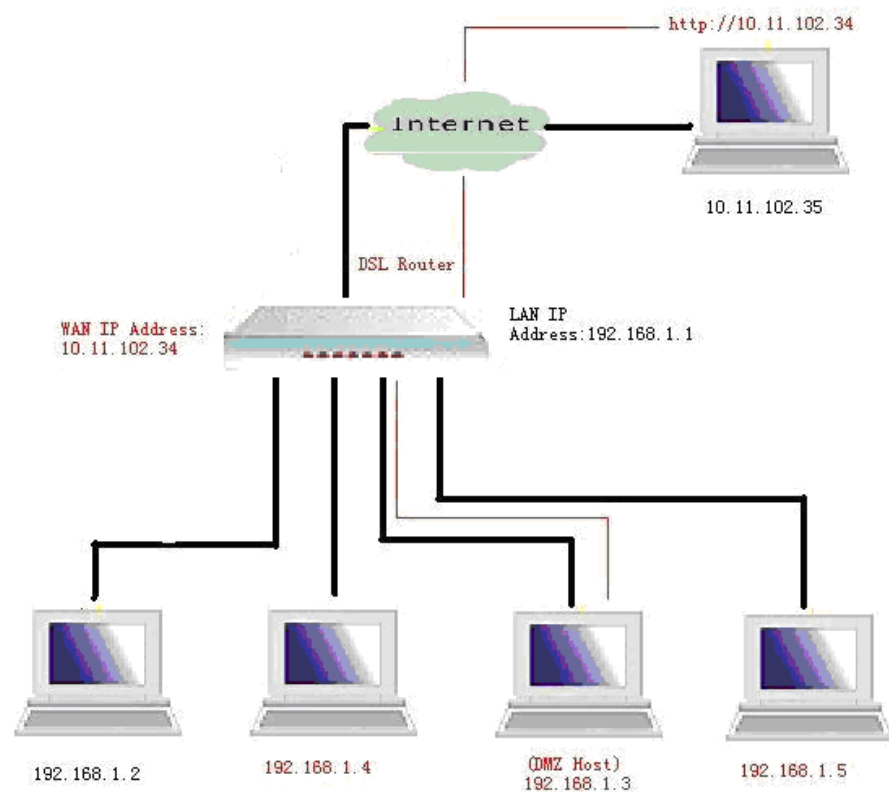
- Users who want to use the Internet service for a special purpose, such as an online game or video conferencing program, that is not present in the Port Forwarding list and for which no port range information is available.
- Users who are not concerned with security and wish to expose one computer to all services without restriction.

Note:

A DMZ host is not protected by the firewall and may be vulnerable to attack. This may also put other computers in the home network at risk. Hence, when designating a DMZ host, you must consider the security implications and protect it if necessary.

You can set up a client in your local network to be the DMZ host, as shown in [Figure 117](#).

FIGURE 117 DMZ HOST



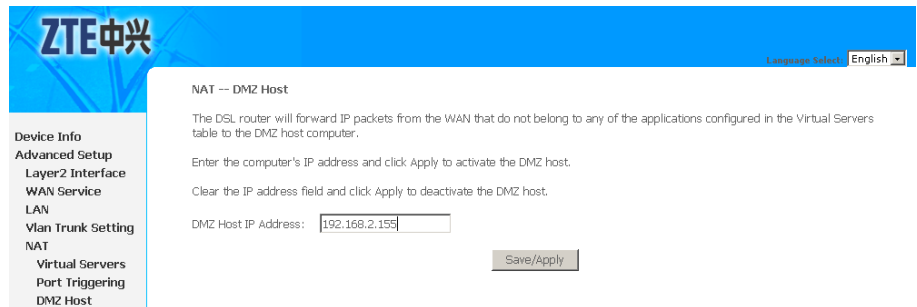
Your device then forwards all incoming data traffic from the Internet to this client. You can, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (for example, hacker attacks). Activate this function only when necessary (for example, to operate a Web server) and when other functions (for example, port forwarding) are inadequate. In this case, you should take appropriate measures for the clients concerned.

 **Note:**

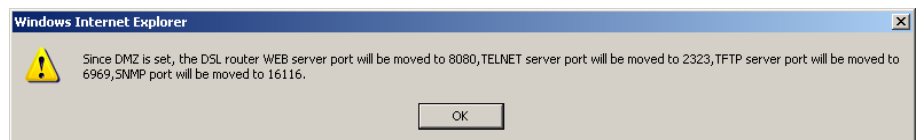
Only one PC per public IP address can be set up as an exposed host.

Adding A DMZ Host

1. Select **Advanced Setup > NAT > DMZ Host** to display the interface as shown in [Figure 118](#).

FIGURE 118 DMZ HOST CONFIGURATION

2. Enter the Local IP address of the PC in **DMZ Host IP Address** field, that is to be enabled as an exposed host.
3. Click **Save/Apply**, a notice will be pop-up as shown in [Figure 119](#).

FIGURE 119 DMZ HOST CONFIGURATION NOTICE

4. Click **OK** to save the configuration so that the changes can take effect.

Removing A DMZ Host

Clear **DMZ Host IP Address** field and click **Save/Apply** to deactivate the DMZ host.

This page is intentionally blank.

Security Configuration

Security is an important function of DSL. It protects resources of a private network from other networks, and prevents unauthorized Internet users from accessing private networks connected to the Internet. All messages entering or leaving the intranet (that is, the local network to which you are connected) must pass through the security checks, which checks each message and blocks those that do not meet the specific security criteria.

There are three basic types of security techniques, IP packet filtering, circuit-level gateway and MAC frame filtering. 931WII supports MAC frame filtering only.

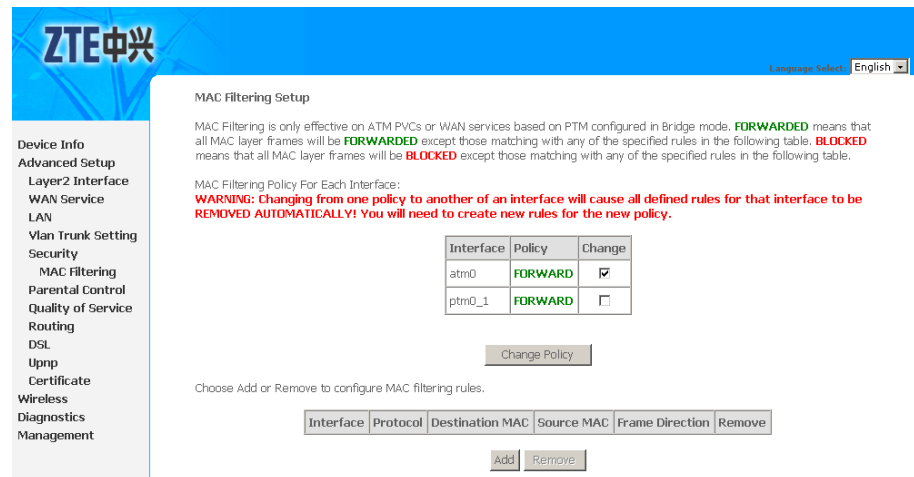
Table of Contents

- Configure MAC Filtering Policy93
- Configure MAC Filtering Rule95
- MAC Filtering - Global Policy FORWARDED.....96
- MAC Filtering - Global Policy BLOCKED97

Configure MAC Filtering Policy

Select **Advanced Setup > Security > MAC Filtering** to display the interface as shown in [Figure 120](#).

FIGURE 120 MAC FILTERING OVERVIEW





Note:

MAC filtering is only effective on ATM PVCs or WAN services based on PTM configured in Bridge mode.

[Table 18](#) is a description of the different options.

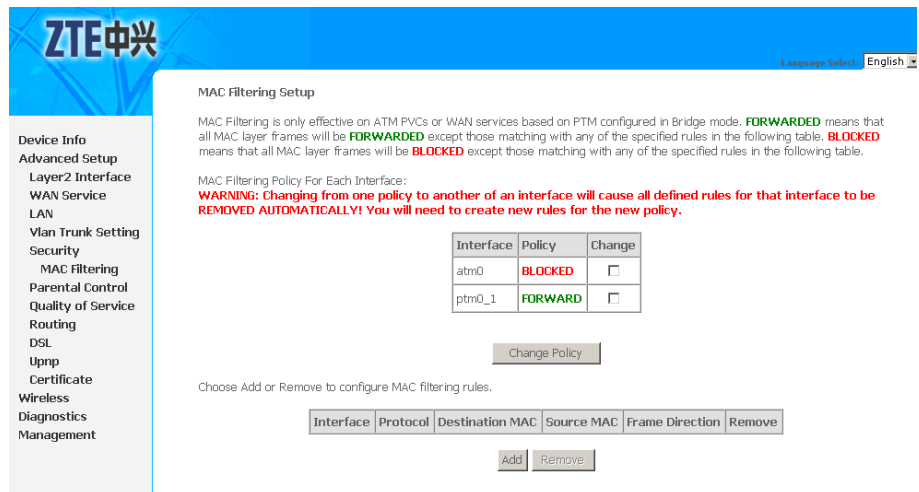
TABLE 18 MAC FILTER POLICY CONFIGURATION OPTIONS

Term	Description
Forward	All MAC layer frames are forwarded except those matching the specified rules.
Blocked	All MAC layer frames are blocked except those matching the specified rules.

Select the **Interface** that needs to change the change the filtering policy, and click the **Change Policy**.

The interface policy is changed, as shown in [Figure 121](#).

FIGURE 121 MAC FILTERING CHANGE POLICY



Caution:

Interface policy change will cause all defined rules for that interface to be removed automatically. You need to create new rules for the new policy.

Configure MAC Filtering Rule

1. Click **Add** in the above interface to enter the interface as shown in [Figure 122](#).

FIGURE 122 ADDING MAC FILTERING RULE

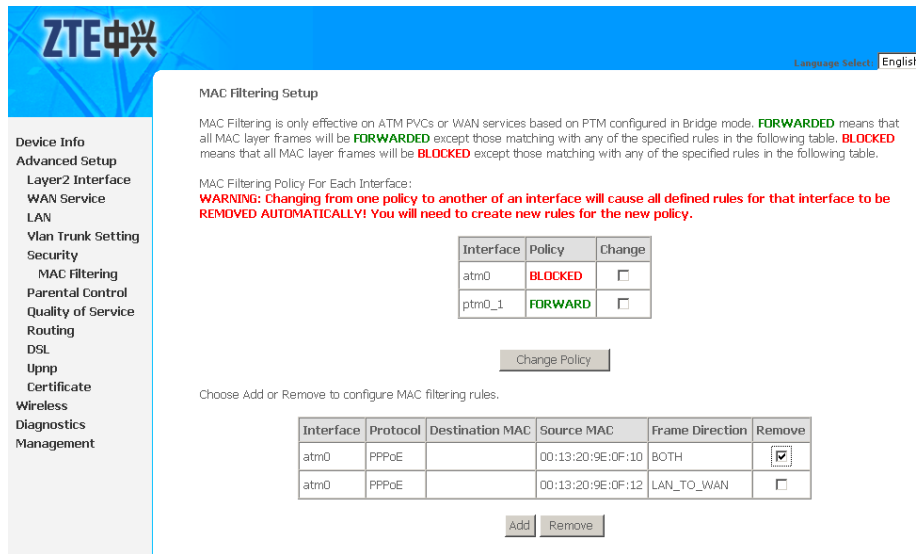
2. [Table 19](#) is a description of the different options.

TABLE 19 MAC FILTERING RULE CONFIGURATION OPTIONS

Field	Description
Protocol Type	Select one from PPPoE IPv4, IPv6, AppleTalk, IPX NETBEUI, and ICMP protocols.
Destination MAC Address	-
Source MAC Address	-
Frame Direction	Direction of transmit frame. You can select LAN->WAN (from LAN to WAN), WAN -> LAN (from WAN to LAN), or LAN <=> WAN.
WAN Interface	Select a WAN interface.

3. Click **Save/Apply** to save the configuration so that the changes can take effect.
4. To remove the MAC Filtering rules, select the dedicate rule in the list and click Remove, as shown in [Figure 123](#).

FIGURE 123 REMOVING MAC FILTERING RULE

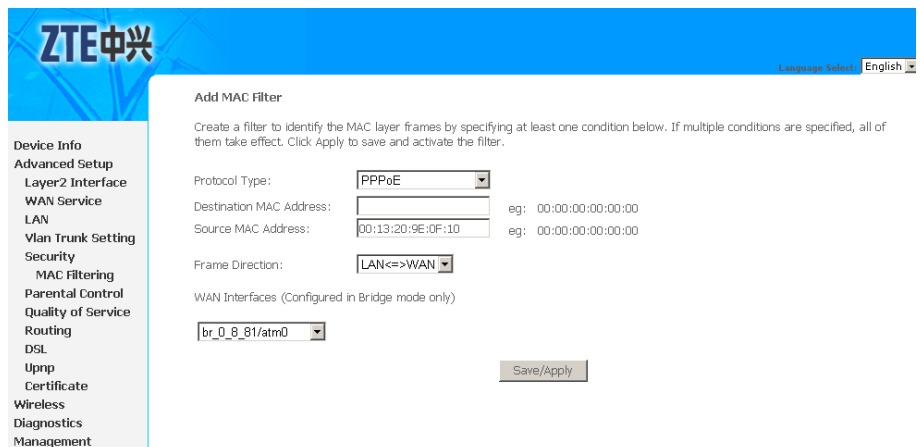


MAC Filtering - Global Policy FORWARDED

The following section describes how to allow the PC whose MAC address is 00:13:20:9E:0F:10 to transmit PPPoE frame to the Internet.

1. Click **Add** in the to enter the interface as shown in [Figure 124](#).

FIGURE 124 ADDING MAC FILTERING - FORWARDED



2. Select **PPPoE** in **Protocol Type** drop-down menu.
3. Input **00:13:20:9E:0F:10** in **Source MAC Address**.

4. Select **LAN <=> WAN** in **Frame Direction** drop-down menu.
5. Select the WAN interface that is used to connect to the Internet.
6. Click **Save/Apply** to save the configuration so that the changes can take effect.

MAC Filtering - Global Policy BLOCKED

The following section describes how to forbid the PC whose MAC address is 00:13:20:9E:0F:12 transmitting PPPoE frame to the Internet.

1. Click **Add** in the to enter the interface as shown in [Figure 125](#).

FIGURE 125 ADDING MAC FILTERING - BLOCKED

The screenshot shows the 'Add MAC Filter' configuration page in the ZTE web management interface. The page has a blue header with the ZTE logo and a language selector set to 'English'. On the left is a sidebar menu with categories like 'Device Info', 'Advanced Setup', 'Security', and 'Management'. The main content area is titled 'Add MAC Filter' and contains the following fields:

- Protocol Type:** A dropdown menu set to 'PPPoE'.
- Destination MAC Address:** An empty text input field with an example 'eg: 00:00:00:00:00:00'.
- Source MAC Address:** A text input field containing '00:13:20:9E:0F:12' with an example 'eg: 00:00:00:00:00:00'.
- Frame Direction:** A dropdown menu set to 'WAN=>LAN'.
- WAN Interfaces (Configured in Bridge mode only):** A dropdown menu set to 'br_0_8_81/atm0'.

A 'Save/Apply' button is located at the bottom right of the configuration area.

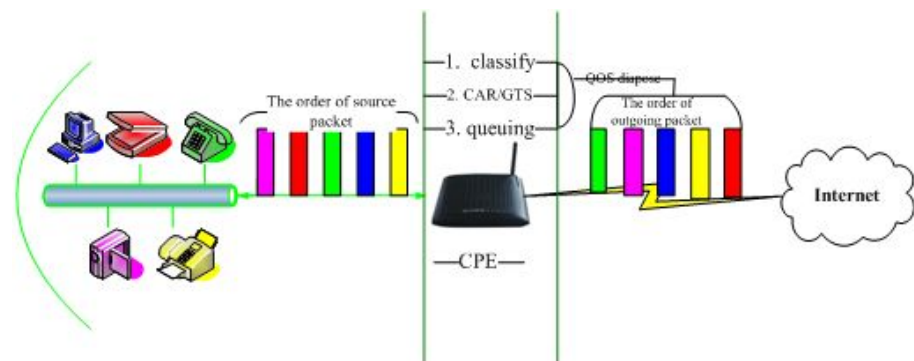
2. Select **PPPoE** in **Protocol Type** drop-down menu.
3. Input 00:13:20:9E:0F:10 in **Source MAC Address**.
4. Select **WAN=> LAN** in **Frame Direction** drop-down menu.
5. Select the WAN interface that is used to connect to the Internet.
6. Click **Save/Apply** to save the configuration so that the changes can take effect.

This page is intentionally blank.

QoS Configuration

Many communication and multimedia applications require large, high speed bandwidths to transfer data between the local network and the Internet. However, for many applications there is often only one Internet connection available with limited capacity. QoS divides this capacity between the different applications and provides continuous data transfer where data packets with higher priority are given preference, as shown in [Figure 126](#).

FIGURE 126 QUALITY OF SERVICE



By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over-provisioning their networks.

Traditionally, the concept of quality in networks meant that all network traffic was treated equally. The result was that all network traffic received the best effort of the network, with no guarantees for reliability, delay, variation in delay, or other performance characteristics. With best-effort delivery service, however, a single bandwidth-intensive application may result in poor or unacceptable performance for all applications.

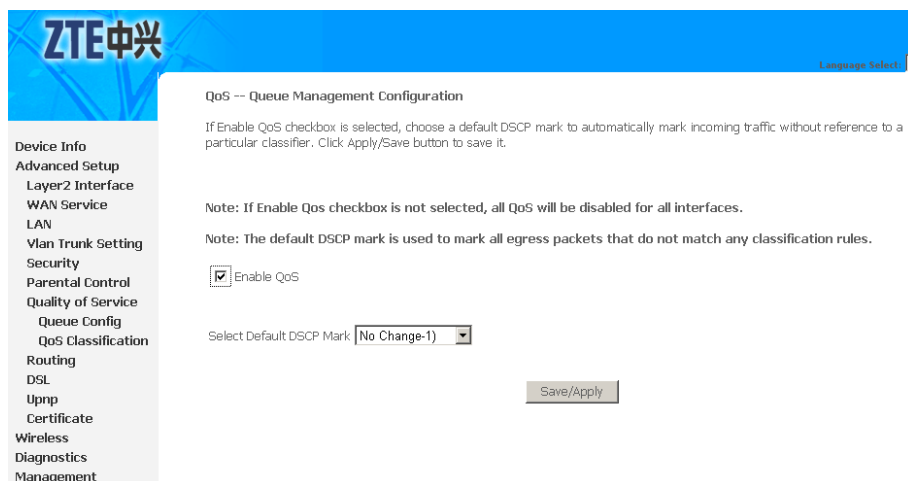
Table of Contents

Enable QoS.....	100
QoS-Queue Config	100
QoS-QoS Classification	103
QoS - DSCP Setting	106

Enable QoS

Select **Advanced Setup > Quality of Service** to display the interface as shown in [Figure 127](#).

FIGURE 127 ENABLE QoS



In this page, you can configure QoS queue management. By default, the system enables QoS and sets a default **DSCP** mark to automatically mark incoming traffic without reference to particular classifier.

Select **Enable QoS** to enable QoS and set the default DSCP mark.

Click **Save/Apply** to save the configuration so that the changes can take effect.

QoS—Queue Config

The queuing in packet QoS becomes effective only when packet is forwarded to QoS-enabled PVC. Packet forwarding is determined by IP routing or bridging, not under control of the packet QoS.

Select **Advanced Setup > Quality of Service > Queue Config** to display the interface as shown in [Figure 128](#).

FIGURE 128 QoS QUEUE CONFIGURATION OVERVIEW

QoS Queue Setup -- A maximum 24 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
<input type="button" value="Add"/> <input type="button" value="Enable"/> <input type="button" value="Remove"/>							

In this interface, you can configure QoS Queue. A maximum of 24 entries can be configured.

QoS Queue Configuration can allocate three queues. Each of the queues can be configured for a precedence value. The queue entry configured is used by the classifier to place ingress packets appropriately.

Note:

Lower integer values for precedence indicate higher priority for this queue relative to others.

For example, add a QoS queue entry and allocate it to a specific network interface (PVC 0/8/81). Set the queue precedence to 1.

1. Click **Add** to display the interface as shown in [Figure 129](#).

FIGURE 129 QoS QUEUE CONFIGURATION

2. [Table 20](#) is a description of the different options.

TABLE 20 QUEUE CONFIGURATION OPTIONS

Field	Description
Name	Define the queue name.
Enable	Set to enable or disable a QoS queue.
Interface	Select a specific network interface. The modem automatically allocates selected network interface to the queue.
Precedence	Select an integer value for queue precedence. After you select an integer value, the queue entry appropriately places to ingress packets. Lower integer values for precedence imply higher priority for this queue relative to others.

3. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in [Figure 130](#).

FIGURE 130 QoS QUEUE CONFIGURATION - COMPLETED

QoS Queue Setup -- A maximum 24 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects.

The QoS function has been disabled. Queues would not take effects.

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove
ADSL	33	atm0	1	Path0		<input type="checkbox"/>	<input type="checkbox"/>

Add Enable Remove

To delete a certain queue, select the queue , click **Disable** and then click **Remove**.

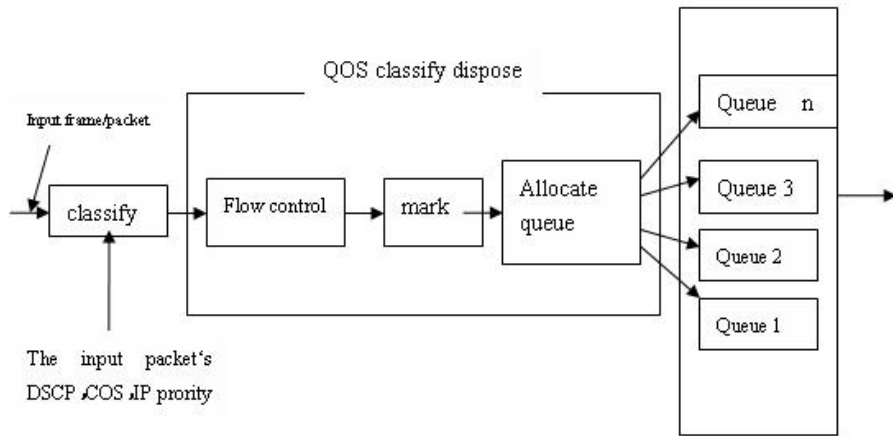
After the queue is configured, you can create several traffic class rules to classify the upstream traffic.

QoS–QoS Classification

Some applications require specific bandwidth to ensure their data be forwarded in time. [QoS](#) classification can creates traffic class rule to classify the upstream traffic. Assign queue which defines the precedence and the interface and optionally overwrite the IP header [DSCP](#) byte. After QoS classification, QoS divides capacity between different applications and provides un-delayed, continuous data transfer where data packet with higher priority is given preference.

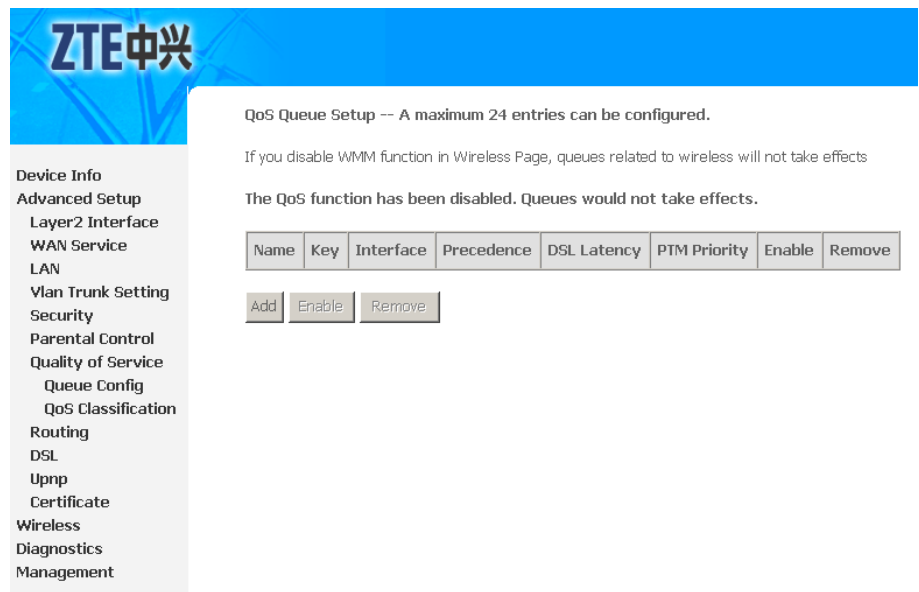
QoS classification model is shown as in [Figure 131](#).

FIGURE 131 QoS CLASSIFICATION



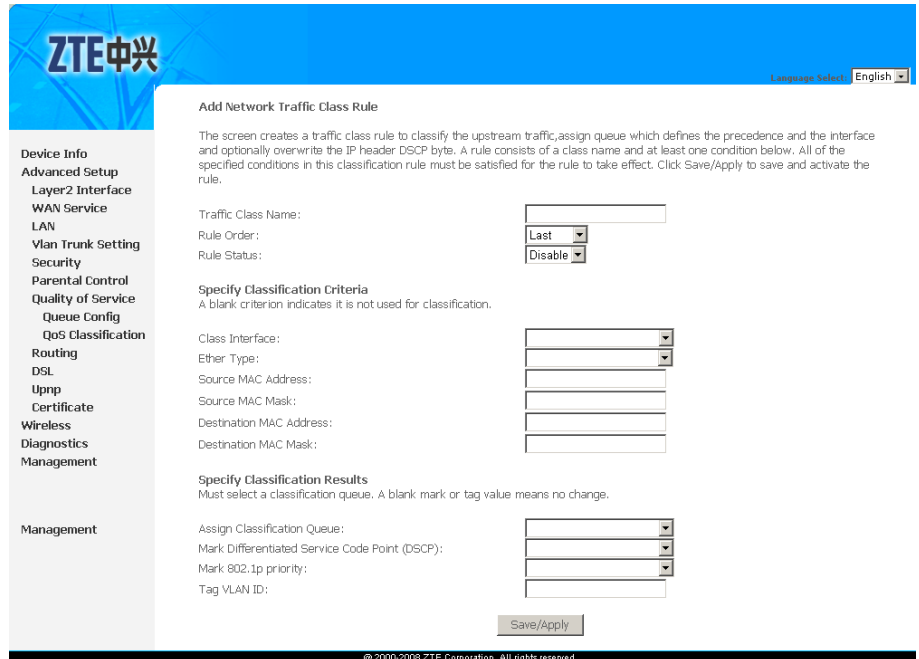
1. Select **Advanced Setup > Quality of Service > QoS Classification** to display the interface as shown in [Figure 132](#).

FIGURE 132 QoS CLASSIFICATION OVERVIEW



2. Click **Add** to display the interface as shown in [Figure 133](#).

FIGURE 133 QoS CLASSIFICATION CONFIGURATION



3. [Table 21](#) is a description of the different options.

TABLE 21 QoS CLASSIFICATION CONFIGURATION OPTIONS

Field	Description
Traffic Class Name	Enter a name of the class.
Rule Order	Select order for queue.
Rule Status	Enable or disable this traffic class rule.
Assign Classification Queue	Select a classification queue.
Assign Differentiated Service Code Point (DSCP) Mark	Select a mark service that modifies the original packet IP header if all rules defined within the classification class are matched. (CS - Mark IP Precedence, AF - Assured Forwarding, EF - Expedited Forwarding).
Mark 802.1p if 802.1q is enabled	Select an 802.1p priority number that serves as the 802.1p value.

4. There are two sets of classification rules. ;

- ▶ Set-1 is based on different fields within TCP/UDP/IP layer plus physical LAN port.
- ▶ Set-2 is based on MAC layer IEEE 802.1p priority field.

Set-1 Rules contain the following:

- ▶ Physical LAN port: Select one among **USB** port, Ethernet ports and wireless port.
- ▶ Protocol: Select one from TCP/UDP TCP UDP and ICMP protocols.
- ▶ Source IP address
- ▶ Source subnet mask
- ▶ UPD/TCP source port or a range of ports
- ▶ Destination IP address
- ▶ Destination subnet mask
- ▶ UPD/TCP destination port or a range of ports
- ▶ Source Mac address
- ▶ Source Mac mask
- ▶ Destination Mac address
- ▶ Destination Mac Mask

Set-2 Rules contain the following:

802.1p priority: The 802.1p header includes a 3-bit prioritization field, which allows packets to be grouped into eight levels of priority (0-7), where level 7 is the highest one.

5. Click **Save/Apply** to save the configuration so that the changes can take effect.

QoS - DSCP Setting

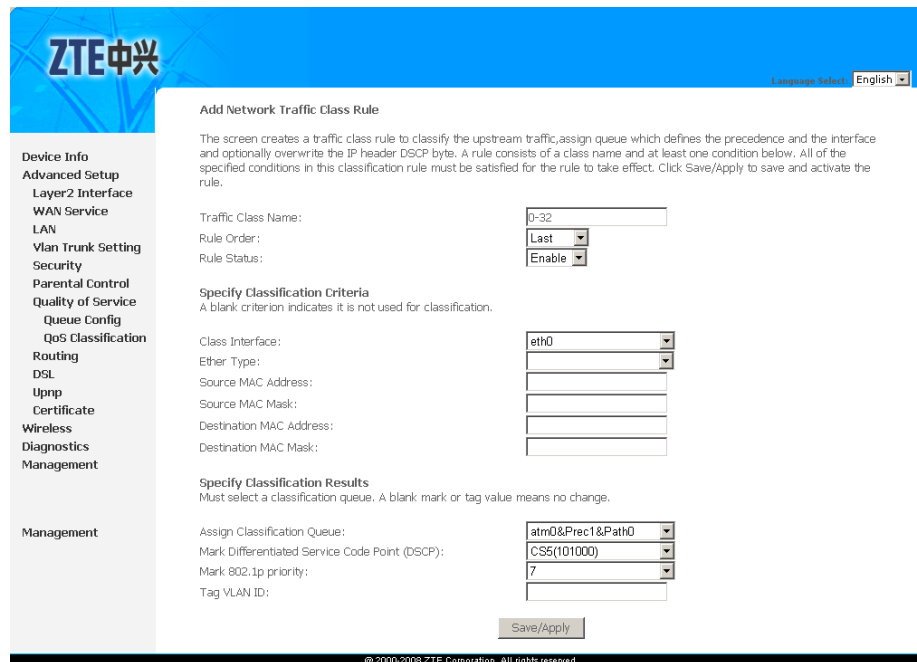
In order to understand what is **DSCP**, you should be familiarized with the Differentiated Services model (Diffserv).

Diffserv is a Class of Service (CoS) model that enhances best-effort Internet services by differentiating traffic by users, service requirements and other criteria. Packets are specifically marked, allowing network nodes to provide different levels of service, via priority queuing or bandwidth allocation, or by choosing dedicated routes for specific traffic flows.

See the following diagram. In the IPV4 packet have a **ToS** field. Diffserv defines TOS field in IP packet headers referred to as DSCP. Hosts or routers that pass traffic to a Diffserv-enabled network typically mark each transmitted packet with an appropriate DSCP. The DSCP markings are used by Diffserv network routers to appropriately classify packets and to apply particular queue handing or scheduling behavior.

For example, mark each transmitted ICMP packet which passing traffic to 0-32 classes with an appropriate DSCP (CS5), as shown in .

FIGURE 134 QoS DSCP CONFIGURATION EXAMPLE



ZTE中兴 Language Select English

Add Network Traffic Class Rule

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click Save/Apply to save and activate the rule.

Traffic Class Name:

Rule Order:

Rule Status:

Specify Classification Criteria

A blank criterion indicates it is not used for classification.

Class Interface:

Ether Type:

Source MAC Address:

Source MAC Mask:

Destination MAC Address:

Destination MAC Mask:

Specify Classification Results

Must select a classification queue. A blank mark or tag value means no change.

Assign Classification Queue:

Mark Differentiated Service Code Point (DSCP):

Mark 802.1p priority:

Tag VLAN ID:

@ 2000-2008 ZTE Corporation. All rights reserved.

Click **Save/Apply** to save the configuration so that the changes can take effect.

This page is intentionally blank.

Chapter 11

Routing Configuration

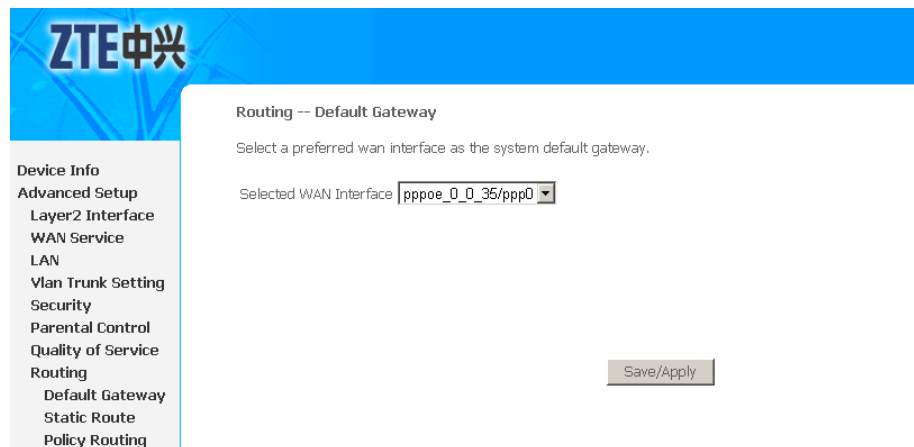
Table of Contents

Routing – Default Gateway	109
Static Routes	110
Policy Routing	111
RIP	113

Routing – Default Gateway

Select **Advanced Setup > Routing > Default Gateway** to display the interface as shown in [Figure 135](#).

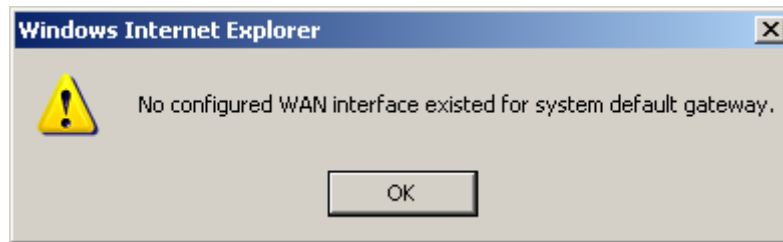
FIGURE 135 DEFAULT GATEWAY



Select the dedicated WAN interface.

If there is no existing WAN interface to be selected for default gateway, notice will be pop-up as shown in [Figure 136](#).

FIGURE 136 DEFAULT GATEWAY NOTICE



Click **Save/Apply** to save the configuration so that the changes can take effect.

Static Routes

Background Networking devices forward packets using route information that is either manually configured or dynamically learned using a routing protocol. Static routes are manually configured and define an explicit path between two networking devices. Unlike a dynamic routing protocol, static routes are not automatically updated and must be manually re-configured if the network topology changes. The benefits of using static routes include security and resource efficiency. Static routes use less bandwidth than dynamic routing protocols and no CPU cycles are used to calculate and communicate routes. The main disadvantage to using static routes is the lack of automatic re-configuration if the network topology changes.

Static routes can be redistributed into dynamic routing protocols but routes generated by dynamic routing protocols cannot be redistributed into the static routing table. No algorithm exists to prevent the configuration of routing loops that use static routes.

Static routes are useful for smaller networks with only one path to an outside network and to provide security for a larger network for certain types of traffic or links to other networks that need more control. In general, most networks use dynamic routing protocols to communicate between networking devices but may have one or two static routes configured for special cases.

Adding Static Route

1. Select **Advanced Setup > Routing > Static Routes** to display the interface as shown in [Figure 137](#).

FIGURE 137 ADDING STATIC ROUTE

ZTE中兴 Language Select: En

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click Save/Apply to add the entry to the routing table.

**Notice: If existing only one IPoE/MER wan connection in the router, please surely use gateway ip address and select default gateway.
But for PPPoE wan connection, you can select interface.**

Destination Network Address:

Subnet Mask:

Use Interface:

Save/Apply

2. Enter the **Destination Nnetwork Address** and **Subnet Mask**.
3. Select the **Use Interface**.
4. If select **LAN/br0** interface, you need to define **Use Gateway IP Address**, as shown in [Figure 138](#).

FIGURE 138 ADDING STATIC ROUTE WITH LAN BRIDGE INTERFACE

ZTE中兴 Language Select: En

Routing -- Static Route Add

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click Save/Apply to add the entry to the routing table.

**Notice: If existing only one IPoE/MER wan connection in the router, please surely use gateway ip address and select default gateway.
But for PPPoE wan connection, you can select interface.**

Destination Network Address:

Subnet Mask:

Use Interface:

Use Gateway IP Address:

Save/Apply

5. Click **Save/Apply** to save the configuration so that the changes can take effect.

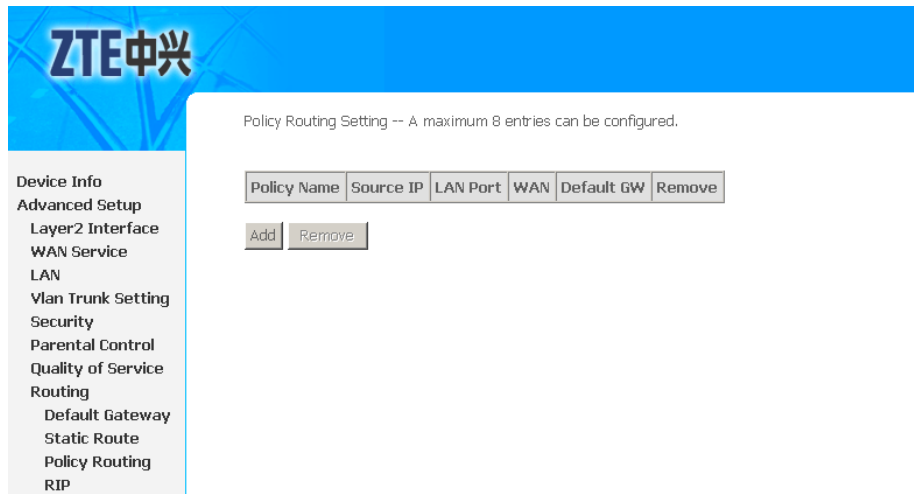
Removing Static Route

Select the **Remove** check box in the table and click **Remove** to apply the settings.

Policy Routing

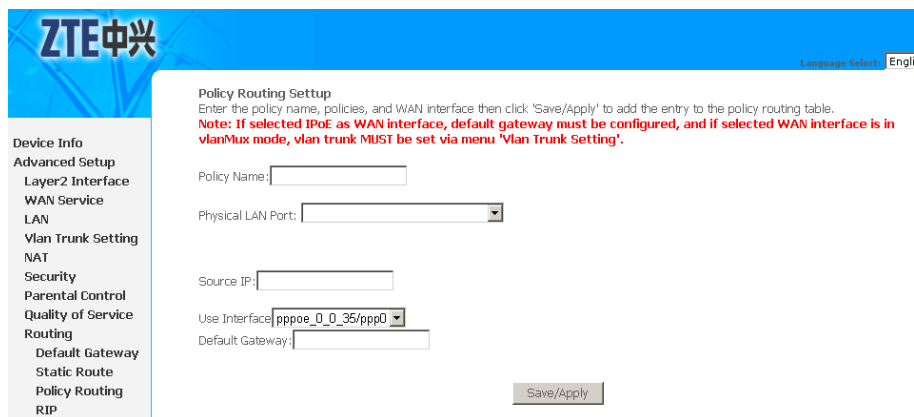
1. Select **Advanced Setup > Routing > Policy Routing** to display the interface as shown in [Figure 139](#).

FIGURE 139 POLICY ROUTING OVERVIEW



2. Click **Add** in the above interface to enter the interface as shown in [Figure 140](#).

FIGURE 140 ADDING POLICY ROUTING



3. [Table 22](#) is a description of the different options.

TABLE 22 POLICY ROUTING CONFIGURATION OPTIONS

Term	Description
Policy Name	Define policy name.
Physical LAN Port	Define physical LAN port.
Source IP	Define source IP address.
Use Interface	Select the WAN interface. If select IPoE as WAN interface, default gateway must be configured, and if selected WAN inter-

Term	Description
	face is in vlanMux mode, VLAN trunk must be set.
Default Gateway	Define default gateway IP address.

- Click **Save/Apply** to save the configuration so that the changes can take effect.

RIP

Background

The Routing Information Protocol (RIP) is one of the most enduring of all routing protocols. RIP is also one of the more easily confused protocols because a variety of RIP-like routing protocols proliferated, some of which even used the same name! RIP and the myriad RIP-like protocols were based on the same set of algorithms that use distance vectors to mathematically compare routes to identify the best path to any given destination address. These algorithms emerged from academic research that dates back to 1957.

The open standard version of RIP today, sometimes referred to as IP RIP, is formally defined in two documents: Request For Comments (RFC) 1058 and Internet Standard (STD) 56. As IP-based networks became more and larger in scale, it became apparent to the Internet Engineering Task Force (IETF) that RIP needed to be updated. Consequently, the IETF released RFC 1388 in January 1993, which then superseded RFC 1723, which described RIP 2 (the second version of RIP) in November 1994. These RFCs described an extension of RIP capabilities but did not attempt to abandon the previous versions of RIP. RIP 2 enabled RIP messages to carry more information, which permitted the use of a simple authentication mechanism to secure table updates. More importantly, RIP 2 supported subnet masks, a critical feature that was not available in RIP.

This section summarizes the basic capabilities and features associated with RIP. Topics include the routing update process, RIP routing metrics, routing stability, and routing timers.

Routing Updates

RIP sends routing-update messages at regular intervals and when the network topology changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. RIP routers maintain only the best route (the route with the lowest metric value) to a destination. After updating its routing table, the 931WII immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send.

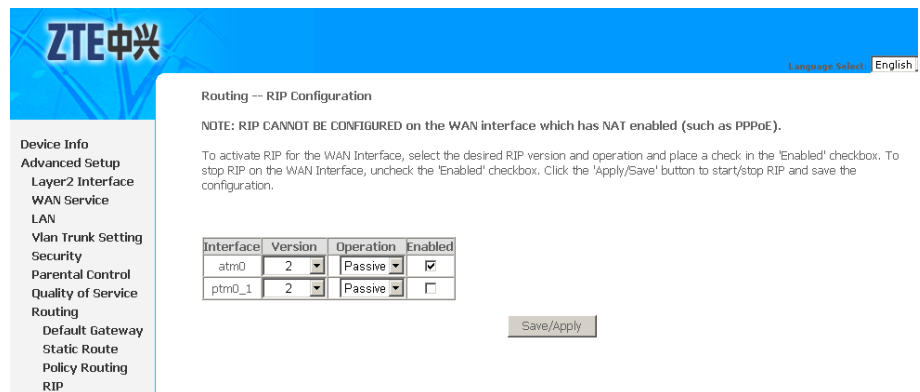
RIP Routing Metric

RIP uses a single routing metric (hop count) to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1. When a router receives a routing update that

contains a new or changed destination network entry, the 931WII adds 1 to the metric value indicated in the update and enters the network in the routing table. The IP address of the sender is used as the next hop.

- RIP Configuration**
1. Select **Advanced Setup > Routing > RIP** to display the interface as shown in [Figure 141](#).

FIGURE 141 RIP CONFIGURATION



2. Select the desired RIP **Version** and **Operation**.
3. Select the **Enabled** check-box.
4. Click **Save/Apply** to save the configuration so that the changes can take effect.

DNS

Table of Contents

DNS Server	115
Dynamic DNS	116

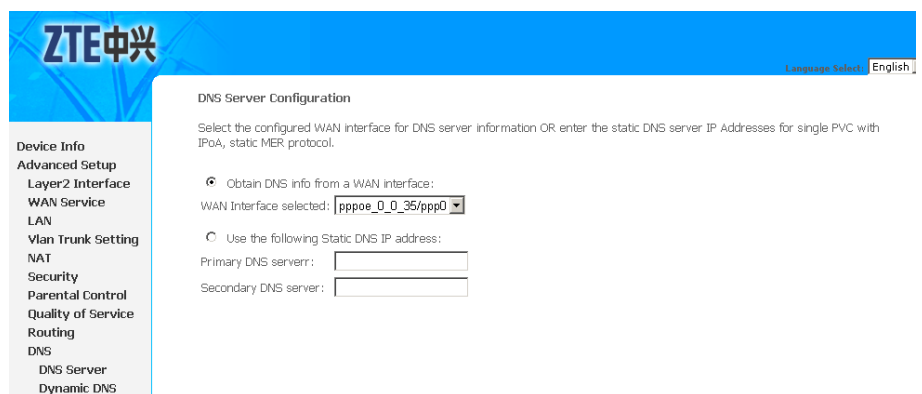
DNS Server

Domain Name System (or Service or Server) (**DNS**) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name *www.example.com* might translate to 198.105.232.4.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks other DNSs one by one, until the correct IP address is returned.

1. Select **Advanced Setup > DNS > DNS Server** to display the interface as shown in [Figure 142](#).

FIGURE 142 DNS SERVER CONFIGURATION OVERVIEW



2. If **Obtain DNS info from a WAN interface** is selected, device accepts the first received DNS assignment from WAN connection.
3. Select the WAN interface from the **WAN Interface selected** drop-down list.

4. If **Use the following Static DNS IP address** is selected, enter the **Primary DNS server** and **Secondary DNS server**.
5. Click **Save** to save the configuration so that the changes can take effect.

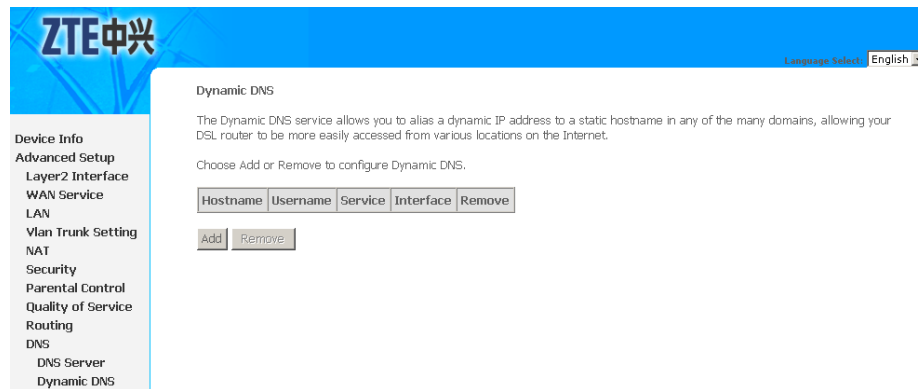
**Note:**

You must reboot the 931WII to effect the new configuration.

Dynamic DNS

1. Select **Advanced Setup > DNS > Dynamic DNS** to display the interface as shown in [Figure 143](#).

FIGURE 143 DYNAMIC DNS CONFIGURATION OVERVIEW



2. Click **Add** to display the interface as shown in [Figure 144](#).

FIGURE 144 ADDING DYNAMIC DNS

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider:

Hostname:

Interface:

DynDNS Settings

Username:

Password:

3. [Table 23](#) is a description of the different options.

TABLE 23 DYNAMIC DNS CONFIGURATION OPTIONS

Field	Description
D-DNS provider	You can add a Dynamic DNS address from DynDNS.org or TZO.
Hostname	Enter the dynamic DNS server hostname.
Interface	Select the used WAN interface.
Username	Enter the dynamic DNS server username.
Password	Enter the dynamic DNS server password.

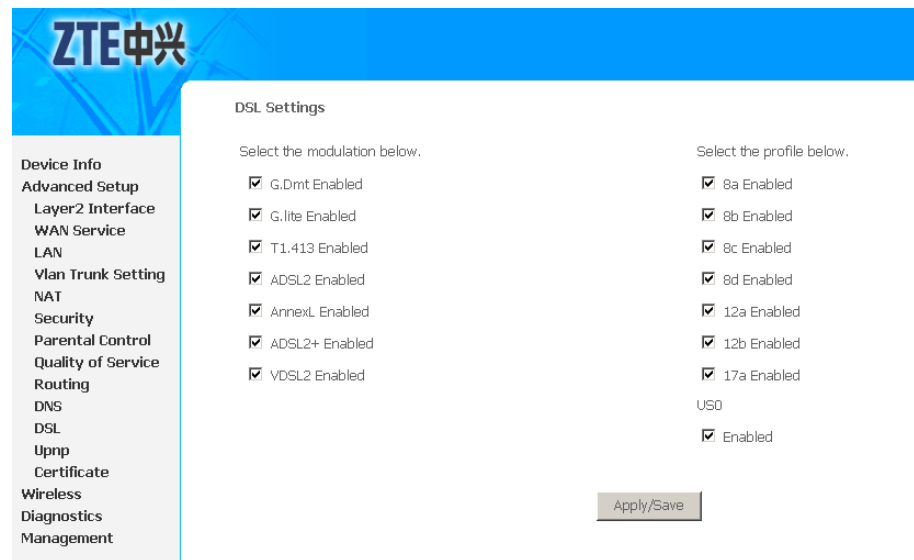
4. Click **Save/Apply** to save the configuration so that the changes can take effect.

This page is intentionally blank.

DSL Configuration

Select **Advanced Setup > DSL** to display the interface as shown in [Figure 145](#).

FIGURE 145 DSL CONFIGURATION



By default, the 931WII is compatible with all modulation methods of **ADSL2+** and **VDSL2**.

Un-check **VDSL2 Enabled** checkbox to disable VDSL2 modulation

Note:

You can only select the modulation you are using to enhance the 931WII performance.

Click **Save/Apply** to save the configuration so that the changes can take effect.

This page is intentionally blank.

IPSec

Internet Protocol Security Associations (IPSec) allows creation of secure tunnels in the Internet Protocol (IP) layer. Secure tunnels are used to construct VPNs over the internet. The IPSec protocol design includes Internet Security Association Key Management Protocol (ISAKMP) framework. The Internet Key Exchange (IKE) protocol is the primary protocol to generate and maintain IPSec Security Associations (SAs), which are the basic building blocks of VPNs over the Internet. IKE uses cryptography extensively. However, cryptography can be regarded as a module to generate a key and use it to encrypt or decrypt the payload. Once the SAs are established, the payload is transferred using IPSec Encapsulating Security Payload (ESP) or Authentication Header (AH) protocols. In the two payload transfer protocols, ESP and AH, the former is most widely used and suitable for NAT operation.

IPSec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

For IPsec to work, the sending and receiving devices must share a public key. This is accomplished through a protocol known as ISAKMP/Oakley, which allows the receiver to obtain a public key and authenticate the sender using digital certificates.

Table of Contents

VPN	121
ISAKMP	122
IKE	123

VPN

A virtual private network (VPN) provides a secure connection between a sender and a receiver over a public non-secure network such as the Internet. A secure connection is generally associated with private networks. (A private network is a network that is owned, or at least controlled via leased lines, by an organization.) Using the techniques discussed later in this chapter, a VPN can transform the characteristics of a public non-secure network into those of a private secure network. VPNs reduce remote access costs by using public network resources. Compared to other solutions, including private networks, a VPN is inexpensive.

VPNs are not new. In fact, they have been used in telephone networks for years and have become more prevalent since the development of the intelligent network. Frame relay networks, which have been around for some time, are VPNs. Virtual private networks are only new to IP networks such as the Internet. Therefore, some authors use the terms Internet VPN and virtual private data network to distinguish the VPN described in this chapter from other VPNs. In this book, the term VPN refers to Internet VPN.

The goal of a VPN is to provide a secure passage for data of users over the non-secure Internet. It enables companies to use the Internet as the virtual backbone for their corporate networks by allowing them to create secure virtual links between their corporate office and branch or remote offices via the Internet. The cost benefits of VPN service have prompted corporations to move more of their data from private [WANs](#) to Internet-based VPNs.

ISAKMP

ISAKMP is a definition of a high level abstract framework for point to point, two party asymmetric key management protocols. Being asymmetric one party assumes the role of initiator, which begins the exchange of protocol messages by sending the first message. The second is the responder which replies to the first message from the initiator. ISAKMP makes a distinction between a key exchange and key management (when the key is rolled to the next one). Key exchange is mainly concerned with exchanging information to generate secret keys shared between two parties. ISAKMP negotiation is divided into two phases. In the first phase ISAKMP SA is established between two entities to protect further negotiation traffic. The second phase SA is used for some security protocol.

The key exchange protocol must:

- Generate a set of secret keys shared between the initiator and the responder.
- Authenticate the identity of the initiator and the responder.
- Ensure independence of the sets of keys generated. This property is also known as Perfect Forward Secrecy (PFS).
- Key exchange protocol must be scalable.

Once the keys are generated and shared, there must be some parameters agreed between the parties to use the keys. The following are the parameters to use the keys:

- Cryptographic algorithms and parameters to the cryptographic algorithms to be used with the keys.
- How to apply the cryptographic algorithms and keys.
- Key lifetime and refreshment policy.

IKE

The Internet Key Exchange (IKE) protocol is a key management protocol standard which is used in conjunction with the IPSec standard. IPSec is an IP security feature that provides robust authentication and encryption of IP packets. IPSec can be configured without IKE, but IKE enhances IPSec by providing additional features, flexibility, and ease of configuration for the IPSec standard.

IKE is a hybrid protocol which implements the OAKLEY key exchange and SKEME key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, OAKLEY, and SKEME are security protocols implemented by IKE.).

- OAKLEY: Describes a specific mechanism for exchanging keys through the definition of various key exchange “modes”. Most of the IKE key exchange process is based on OAKLEY.
- SKEME: Describes a different key exchange mechanism than OAKLEY. IKE uses some features from SKEME, including its method of public key encryption and its fast re-keying feature.

This page is intentionally blank.

Chapter 15

Parental Control

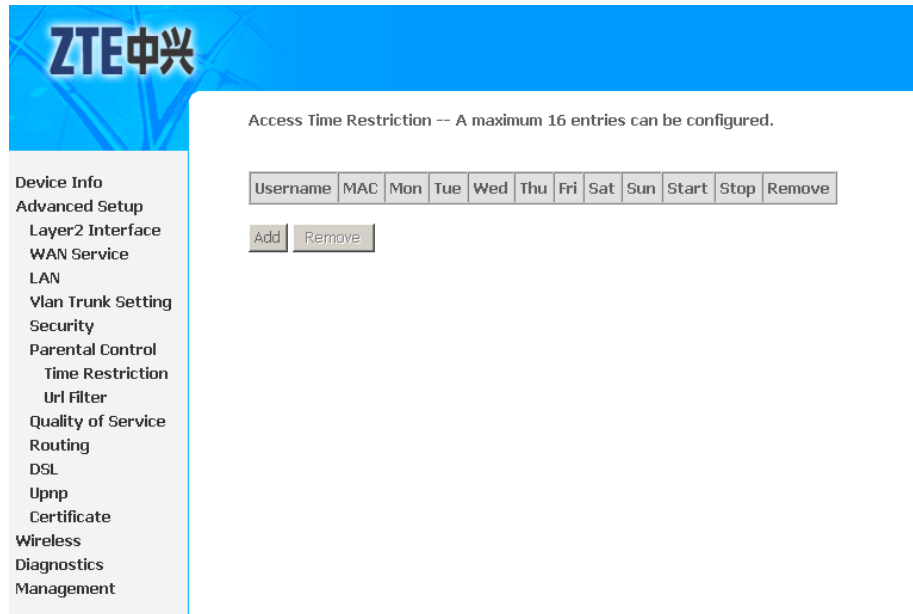
Table of Contents

Time Restriction	125
URL Filter	126

Time Restriction

Select **Advanced Setup > Parental Control > Time Restriction** to display the interface as shown in [Figure 146](#).

FIGURE 146 TIME RESTRICTION OVERVIEW



Click **Add** to display the interface as shown in [Figure 147](#).

FIGURE 147 TIME RESTRICTION CONFIG

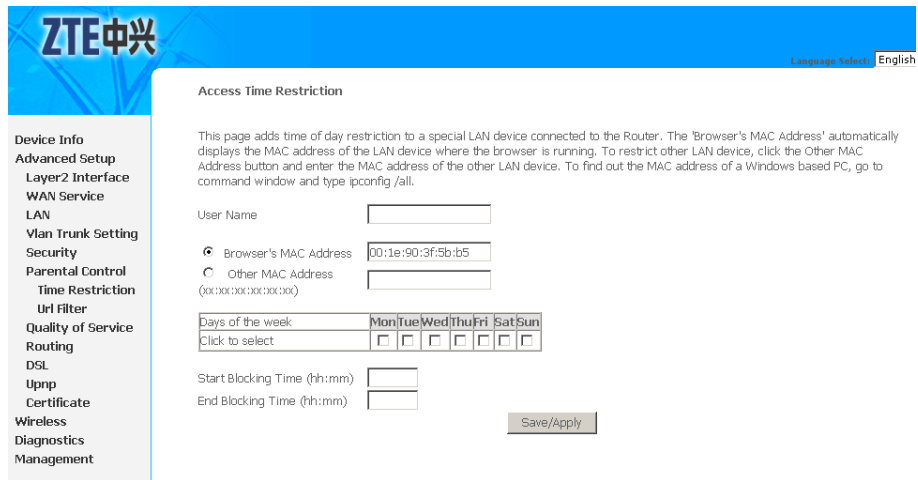


Table 24 is a description of the different options.

TABLE 24 TIME RESTRICTION CONFIGURATION OPTIONS

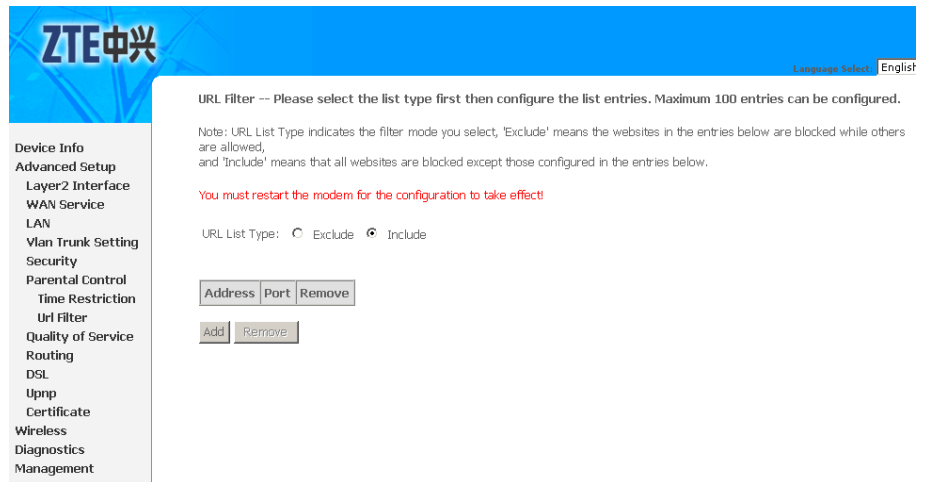
Term	Description
User name	Define the restriction name.
Browser’s MAC Address	Automatically displays the MAC address of the LAN device where the browser is running.
Other MAC Address	To restrict other LAN device, enter the MAC address of the other LAN devices.
Days Of the Week	Select the blocking day in a week.
Starting Blocking Time/Ending Blocking Time	Define the starting and tending blocking time.

Click **Save/Apply** to save the configuration so that the changes can take effect.

URL Filter

1. Select **Advanced Setup > Parental Control > URL Filter** to display the interface as shown in [Figure 148](#).

FIGURE 148 URL FILTER OVERVIEW



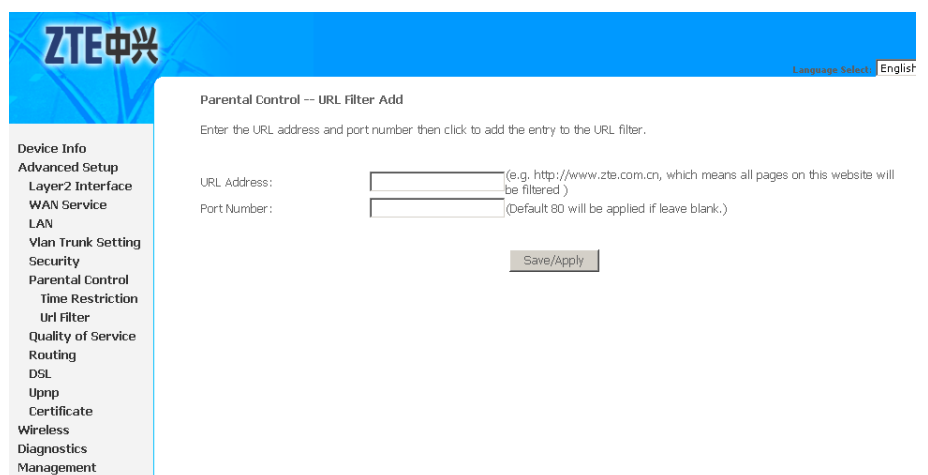
2. [Table 25](#) is a description of the different options.

TABLE 25 URL FILTER BASIC CONFIGURATION OPTIONS

Term	Description
Exclude	Websites in the entries are blocked while others are allowed.
Include	All websites are blocked except those configured in the entries below.

3. Click **Add** to enter the interface as shown in [Figure 149](#).

FIGURE 149 URL FILTER CONFIG



4. Input the **URL Address** and **Port Number**.
5. Click **Save/Apply** to save the configuration so that the changes can take effect.



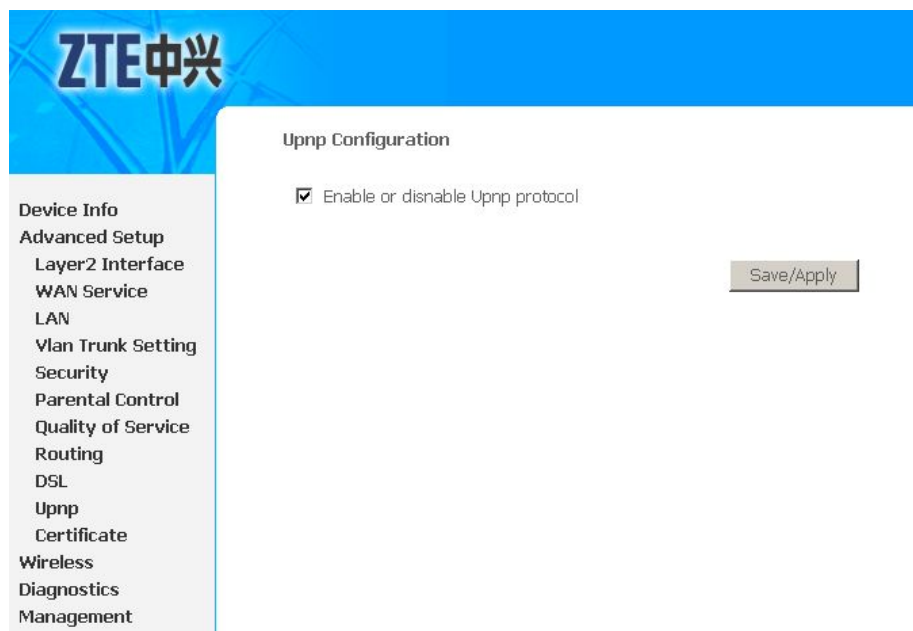
Note:

You must restart the Modem for the configuration to take effect.

UPNP Configuration

Select **Advanced Setup > Upnp** to display the interface as shown in [Figure 150](#).

FIGURE 150 UPNP CONFIG



Select **Enable or disable Upnp protocol** checkbox to enable the UPNP function

Click **Save/Apply** to save the configuration so that the changes can take effect.

Note:

The operating system of the PC must be Windows ME or Windows XP. Check whether the UPnP function is installed in the PC. You may need to retrospectively install the UPnP components, even on systems with Windows XP or Windows ME. Refer to the User Guide of your PC.

After you install UPnP in the operating system of a PC and activate it in the 931WII, applications on this PC (for example, Microsoft Messenger) can communicate via the Internet without authorization. In this case, the 931WII automatically implements port for-

warding, thereby facilitating communication via the Internet. The task bar in the PC in which UPnP is installed contains an icon for the 931WII. In a Windows XP system, the icon is also shown under network connections. Click this icon and the user interface of the 931WII appears.

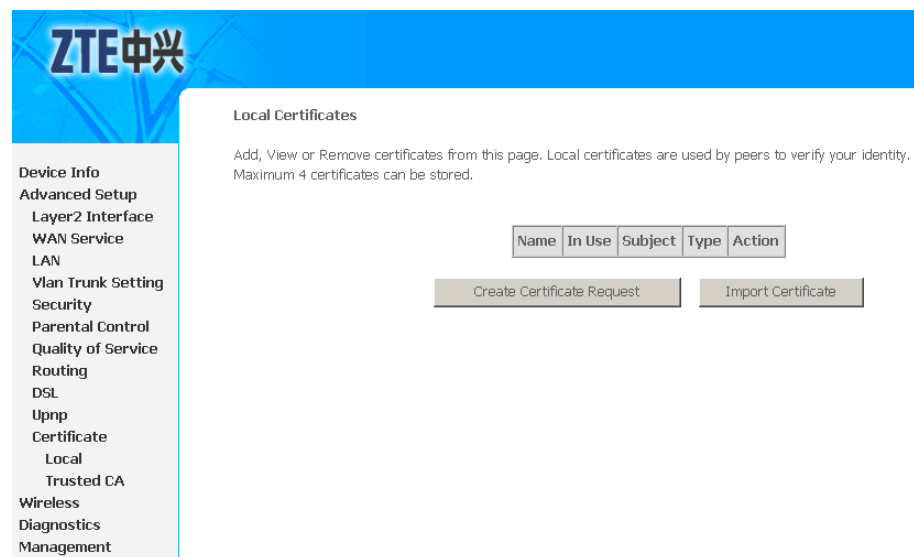
**Note:**

When the UPnP function is active, system applications can assign and use ports on a PC. This poses a security risk.

Certificate Configuration

Select **Advanced Setup > Certificate** to display the interface as shown in [Figure 151](#).

FIGURE 151 LOCAL CERTIFICATE OVERVIEW



For either type of certificate, the page shows a list of certificates stored in the modem.

In this menu, two items appear: **Local** and **Trusted CA**:

- **Local**: local certificates, to preserve the identity of the modem.
- **Trusted CA**: trusted Certificate Authority certificates which are used by the modem to verify certificates from other hosts.

You can create local certificates in either of the following two ways:

- Create a new certificate request, have it signed by a certificate authority and load the signed certificate.
- Import an existing signed certificate directly.

Table of Contents

Create New Local Certificate	132
Import An Existing Local Certificate.....	134
Import Trusted CA Certificates.....	135

Create New Local Certificate

1. Click **Create Certificate Request** in above interface to enter the interface as shown in [Figure 152](#).

FIGURE 152 CREATE NEW CERTIFICATE REQUEST

ZTE中兴 Language Select: English

Create new certificate request

To generate a certificate signing request you need to include Common Name, Organization Name, State/Province Name, and the 2-letter Country Code for the certificate.

Certificate Name:

Common Name:

Organization Name:

State/Province Name:

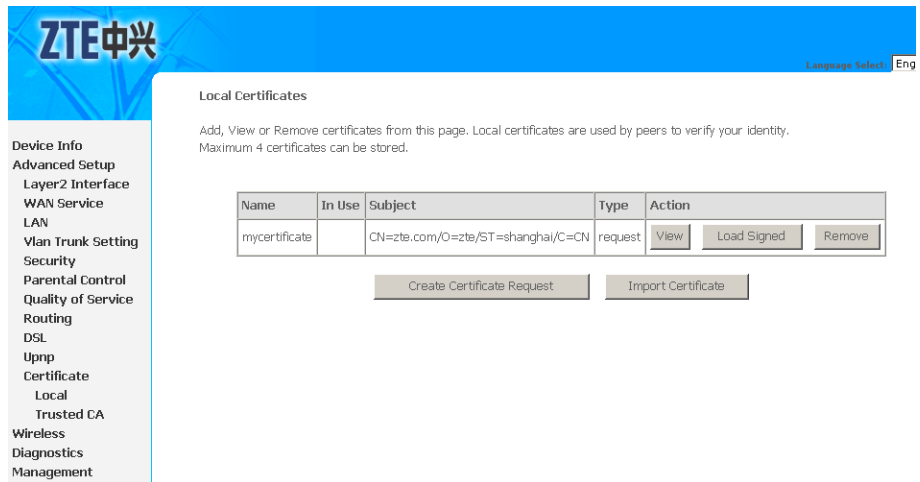
Country/region Name:

[Table 26](#) is a description of the different options.

TABLE 26 CREATE CERTIFICATE REQUEST CONFIGURATION OPTIONS

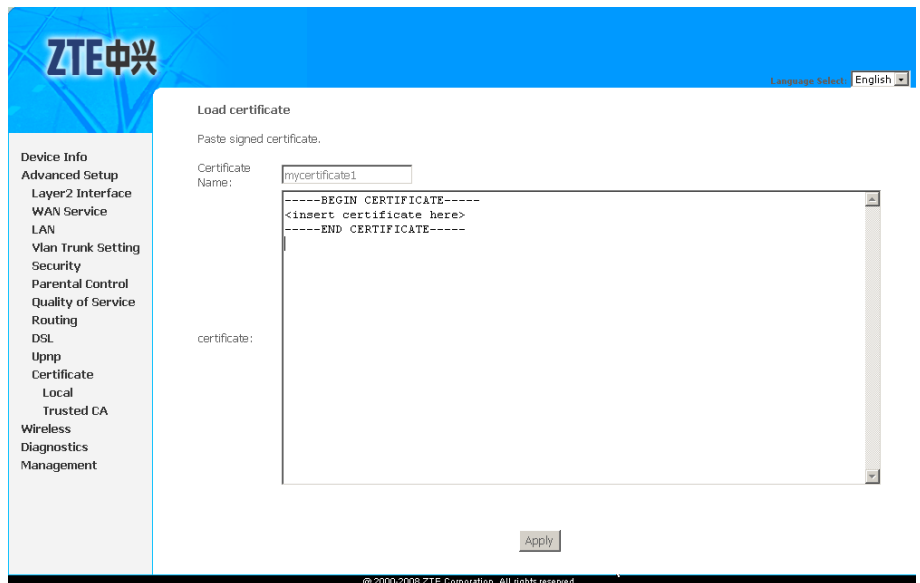
Field	Description
Certificate name	Creates an SSL certificate in the specified certificate repository (administrator's or domain's repository) by using a private key file and a corresponding certificate file.
Common Name	The common name is the fully qualified domain name (FQDN) used for DNS lookups of your server (for example, www.my-domain.com). Browsers use this information to identify your Web site. Some browsers refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Do not include the protocol specifier "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as * or ?, and do not use an IP address.
Organization Name	The name of the organization to which the entity belongs (such as the name of a company).

FIGURE 154 GENERATED CERTIFICATE COMPLETED



5. Paste the signed certificate as shown in [Figure 155](#).

FIGURE 155 LOAD CERTIFICATE

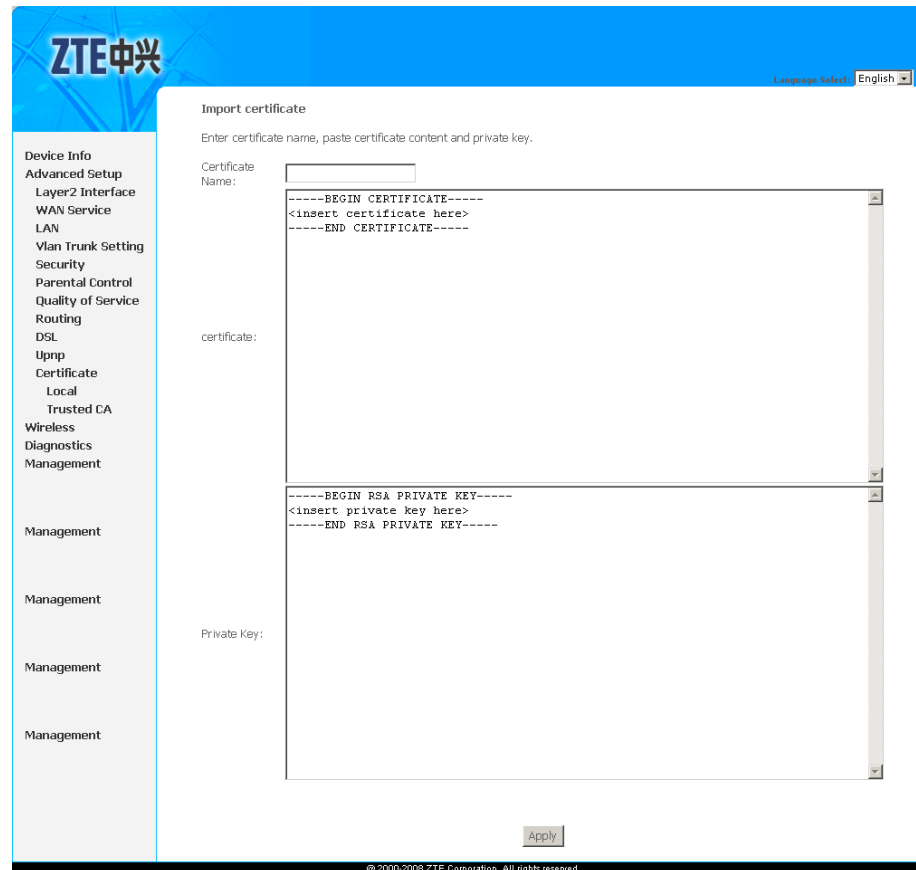


Import An Existing Local Certificate

Click **Import Certificate** in above interface to enter the interface as shown in .

Paste both certificate and corresponding private key, as shown in [Figure 156](#).

FIGURE 156 IMPORT CERTIFICATE



Import certificate

Enter certificate name, paste certificate content and private key.

Certificate Name:

certificate:

```
-----BEGIN CERTIFICATE-----  
<insert certificate here>  
-----END CERTIFICATE-----
```

Private Key:

```
-----BEGIN RSA PRIVATE KEY-----  
<insert private key here>  
-----END RSA PRIVATE KEY-----
```

Apply

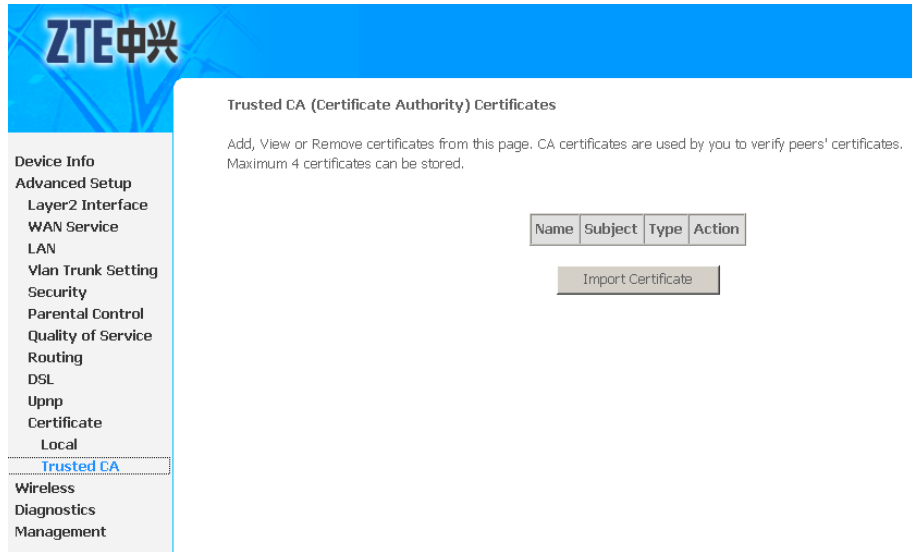
@ 2000-2008 ZTE Corporation. All rights reserved.

Click **Apply** to save the configuration so that the changes can take effect.

Import Trusted CA Certificates

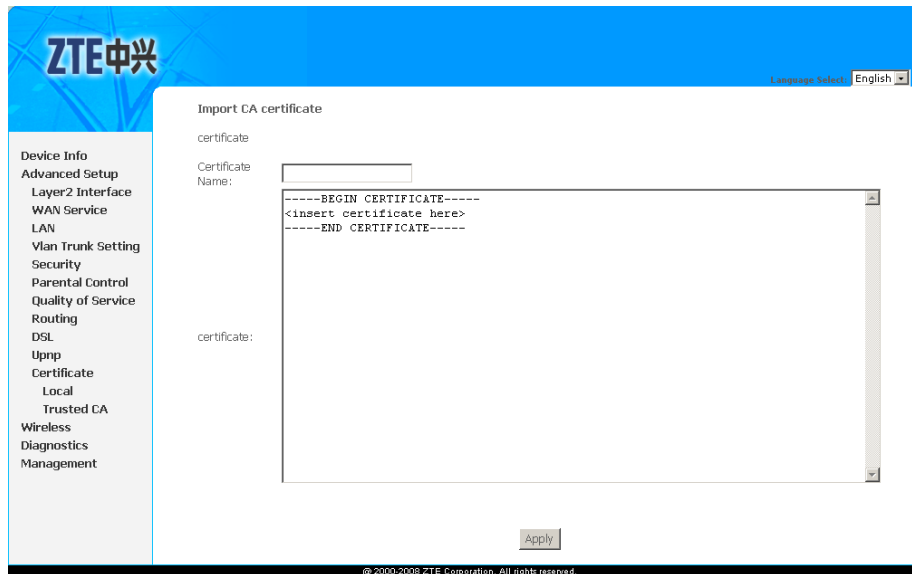
Select **Advanced Setup > Certificate > Trusted CA** to display the interface as shown in [Figure 157](#).

FIGURE 157 TRUSTED CA CERTIFICATES



Click **Import Certificate** to display the interface as shown in [Figure 158](#), CA certificate can only be imported.

FIGURE 158 IMPORT CERTIFICATE



Chapter 18

Wireless Configuration

Table of Contents

Overview	137
Wireless LAN Basics	139
Configure Wireless Connection	147

Overview

Wireless Network

There are two types of wireless network set up:

- Client Mode (infrastructure)
- Ad Hoc Mode (peer-to-peer)

Client Mode Client Mode is an 802.11 networking framework, as shown in [Figure 159](#), in which devices communicate with each other by first going through a wireless router or access point. Wireless devices can communicate with each other or can communicate with a wired network. Generally, a majority of small businesses and home users operate in Client Mode because they require access to the wired LAN (usually from broadband or cable Internet providers) in order to use services such as file servers or printers.

FIGURE 159 CLIENT MODE



Ad Hoc Mode Ad Hoc (sometimes referred to as peer-to-peer), is a type of wireless network allowing a wireless adapter or other Ethernet-ready device to connect directly to another wireless adapter or Ethernet-ready device. Its network protocol is as shown in [Figure 160](#).

FIGURE 160 AD HOC MODE



About the Guw5.5Z66-5

The Guw5.5Z66-5 Wi-Fi® certified IEEE 802.11g compliant wireless access point allows multiple computers to connect wirelessly to your local network over the Guw5.5Z66-5 Wireless LAN environment.

The Guw5.5Z66-5 is backward compatible with IEEE 802.11b, which means 802.11b and 802.11g devices can coexist in the same wireless network.

The Wireless Distribution System (WDS) on your Guw5.5Z66-5 allows you to extend the range of your wireless network. To be able to use WDS, you need to introduce an additional WDS-enabled access point into your wireless network. To be able to connect the computers, make sure that a wireless client adapter (**WLAN** client) is installed on each computer you want to connect via the WLAN.

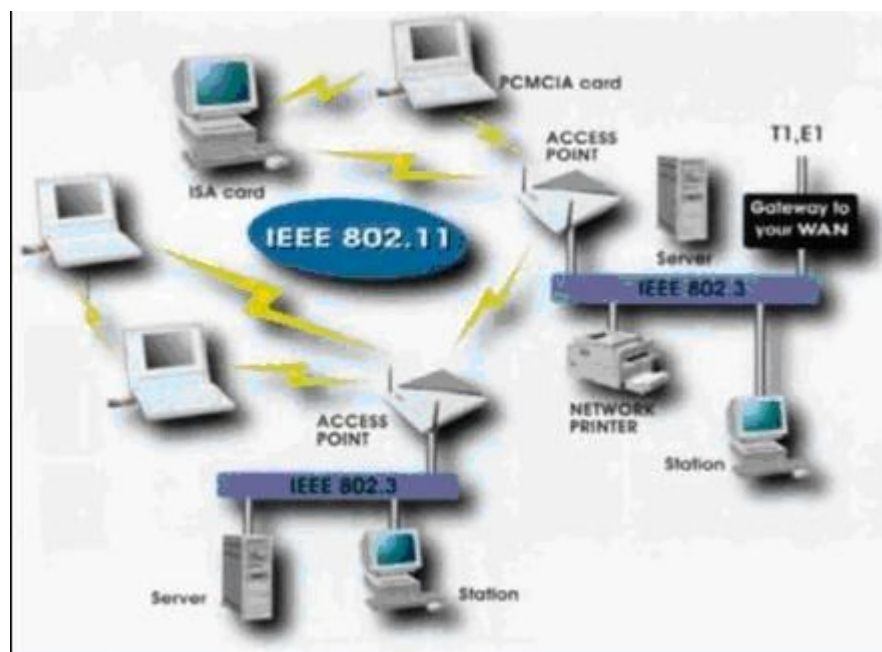
Wireless LAN Basics

Some basic understanding of 802.11b/g wireless technology and terminology is useful when you are setting up the 931WII or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

Basic terms

Typical wireless network topology is as shown in [Figure 161](#).

FIGURE 161 TYPICAL WIRELESS NETWORK TOPOLOGY



A few terms in the figure should be understood, explanation is as shown in [Table 27](#).

TABLE 27 WLAN BASIC TERMS

Term	Description
AP	Short for Access Point, a hardware device or the software of a computer that acts as a communication hub for users of a wireless device to connect to a wired LAN. APs are important for providing reinforced wireless security and for extending the physical range of service a wireless user has access to.
STA	Any device that contains an IEEE 802.11 conformant medium access control (MAC) or physical layer (PHY) interface to the wireless medium (WM).
SSID	Wireless networks use a Service Set Identifier (SSID) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set to use the same SSID, so that wireless stations can move from one location to another without losing connection to the wireless network. The Guw5.5Z66-5 operates in Infrastructure mode. It controls network access on the wireless interface in its broadcast area. It allows access to the wireless network by devices that use the correct SSID after a negotiation process takes place. By default, the Guw5.5Z66-5 broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate. You may disable SSID broadcast.

Wireless Standard

Wireless Standard includes 802.11a, 802.11b, 802.11g, and 802.11n.

- 802.11b

IEEE expanded the original 802.11 standard in July 1999, creating the 802.11b specification. 802.11b supports bandwidth

up to 11 Mbps, comparable to traditional Ethernet. 802.11b uses the same unregulated radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs.

Being unregulated, 802.11b devices can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b devices a reasonable distance from other appliances, interference can easily be avoided.

- 802.11g

In 2002 and 2003, WLAN products supporting a newer standard called 802.11g emerged on the market. 802.11g attempts to combine the best of both 802.11a and 802.11b.

802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points work with 802.11b wireless network adapters and vice versa.

- 802.11a

While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called 802.11a. Because 802.11b gained popularity much faster than 802.11a, it is believed that 802.11a was created after 802.11b. In fact, 802.11a was created at the same time. Due to its higher cost, 802.11a is usually found on business networks whereas 802.11b better serves the home market.

802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions.

Because 802.11a and 802.11b utilize different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid 802.11a/b network devices, but these products merely implement the two standards side by side (each connected devices must use one or the other).

Use [Table 28](#) below to get some quick information to help you differentiate between the available wireless networking standards.

TABLE 28 WIRELESS NETWORKING STANDARDS

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons & More Info
IEEE802.11	Up to 2 Mbps in the 2.4 GHz band	FHSS or DSSS	WEP & WPA	This specification has been extended into 802.11b.

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons & More Info
IEEE 802.11a (Wi-Fi)	Up to 54 Mbps in the 5 GHz band	OFDM	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified". Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE 802.11b (Wi-Fi)	Up to 11 Mbps in the 2.4 GHz band	DSSS with CCK	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified". Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons & More Info
				the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.11g (Wi-Fi)	Up to 54 Mbps in the 2.4 GHz band	OFDM above 20Mbps, DSSS with CCK below 20 Mbps	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified". May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.

 **Note:**

Maximum wireless signal rate based on IEEE Standard 802.11g specifications is 54 Mbps. But actual data throughput varies. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead causes lower actual data throughput rate.

Wireless Security

Various security options are available on the Guw5.5Z66-5 including open or WEP, 802.1x, WPA, WPA-PSK, WPA2 and WPA2-PSK. The following section describes some authentications.

WEP Wireless Encryption Protocol (WEP) is part of the IEEE 802.11 wireless networking standard and was designed to provide the same level of security as that of a wired LAN. Because wireless networks broadcast messages using radio, they are susceptible to eavesdropping, WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

WEP was the encryption scheme considered to be the initial standard for first generation wireless networking devices. However, it has been found that WEP is not as secure as once believed. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security.

The major weakness of WEP is its use of static encryption keys. When you set up a router with a WEP encryption key, that key is used by every device on your network to encrypt every packet that is transmitted. But the fact that packets are encrypted does not prevent them from being intercepted, and due to some technical flaws it is entirely possible for an eavesdropper to intercept enough WEP-encrypted packets to eventually deduce what the key is.

WPA Wi-Fi Protected Access (WPA) debuts to address many shortcomings of WEP. It includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the key is not tampered.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

To encrypt a network with WPA Personal/PSK, you should set up your router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. Using a technology called TKIP, that passphrase, along with the network SSID, is used to generate unique encryption keys, which are constantly changed, for each wireless client. Although WEP also supports passphrases, it does so only as a way to more easily create static keys, which are usually comprised of the hex characters 0-9 and A-F.

802.1x The 802.1x standard is designed to enhance the security of wireless local area networks (WLANs) that follow the IEEE 802.11 standard. 802.1x provides an authentication framework for wireless LANs, allowing a user to be authenticated by a central authority. The actual algorithm that is used to determine whether a user is authentic is left open and multiple algorithms are possible.

802.1X uses an existing protocol, the Extensible Authentication Protocol (EAP, RFC 2284), that works on Ethernet, Token Ring, or wireless LANs, for message exchange during the authentication process.

In a wireless LAN with 802.1X, a user (known as the supplicant) requests access to an access point (known as the authenticator). The access point forces the user (actually, the client software of the user) into an unauthorized state that allows the client to send only an EAP start message. The access point returns an EAP message requesting the identity of the user. The client returns the identity, which is then forwarded by the access point to the authentication server, which uses an algorithm to authenticate the user and then returns an accept or reject message back to the access point. Assuming an accept was received, the access point changes the client's state to authorized and normal transmission can take place.

The authentication server may use the Remote Authentication Dial-In User Service (RADIUS), although 802.1x does not specify it.

WPS Wi-Fi Protected Setup (WPS), was introduced and developed by the Wi-Fi Alliance (<http://www.wi-fi.org/>) to help standardize and simplify ways of setting up and configuring security on a wireless network.

Traditionally, users would have to manually create a wireless network name (SSID), and manually enter a creative, yet predictable security key on both the access point and the client, to prevent unwanted access to their wireless network. This entire process requires the users to have the background knowledge of the Wi-Fi devices and the ability to make the necessary configuration changes.

WPS was introduced to relieve and remove all of the guess work of securing a wireless network by typing a short PIN (numeric code) or pushing a button (Push-Button Configuration, or PBC). On a new wireless network, WPS automatically configures a wireless network with a network name (SSID) and strong WPA data encryption and authentication. WPS is designed to support various Wi-Fi certified 802.11 products ranging from access points, wireless adapters, Wi-Fi phones, and other consumer electronics devices.

Advantages of WPS:

- WPS automatically configures the network name (SSID) and WPA security key for the access point and the WPS enabled client devices on a network. You do not need to know the SSID and security keys or passphrases when connecting WPS-enabled devices.
- No one can guess or figure out your security keys or passphrase because the keys are randomly generated. You need not enter predictable passphrases or long sequences of hexadecimal. Information and network credentials are securely exchanged over the air using the EAP, one of the authentication protocols used in WPA2.
- WPS has been integrated and supported in Windows Vista. Currently, Windows Vista only works in Registrar mode.

Disadvantages of WPS:

- It does not support Ad-Hoc mode or network where wireless devices communicate directly with each other without an access point. All Wi-Fi devices in the network must be WPS certified or WPS-compatible, otherwise you cannot take advantage of the ease of securing the network.
- Difficult to add a non-WPS client device to the network because of the long sequences of hexadecimal characters generated by the WPS technology. As this technology is fairly new, not every vendor supports the WPS technology.

Wireless Client requirements

Radio Transmission

WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the WLAN nodes in its broadcast range. WLAN nodes transmit digital data using frequency modulation (FM) radio signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. Digital data is superimposed onto the carrier signal. This radio signal carries data to WLAN devices within range of the transmitting device.

The antennae of WLAN devices listen for and receive the signal. The signal is demodulated and the transmitted data is extracted. The transmission method used by the access point is called Direct Sequence Spread Spectrum (DSSS) and DSSS is operated in a range of the radio spectrum between 2.4 GHz and 2.5 GHz for transmission. See the expert technical specifications for more details on wireless operation.

Antenna

Direct the external antenna to allow optimization of the wireless link. If for example the antenna is erect, wireless links in the horizontal plane are favored.

Note that the antenna characteristics are influenced by the environment, that is, by reflections of the radio signal against walls or ceilings. It is advisable to use the received signal strength as indicated by the wireless client manager to optimize the antenna position for the link to a given client. Concrete walls weaken the radio signal and thus affect the connection.

Range

Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the 931WII in a location between the WLAN devices that maintains a roughly equal straight-line distance to all devices that need to access the 931WII through the wireless interface. Adding more 802.11g access points to rooms where the signal is weak can improve signal strength.

Radio Channel

The 802.11g standard allows several WLAN networks using different radio channels to be co-located. The Guw5.5Z66-5 supports multiple radio channels and is able to select the best radio channel at each startup. You can choose to set the channels automatically or manually. Different channels overlap. To avoid interference with another access point, make sure that the separation (in terms of frequency) is as high as possible. It is recommended to keep at least 3 channels between 2 different access points.

The Guw5.5Z66-5 supports all channels allowed for wireless networking. However, depending on local regulations, the number of channels actually allowed to be used may be restricted, as shown in [Table 29](#).

TABLE 29 RADIO CHANNEL RESTRICTION

Regulatory Domain	Allowed Radio Channels
China	1 to 13
Europe	1 to 13
Israel	5 to 8
Japan	1 to 14
Jordan	10 to 13
Thailand	1 to 14
USA / Canada	1 to 11

Wireless Distribution System

The [WLAN](#) series of APs use wireless ports to interconnect BSS areas.

WDS is commonly used in areas requiring multiple APs, where wiring is not possible or costly, and is used for providing backup paths between APs.

The number of ports on an AP available for the WDS depends on the AP model. The 520wl for example, allows up to six WDS links. The same frequency channels must be used on each end of a WDS link.

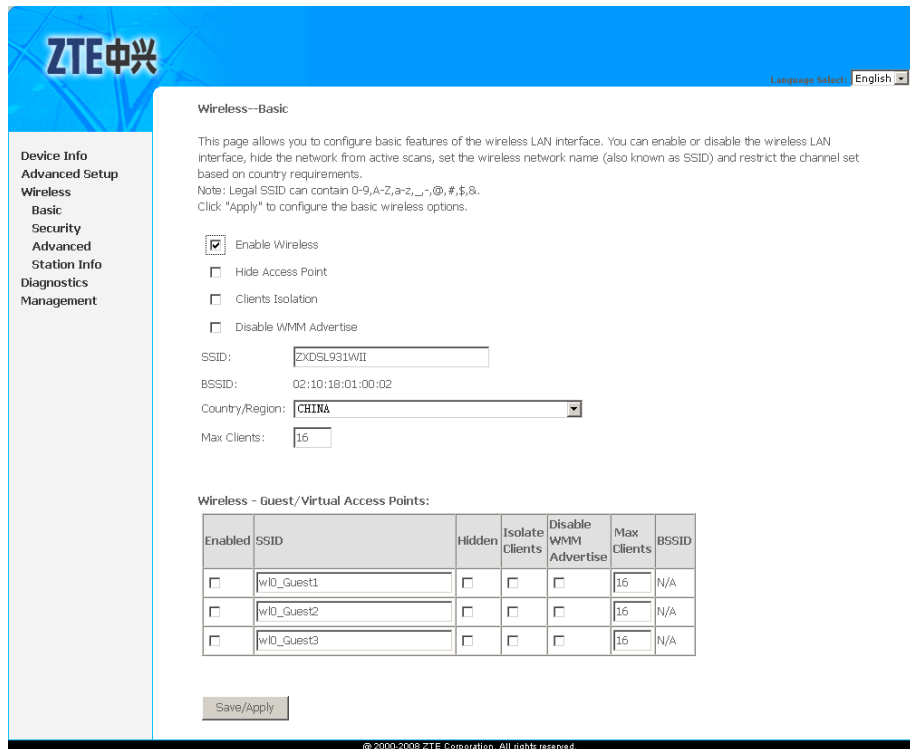
The same PC card that supports a BSS area can be used for a WDS link. The packet flow through the WDS is very similar to the standard DS except it uses the wireless ports instead of the Ethernet port.

Configure Wireless Connection

Wireless - Basic

Select **Wireless > Basic** to display the interface as shown in [Figure 162](#).

FIGURE 162 WIRELESS - BASIC



This page allows you to configure basic features of the **WLAN** interface. You can enable or disable the WLAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.

[Table 30](#) is the description of the different options.

TABLE 30 WIRELESS BASIC CONFIGURATION OPTIONS

Field	Description
Enable Wireless	Select this check box to enable wireless. If this check box is not selected, the Hide Access Point, Clients Isolation, Disable WMM Advertise, SSID, BSSID, Country/Region, Max Clients, Wireless - Guest/Virtual Access Points boxes are not displayed.
Hide Access Point	Select this check box if you want to hide any access point for your router, so a station cannot obtain the SSID through passive scanning.

Field	Description
Clients Isolation	When many clients connect to the same access point, they can access each other. If you want to disable the access between clients which connect the same access point, you can select this check box.
Disable WMM Advertise	Wi-Fi multimedia (WMM) can provide high-performance multimedia voice and video data transfers.
SSID	The SSID is the network name shared among all points in a wireless network. The SSID must be identical for all points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). Make sure this setting is the same for all points in your wireless network. For added security, you should change the default SSID to a unique name.
Country/Region	The name of the country with which your gateway is configured. This parameter further specifies your wireless connection. For example, the channel adjusts according to the region to adapt to the frequency provision of the specific region.
Max Clients	Specifies the maximum number of wireless client stations that can be connected to the AP. Once the clients exceed the max value, all other clients are refused. The value range is between six and ten.
Wireless - Guest/Virtual Access Points	If you want to make Guest/Virtual network function available, you must select those check boxes in the table below. In the current software version, three virtual access points can be configured.

Click **Save/Apply** to save the basic wireless options so that the changes can take effect.

Wireless–Security

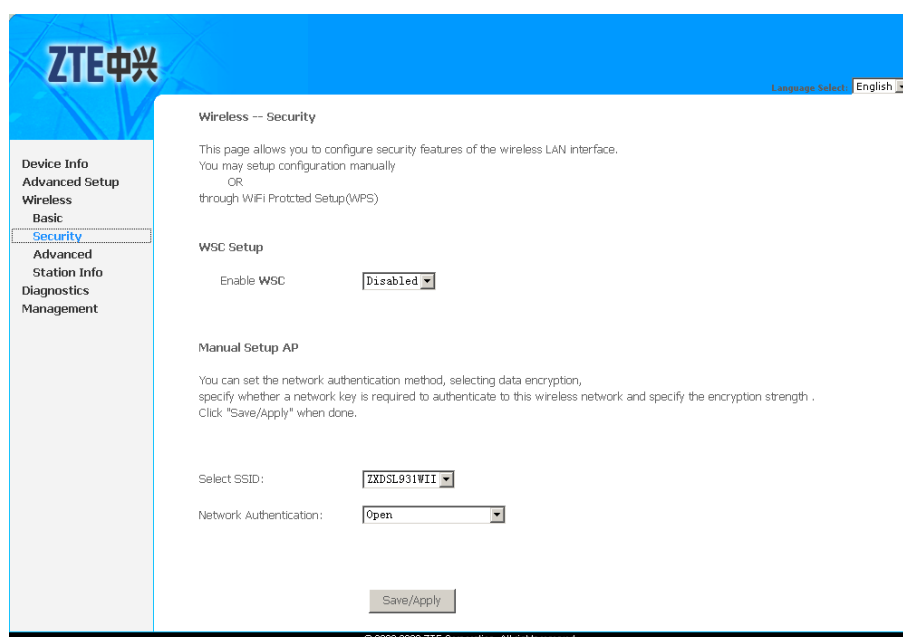
This device is equipped with 802.1X and WPA/WPA2 (Wi-Fi Protected Access), the latest security standard. It also supports the legacy security standard WEP.

By default, wireless security is disabled and authentication is open. Before enabling the security, consider your network size, complexity, and existing authentication infrastructure, and then determine the solution to adopt.

No Encryption

Select **Wireless > Security** to display the interface as shown in [Figure 163](#).

FIGURE 163 WIRELESS-SECURITY (NO ENCRYPTION)



This page allows you can configure security features of the WLAN interface. You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.

[Table 31](#) is the description of the different options.

TABLE 31 WLAN SECURITY NO ENCRYPTION CONFIGURATION OPTIONS

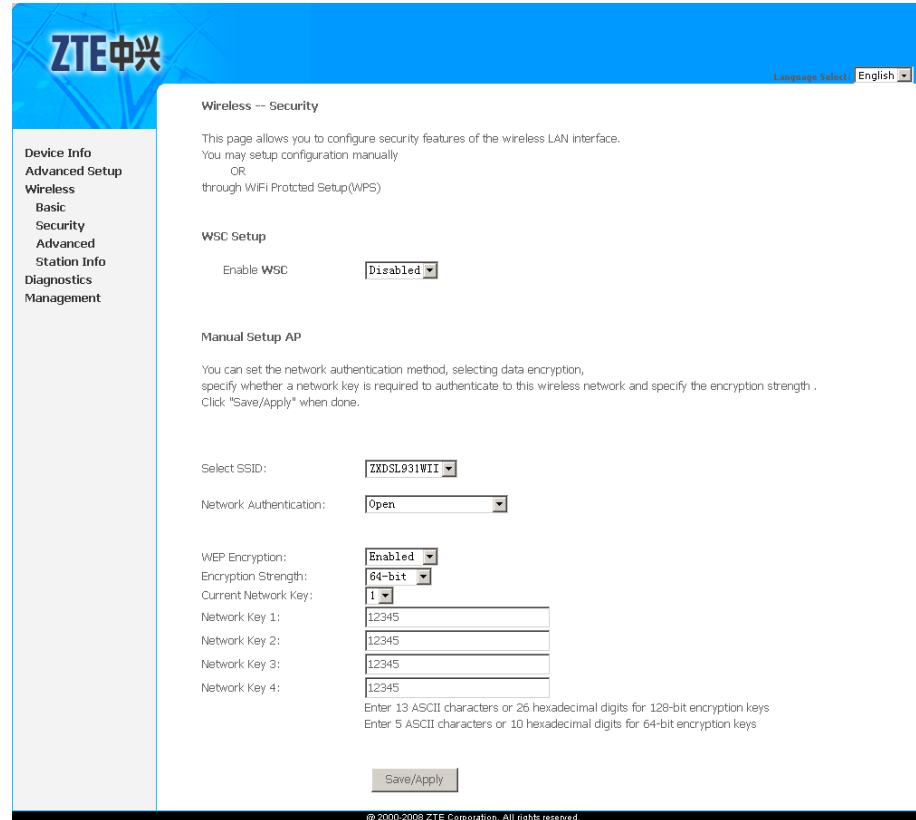
Field	Description
Select SSID	Select the wireless LAN of SSID to configure security features.
Network Authentication	Set the authentication mode for the selected wireless LAN of SSID to Open .

Click **Save/Apply** to save the WLAN security options so that the changes can take effect.

64-bit WEP

Select **Wireless > Security** to enter Security configuration interface. Select **64-bit** in **Encryption Strength** to display the interface as shown in [Figure 164](#).

FIGURE 164 WIRELESS-SECURITY (64-BIT WEP)



[Table 32](#) is the description of the different options.

TABLE 32 WLAN SECURITY 64-BIT WEP ENCRYPTION CONFIGURATION OPTIONS

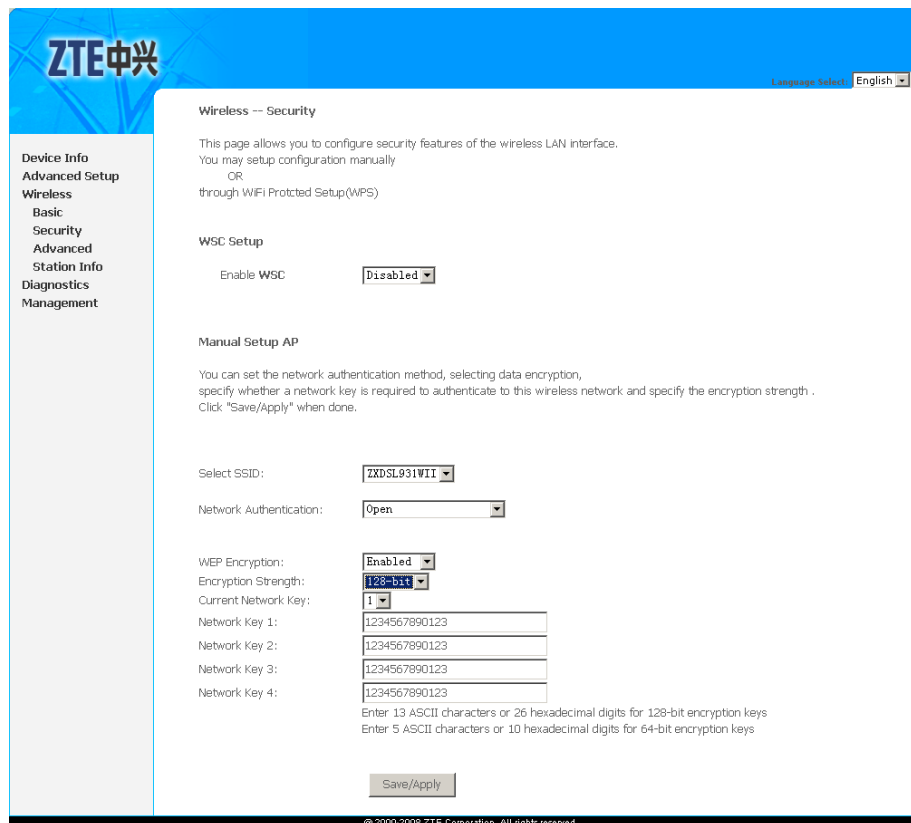
Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be Open or Shared .
WEP Encryption	Enable WEP Encryption.
Encryption Strength	Set the data security type to 64-bit .
Current Network Key	Select one of network key that you set on the Key boxes as the default one.
Network Key 1 to 4	Enter 5 ASCII characters or 10 hexadecimal digits for a 64-bit encryption key. You can set up to 4 WEP keys.

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

128-bit WEP

Select **Wireless > Security** to enter Security configuration interface. Select **128-bit** in **Encryption Strength** to display the interface as shown in [Figure 165](#).

FIGURE 165 WIRELESS-SECURITY (128-BIT WEP)



[Table 33](#) is the description of the different options.

TABLE 33 WLAN SECURITY 128-BIT WEP ENCRYPTION CONFIGURATION OPTIONS

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be Open or Shared .
WEP Encryption	Enable WEP Encryption.
Encryption Strength	Set the data security type to 128-bit .

Field	Description
Current Network Key	Select one of network key that you set on the Key boxes as the default one.
Network Key 1 to 4	Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys. You can set 4 WEP keys.

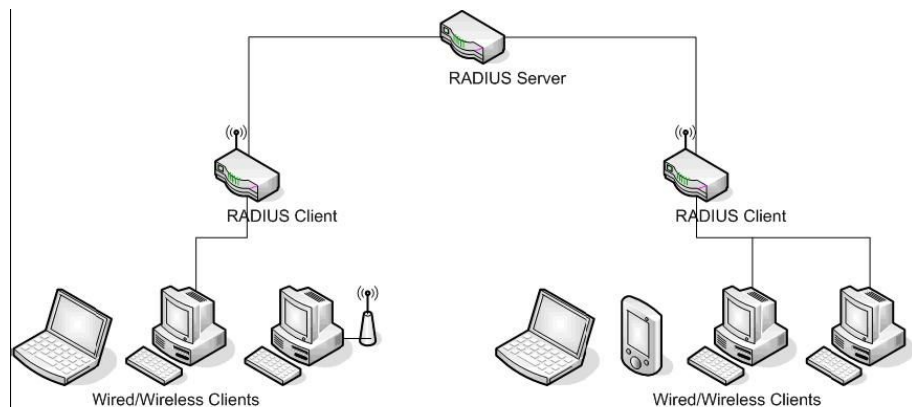
Click **Save/Apply** to save the wireless security options so that the changes can take effect.

802.1x Authentication

Before introducing the following authentications, you need to understand the Radius server. Radius server is usually a third party server, used for authentication of wireless clients who wish to connect to an access point. The wireless client contacts an access point (a Radius client), which in turn communicates with the Radius server.

The Radius server performs the authentication by verifying the credentials of the client, to determine whether the device is authorized to connect to the LAN interface of the access point. If the Radius server accepts the client, it responds by exchanging data with the access point, including security keys for subsequent encrypted sessions. A typical topology which adopt the radius server is displayed in [Figure 166](#).

FIGURE 166 AUTHENTICATION TOPOLOGY ADOPTING RADIUS SERVER



Select **Wireless > Security** to enter Security configuration interface. Select **802.1x** in **Network Authentication** display the interface as shown in [Figure 167](#).

FIGURE 167 WIRELESS-SECURITY (802.1X AUTHENTICATION)

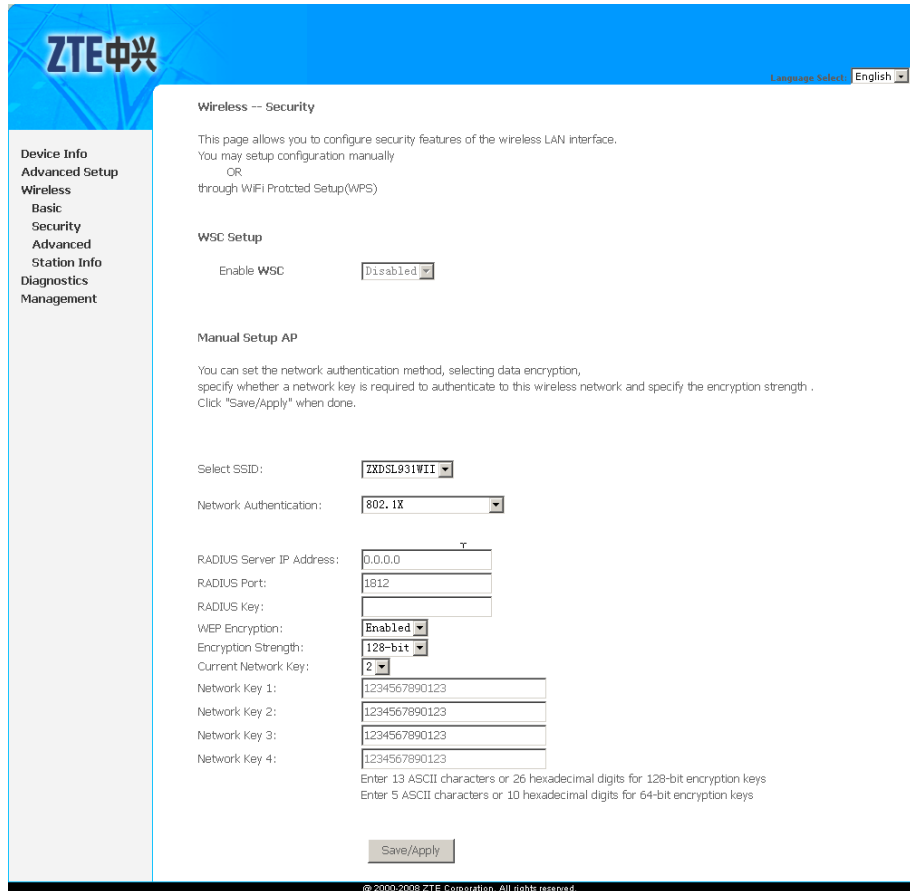


Table 34 is the description of the different options.

TABLE 34 WLAN SECURITY 802.1X AUTHENTICATION CONFIGURATION OPTIONS

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be 802.1x .
Radius Server IP Adress	Enter the IP Address of the authentication server.
Radius Port	Enter the port number of the authentication server. The default port number is 1812 .
Radius Key	Enter the same key as that on the Radius server.
WEP Encryption	Enable WEP Encryption. The default is <u>Enabled</u> .
Encryption Strength	Set the data security level to 64-bit or 128-bit .

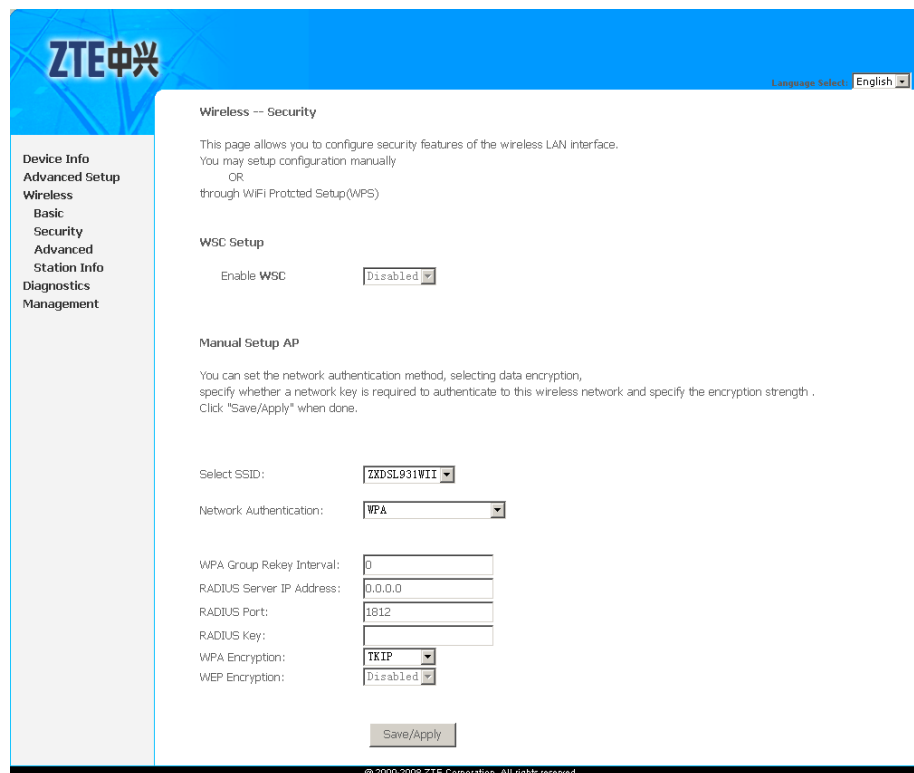
Field	Description
Current Network Key	Select one of network key that you set on the Key boxes as the default one.
Network Key 1 to 4	For a 64-bit encryption key, enter 5 ASCII characters or 10 hexadecimal digits. For a 128-bit encryption key, enter 13 ASCII characters or 26 hexadecimal digits. You can set 4 WEP keys.

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

WPA Authentication

Select **Wireless > Security** to enter Security configuration interface. Select **WPA** in **Network Authentication** display the interface as shown in [Figure 168](#).

FIGURE 168 WIRELESS-SECURITY (WPA AUTHENTICATION)



[Table 35](#) is the description of the different options.

TABLE 35 WLAN SECURITY WPA AUTHENTICATION CONFIGURATION OPTIONS

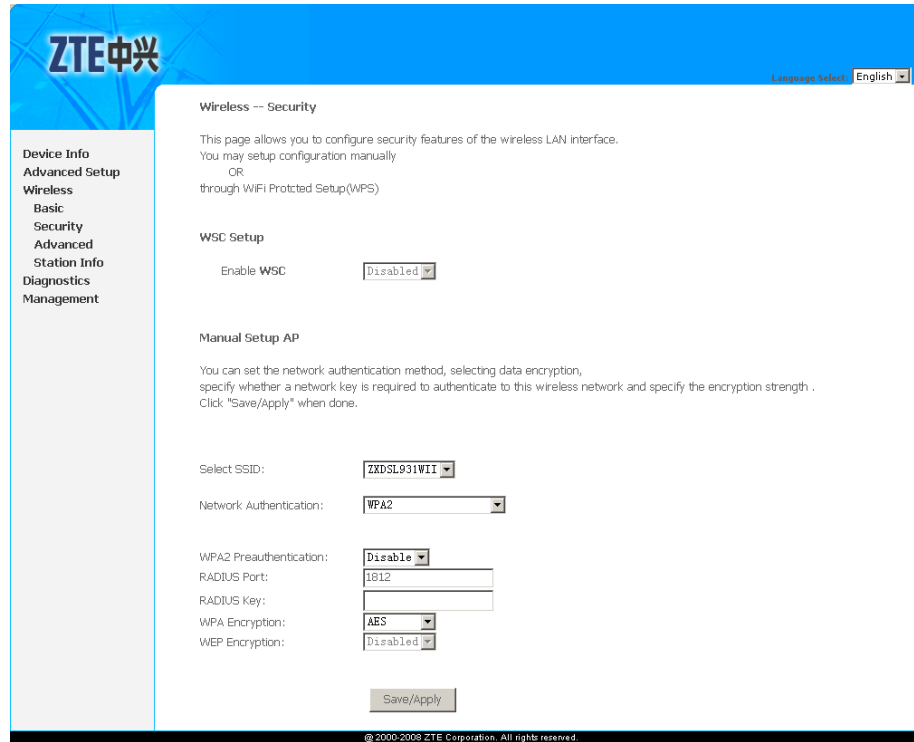
Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be WPA-PSK .
WPA Group Rekey Interval	Specifies the time interval for which the WPA key remains unchanged. The value 0 indicates that you need not change the WPA key. The change is done automatically between the server and the client.
Radius Server IP Address	Enter the IP address of the authentication server.
Radius Port	Enter the port number of the authentication server. The default port number is 1812 .
Radius Key	Enter the same key as that on the Radius server.
WPA Encryption	Select TKIP, AES or TKIP + AES. TKIP is the default encryption mode. The TKIP + AES encryption mode means AP auto adjusts to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

WPA2 Authentication

Select **Wireless > Security** to enter Security configuration interface. Select **WPA2** in **Network Authentication** display the interface as shown in [Figure 169](#).

FIGURE 169 WIRELESS–SECURITY (WPA2 AUTHENTICATION)



[Table 36](#) is the description of the different options.

TABLE 36 WLAN SECURITY WPA2 AUTHENTICATION CONFIGURATION OPTIONS

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be WPA2 .
WPA2 Preauthentication	Select Enable or Disable .
Network Re-auth Interval	Specifies the time of re-authentication between the server and the client.
WPA Group Rekey Interval	Specifies the time interval after which the WPA key must change. If the value is set to 0, the key needs not to be changed. The change is done automatically between the server and the client.
Radius Server IP Adress	Enter the IP address of the authentication server.
Radius Port	Enter the port number of the authentication server. The default port number is 1812 .

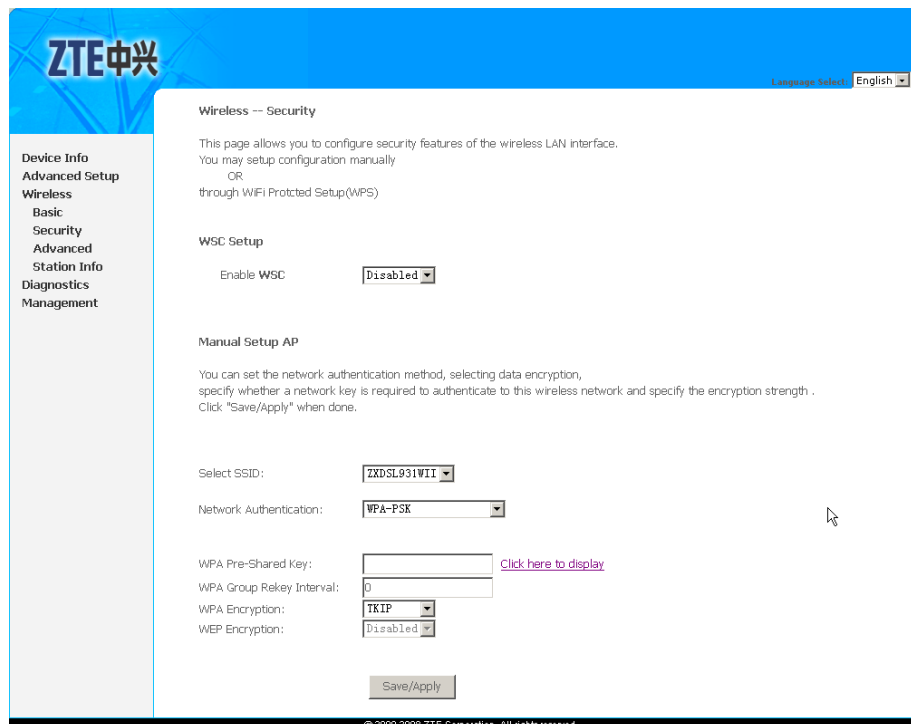
Field	Description
Radius Key	Enter the same key as that on the Radius server.
WPA Encryption	Select TKIP, AES or TKIP + AES. AES is the default encryption mode. The TKIP + AES encryption mode means that the AP automatically adjusts to use TKIP or AES according to wireless clients.

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

WPA-PSK Authentication

Select **Wireless > Security** to enter Security configuration interface. Select **WPA-PSK** in **Network Authentication** display the interface as shown in [Figure 170](#).

FIGURE 170 WIRELESS-SECURITY (WPA-PSK AUTHENTICATION)



[Table 37](#) is the description of the different options.

TABLE 37 WLAN SECURITY WPA AUTHENTICATION CONFIGURATION OPTIONS

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be WPA-PSK .
WPA Pre-Shared Key	Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Refer to Table 38 for instructions when entering the key.
WPA Group Rekey Interval	Specifies the time interval after which the WPA key must change. If the value is set to 0, the key needs not to be changed. The change is done automatically between the server and the client.
WPA Encryption	Select TKIP, AES or TKIP + AES. AES is the default encryption mode. The TKIP + AES encryption mode means that the AP automatically adjusts to use TKIP or AES according to wireless clients.

TABLE 38 WPA PRE-SHARED KEY

Format	Minimum Characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

WPA2-PSK Authentication

Select **Wireless > Security** to enter Security configuration interface. Select **WPA2-PSK** in **Network Authentication** display the interface as shown in [Figure 171](#).

FIGURE 171 WIRELESS-SECURITY (WPA2-PSK AUTHENTICATION)

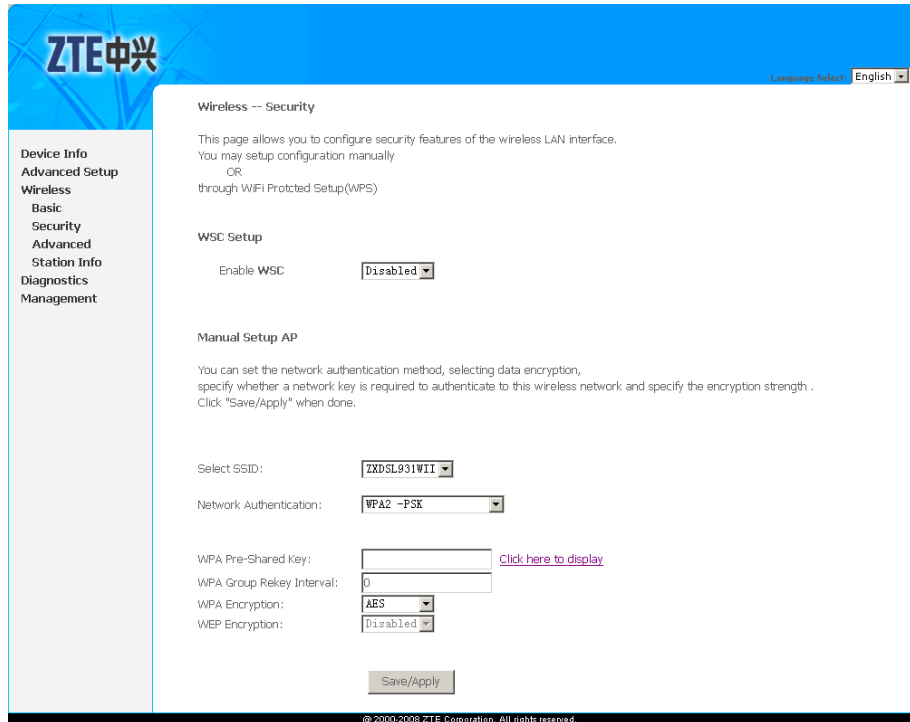


Table 39 is the description of the different options.

TABLE 39 WLAN SECURITY WPA2 AUTHENTICATION CONFIGURATION OPTIONS

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be WPA2-PSK .
WPA Pre-Shared Key	Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Refer Table 40 to for instructions when entering the key.
WPA Group Rekey Interval	Specifies the time interval after which the WPA key must change. If the value is set to 0, the key needs not to be changed. The change is done automatically between the server and the client.
WPA Encryption	Select TKIP, AES or TKIP + AES. AES is the default encryption mode. The TKIP + AES encryption mode means that the AP automatically adjusts to use TKIP or AES according to wireless clients.

TABLE 40 WPA PRE-SHARED KEY

Format	Minimum Characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

Mixed WPA2/WPA-PSK Authentication

Select **Wireless > Security** to enter Security configuration interface. Select **Mixed WPA2/WPA-PSK** in **Network Authentication** display the interface as shown in [Figure 172](#).

FIGURE 172 WIRELESS-SECURITY (MIXED WPA2/WPA-PSK AUTHENTICATION)

The screenshot shows the 'Wireless -- Security' configuration page. The page title is 'Wireless -- Security'. Below the title, there is a description: 'This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WIFI Protected Setup(WPS)'. Under 'WPS Setup', the 'Enable WPS' option is set to 'Disabled'. Under 'Manual Setup AP', there is a description: 'You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click "Save/Apply" when done.' The configuration fields are: 'Select SSID' set to 'ZXDSL931WII', 'Network Authentication' set to 'Mixed WPA2/WPA -PSK', 'WPA Pre-Shared Key' (empty), 'WPA Group Rekey Interval' set to '0', 'WPA Encryption' set to 'TKIP+AES', and 'WEP Encryption' set to 'Disabled'. A 'Save/Apply' button is at the bottom. The footer contains the copyright notice: '@ 2000-2008 ZTE Corporation. All rights reserved.'

[Table 41](#) is the description of the different options.

TABLE 41 WIRELESS-SECURITY (WPA-PSK AUTHENTICATION)

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA-PSK .
WPA Pre-Shared Key	Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Refer to Table 42 for instructions when entering the key.
WPA Group Rekey Interval	Specifies the time interval after which the WPA key must change. If the value is set to 0, the key needs not to be changed. The change is done automatically between the server and the client.
WPA Encryption	Select TKIP, AES or TKIP + AES. AES is the default encryption mode. The TKIP + AES encryption mode means that the AP automatically adjusts to use TKIP or AES according to wireless clients.

TABLE 42 WPA PRE-SHARED KEY

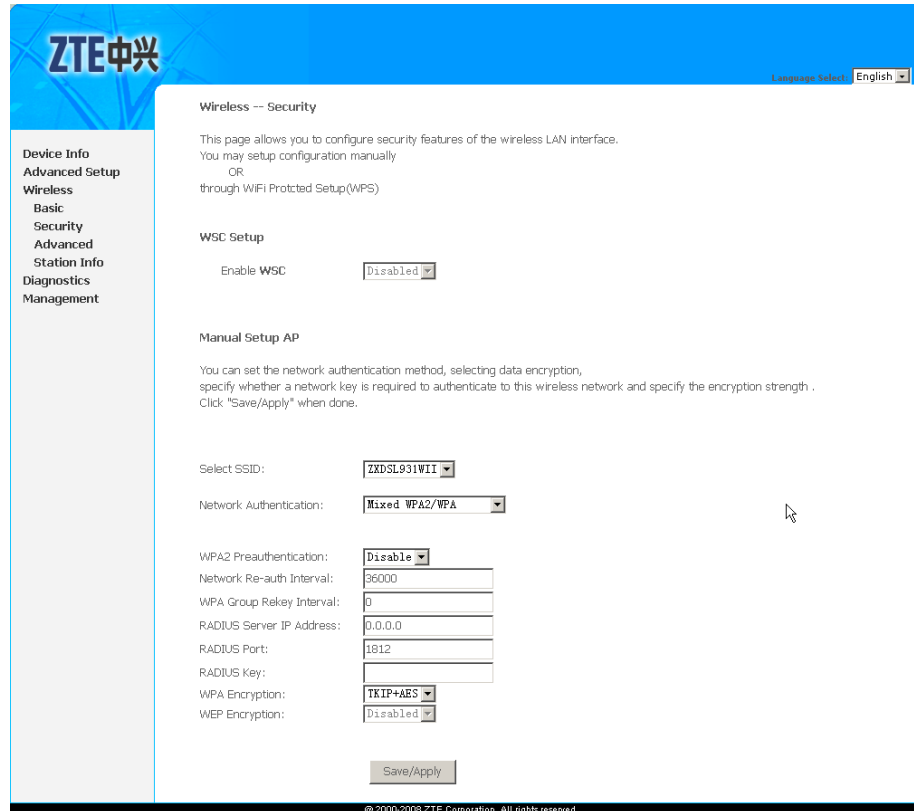
Format	Minimum Characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

Mixed WPA2/WPA Authentication

Select **Wireless > Security** to enter Security configuration interface. Select **Mixed WPA2/WPA** in **Network Authentication** display the interface as shown in [Figure 173](#).

FIGURE 173 WIRELESS–SECURITY (MIXED WPA2/WPA AUTHENTICATION)



[Table 43](#) is the description of the different options.

TABLE 43 WIRELESS–SECURITY (MIXED WPA2/WPA AUTHENTICATION)

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be Mixed WPA2/WPA .
WPA Pre-Shared Key	Enter the pre-shared key for WPA. Client stations must use the same key in order to connect with this device. Refer to Table 44 for instructions when entering the key.
WPA2 Preauthentication	Select Enable or Disable .
Network Re-auth Interval	Specifies the time interval for re-authentication between the server and the client.
WPA Group Rekey Interval	Specifies the time interval after which the WPA key must change. If the value is set to 0, the key needs not to be changed. The change is done automatically between the server and the client.

Field	Description
Radius Server IP Adress	Enter the IP address of the authentication server.
Radius Port	Enter the port number of the authentication server. The default port number is 1812 .
Radius Key	Enter the same key as that on the Radius server.
WPA Encryption	Select TKIP, AES or TKIP + AES. AES is the default encryption mode. The TKIP + AES encryption mode means that the AP automatically adjusts to use TKIP or AES according to wireless clients.

TABLE 44 WPA PRE-SHARED KEY

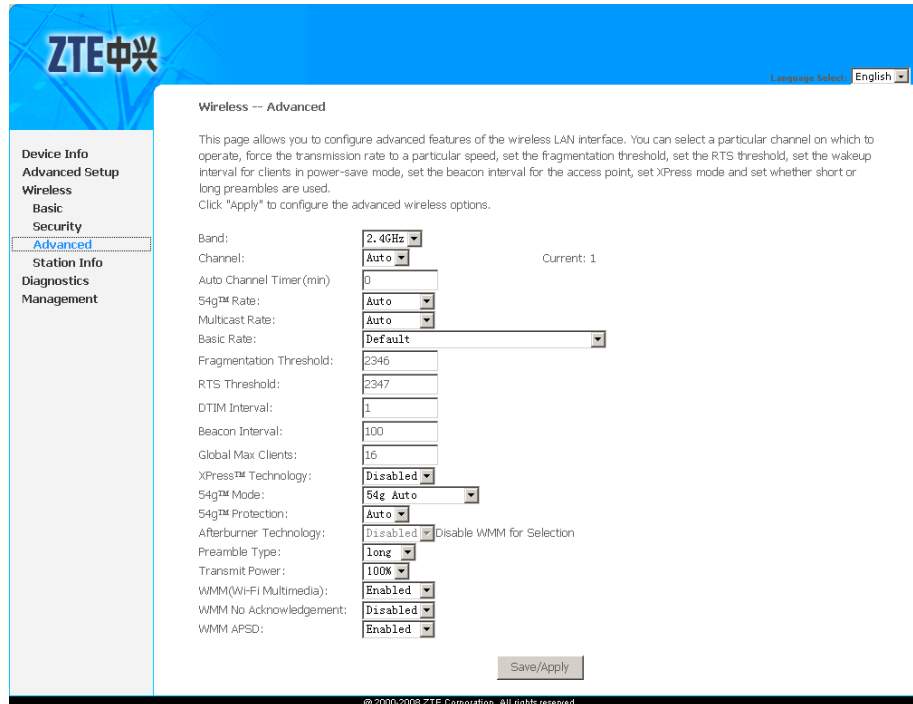
Format	Minimum Characters	Maximum Characters
ASCII	8	63
Hexadecimal	8	64

Click **Save/Apply** to save the wireless security options so that the changes can take effect.

Wireless - Advanced

Select **Wireless > Advanced** to display the interface as shown in [Figure 174](#).

FIGURE 174 WIRELESS - ADVANCED



This page allows you to configure advanced features of the WLAN interface. You can select a particular channel on which to operate, set a particular transmission rate, fragmentation threshold, RTS threshold, wakeup interval for clients in power-save mode, beacon interval for the access point, XPress mode, and set whether short or long preambles are used.

[Table 45](#) is the description of the different options.

TABLE 45 WIRELESS ADVANCED CONFIGURATION OPTIONS

Field	Description
Band	Select 802.11b/g using wireless frequency band range. The radio frequency remains at 2.437 GHz.
Channel	Enter the appropriate channel to correspond with your network settings. The default channel is 11. All devices in your wireless network must use the same channel in order to work correctly. This router supports auto-channeling.
Auto Channel Timer(min)	Specify the time interval for auto-channelling.

Field	Description
54g™ Rate	Select the transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the 931WII automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback negotiates the best possible connection speed between the 931WII and a wireless client. The default value is Auto .
Multicast Rate	Select the multicast transmission rate for the network. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select Auto to have the 931WII automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback negotiates the best possible connection speed between the 931WII and a wireless client. The default value is Auto .
Basic Rate	Select the basic transmission rate ability for the AP.
Fragmentation Threshold	Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the fragmentation threshold if you encounter high packet error rates. Do not set the threshold too low, since this may result in reduced networking performance.
RTS Threshold	This value should remain at its default setting of 2347. If you encounter inconsistent data flow, only minor reduction of the default value, 2347, is recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism is not enabled. The 931WII sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Field	Description
DTIM Interval	Enter a value between 1 – 255 for the Delivery Traffic Indication Message (DTIM). A DTIM is a count-down informing clients of the next window for listening to broadcast and multicast messages.
Beacon Interval	A beacon is a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval is in milliseconds (ms). The default value 100 is recommended.
XPress™ Technology	Select Enabled or Disabled . This is a special accelerating technology for IEEE802.11g. The default is Disabled.
54g™ Mode	Compatible with IEEE 802.11b and IEEE 802.11g. Select a standard from the drop-down list. The default is 54g Auto. The drop-down list box includes the following modes:
	802.11b Only: Only stations that are configured in 802.11b mode can associate. If you select it, the rate of transmission can be 1 Mbps, 2 Mbps, 5.5 Mbps, or 11 Mbps. For other selections, you can select the rate of transmission from more options, including 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.
	54g LRS: This is a special compatibility mode for 802.11b/g and is in fact designed for older types of b-clients. Use this mode if you are experiencing problems with wireless clients that connect to the Guw5.5Z66-5 Access Point. If you select it, the preamble type is disabled and cannot be set.
	54g Auto: Only stations that are configured in 802.11b/g mode can associate.
54g Performance : Only stations that are configured in 802.11g mode can associate. Similar to 54g LRS, if you select it, the preamble type is disabled and cannot be set.	

Field	Description
54g™ Protection	The 802.11g standards provide a protection method so that 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 54g Protection as 802.11b device may need to use your wireless network. In Auto Mode, the wireless device uses RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection OFF to maximize 802.11g throughput under most conditions.
Preamble Type	Preambles are a sequence of binary bits that help the receivers synchronize and ready for receipt of a data transmission. Some older wireless systems like 802.11b implementation use shorter preambles. If you are having difficulty connecting to an older 802.11b device, try using a short preamble. You can select short preamble only if the 54g mode is set to 802.11b.
Transmit Power	Adjust the transmission range here. This tool can be helpful for security purposes if you wish to limit the transmission range.
WMM	Select whether WMM is enabled or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.
WMM No Acknowledgement	Select whether ACK in WMM packet is enabled or disabled. By default, the Ack Policy for each access category is set to Disabled, meaning that an acknowledge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which decreases performance. Disabling the acknowledgement can be useful for voice, for example, where speed of transmission is important and packet loss is tolerable to a certain degree.
WMM APSD	APSD is short for automatic power save delivery. Select Enable for very low power consumption mode. WMM Power Save is an improvement to the 802.11e amendment adding advanced

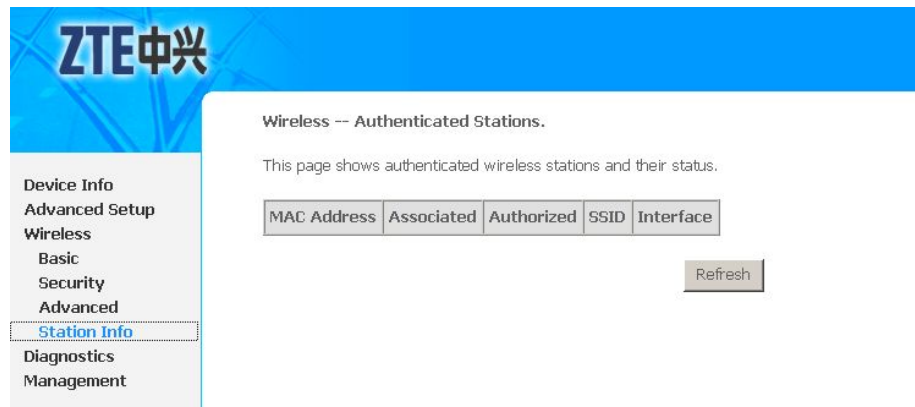
Field	Description
	power management functionality to WMM.

Click **Save/Apply** to save the advanced wireless options so that the changes can take effect.

Wireless - Station Info

Select **Wireless > Station Info** to display the interface as shown in [Figure 175](#).

FIGURE 175 WIRELESS - AUTHENTICATED STATIONS



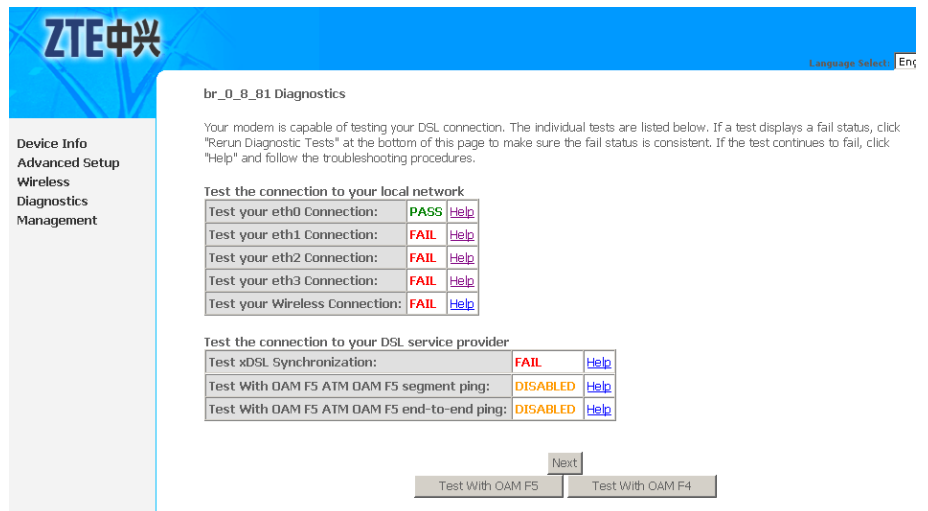
The above figure shows authenticated wireless stations and their status about association and authentication.

This page is intentionally blank.

Diagnostics Configuration

1. Select **Diagnostics** to display the interface as shown in [Figure 176](#).

FIGURE 176 DIAGNOSTICS



2. If a test displays a fail status, click **Help** to enter Wireless Connection Test interface , as shown in [Figure 177](#).

FIGURE 177 TROUBLESHOOTING PROCEDURES

The screenshot shows the ZTE DSL Router web interface. The top navigation bar includes the ZTE logo and a language selector set to English. A left-hand navigation menu lists: Device Info, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled 'Wireless Connection Test' and contains the following information:

Pass:	Indicates that the Wireless interface from your computer is connected to the LAN port of your DSL Router. A flashing or solid green LAN LED on the router also signifies that an Wireless connection is present and that this test is successful.
Down:	Indicates that the DSL Router does not detect the Wireless interface on your computer.

If the test fails, follow the troubleshooting procedures listed below and rerun the diagnostics tests by clicking on the **Rerun Diagnostic Tests** button at the bottom of this page. If all the tests pass, close and restart your Web browser to access the Internet.

Troubleshooting:

1. Verify that the Wireless configurations from your computer and your DSL router are matched and corrected.
2. Turn off the DSL Router, wait 10 seconds and turn it back ON.
3. With the router on, press the reset button on the DSL Router for at least five seconds and release it. This resets the DSL Router to its default settings. Wait for the DSL Router to initialize, then close and restart your Web browser. To reconfigure the router, type your DSL Account username and password.

At the bottom of the page, there is a button labeled 'Rerun Diagnostic Tests' and a note: 'Contact ISP Technical Support if you have tried all of the above and still are experiencing a fail condition.'

3. Follow the troubleshooting procedures to troubleshoot the failure.
4. Click **Rerun Diagnostic Tests** at the bottom of the above interface to conform the fail status.
5. Click Next to re-test the connection again.
6. Click **Test with OAM F5** to test the connection with OAM F5 method.
7. Click **Test with OAM F4** to test the connection with OAM F4 method.

Chapter 20

Management Configuration

Table of Contents

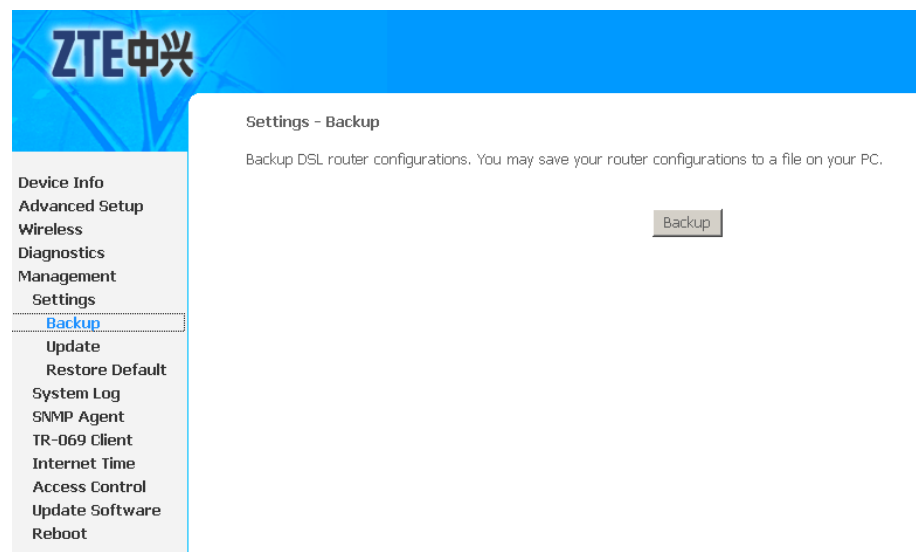
Settings	173
System Log	175
SNMP Agent.....	177
TR-069 Client Management.....	178
Internet Time.....	181
Access Control	182
Update Software	183
Reboot	184

Settings

Setting Backup

Select **Management > Settings > Backup** to display the interface as shown in [Figure 178](#).

FIGURE 178 BACKUP CONFIG

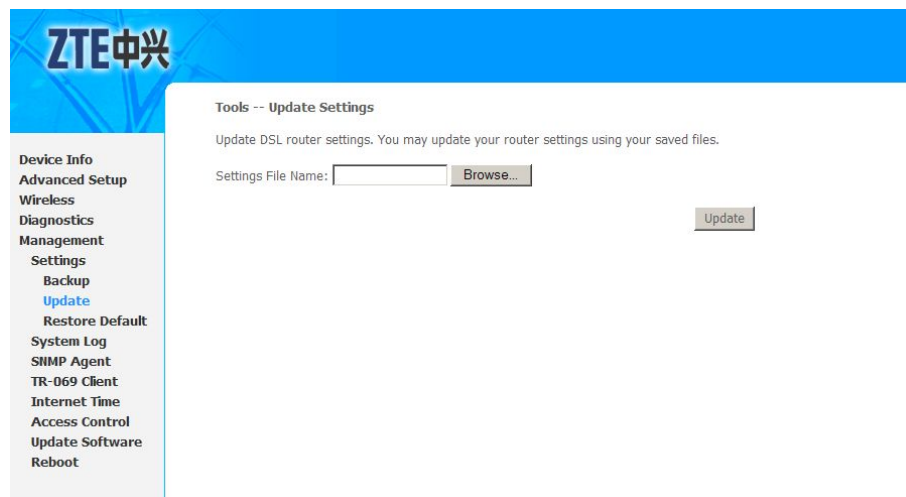


Click **Backup** to backup the configuration of the 931WII.

Setting Update

1. Select **Management > Settings > Update** to display the interface as shown in [Figure 179](#).

FIGURE 179 UPDATE CONFIG

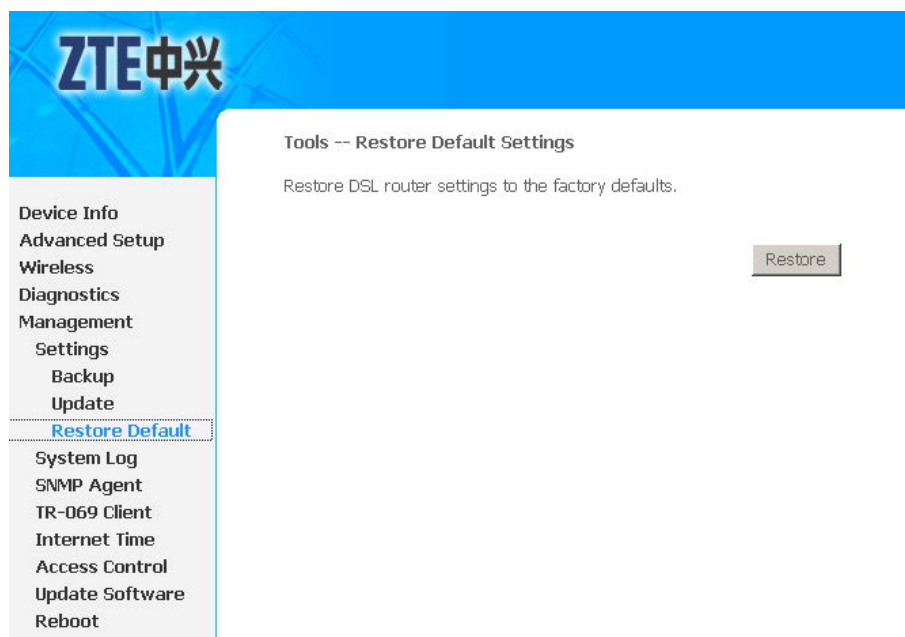


2. Click **Browse** to select the correct update configure settings file.
3. Click **Update** to update the configuration of the 931WII.

Setting Restore Default

Select **Management > Settings > Restore Default** to display the interface as shown in [Figure 180](#).

FIGURE 180 RESTORE DEFAULT CONFIG

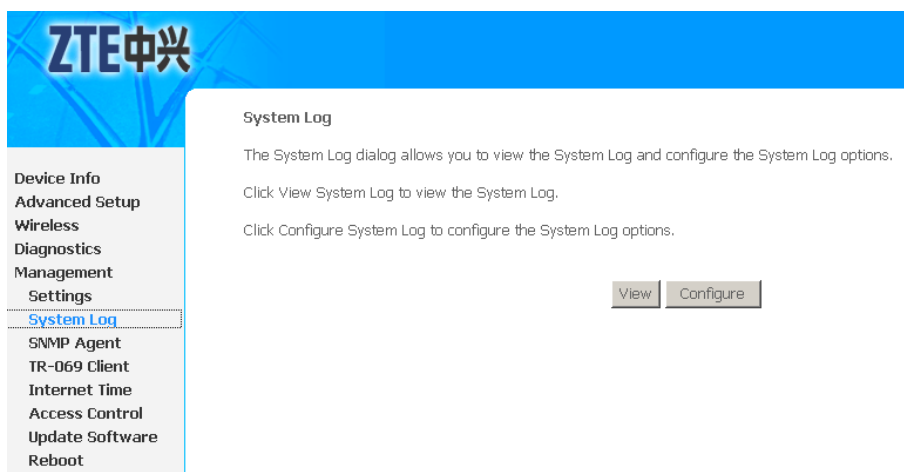


Click **Restore** to restore the settings of the 931WII to factory defaults.

System Log

1. Select **Management > System Log** to display the interface as shown in [Figure 181](#).

FIGURE 181 SYSTEM LOG



2. Click **Configure** to display the interface as shown in [Figure 182](#).

FIGURE 182 ENABLING SYSTEM LOG

System Log -- Configuration

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is 'Remote' or 'Both,' events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is 'Local' or 'Both,' events will be recorded in the local memory.

Select the desired values and click 'Save/Apply' to configure the system log options.

Log: Disable Enable

Log Level:

Display Level:

Mode:

3. Select **Enable** to enable the system log.
4. Select the proper parameters in **Log Level** and **Display Level** drop-down menu. The Default log level is **Debugging** and the default display level is **Error**.
5. The mode options are **Local**, **Remote**, and **Both**. The default is **Local**.
6. If you select **Remote** or **Both**, all events are transmitted to the specified UDP port of the specified log server, as shown in [Figure 183](#).

FIGURE 183 LOG SERVER CONFIG

The screenshot shows the 'System Log -- Configuration' page with a sidebar on the left containing navigation options: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, TR-069 Client, Internet Time, Access Control, Update Software, and Save/Reboot. The main content area includes the same introductory text as Figure 182, followed by the configuration options:

Log: Disable Enable

Log Level:

Display Level:

Mode:

Server IP Address:

Server UDP Port:

7. Click **Save/Apply** to save the configuration so that the changes can take effect.
8. Click **View** to display the system log as shown in [Figure 184](#).

FIGURE 184 SYSTEM EVENT LOGS

System Log

Date/Time	Facility	Severity	Message
Jan 1 01:38:08	user	crit	kernel: ADSL G.994 training
Jan 1 01:38:16	user	crit	kernel: ADSL G.992 started
Jan 1 01:38:20	user	crit	kernel: ADSL G.992 channel analysis
Jan 1 01:38:24	user	crit	kernel: ADSL G.992 message exchange
Jan 1 01:38:25	user	crit	kernel: ADSL link up, interleaved, us=1146, ds=25505
Jan 1 01:38:26	daemon	crit	pppd[628]: PPP server detected.
Jan 1 01:38:26	daemon	crit	pppd[628]: PPP session established.
Jan 1 01:38:27	daemon	err	pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27	daemon	err	pppd[628]: Couldn't increase MRU to 1500
Jan 1 01:38:27	daemon	crit	pppd[628]: PPP LCP UP.
Jan 1 01:38:27	daemon	crit	pppd[628]: Received valid IP address from server. Connection UP.
Jan 1 01:38:33	daemon	err	user: tr69c: Unable to retrieve attributes in scratch PAD
Jan 1 01:38:33	daemon	err	user: Stored Parameter Attribute data is corrupt or missing

SNMP Agent

Select **Management > SNMP Agent** to display the interface as shown in [Figure 185](#).

FIGURE 185 SNMP AGENT

This page allows you to configure modem to be a [SNMP](#) agent, so that the modem can be managed by NMS as a network element. You can enable or disable the SNMP agent function.

[Table 46](#) is a description of the different options.

TABLE 46 SNMP AGENT CONFIGURATION OPTIONS

Field	Description
Read Community	Define the SNMP read community name.
Set Community	Define the SNMP set community name.
System Name	Define system name used in NMS.
System Location	Fill in system location.
System Contact	Fill in Contact information to contact the maintenance personnel if the system fails.
Trap Manager IP	Define NMS server IP address to receive system SNMP trap reports.

Click **Save/Apply** to save the configuration so that the changes can take effect.

**Note:**

You must restart SNMP agent by first disabling and then enabling it for the configuration of Read/Set Community to take effect.

TR-069 Client Management

Protocol Components

TR-069 is one of the [CPE WAN](#) Management Protocol. It comprises several components that are unique to this protocol, and makes use of several standard protocols. The protocol stack defined by the CPE WAN Management Protocol is shown in [Figure 186](#).

FIGURE 186 PROTOCOL STACK

CPE/ACS Management Application
RPC Methods
SOAP
HTTP
SSL/TLS
TCP/IP

A brief description of each layer is provided in [Table 47](#).

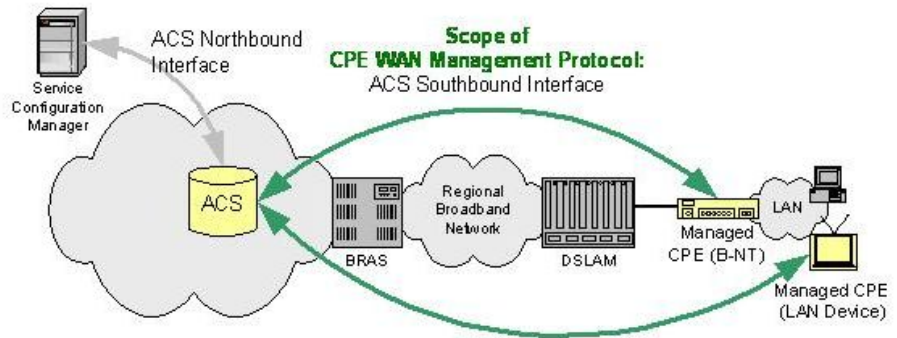
TABLE 47 PROTOCOL LAYER SUMMARY

Layer	Description
CPE/ACS Application	The application uses the CPE WAN Management Protocol on the CPE and ACS, respectively. The application is locally defined and not specified as part of the CPE WAN Management Protocol.
RPC Methods	The specific RPC methods that are defined by the CPE WAN Management Protocol.
SOAP	A standard XML-based syntax used here to encode remote procedure calls. Specifically SOAP 1.1.
HTTP	HTTP 1.1.
SSL/TLS	The standard Internet transport layer security protocols. Specifically, SSL 3.0 or TLS 1.0. Use of SSL/TLS is recommended but is not required.
TCP/IP	Standard TCP/IP.

Protocol Application

The [CPE WAN](#) Management Protocol is proposed as the protocol to be used on the ACS Southbound Interface between an Auto-Configuration Server (ACS). This protocol may be used to manage other types of CPE as well, including stand-alone routers and LAN-side client devices, as also shown in [Figure 187](#).

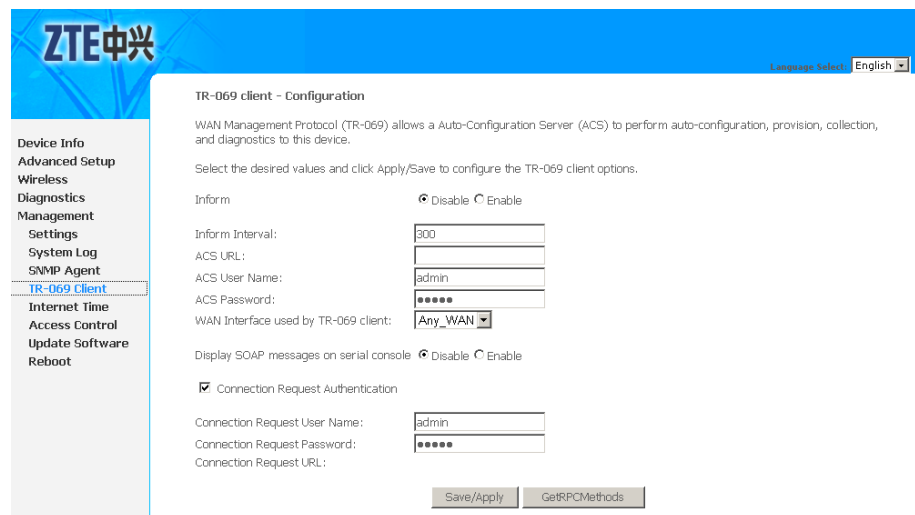
FIGURE 187 POSITIONING IN THE AUTO-CONFIGURATION ARCHITECTURE



TR-069 Client Configuration

Select **Management > TR-069 Client** to display the interface as shown in [Figure 188](#).

FIGURE 188 TR-069 CLIENT CONFIG



[Table 48](#) is a description of the different options.

TABLE 48 TR-069 CLIENT CONFIGURATION OPTIONS

Field	Description
Inform	If the Enable option is selected, the CPE accepts the commands from ACS. If the Disable option is selected, the CPE does not accept the commands from ACS.
Inform Interval	The seconds between two attempts of the CPE to inform the ACS to connect.

Field	Description
ACS URL	Enter the ACS URL.
ACS User Name	The ACS user name is same as that the TR-069 service provide to you.
ACS Password	The ACS password is same as that the TR-069 service provide to you.
WAN Interface used by TR-069 client:	Define the WAN interface used to transfer TR-069 message, Any_WAN , LAN , and Loopback .
Display SOAP messages on serial console	When Enable is selected, the SOAP information is displayed on the serial console, when Disable is selected, the information is not displayed. .
Connection Request Authentication	If this checkbox is selected, you need to enter the Connection Request , User Name , and the Connection Request Password . If this check box is not selected, you do need not to enter any information.
Connection Request User Name	The connection user name that the TR-069 service provides to you.
Connection Request Password	The connection request password that the TR-069 service provides to you.

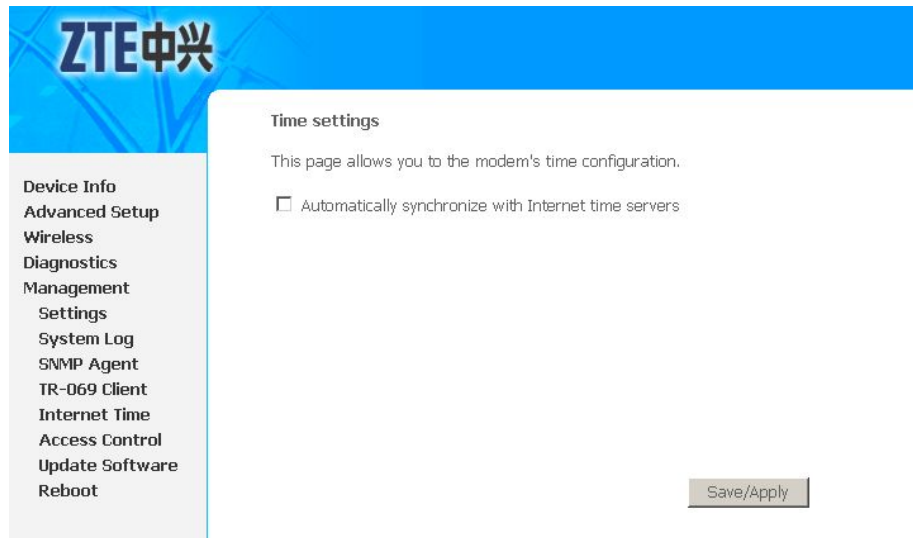
Click **GetRPCMethods** to query the maximum number of RPC method that NMS supported.

Click **Save/Apply** to save the configuration so that the changes can take effect.

Internet Time

Select **Management > Internet Time** to display the interface as shown in [Figure 189](#).

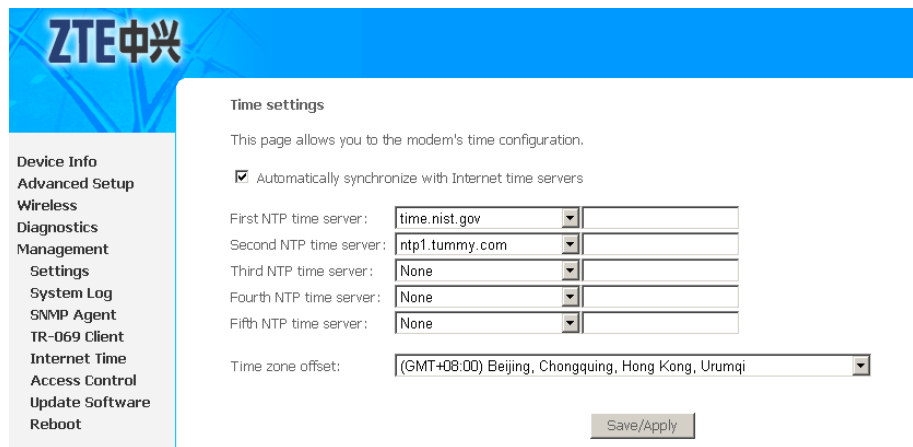
FIGURE 189 INTERNET TIME OVERVIEW



In this interface, the modem can be configured to synchronize with Internet time servers.

After enabling **Automatically synchronize with Internet time servers**, the interface is displayed as shown in [Figure 190](#).

FIGURE 190 INTERNET TIME SETUP

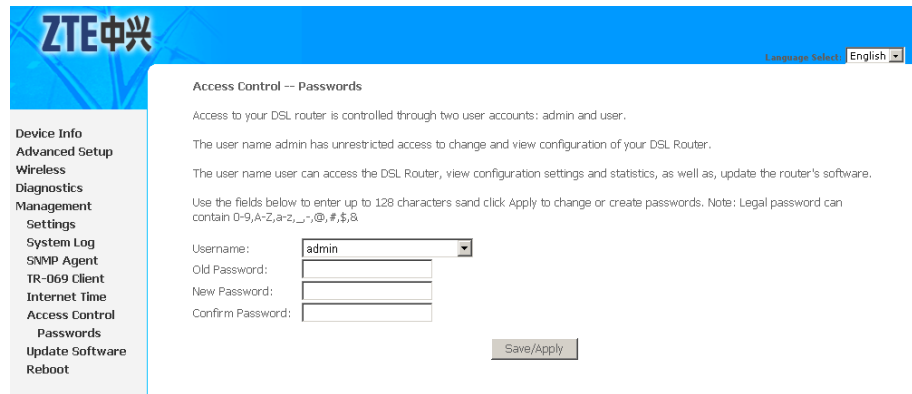


Click **Save/Apply** to save the configuration so that the changes can take effect.

Access Control

Select **Management > Access Control > Password** to display the interface as shown in [Figure 191](#).

FIGURE 191 ACCESS CONTROL



In the interface, you can change the passwords of the accounts:

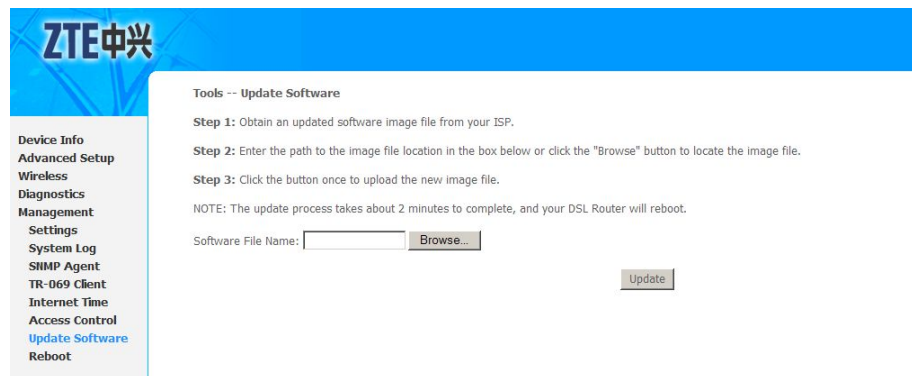
- admin: unrestricted access to change and view configuration of 931WII
- user: view configuration settings, statistics, as well as update the router's software

Click **Save/Apply** to save the configuration so that the changes can take effect.

Update Software

Select **Management > Update Software** to display the interface as shown in [Figure 192](#).

FIGURE 192 UPDATE SOFTWARE



Click **Browse** to find the right version file and click **Update** to update Modem firmware.

Note:

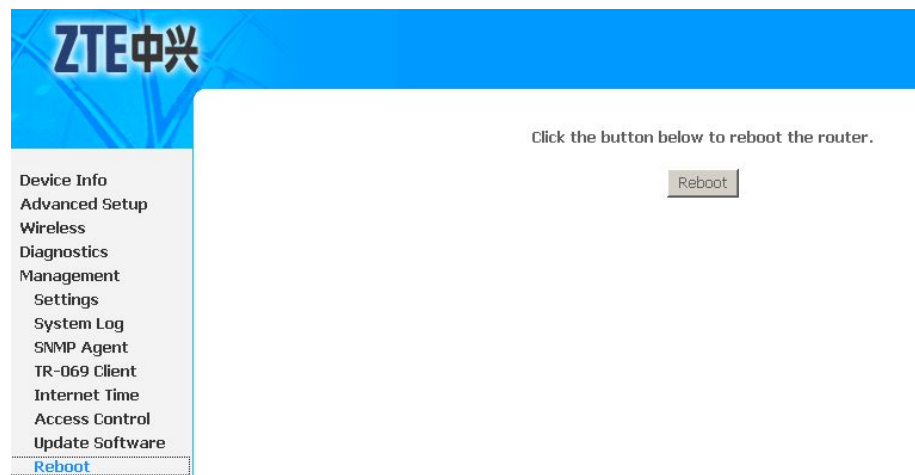
Do not turn off your modem during firmware update. When the update is complete, the modem reboots automatically. Do not turn off your modem either before the reboot is over. You must guarantee the update software is correct and accurate. It is strictly forbidden to use other software for updates.

After software update, it is recommended to restore the modem to the factory defaults and configure it again.

Reboot

Select **Management > Reboot** to display the interface as shown in [Figure 193](#).

FIGURE 193 REBOOT



Click **Reboot** to reboot the 931WII.

Figures

Figure 1 Front Panel LED Diagram.....	10
Figure 2 Rear Panel Interface Diagram	12
Figure 3 Connection of Modem, PC and Telephones	14
Figure 4 Hardware Configuration	18
Figure 5 IP and DNS Configuration.....	19
Figure 6 Web-based Management - Home Page	21
Figure 7 Web-based Management - Login Authentication Page	22
Figure 8 Device Info Menu	23
Figure 9 Device Information Summary	23
Figure 10 LAN Statistics	24
Figure 11 WAN Statistics	25
Figure 12 xDSL Statistics.....	26
Figure 13 ADSL BER Test	27
Figure 14 ADSL BER Test Result.....	27
Figure 15 Route Table	28
Figure 16 ARP Table	29
Figure 17 ADSL PVC Configuration Overview	31
Figure 18 Adding EOA PVC.....	32
Figure 19 EOA PVC Configuration Completed	33
Figure 20 WAN Service Overview	33
Figure 21 Select Layer2 Interface	34
Figure 22 Select WAN Service Type	34
Figure 23 PPPoE Configuration.....	35
Figure 24 Default Gateway Configuration	36
Figure 25 DNS Configuration.....	36
Figure 26 EOA PPPoE WAN Connection Setup Summary	37
Figure 27 EOA PPPoE WAN Connection Configuration Completed.....	37
Figure 28 ADSL PVC Configuration Overview	38
Figure 29 Adding EOA PVC.....	38
Figure 30 EOA PVC Configuration Completed	39
Figure 31 WAN Service Overview	39
Figure 32 Select Layer2 Interface	40

Figure 33 Select WAN Service Type	40
Figure 34 WAN IP Configuration.....	40
Figure 35 NAT Configuration.....	41
Figure 36 Default Gateway Configuration	41
Figure 37 DNS Configuration	42
Figure 38 EOA IPoE WAN Connection Setup Summary	42
Figure 39 EOA IPoE WAN Connection Configuration Completed.....	43
Figure 40 ADSL PVC Configuration Overview	43
Figure 41 Adding EOA PVC.....	44
Figure 42 EOA PVC Configuration Completed	45
Figure 43 WAN Service Overview	45
Figure 44 Select Layer2 Interface	46
Figure 45 Select WAN Service Type	46
Figure 46 EOA Bridge WAN Connection Setup Summary.....	47
Figure 47 EOA Bridge WAN Connection Configuration Completed.....	47
Figure 48 ADSL PVC Configuration Overview	48
Figure 49 Adding PPPoA PVC	48
Figure 50 PPPoA PVC Configuration Completed	49
Figure 51 WAN Service Overview	49
Figure 52 Select Layer2 Interface	50
Figure 53 WAN Service Configuration	50
Figure 54 PPPoA Configuration.....	50
Figure 55 Default Gateway Configuration	51
Figure 56 DNS Configuration	52
Figure 57 PPPoA WAN Connection Setup Summary.....	52
Figure 58 PPPoA WAN Connection Configuration Completed.....	53
Figure 59 ADSL PVC Configuration Overview	53
Figure 60 Adding IPoA PVC	54
Figure 61 IPoA PVC Configuration Completed.....	54
Figure 62 WAN Service Overview	55
Figure 63 Select Layer2 Interface	55
Figure 64 WAN Service Configuration	56
Figure 65 WAN IP Configuration.....	56
Figure 66 NAT Configuration.....	56
Figure 67 Default Gateway Configuration	57
Figure 68 DNS Configuration	57
Figure 69 IPoA WAN Connection Setup Summary	58
Figure 70 IPoA WAN Connection Configuration Completed	58

Figure 71 VDSL2 PTM Interface Configuration Overview	59
Figure 72 Adding PTM Interface	59
Figure 73 WAN Service Overview	60
Figure 74 Select Layer2 Interface	60
Figure 75 Select WAN Service Type	61
Figure 76 PPPoE Configuration.....	61
Figure 77 Default Gateway Configuration	62
Figure 78 DNS Configuration	63
Figure 79 PTM Interface PPPoE WAN Connection Setup Summary	63
Figure 80 PTM Interface PPPoE WAN Connection Configuration Completed	64
Figure 81 VDSL2 PTM Interface Configuration Overview	64
Figure 82 Adding PTM Interface	65
Figure 83 WAN Service Overview	65
Figure 84 Select Layer2 Interface	66
Figure 85 Select WAN Service Type	66
Figure 86 PTM Interface Bridge WAN Connection Setup Summary	67
Figure 87 PTM Interface Bridge WAN Connection Configuration Completed	67
Figure 88 VDSL2 PTM Interface Configuration Overview	68
Figure 89 Adding PTM Interface	68
Figure 90 WAN Service Overview	69
Figure 91 Select Layer2 Interface	69
Figure 92 Select WAN Service Type	69
Figure 93 WAN IP Configuration.....	70
Figure 94 Default Gateway Configuration	70
Figure 95 DNS Configuration	71
Figure 96 NAT Configuration.....	71
Figure 97 Default Gateway Configuration	72
Figure 98 DNS Configuration	72
Figure 99 PTM Interface IPoE WAN Connection Setup Summary	73
Figure 100 PTM Interface IPoE WAN Connection Configuration Completed	73
Figure 101 LAN Configuration Overview	75
Figure 102 Adding DHCP Static IP Lease	76
Figure 103 Configure Second IP Address.....	76
Figure 104 VLAN Trunking Overview	79

Figure 105 VLAN Trunking Notice	79
Figure 106 WAN Service Overview	80
Figure 107 Select Layer2 Interface	80
Figure 108 Select WAN Service Type	81
Figure 109 PTM Interface Bridge WAN Connection Setup Summary	81
Figure 110 PTM Interface Bridge WAN Connection Configuration Completed	82
Figure 111 VLAN Trunking Configuration	82
Figure 112 Virtual Server.....	85
Figure 113 Virtual Servers Overview	86
Figure 114 Adding Virtual Servers.....	87
Figure 115 Port Triggering Overview.....	88
Figure 116 Adding Port Triggering	88
Figure 117 DMZ host.....	90
Figure 118 DMZ host Configuration	91
Figure 119 DMZ Host Configuration Notice	91
Figure 120 MAC Filtering Overview.....	93
Figure 121 MAC Filtering Change Policy	94
Figure 122 Adding MAC Filtering Rule	95
Figure 123 Removing MAC Filtering Rule.....	96
Figure 124 Adding MAC filtering - Forwarded	96
Figure 125 Adding MAC filtering - Blocked.....	97
Figure 126 Quality of Service	99
Figure 127 Enable QoS	100
Figure 128 QoS Queue Configuration Overview	101
Figure 129 QoS Queue Configuration.....	102
Figure 130 QoS Queue Configuration - Completed.....	103
Figure 131 QoS Classification	104
Figure 132 QoS Classification Overview	104
Figure 133 QoS Classification Configuration.....	105
Figure 134 QoS DSCP Configuration Example	107
Figure 135 Default Gateway	109
Figure 136 Default Gateway Notice	110
Figure 137 Adding Static Route	111
Figure 138 Adding Static Route with LAN Bridge Interface	111
Figure 139 Policy Routing Overview.....	112
Figure 140 Adding Policy Routing	112
Figure 141 RIP Configuration.....	114
Figure 142 DNS Server Configuration Overview	115

Figure 143 Dynamic DNS Configuration Overview	116
Figure 144 Adding Dynamic DNS	117
Figure 145 DSL Configuration.....	119
Figure 146 Time Restriction Overview.....	125
Figure 147 Time Restriction Config.....	126
Figure 148 URL Filter Overview.....	127
Figure 149 URL Filter Config.....	127
Figure 150 UPNP Config.....	129
Figure 151 Local Certificate Overview	131
Figure 152 Create New Certificate Request.....	132
Figure 153 Generate Certificate Request	133
Figure 154 Generated Certificate Completed.....	134
Figure 155 Load Certificate	134
Figure 156 Import Certificate	135
Figure 157 Trusted CA Certificates	136
Figure 158 Import Certificate	136
Figure 159 Client Mode.....	138
Figure 160 Ad Hoc Mode.....	138
Figure 161 Typical Wireless Network Topology	139
Figure 162 Wireless - Basic	148
Figure 163 Wireless-Security (No Encryption)	150
Figure 164 Wireless-Security (64-bit WEP)	151
Figure 165 Wireless-Security (128-bit WEP).....	152
Figure 166 Authentication Topology Adopting Radius Server ..	153
Figure 167 Wireless-Security (802.1x Authentication)	154
Figure 168 Wireless-Security (WPA Authentication).....	155
Figure 169 Wireless-Security (WPA2 Authentication).....	157
Figure 170 Wireless-Security (WPA-PSK Authentication)	158
Figure 171 Wireless-Security (WPA2-PSK Authentication)	160
Figure 172 Wireless-Security (Mixed WPA2/WPA-PSK Authentication)	161
Figure 173 Wireless-Security (Mixed WPA2/WPA Authentication)	163
Figure 174 Wireless - Advanced.....	165
Figure 175 Wireless - Authenticated Stations.....	169
Figure 176 Diagnostics	171
Figure 177 Troubleshooting Procedures.....	172
Figure 178 Backup Config	173
Figure 179 Update Config	174
Figure 180 Restore Default Config.....	175

Figure 181 System Log	175
Figure 182 Enabling System Log	176
Figure 183 Log Server Config	176
Figure 184 System Event Logs	177
Figure 185 SNMP Agent	177
Figure 186 Protocol Stack	179
Figure 187 Positioning in the Auto-configuration Architecture ..	180
Figure 188 TR-069 Client Config	180
Figure 189 Internet Time Overview	182
Figure 190 Internet Time Setup	182
Figure 191 Access Control	183
Figure 192 Update Software	183
Figure 193 Reboot	184

Tables

Table 1 Wireless Specifications	2
Table 2 VDSL2 Service Information Requirement.....	5
Table 3 ADSL Service Information Requirement	6
Table 4 Device Information Requirement.....	8
Table 5 PC Information Requirement	9
Table 6 Front Panel LED Status	11
Table 8 EOA PVC Configuration Options.....	32
Table 9 PPPoE Configuration Options	35
Table 10 EOA PVC Configuration Options.....	38
Table 11 EOA PVC Configuration Options.....	44
Table 12 PPPoA PVC Configuration Options	48
Table 13 PPPoA Configuration Options.....	51
Table 14 IPoA PVC Configuration Options	54
Table 15 PPPoE Configuration Options.....	62
Table 16 LAN Configuration Options	76
Table 17 Custom Port Triggering Configuration Options	89
Table 18 MAC Filter Policy Configuration Options	94
Table 19 MAC Filtering Rule Configuration Options.....	95
Table 20 Queue Configuration Options	102
Table 21 QoS Classification Configuration Options	105
Table 22 Policy Routing Configuration Options.....	112
Table 23 Dynamic DNS Configuration Options.....	117
Table 24 Time Restriction Configuration Options.....	126
Table 25 URL Filter Basic Configuration Options	127
Table 26 Create Certificate Request Configuration Options.....	132
Table 27 WLAN Basic Terms	140
Table 28 Wireless Networking Standards.....	141
Table 29 Radio Channel Restriction.....	147
Table 30 Wireless Basic Configuration Options	148
Table 31 WLAN Security No Encryption Configuration Options	150
Table 32 WLAN Security 64-bit WEP Encryption Configuration Options	151

Table 33 WLAN Security 128-bit WEP Encryption	
Configuration Options.....	152
Table 34 WLAN Security 802.1x Authentication Configuration	
Options	154
Table 35 WLAN Security WPA Authentication Configuration	
Options	156
Table 36 WLAN Security WPA2 Authentication Configuration	
Options	157
Table 37 WLAN Security WPA Authentication Configuration	
Options	159
Table 38 WPA Pre-Shared Key	159
Table 39 WLAN Security WPA2 Authentication Configuration	
Options	160
Table 40 WPA Pre-Shared Key	161
Table 41 Wireless-Security (WPA-PSK Authentication)	162
Table 42 WPA Pre-Shared Key	162
Table 43 Wireless-Security (Mixed WPA2/WPA	
Authentication)	163
Table 44 WPA Pre-Shared Key	164
Table 45 Wireless Advanced Configuration Options	165
Table 46 SNMP Agent Configuration Options	178
Table 47 Protocol Layer Summary	179
Table 48 TR-069 Client Configuration Options	180