## ZTE中兴

## 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 CORPO-RATION 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.	<b>Revision Date</b>	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	
Setting Up WAN and LAN Connections	
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	
QoS-QoS Classification	
QoS - DSCP Setting	106
Routing Configuration	109
Routing – Default Gateway	
Static Routes	110
Policy Routing	
RIP	113
DNS	115
DNS Server	
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	
Wireless Network	137
About the Guw5.5Z66-5	
Wireless LAN Basics	139
Basic terms	
Wireless Standard	
Wireless Security	144
Wireless Client requirements	146
Wireless Distribution System	147
Configure Wireless Connection	
Wireless - Basic	
Wireless–Security	
No Encryption	
64-bit WEP	
802.1X Authentication	
WPA Authentication	
WPA-PSK Authentication	
Mixed WPA2/WPA-PSK Authentication	
Mixed WPA2/WPA Authontication	101
Wireless - Advanced	164
Wireless - Station Info	
Diagnostics Configuration	
Management Configuration	

Settings	
Setting Backup	
Setting Update	
Setting Restore Default	
System Log	
SNMP Agent	
TR-069 Client Management	
Protocol Components	
Protocol Application	
TR-069 Client Configuration	
Internet Time	
Access Control	
Update Software	
Reboot	
Figures	
Tables	

### 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
	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

TF中兴

- 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

Natural Chardend	IEEE 802.11b,		
Network Standard	IEEE 802.11g		
Frequency Range	2.40 GHz~2.4835 GHz, ISM Band		
	802.11b: DBPSK, DQPSK, CCK		
Modulation	802.11g: BPSK, QPSK, 16 QAM, 64 QAM		
	Max.: 20 dBm		
RF Power	802.11b: Typ. 18 dBm@Normal Temp Range		
	802.11g: Typ. 15 dBm@Normal Temp Range		
	Access user quantity	50~80Pcs/AP	
		US and Canada: 11	
	Number of channels	Europe and China: 13	
AP Capacity		Japan: 14	
Ar Capacity	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, 48 Mbps, 54 Mbps
	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
Payload Rate	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
	Outdoor	100~150
Radio Cover Rage (m)	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 <u>Table 2</u> is very helpful for your VDSL2 configuration. You can collect it from your VDSL2 service provider:

Item	Description	Enter Information in This Column
РТМ	Most users are not re- quired to change this setting. The Packet Transfer Mode (PTM) interface is used to identify the data path between the network of your VDSL2 serv- ice provider and your computer. If you are setting up the 931WII for multiple connec- tions, you need to configure the PTM in- terface as instructed by your VDSL2 serv- ice provider for ad- ditional connections. You can change this setting by accessing the layer-2 configura- tion 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 pro- vider. It is usu- ally in the form of user@isp.com. Your VDSL2 service pro- vider 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 net- work of your VDSL2 service provider. It is used to verify the identity of your ac- count.	

#### TABLE 2 VDSL2 SERVICE INFORMATION REQUIREMENT

The following information in <u>Table 3</u> is very helpful for your ADSL configuration. You can collect it from your ADSL service provider:

Item	Description	Enter Information in This Column
VPI	Most users are not re- quired to change this setting. The virtual path identifier (VPI) is used in conjunction with the virtual chan- nel identifier (VCI) to identify the data path between the network of your ADSL serv- ice 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 serv- ice provider for ad- ditional connections. You can change this setting by accessing the layer-2 configura- tion and WAN menu of the web management interface.	
VCI	Most users are not required to change this setting. The VCI is used in conjunc- tion with the VPI to identify the data path between the network of your ADSL serv- ice 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 serv- ice provider for ad- ditional connections. You can change this setting by accessing the layer-2 configura- tion and WAN menu of the web management interface.	

#### TABLE 3 ADSL SERVICE INFORMATION REQUIREMENT

Item	Description	Enter Information in This Column
Connection and En- capsulation Type	This is the method your ADSL serv- ice provider uses to transmit data be- tween the Internet and your computer. Most users use the default PPPoE con- nection type. The Setup Wizard can be used to config- ure a PPPoE connec- tion type. You may need to specify one of the following con- nection types: PPPoE, LLC. Other available connections and en- capsulation combina- tions must be config- ured by using the Web manager. These in- clude 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 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 net- work of your ADSL service provider. It is used to verify the identity of your ac- count.	

Necessary information about your 931WII is as follows in Table 4.

Item	Description	Enter Information in This Column
LAN IP addresses	This is the IP address you enter in the Ad- dress field in the Web browser to access the configuration graph- ical user interface (GUI) of the gateway. The default IP ad- dress 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 serv- ice on the LAN when DHCP is enabled.	
LAN Subnet Mask	This is the sub- net mask used by the 931WII, and is used throughout your LAN. The de- fault subnet mask is 255.255.255.0. You can change it later.	
Username	This is the user name used to access the management inter- face of the gateway, when you attempt to connect to the de- vice through a web browser. The de- fault username of the 931WII is admin. It cannot be changed.	
Password	This is the password required when you access the manage- ment interface of the gateway. The default password is admin. It cannot be changed.	

#### TABLE 4 DEVICE INFORMATION REQUIREMENT

Necessary information about your LAN or computer is as follows in  $\underline{\text{Table 5}}.$ 

Item	Description	Enter Information in This Column
Ethernet NIC	If your computer has an Ethernet NIC, you can connect the 931WII to this Ether- net 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 ad- dress, a subnet mask, and a default gate- way address to com- puters 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 com- puter (or computers) to Obtain an IP ad- dress automatically (that is, to set com- puters as DHCP cli- ents.)	

#### TABLE 5 PC INFORMATION REQUIREMENT

## 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



Indicator	Color	Status	Description
		OFF	Power OFF
Power	Blue/Red	Red	Power ON, HW Testing
		Blue	Power ON, HW Test ok
		OFF	The modem is in the non- communication state
DSL	Green	Flash	The modem is in training state
		ON	The modem is in the communica-tion state
		OFF	No detected data
Internet	Green	Flash	WAN port is re- ceiving or send- ing data
		ON	WAN port is in communication status
		OFF	No detected ra- dio signal
WLAN	Green	Flash	WLAN port is re- ceiving or send- ing data
		ON	WLAN interface is ready to work
		OFF	WPS function is OFF
	Green	Flash	WLAN port is in negotiation sta- tus
WPS		ON	WPS function is ON
	Red	Flash	WLAN port ne- gotiation is fail- ure

#### TABLE 6 FRONT PANEL LED STATUS

Indicator	Color	Status	Description
		OFF	The Ethernet port is in the non-communi- cation state
LAN 1 - LAN 4	Green	ON	The Ethernet port is in the communication state
		Flash	Ethernet inter- face 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 theVDSL2 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 sec- onds to reset the current settings to the factory default setting, and then the system restarts automati- cally
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	Configura-	
tion								.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.

General	Alternate Con	figuration					
You can this cap the app	a get IP setting ability. Otherwi ropriate IP sett	s assigne se, you n ings.	d autom eed to a	atically if isk your r	your ne network	twork su administ	ipports rator for
() Ob	otain an IP add	ress autor	natically	1			
OU	e the following	IP addre	ss:				
IP ad	ldress:						
Subr	net mask:				±2	1.00	
Defa	ult gateway.				- 45	200	
() Ot	tain ONS serv	er addres	s autom	atically			
OU	e the following	DNS ser	ver add	resses:			
Piefr	ared ONS serv	PT.					
Alter	nate DNS serv	er:			T.		
						Adv	anced
				C			-

#### FIGURE 5 IP AND DNS CONFIGURATION



Windows XP	1.	Choose <b>Start &gt; Control Panel</b> to open the control panel. Open <b>Network Connection</b> form the <b>control panel</b> .
	2.	Right-click the Ethernet connection icon and choose Prop-
	3.	on the General tab, select the Internet Protocol (TCP/IP) component and click Properties. The Internet Protocol (TCP/IP) Properties window appears
	4. 5.	Select the <b>Obtain DNS server address automatically</b> radio button. Select the <b>Obtain DNS server address automatically</b> radio button
	6.	Click <b>OK</b> to save the settings.
Windows	1.	Choose Start > Control Panel > Network and Dialing Con-
2000/98/98	2.	Right-click the <b>Ethernet connection</b> icon and choose <b>Prop</b> -
	3.	erties. Select the Internet Protocol (TCP/IP) component and click Properties. The Internet Protocol (TCP/IP) Properties window appears
	4. 5.	Select the <b>Obtain an IP address automatically</b> radio button. Select the <b>Obtain DNS server address automatically</b> radio button
	6.	Click <b>OK</b> to save the settings.
Windows NT	1. 2.	Choose <b>Start &gt; Control Panel &gt; Network</b> from the desktop. On the <b>Protocol</b> tab, select the <b>Internet Protocol (TCP/IP)</b> component and click <b>Properties</b>
	3.	On the <b>IP Address</b> tab, select the <b>Obtain an IP address</b>
	4.	<b>automatically</b> radio button. On the <b>DNS</b> tab, verify that no DNS server is defined in the <b>DNS Service Search Order</b> box and no suffix is defined in the <b>Domain Suffix Search Order</b> 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
- name.
- Enter ifconfig again to view the newly allocated IP address.
   Ensure that no firewall is active on device <dev>.



# **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



Device Info Advanced Setup Wireless Diagnostics Management

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

Connect to 19	2.168.1.1
) 10 DSL Router User name:	🖸 admin
_ <u>P</u> assword:	•••••

- 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 Info Summary WAN Statistics Route ARP

### **Device Information Summary**

Click **Device Info > Summary** to display the interface as shown in Figure 9 .

#### FIGURE 9 DEVICE INFORMATION SUMMARY

	Device Info					
1	Board ID:	Board ID: 96368MVWG				
vice Info	Software Version:	ZXDSL 931WII V1.2.0c_Z31_OV				
Summary	Bootloader (CFE) Version:	1.0.37-102.6				
Statistics	Wireless Driver Version:	4.174.64.19.cpe4.402				
Route ARP Ivanced Setup	This information reflects the cu	urrent status of your DSL con	inect			
anostics	Line Rate - Downstream (I	Kbps):				
lanagement	LAN IPv4 Address:	192.168.1.1				
anagement						
anagement	Default Gateway:					
anagement	Default Gateway: Primary DNS server:					

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

下中兴

- 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

ZIE中兴	Statistics -	
	Interface	
Device Info		B
Summary	eth0	0
WAN	eth1	0
Statistics	eth2	0
WAN Service	eth3	0
xDSL	wlan	0
Route	·	_
ARP		
Advanced Setup	Reset	
Wireless		
Diagnostics		
Management		

Received Transmitted Pkts Errs Drops Bytes Pkts Errs Drops 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0

You can query information of packets recevied 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: receieved 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

ZTE中兴										
	Statistics	WAN								
	Interface	Description		Rece	eived	l	T	ransi	mitte	ed
Device Info			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Summary	atmO	br_0_8_81	0	0	0	0	0	0	0	0
WAN	ptm0_1	br_0_0_1_1	0	0	0	0	0	0	0	0
Statistics										
LAN	Deast									
WAN Service	Reset S	tatistics								
xDSL										
Route										
ARP										
Advanced Setup										
Wireless										
Diagnostics										
Management										

You can query information of packets recevied 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

 Click **Device Info > Statistics > xDSL** to display the interface as shown in <u>Figure 12</u>.

ZTE中兴

#### FIGURE 12 XDSL STATISTICS

776曲》			
2			
	Statistics xDSL		
Device Info	Mode:		
Summary	Traffic Type:		
WAN	Status:		NoSianal
Chantinaine	Link Power State:		LO
Statistics			
LAN		Downstream	Upstream
WAN Service	Line Coding(Trellis):		-
xDSL	SNR Margin (0.1 dB):		
Route	Attenuation (0.1 dB):		
ARP	Output Power (0.1 dBm):		
Advanced Setup	Attainable Rate (Kbps):		
Wireless	Rate (Kbps):		
Diagnostics			
Management	Super Frames:		
3	Super Frame Errors:		
	RS Words:		
	RS Correctable Errors:		
	RS Uncorrectable Errors:		
	HEU Errors:		
	UCD Errors:		
	LUD Errors: Total Callor		
	Data Colle:		
	Bit Errors:		
	bit Errors.		
	Total ES:		
	Total SES:		
	Total UAS:		
		1	
	xDSL Reset		
		@ 2000-2008	ZTE Corporat

- 2. You can query information of packets recevied 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

ADSL BER Test With OAM F5 - Start
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is done by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors.
Select the test duration below and click "Start".
Tested Time (sec): 5
Start Close

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

#### FIGURE 14 ADSL BER TEST RESULT

🚰 http://192.168.1.1/berrun.tst?berTime=5 - 🖬 💶 🗙
ADSL BER Test With OAM F5 - Running
The xDSL BER test is in progress. The connection speed is Kbps. The test will run for 5 seconds.
Click "Stop" to terminate the test.
Stop Close

### **Route Table Information**

Click **Device Info > Route** to display the interface as shown in Figure 15.

#### FIGURE 13 ADSL BER TEST

ZTE中兴

#### FIGURE 15 ROUTE TABLE

ZTE中兴							
	Device Info	Route					
evice Info	Flags: U - up, ! D - dynamic (re	- reject, G edirect), M -	- gateway, H - h · modified (redire	ost, R ect).	- reinsta	te	
WAN	Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
Statistics	192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
Route							
ARP							
lvanced Setup							
reless							
agnostics							

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.



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 <u>Figure 17</u>.

#### FIGURE 17 ADSL PVC CONFIGURATION OVERVIEW

<b>ZTE中兴</b>									Language	e Select:	English 💌
				DSL Choose Add, or	ATM Interi	ace Config configure DS	u <b>ration</b> 5L ATM interfaces.				
Device Info											
Advanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove		
Layer2 Interface	atm0	8	81	PathO	UBR	EoA	DefaultMode	Enabled			
PTM Interface WAN Service LAN					Add	Remove					

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.

ZTE中兴

FIGURE 18 ADDING EOA PVC

7TE由兴	
LILTA	Language Select: English 💌
Device Info Advanced Setup	ATM PVC Configuration his screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.
Layer2 Interface	VPI: [0-255] 0
ATM Interface	VCI: [32-65535] 35
PTM Interface	
WAN Service	Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
LAN Vien Truck Cotting	
Socurity	
Parental Control	⊖ Iboa
Quality of Service	Encapsulation Mode: LLC/SNAP-BRIDGING
Routing	
DSL	Service Category: UBR Without PCR 💌
Upnp Certificate	Enable Quality Of Service
Wireless	Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and
Diagnostics Management	Realtime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Serviceto assign priorities for the applications.
	Enable Quality Of Service.
	Back Save/Apply
	@ 2000.2009.7TE Conservation. All lighty reserved

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 <b>EOA</b> , 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

<b>ZTE中兴</b>									Language
				DSL	ATM Interf	ace Config	uration		Language
Device Info				Choose Add, or	Remove to	configure D9	GL ATM interfaces.		
Advanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
Layer2 Interface	atm0	8	81	PathO	UBR	EoA	DefaultMode	Enabled	
ATM Interface			_						
PTM Interface	atm1	8	35	PathO	UBR	EoA	DefaultMode	Enabled	
WAN Service									
LAN					Add	Remove			
Vlan Trunk Setting									
Security									
Parental Control									

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



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

ZTE中兴									L	anguage Selec
		Choose A	<b>v</b> dd, or R	<b>/ide Area Ne</b> emove to con	twork (WAN	l <b>) Service</b> service of	e Setup ver a selec	ted interf	ace.	
Device Info										
Advanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atm0	br 0 8 81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface										
PTM Interface	ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	
WAN Service										
LAN					_	_				
Vlan Trunk Setting				1	Add Remov	'e				

By default, system preset WAN Interface is atm0 and ptm0\_1.

6. Click **Add** to display the interface as shown in Figure 21, and select the Layer 2 interface.

ZTE中兴





7. Click **Next** to enter the interface as shown in Figure 22.

#### FIGURE 22 SELECT WAN SERVICE TYPE

Device Info       Select WAN service type:         Advanced Setup       © PPP over Ethernet (PPPoE)         Layer2 Interface       © Bridging         ATM Interface       PIM Interface         VAN Service       Service Description: pppoe_0_0_35         LAN       Vlan Trunk Setting         Security       Back Next	ZTE中兴		
Device Info   Advanced Setup   Layer2 Interface   PTM Interface   PTM Interface   WAN Service   LAN   Vlan Trunk Setting   Security   Select WAN service type:    Select WAN service type:    Select WAN service type:    Select WAN service type:      Device Info     © PPP over Ethernet (PPPoE)     © Bridging   Service Description: pppoe_0_0_35   Back Next		WAN Service Configuration	
Device Info <ul> <li>PPP over Ethernet (PPPoE)</li> </ul> <li>Advanced Setup             <ul> <li>I p over Ethernet (PPPoE)</li> <li>I p over Ethernet</li> <li>I p over Ethernet</li> <li>Bridging</li> <li>ATM Interface</li> <li>PTM Interface</li> <li>Service Description: pppoe_0_0_35</li> <li>Security</li> <li>Back Next</li> </ul></li>		Select WAN service type:	
Advanced Setup     C IP over Ethernet       Layer2 Interface     C Bridging       ATM Interface     Service Description: pppoe_0_0_35       WAN Service     Service Description: pppoe_0_0_35       LAN     Jan Trunk Setting       Security     Back Next	Device Info	PPP over Ethernet (PPPoE)	
Layer2 Interface     O Bridging       ATM Interface     PTM Interface       PTM Interface     Service Description: pppoe_0_0_35       WAN Service     Back Next       Security     Back Next	Advanced Setup	C IP over Ethernet	
ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting Security Back Next	Layer2 Interface	C Bridging	
PTM Interface     Service Description: pppoe_0_0_35       WAN Service     LAN       Vlan Trunk Setting     Back Next	ATM Interface		
WAN Service     Service Description: pppoe_0_0_35       LAN     Vlan Trunk Setting       Security     Back Next	PTM Interface		
LAN Vlan Trunk Setting Security Back Next	WAN Service	Service Description: pppoe_0_0_35	
Vian Trunk Setting Security Back Next	LAN		
Security	Vlan Trunk Setting		Back Novt
	Security		Dack Next
Parental Control	Parental Control		

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

#### FIGURE 23 PPPOE CONFIGURATION

77日由州	
LICHY	Language Select: E
	PPP Username and Password
Device Info	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.
Advanced Setup	
Laver2 Interface	
ATM Interface	PPR L loors amout
PTM Interface	
WAN Service	PPP Password:
LAN	PPPoE Service Name: zte
Vlan Trunk Setting	Authentication Method: AUTO
Security	
Parental Control	PPP IP extension
Quality of Service	Footble NAT
Routing	
DSL	Use Static IPv4 Address
Upnp	
Certificate	
Wireless	
Diagnostics	IGMP Multicast
Management	Enable IGMP Multicast
	Back Next

<u>Table 9</u> is a description of the different options.

TABLE 9	<b>PPPoE</b>	CONFIGURATION	<b>O</b> PTIONS
---------	--------------	---------------	-----------------

Field	Description
PPP Username	The user name that your ISP provides to you.
PPP Password	The password that your ISP pro- vides 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 <b>AUTO</b> , <b>PAP</b> , <b>CHAP</b> , or <b>MSCHAP</b> . Usually, you can select <b>AUTO</b> .
Enable NAT	Select it to enable the NAT func- tions 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 equip- ment. 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

ZTE中兴	
	Routing Default Gateway
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing	Select a preferred wan interface as the system default gateway. Selected WAN Interface pppoe_0_8_35/ppp0 V

11. Click **Next** to enter the interface as shown in Figure 25.

#### FIGURE 25 DNS CONFIGURATION

<b>ZTE中兴</b>	Language Select: En
	DNS Server Configuration
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface	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. Obtain DNS info from a WAN interface: WAN Interface selected: ppppee_0_35/ppp0 v
WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service	C Use the following Static DNS IP address: Primary DNS server: Secondary DNS server:

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.

ZTE中兴			
	WAN Setup - Summa	ary	
	Make sure that the set	tings below match the se	ttings provided by your ISP.
Device Info			1
Advanced Setup	Connection Type:	PPPoE	
Layer2 Interface	Service Name:	pppoe_0_8_35	
ATM Interface	Service Category:	UBR	
PTM Interface	IP Address:	Automatically Assigned	
WAN Service			
LAN	Service State:	Enabled	
Vlan Trunk Setting	NAT:	Enabled	
Security	Full Cone NAT:	Disabled	
Parental Control	Firewall:	Enabled	
Quality of Service	IGMP Multicast:	Enabled	
Routing	Quality Of Complexit	Enabled	
DSL	quality of service.		
Upnp	Click Apply (Caup to ba	ua thia interface to be off	active. Click Back to wake any modifications
Certificate	снок жирнулаалы ш па	ve uns interrace to be en	Body Cove/Apply
Wireless			back Save/Apply

#### FIGURE 26 EOA PPPOE WAN CONNECTION SETUP SUMMARY

13. 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										
			wi	ide Area Net	work (WAN)	Service	Setup			
	Choose Add, or Remove to configure a WAN service over a selected interface.									
Device Info Advanced Setun	Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Iamp	NAT	Firewall	Remove
Layer2 Interface	atmO	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface PTM Interface	ppp0	pppoe_0_8_35	PPPoE	N/A	N/A	N/A	Enabled	Enabled	Enabled	
WAN Service	ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	
Vian Trunk Setting	<u>.                                    </u>	-				-				
Security Parental Control				A	dd Remove	Э				
Quality of Service										

14. 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

ZTE中兴	ŧ									Language	: Select: Engli:
		DSL ATM Interface Configuration									
		Choose Add, or Remove to configure DSL ATM interfaces.									
Device Info											
Advanced Setup	Interfa	ce 🛛	/pi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove	
Layer2 Interface	atm0		8	81	Path0	UBR	EoA	DefaultMode	Enabled		
ATM Interface			-								
PTM Interface						Add	Bomovo				
WAN Service						Auu	Kelligve				
LAN											

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

77日由ツ	
LILTT	Language Select: English
	Cangeoge Verecci 1999
	ATM PVC Configuration
	his tree allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise
Device Info	choose an existing interface by selecting the checkbox to enable it.
Advanced Setup	
Layer2 Interface	VPI: [0-255] 0
ATM Interface	VCI: [32-65535] 35
PTM Interface	
WAN Service	Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
LAN	• EOA
Vlan Trunk Setting	C PPPoA
Security	C IPOA
Parental Control	
Quality of Service	
Rouung	Service Category: UBR Without PCR -
Uppp	
Certificate	Enable Quality Of Service
Wireless	Fashing assignt level Occ. For a DVC investory performance for calented classes of analyziting. Occ. second to cat for OD, and
Diagnostics	Realing packet even gos to a rive improves period market to select classes of applications. Gos control can and Realing VBR, OoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality
Management	of Service to assign priorities for the applications.
_	Smahle Quality Of Service
	Entry characterized of the second
	Back Save/Apply
	@ 2000-2008 ZTE Corporation. All rights reserved.

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 <b>EOA</b> , 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.

3. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in Figure 30.

ZTE中兴									Languag
	DSL ATM Interface Configuration								
ce Info				· · · ·					
nced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
er2 Interface	atm0	8	81	Path0	UBR	FnA	DefaultMode	Enabled	
M Interface							Deraditeribate	Enderod	
M Interface	atm1	8	35	Path0	UBR	EoA	DefaultMode	Enabled	
AN Service									
l i i i i i i i i i i i i i i i i i i i					Add	Remove			
Trunk Setting									
urity									
ntal Control									

FIGURE 30 EOA PVC CONFIGURATION COMPLETED

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



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

ZTE中兴										
		Choose A	<b>W</b> .dd, or R	<b>Vide Area Ne</b> emove to con	twork (WAN figure a WAN	I <b>) Servic</b> e service o	e Setup ver a selec	cted interfa	ace.	anguage sele
Device Info Advanced Setun	Interface	Description	Type	Vlan8021n	VlanMuxId	ConnId	Iamp	NAT	Firewall	Remove
Layer2 Interface	atm0	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface PTM Interface	ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	
WAN Service LAN Vlan Trunk Setting			1		Add Remov	/e		1	1	<u>.                                    </u>

By default, system preset WAN Interface is **atm0** and **ptm0\_1**.

6. Click **Add** to display the interface as shown in Figure 32, and select the Layer 2 interface.

ZTE中兴





7. Click **Next** to enter the interface as shown in Figure 33.

#### FIGURE 33 SELECT WAN SERVICE TYPE

ZTE中兴		
	WAN Service Configuration	
	Select WAN service type:	
Device Info	C PPP over Ethernet (PPPoE)	
Advanced Setup	• IP over Ethernet	
Layer2 Interface	C Bridging	
ATM Interface		
PTM Interface WAN Service	Service Description: poe_0_8_35	
Vlan Trunk Setting Security		Back Next

- 8. Select IP over Ethernet .
- 9. Click **Next** to enter the interface as shown in Figure 34.

#### FIGURE 34 WAN IP CONFIGURATION

<b>ZTE中兴</b>	Language Sol
	WAN IP Settings
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing DSL Upnp Certificate	Enter information provided to you by your ISP to configure the WAN IP settings. Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.  C Obtain an IP address automatically Option 60 Vendor ID:  C Use the following Static IP address: WAN IP Address: WAN JP Address: WAN gateway IP Address: WAN gateway IP Address:

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

<b>ZTE中</b> 兴	Language Select English
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vian Trunk Setting Security Parental Control	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).         Imable Device The Set of the Set
Quality of Service Routing DSL	Back Next

11. Click **Next** to enter the interface as shown in Figure 36.

ZTE中兴	
	Routing Default Gateway
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting	Select a preferred wan interface as the system default gateway. Selected WAN Interface ipoe_0_8_35/atm1 💌
Security Parental Control Quality of Service Routing	Back Next

12. Click **Next** to enter the interface as shown in Figure 37.

FIGURE 36 DEFAULT GATEWAY CONFIGURATION



#### FIGURE 37 DNS CONFIGURATION

ZTE中兴	
	DNS Server Configuration
evice Info	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.
dvanced Setup	
Layer2 Interface	Obtain DNS info from a WAN interface:
ATM Interface	WAN Interface selected; ippe 0 8 35/atm1 💌
PTM Interface	
WAN Service	O Use the following Static DNS IP address:
LAN	Primary DNS server:
Vlan Trunk Setting	
Security	Secondary UNS server:
Parental Control	
Quality of Service	
Routing	

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

ZTE中兴			
	WAN Setup - Summa	агу	
	Make sure that the set	tings below match the se	ttings provided by your ISP.
Device Info			1
Advanced Setup	Connection Type:	IPOE	
Layer2 Interface	Service Name:	ipoe_0_8_35	
ATM Interface	Service Category:	UBR	
PTM Interface	IP Address:	Automatically Assigned	
WAN Service	Coruico Stato:	Enabled	
LAN	service state.		
Vlan Trunk Setting	NAT:	Enabled	
Security	Full Cone NAT:	Disabled	
Parental Control	Firewall:	Enabled	
Quality of Service	IGMP Multicast:	Disabled	
Routing	Quality Of Service:	Disabled	
DSL	Quality of Service.		
Upnp	Click Apply/Save to ba	ve this interface to he effi	ective. Click Back to make any modifications
Certificate			Back Save Apply
Wireless			Contraction (Pp)

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

ZTE中兴									L	anguage Seli
			Ŵ	/ide Area Ne	twork (WAN	l) Service	e Setup			
		Choose A	.dd, or R	emove to con	figure a WAN	service of	ver a seleo	ted interfa	ace.	
evice Info			_				-			-
dvanced Setup	Interface	Description	Type	Vian8021p	VianMuxId	Connid	Igmp	NAT	Hrewall	Remove
.ayer2 Interface	atm0	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface			-							
PTM Interface	atm1	ipoe_0_8_35	IPoE	N/A	N/A	N/A	Disabled	Enabled	Enabled	
VAN Service	ptm0 1	br 0 0 1 1	Bridae	N/A	N/A	1	Disabled	Disabled	Disabled	Г
AN	Percent.					_			-	
Vlan Trunk Setting										
Security					Add Remov	10				
Parental Control				1	- TOTTO					
uality of Service										
outing										
151										

#### FIGURE 39 EOA IPOE 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 ADSL EoA Bridge WAN Connection

1. Select **Advanced Setup > Layer2 Interface > ATM Interface** to display the interface as shown in Figure 40.

FIGURE 40 ADSL PVC CONFIGURATION OVERVIEW

ZTE中兴									Language	e Select:	English 💌
				DSL Choose Add, or	ATM Interi	ace Config configure DS	u <b>ration</b> 5L ATM interfaces.				
Device Info			_								
Advanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove		
Layer2 Interface	atmO	8	81	PathO	UBR	EoA	DefaultMode	Enabled			
PTM Interface WAN Service LAN					Add	Remove					

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 41.

ZTE中兴

FIGURE 41 ADDING EOA PVC

TTELW	
<b>ZIE</b> 甲兴	Language Select: English 👱
Device Info Advanced Setup Layer2 Interface ATM Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing DSL Upnp Certificate Wireless Diagnostics Management	ATM PVC Configuration         his screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose are instituty interface by selecting the checkbox to enable it.         VPI: [0-255]       □         VCI: [32-65556]       □         Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)       ●         ●       ●         ●       PPPoA         ○       PPoA         ●       ProA         Encapsulation Mode: [LIC/SNAP-BRIDGING ▼         Service Category:       UBR Without PCR ▼         Enable Quality Of Service       ProA         Rabiling packet level QOS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Rabiling VBR. QoS consume system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Serviceto assign priorities for the applications.
	Enable Quality Of Service.
	Back Save/Apply
	@ 2000.2009 ZTE Constration. All sight recorded

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 <b>EOA</b> , 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

ZTE中兴									
				DSL	ATM Interi	ace Config	uration		Language
Device Info				Choose Add, o	r Remove to	configure D9	SL ATM interfaces.		
dvanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
Layer2 Interface	atmO	8	81	Path0	UBR	FnA	DefaultMode	Enabled	
ATM Interface									
PTM Interface	atm1	8	35	Path0	UBR	EoA	DefaultMode	Enabled	
WAN Service									
LAN					Add	Remove			
Vlan Trunk Setting									
Security									
Parental Control									

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



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

ZTE中兴									L	anguage Selec
		Choose A	<b>v</b> dd, or R	<b>/ide Area Ne</b> emove to con	twork (WAN	l <b>) Service</b> service of	e Setup ver a selec	ted interf	ace.	
Device Info										
Advanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atm0	br 0 8 81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface										
PTM Interface	ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	
WAN Service										
LAN					_	_				
Vlan Trunk Setting				1	Add Remov	'e				

By default, system preset WAN Interface is atm0 and ptm0\_1.

6. Click **Add** to display the interface as shown in Figure 44, and select the Layer 2 interface.

上田茶

#### FIGURE 44 SELECT LAYER2 INTERFACE

ZTE中兴	
	WAN Service Interface Configuration
	Select a layer 2 interface for this service
Device Info	
Advanced Setup	Note: For PTM interface, the descriptor string is (portId_high_low)
Layer2 Interface	Where portId=0> DSL Latency PATHO
ATM Interface	portid=1> DSL Latency PATH1
PTM Interface	low =0> Low PTM Priority not set
WAN Service	low =1> Low PTM Priority set
LAN	high =0> High PTM Priority not set
Vlan Trunk Setting	high =1> High PTM Priority set
Security	atm1/(0_8_35) 💌
Parental Control	
Quality of Service	
Routing	Back Next
DSL	

7. Click **Next** to enter the interface as shown in Figure 45.

#### FIGURE 45 SELECT WAN SERVICE TYPE

ZTE中兴		
	WAN Service Configuration Select WAN service type:	
Device Info	C PPP over Ethernet (PPPoE)	
Advanced Setup	C IP over Ethernet	
Layer2 Interface	Bridging	
ATM Interface		
PTM Interface	Service Description: br. 0, 8, 35	
WAN Service	Service Description, [bi_0_0_0]	
LAN		
Vlan Trunk Setting		Back Next
Security		DUCK
Parental Control		

- Select **Bridging**.
   Click **Next** to enter the interface as shown in <u>Figure 46</u>.

ZTE中兴	WAN Setup - Summ	ary	to the cottings provided by use in 100
Device Info	Make sure that the set	tings below mat	n the settings provided by your ISP.
Advanced Setup	Connection Type:	Bridge	
Layer2 Interface	Service Name:	br_0_8_35	
ATM Interface	Service Category:	UBR	
PTM Interface	IP Address:	Not Applicable	
WAN Service	Service State:	Enabled	
LAN	Service State.		
Vlan Trunk Setting	NAT:	Disabled	
Security	Full Cone NAT:	Disabled	
Parental Control	Firewall:	Disabled	
Quality of Service	IGMP Multicast:	Not Applicable	
Routing	Quality Of Comission	Dissibled	
DSL	quality of service:	Disableu	
Upnp Certificate Wireless	Click Apply/Save to ha	ve this interface	to be effective. Click Back to make any modifications. Back Save/Apply

#### 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 <u>Figure 48</u>.



#### FIGURE 48 ADSL PVC CONFIGURATION OVERVIEW

ZTE中兴	ł								Language	Select: English 💌	
				DSL	ATM Interf	face Config	uration				
		Choose Add, or Remove to configure DSL ATM interfaces.									
Device Info											
Advanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove		
Layer2 Interface	atm0	8	81	Path0	UBR	EoA	DefaultMode	Enabled			
ATM Interface											
PTM Interface					Add	Pamova					
WAN Service					Maa	Remove					
LAN											

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

2. To add PPPoA PVC, click **Add** to display the interface as shown in Figure 49.

#### FIGURE 49 ADDING PPPOA PVC

	Language Select. English 👤
	ATM PVC Configuration
	his screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise
Device Info	choose an existing interface by selecting the checkbox to enable it.
Advanced Setup	
Layer2 Interface	VPI: [0-255]  8
ATM Interface	VCI: [32-65535] 35
PTM Interface	
WAN Service	Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge.)
LAN	O EOA
Vlan Trunk Setting	© PPPoA
Security	C IPOA
Parental Control	
Quality of Service	Encapsulation Mode: VC/MUX
Routing	
DSL	Service Category: UBR Without PCR 💌
Upnp	Enable Quality Of Service
Certificate	
Wireless	Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and
Diagnostics	Realitime VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Security actions provide for the applications.
Management	or der andere assign privilities für die applications.
	Enable Quality Of Service.

#### 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 <b>PPPoA</b> .
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 50.

FIGURE 50 PPPOA PVC CONFIGURATION COMPLETED

ZTE中兴									Langua
				DSL Choose Add, o	ATM Inter	face Config configure D	<b>uration</b> BL ATM interfaces.		
evice Info dvanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
Layer2 Interface	atmO	8	81	Path0	UBR	EoA	DefaultMode	Enabled	
PTM Interface	atm1	8	35	Path0	UBR	PPPoA	DefaultMode	Disabled	
WAN Service LAN Vlan Trunk Setting					Add	Remove			

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



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.

ZTE中兴									L	anguage Se
		Choose A	.dd, or R	<b>ride Area Ne</b>	twork (WAN	I <b>) Servic</b> e service o	e Setup ver a selec	ted interfa	ace.	
Device Info				(	(					
Advanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atmO	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
PTM Interface	ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	
WAN Service							-			
LAN					_	_				
Vlan Trunk Setting					Add Remov	e				

By default, system preset WAN Interface is **atm0** and **ptm0\_1**.

6. Click **Add** to display the interface as shown in <u>Figure 52</u>, and select the Layer 2 interface.

#### FIGURE 51 WAN SERVICE OVERVIEW

**ZTE**中兴



ZTE中兴	
	WAN Service Interface Configuration
	Select a layer 2 interface for this service
Device Info	
Advanced Setup	Note: For PTM interface, the descriptor string is (portId_high_low)
Layer2 Interface	Where portId=0> DSL Latency PATHO
ATM Interface	portid=1> DSL Latency PATH1
PTM Interface	low =0> Low PTM Priority not set
WAN Service	low =1> Low PTM Priority set
LAN	high =0> High PTM Priority not set
Vlan Trunk Setting	high =1> High PTM Priority set
Security	atm1/(0, 8, 35) 💌
Parental Control	
Quality of Service	
Routing	Back Next
DSL	

7. Click **Next** to enter the interface as shown in Figure 53.

#### FIGURE 53 WAN SERVICE CONFIGURATION

ZTE中兴		
	WAN Service Configuration	
Device Info Advanced Setup Laver2 Interface	Service Description: pppoa_0_8_35	
ATM Interface PTM Interface WAN Service		Back Next

8. Click **Next** to enter the interface as shown in Figure 54.

#### FIGURE 54 PPPOA CONFIGURATION

<b>ZTE中兴</b>	Language Select, E
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing DSL Upnp Certificate Wireless Diagnostics Management	PPP Username and Password  PPP username 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:
	Back Next

Table 13 is a description of the different options.

Field	Description
PPP Username	The user name that your ISP provides to you.
PPP Password	The password that your ISP pro- vides to you.
Authentication Method	The value can be <b>AUTO</b> , <b>PAP</b> , <b>CHAP</b> , or <b>MSCHAP</b> . Usually, you can select <b>AUTO</b> .
Enable NAT	Select it to enable the NAT func- tions 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 equip- ment. 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.

#### TABLE 13 PPPOA CONFIGURATION OPTIONS

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

ZTE中兴	Language Select: Erg
	DNS Server Configuration
evice Info dvanced Setup	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.
Layer2 Interface	Obtain DNS info from a WAN interface:
PTM Interface	WAN Interface selected: pppoa_0_8_35/pppoa0 💌
WAN Service	O Use the following Static DNS IP address:
LAN	Primary DNS server:
Vlan Trunk Setting	
Security	Secondary Drys Server.
Parental Control	
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**.

11. Click **Next** to enter the interface as shown in Figure 57.

#### FIGURE 57 PPPOA WAN CONNECTION SETUP SUMMARY

ZTE中兴			
Denire Infe	WAN Setup - Summa	a <b>ry</b> ttings below match the se	ttings provided by your ISP.
Advanced Setun	Connection Type:	PPPoA	1
Laver2 Interface	Service Name:	nnnoa 0 8 35	
ATM Interface	Corvice Name.		
PTM Interface	TD Addresses		
WAN Service	IP Address:	Automatically Assigned	
LAN	Service State:	Enabled	
Vian Trunk Setting	NAT:	Enabled	
Security	Full Cone NAT:	Disabled	
Parental Control	Firewall:	Enabled	
Quality of Service	IGMP Multicast:	Disabled	
Routing	Quality Of Service:	Disabled	
DSL	Quality of betvice.		
Upnp	Click Apply/Save to ha	ve this interface to be eff	ective. Click Back to make any modifications.
Certificate			Back Save/Apply
Piegeneotics			
Management			
management			

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

ZTE中兴									Li	anguage Sel
			W	ide Area Net	work (WAN)	Service	Setup			
		Choose Ac	ld, or Re	emove to confi	igure a WAN s	service ov	er a selec	ted interfa	ce.	
vice Info										
vanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
ayer2 Interface	atm0	br 0 8 81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface									I	
PTM Interface	pppoa0	pppoa_0_8_35	PPPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
VAN Service	ntm0 1	hr 0 0 1 1	Bridge	N/A	N/A	1	Disahled	Disabled	Disahled	
AN						-				
'lan Trunk Setting										
ecurity				۵	dd Remove					
arental Control										
Juality of Service										

#### 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 <u>Figure 59</u>.

FIGURE 59 ADSL PVC CONFIGURATION OVERVIEW

ZTE中兴									Language
				DSL Choose Add, or	ATM Interi	í <mark>ace Config</mark> configure DS	u <b>ration</b> 5L ATM interfaces.		
Device Info Advanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
Layer2 Interface	atmO	8	81	Path0	UBR	EoA	DefaultMode	Enabled	
PTM Interface WAN Service LAN					Add	Remove			

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.

ZTE中兴

#### FIGURE 60 ADDING IPOA PVC

ZTE中兴	Language Select English
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing DSL Uppp Certificate Wireless Diagnostics Management	ATM PVC Configuration  his screen allows you to configure an ATM PVC identifier (VPI and VCI), select DSL latency, select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.  VPI: [0-255]  VCI: [32-65535]  Select DSL Link Type (EoA is for PPPoE, IPOE, and Bridge.)  C EoA  PPPoA  ProA  Encapsulation Mode: LLC/SNAP-ROUTING  Service Category: UBR Without PCR  Enabling packet level QoS for a PVC improves performance for selected classes of applications. QoS cannot be set for CBR and Realtimp VBR. QoS consumes system resources; therefore the number of PVCs will be reduced. Use Advanced Setup/Quality of Service category in the applications.
	Back Save/Apply

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.

3. 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

ZTE中兴									Langua
				DSL Choose Add, o	<b>ATM Inter</b> r Remove to	face Config	<b>uration</b> SL ATM interfaces.		
)evice Info				1					
dvanced Setup	Interface	Vpi	Vci	DSL Latency	Category	Link Type	Connection Mode	QoS	Remove
Layer2 Interface	atmO	8	81	Path0	UBR	EoA	DefaultMode	Enabled	П
ATM Interface		<u> </u>							
PTM Interface	ipoa0	8	35	Path0	UBR	IPoA	DefaultMode	Disabled	
WAN Service									
AN					Add	Remove			
Vlan Trunk Setting									

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

O 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 <u>Figure 62</u>.

<b>ZTE中兴</b>									L	anguage Selec	t:
		Choose A	<b>v</b> .dd, or R	<b>/ide Area Ne</b> emove to con	twork (WAN	I <b>) Servic</b> e service o	e Setup ver a selec	ted interfa	ace.		
Device Info											
Advanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove	
Layer2 Interface	atmO	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled		
ATM Interface							l		l		
PTM Interface	ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled		
WAN Service											
LAN											
Vlan Trunk Setting					Add Remov	/e					

By default, system preset WAN Interface is **atm0** and **ptm0\_1**.

6. Click **Add** to display the interface as shown in Figure 63, and select the Layer 2 interface.

ZTE中兴	
	WAN Service Interface Configuration
	Select a layer 2 interface for this service
Device Info	
Advanced Setup	Note: For PTM interface, the descriptor string is (portId_high_low)
Layer2 Interface	Where portid=0> DSL Latency PATH0
ATM Interface	portid=1> DSL Latency PATH1 nortid=4> DSL Latency PATH08.1
PTM Interface	low =0> Low PTM Priority not set
WAN Service	low =1> Low PTM Priority set
LAN	high =0> High PTM Priority not set
Vian Trunk Setting	high =1> High PTM Priority set
Security	inca0/(0.8.35) 💌
Parental Control	
Quality of Service	
Routing	Back Next
DSL	

FIGURE 63 SELECT LAYER2 INTERFACE

FIGURE 62 WAN SERVICE OVERVIEW

7. Click **Next** to enter the interface as shown in Figure 64.



#### FIGURE 64 WAN SERVICE CONFIGURATION

ZTE中兴		
	WAN Service Configuration	
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting	Service Description: poa_0_8_35	Back Next

#### 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 provid	ded to you by your ISP to a	configure the WAN IP settings.
Device Info			
Advanced Setup	WAN IP Address:	10.1.1.1	
Layer2 Interface	WAN Subnet Mask:	255.255.255.0	
ATM Interface		đ.	
PTM Interface			Back Next
WAN Service			
LAN			

9. Click **Next** to enter the interface as shown in Figure 66.

#### FIGURE 66 NAT CONFIGURATION

<b>7TF</b> 中兴	
	Language Select: Englis
	Network Address Translation Settings
	Network Address Translation (NAT) allows you to share one Wide Area Network(WAN) IP address for multiple computers on your
Device Info	Local Area Network (LAN).
Advanced Setup	
Layer2 Interface	Enable NAT
ATM Interface	Enable Fullrane NAT
PTM Interface	
WAN Service	
LAN	IGMP Multicast
Vlan Trunk Setting	
Security	Enable IGMP Multicast
Parental Control	
Quality of Service	
Routing	Back Next
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

ZTE中兴	Langeauge Select English 2
	DNS Server Configuration
Device Info Advanced Setun	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.
Layer2 Interface	O Obtain DNS info from a WAN interface:
ATM Interface	WAN Interface selected: NO CONFIGURED INTERFACE
WAN Service	O Use the following Static DNS IP address:
LAN	Primary DNS server: 10.63.1.1
Vlan Trunk Setting Security	Secondary DNS server: 10.65.1.1
Parental Control	
Routing	

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

ZTE中兴			
	WAN Setup - Summa Make sure that the set	<b>ary</b> tings below ma	tch the settings provided by your ISP.
Device Info			
Advanced Setup	Connection Type:	IPoA	
Layer2 Interface	Service Name:	ipoa_0_8_35	
ATM Interface	Service Category:	UBR	
PTM Interface	IP Address:	10.1.1.1	
WAN Service	Complex Obstat	Exceleted.	
LAN	service state:	Enabled	
Vlan Trunk Setting	NAT:	Enabled	
Security	Full Cone NAT:	Disabled	
Parental Control	Firewall:	Enabled	
Quality of Service	IGMP Multicast:	Disabled	
Routing	Quality Of Service:	Disabled	
DSL	danci or ser neer		
Upnp	Click Apply/Save to ha	ve this interface	e to be effective. Click Back to make any modifications.
Certificate			Back Save/Apply
Wireless			
Diagnostics			

13. 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

ZTE中兴									L	anguage Sele
			W	/ide Area Ne	twork (WAN	) Service	e Setup			
	Choose Add, or Remove to configure a WAN service over a selected interface.									
Device Info			-				-			-
dvanced Setup	Interface	Description	Туре	Vlan8021p	VianMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atmO	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface										-
PTM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
WAN Service	ptm0_1	br_0_0_1_1	Bridge	N/A	N/A	1	Disabled	Disabled	Disabled	
LAN										1
Vlan Trunk Setting										
Security					Add Remov	e l				
Parental Control				1	10011101	-				
Quality of Service										

14. 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

ZTE中兴						
		DSL Choose Add, o	. PTM Interfac	e Configuration	rfaces.	
evice Info					(	
lvanced Setup	Interface	DSL Latency	PTM Priority	Connection Mode	QoS	Remov
ayer2 Interface	ntmD	PathO	Normal	DefaultMode	Enabled	
ATM Interface	P					
PTM Interface			Add D			
VAN Service			Ruu	amove		
AN						
/lan Trunk Setting						

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

### **O** 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.



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

<b>ZTE中兴</b>	Language Select , English 💌
	PTM Configuration
Device Info	Select PTM Priority
Advanced Setup	Mormal Priority
Layer2 Interface	Enable Quality Of Service
ATM Interface	
PTM Interface	Enabling packet level QoS for this PTM interface. Use Advanced Setup/Quality of Service to assign priorities for the
WAN Service	applications.
LAN	turned
Vlan Trunk Setting	Enable Quality Of Service
NAT	
Security	Back Save/Apply
Parental Control	
Quality of Service	

- 4. 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 inFigure 73.

#### FIGURE 73 WAN SERVICE OVERVIEW

ZTE中兴									ı	.anguage Se
		Choose A	<b>W</b> .dd, or R	<b>/ide Area Ne</b>	<b>twork (WAN</b> figure a WAN	I <b>) Servic</b> e service o	e Setup ver a selec	ted interfa	ace.	
Device Info										
dvanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atm0	br 0 8 81	Bridae	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface										
PTM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
WAN Service					1					
LAN										
Vlan Trunk Setting					Add Remov	e l				
NAT				-						

By default, system preset WAN Interface is **atm0** and **ptm0\_1**.

6. Click **Add** to display the interface as shown in <u>Figure 74</u>, and select the Layer 2 interface.

FIGURE 74 SELECT LAYER2 INTERFACE

ZTE中兴	
	WAN Service Interface Configuration
	Select a layer 2 interface for this service
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting NAT Security	Note: For PTM interface, the descriptor string is (portId_high_low) Where portId=0> DSL Latency PATH0 portId=1> DSL Latency PATH1 portId=4> DSL Latency PATH1 low =0> Low PTM Priority not set low =1> Low PTM Priority set high =0> High PTM Priority not set high =1> High PTM Priority set
Parental Control Quality of Service Routing DNS	Back Next

7. Click **Next** to enter the interface as shown in Figure 75.

<b>ZTE</b> 中兴	
	WAN Service Configuration
	Select WAN service type:
Device Info	PPP over Ethernet (PPPoE)
Advanced Setup	O IP over Ethernet
Layer2 Interface	O Bridging
ATM Interface	
PTM Interface	
WAN Service	Service Description: pppoe_0_0_1
LAN	
Vlan Trunk Setting	
NAT	Enable VLAN Mux - Supporting Multiple Protocols Over a Single PTM interface
Security	Enter 802.1P Priority [0-7]: 7
Parental Control	Enter 802.1Q VLAN ID [1-4094]: 2
Quality of Service	
Routing	
DNS	Back Next
DSL	

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

7TEmw	
LICHT	Language Select: E
	PPP Username and Password
Device Info	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.
Advanced Setup	
Layer2 Interface ATM Interface	PPP Username: zte
PTM Interface	PPP Password:
LAN	PPPoE Service Name: zte
Vlan Trunk Setting Security	Authentication Method: AUTO
Parental Control	PPP IP extension
Quality of Service Routing	Enable NAT
DSL	Use Static IPv4 Address
Upnp Certificate	
Wireless Diagnostics	IGMP Multicast
Management	Enable IGMP Multicast
	Back Next

Table 15 is a description of the different options.

Field	Description
PPP Username	The user name that your ISP provides to you.
PPP Password	The password that your ISP pro- vides 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 <b>AUTO</b> , <b>PAP</b> , <b>CHAP</b> , or <b>MSCHAP</b> . Usually, you can select <b>AUTO</b> .
Enable NAT	Select it to enable the NAT func- tions 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 equip- ment. 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.

#### TABLE 15 PPPOE CONFIGURATION OPTIONS

11. Click **Next** to enter the interface as shown in Figure 77.

#### FIGURE 77 DEFAULT GATEWAY CONFIGURATION

ZTE中兴	
	Routing Default Gateway
Device Info	Select a preferred wan interface as the system default gateway.
Advanced Setup	
Layer2 Interface	Selected wain Interface pppoe_0_0_1.2/ppp0.2
ATM Interface	
WAN Service	
LAN	
Vlan Trunk Setting	
NAT	
Security	
Parental Control	Back Next
Quality of Service	
Routing	

12. Click **Next** to enter the interface as shown in Figure 78.

#### FIGURE 78 DNS CONFIGURATION

ZTE中兴	Language Select: English
	DNS Server Configuration
Device Info	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.
Advanced Setup	
Layer2 Interface	Obtain DNS info from a WAN interface:
ATM Interface	WAN Interface selected: pppoe_0_0_1.2/ppp0.2 💌
PTM Interface	
WAN Service	O Use the following Static DNS IP address:
LAN	Primary DNS server:
Vlan Trunk Setting	
NAT	Secondary DNS server:
Security	
Parental Control	
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**.

13. Click **Next** to enter the interface as shown in Figure 79.

#### FIGURE 79 PTM INTERFACE PPPOE WAN CONNECTION SETUP SUMMARY

ZTE中兴			
	WAN Setup - Summa Make sure that the set	<b>ary</b> tings below match the se	ttings provided by your ISP.
Device Info			1
Advanced Setup	Connection Type:	PPPOE	
Layer2 Interface	Service Name:	pppoe_0_0_1.2	
ATM Interface	Service Category:	UBR	
PTM Interface	IP Address:	Automatically Assigned	
WAN Service	Service State:	Enabled	
LAN	NAT.	Enabled	
Vlan Trunk Setting	INAT:	Enableu	
NAT	Full Cone NAT:	Disabled	
Security	Firewall:	Enabled	
Parental Control	IGMP Multicast:	Disabled	
Quality of Service	Quality Of Service:	Enabled	
DNS DSL Upnp Certificate	Click Apply/Save to ha	• ve this interface to be effi	active. Click Back to make any modifications. Back Save/Apply

14. Click **Save/Apply** to save the configuration so that the changes can take effect, as shown in <u>Figure 80</u>.



### FIGURE 80 PTM INTERFACE PPPOE WAN CONNECTION CONFIGURATION COMPLETED

ZTE中兴										
			wi	de Area Net	work (WAN)	Service	Setup		La	nguage Selei
		Choose Ad	d, or Re	move to confi	gure a WAN s	ervice ove	er a select	ed interfa	Ie.	
evice Info										
dvanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atmO	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface			-							_
PTM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
WAN Service	2.0000	ppppe 0 0 1.2	PPPoE	7	2	N/A	Disabled	Enabled	Enabled	
AN										
Vlan Trunk Setting										
NAT				A	dd Remove	3				
Security										
Parental Control										
Quality of Service										
Routing										

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 <u>Figure 81</u>.

FIGURE 81 VDSL2 PTM INTERFACE CONFIGURATION OVERVIEW

ZTE中兴						
		DSL Choose Add, o	. <b>PTM Interfac</b> r Remove to co	e Configuration	rfaces.	
Jevice Into Advanced Setun	Interface	DSL Latency	PTM Priority	Connection Mode	OoS	Remove
Layer2 Interface	ntmD	Path0	Normal	DefaultMode	Enabled	
ATM Interface	pano	10010	- Hormon			
PTM Interface			add R	emove		
WAN Service			COMM 10	SHIDIO		
LAN						
Vlan Trunk Setting						

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



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.

### **D** Note:

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

3. To add new PTM interface, click **Add** to display the interface as shown in Figure 82.

#### FIGURE 82 ADDING PTM INTERFACE

<b>ZTE中</b> 兴	Language Select, English 💌
	PTM Configuration
Device Info	Select PTM Priority
Advanced Setup	Normal Priority
Layer2 Interface	Enable Quality Of Service
ATM Interface	anale quarty of our nee
PTM Interface	Enabling packet level QoS for this PTM interface. Use Advanced Setup/Quality of Service to assign priorities for the
WAN Service	applications.
LAN	turned
Vlan Trunk Setting	Enable Quality Of Service
NAT	
Security	Back Save/Apply
Parental Control	
Quality of Service	

- 4. Click **Save/Apply** to save the configuration so that the changes can take effect.
- 5. Select **Advanced Setup > WAN Service** to display the interface as shown in<u>Figure 83</u>.

ZTE中兴										anguage Seli
		Choose à	W	/ide Area Ne emove to con	twork (WAN	l) Service	e Setup ver a seler	ted interf	are.	
Device Info		01100001			ngaro a torni	0011100-0				
dvanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atm0	br 0 8 81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface		0.7070704	e nage				Diodelea	01000100	E IOGEIOG	-
PTM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
WAN Service LAN Vlan Trunk Setting NAT				1	Add Remov	/8				

FIGURE 83 WAN SERVICE OVERVIEW

By default, system preset WAN Interface is atm0 and ptm0\_1.

6. Click **Add** to display the interface as shown in <u>Figure 84</u>, and select the Layer 2 interface.

7TF中兴

#### FIGURE 84 SELECT LAYER2 INTERFACE

ZTE中兴	
	WAN Service Interface Configuration
	Select a layer 2 interface for this service
Device Info	
Advanced Setup	Note: For PTM interface, the descriptor string is (portId_high_low)
Layer2 Interface	Where portid=0> DSL Latency PATHO
ATM Interface	portid=1> DSL Latency PATH0 portid=4> DSL Latency PATH021
PTM Interface	low =0> Low PTM Priority not set
WAN Service	low =1> Low PTM Priority set
LAN	high =0> High PTM Priority not set
Vlan Trunk Setting	high =1> High PTM Priority set
NAT	ntm0//0_0_1) 💌
Security	
Parental Control	
Quality of Service	Back Next
Routing	
DNS	

7. Click **Next** to enter the interface as shown in Figure 85.

#### FIGURE 85 SELECT WAN SERVICE TYPE

ZTE中兴	
	WAN Service Configuration Select WAN service type:
Device Info	O PPP over Ethernet (PPPoE)
Advanced Setup	, C., IP over Ethernet
Layer2 Interface	Bridging
ATM Interface	
PTM Interface	
WAN Service	Service Description: pr_u_u_i
LAN	
Vlan Trunk Setting	Enable VLAN Mux - Supporting Multiple Protocols Over a Single PTM interface
NAT	
Security	Enter 802.1P Priority [0-7]: 5
Parental Control	Enter 802.1Q VLAN ID [1-4094]: 2
Quality of Service	
Routing	
DNS	Back Next
DSL	
Upnp	
Certificate	

- Select Bridging.
   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.
| 7TF由兴                         |                        |                   |  |
|-------------------------------|------------------------|-------------------|--|
| LIETA                         |                        |                   |  |
|                               | WAN Cotup - Cumm       | 284               |  |
|                               | Whitedap balling       | лy                |  |
| Della Trife                   | Make sure that the set | tings below mate  | h the settings provided by your ISP.                   |
| Device Info<br>Advanced Setup | Connection Type:       | Bridge            |  |
| Laver2 Interface              | Service Name:          | br 0 0 1 2        |  |
| ATM Interface                 | Corvice Name.          |                   |  |
| PTM Interface                 | TD Addresses           |                   |  |
| WAN Service                   | IP Aduress:            | Not Applicable    |  |
| LAN                           | Service State:         | Enabled           |  |
| Vlan Trunk Setting            | NAT:                   | Disabled          |  |
| NAT                           | Full Cone NAT:         | Disabled          |  |
| Security                      | Firewall:              | Disabled          |  |
| Parental Control              | IGMP Multicast:        | Not Applicable    |  |
| Quality of Service            | Quality Of Service:    | Enabled           |  |
| Routing                       | quality of bervice.    |                   |  |
| DNS                           | Click Apply/Save to ha | ve this interface | to be effective. Click Back to make any modifications. |
| DSL                           |                        |                   | Back Save/Apply  |
| Upnp                          |                        |                   |  |
| Uertificate                   |                        |                   |  |
| Diagnostics                   |                        |                   |  |
| Management                    |                        |                   |  |

#### 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

ZTE中兴									L	anguage Seli
			W	/ide Area Ne	twork (WAN	) Service	e Setup			
		Choose A	dd, or R.	temove to con	figure a WAN	service o	ver a selec	ted interfa	ice.	
vice Info vanced Setun	Interface	Description	Type	Vlan8021p	VlanMuxId	ConnId	Iqmp	NAT	Firewall	Remove
yer2 Interface	atm0	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
AN Service	ptm0.2	br_0_0_1.2	Bridge	5	2	N/A	Disabled	Disabled	Disabled	
.AN Vlan Trunk Setting	<u> </u>				1	· ·		1		
IAT					Add Remov	/e				
curity rental Control										

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 <u>Figure 88</u>.



#### FIGURE 88 VDSL2 PTM INTERFACE CONFIGURATION OVERVIEW

ZTE中兴						
		DSL Choose Add, o	. <b>PTM Interfac</b> r Remove to co	e Configuration	rfaces.	
vice Info						
vanced Setup	Interface	DSL Latency	PTM Priority	Connection Mode	QoS	Remove
ayer2 Interface	ptm0	Path0	Normal	DefaultMode	Enabled	
ATM Interface						
PTM Interface			Add D	omovo		
AN Service			Buu	sinove		
AN .						
an Trunk Setting						

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



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.

3. To add new PTM interface, click Add to display the interface as shown in Figure 89.

#### FIGURE 89 ADDING PTM INTERFACE

<b>ZTE中</b> 兴	Language Select: English 💌
	PTM Configuration
Device Info	Select PTM Priority
Advanced Setup	M Normal Priority
Layer2 Interface	Enable Quality Of Service
ATM Interface	
PTM Interface	Enabling packet level QoS for this PTM interface. Use Advanced Setup/Quality of Service to assign priorities for the
WAN Service	applications.
LAN	
Vlan Trunk Setting	Enable Quality Of Service
NAT	
Security	Back Save/Apply
Parental Control	
Quality of Service	

- 4. Click Save/Apply to save the configuration so that the changes can take effect.
- 5. Select Advanced Setup > WAN Service to display the interface as shown in Figure 90.

#### FIGURE 90 WAN SERVICE OVERVIEW

FIGURE 91 SELECT LAYER2 INTERFACE

ZTE中兴									L	anguage So
		Choose A	<b>W</b> dd, or R	<b>/ide Area Ne</b> .emove to con	twork (WAN figure a WAN	l <b>) Service</b> service o	e <b>Setup</b> ver a selec	ted interfa	ace.	
Device Info										
Advanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atm0	br 0 8 81	Bridae	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface						<u> </u>				
PTM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
WAN Service										
LAN					_	_				
Vlan Trunk Setting				,	Add Remov	/8				
-										

By default, system preset WAN Interface is **atm0** and **ptm0\_1**.

 Click Add to display the interface as shown in <u>Figure 91</u>, and select the Layer 2 interface.

#### ZTE中兴 WAN Service Interface Configuration Select a layer 2 interface for this service Device Info Note: For PTM interface, the descriptor string is (portId\_high\_low) Advanced Setup TM interface, the descriptor string is (portI Where portId=0 --> DSL Latency PATH0 portId=1 --> DSL Latency PATH1 low =0 --> Low PTM Priority not set low =1 --> Low PTM Priority set high =0 --> High PTM Priority not set high =1 --> High PTM Priority set Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting NAT ptm0/(0\_0\_1) 💌 Security Parental Control Back Next Quality of Service Routing DNS

7. Click **Next** to enter the interface as shown in Figure 92.

FIGURE 92 SELECT WAN SERVICE ITPE	FIGURE	92	SELECT	WAN	SERVICE	Түре
-----------------------------------	--------	----	--------	-----	---------	------

<b>ZTE</b> 中兴	
	WAN Service Configuration
	Select WAN service type:
Device Info	C PPP over Ethernet (PPPoE)
Advanced Setup	◎ IP over Ethernet
Layer2 Interface	O Bridging
ATM Interface	
PTM Interface	Constan Descriptions Inco. 0. 0. 4
WAN Service	Service Description: [ipoe_U_U_1
LAN	
Vlan Trunk Setting	Epoble VI AN Mux - Supporting Multiple Protocole Over a Single PTM interface
NAT	Enable VLAN Mux - Supporting Muniple Froncois Over a Single From Internace
Security	Enter 802.1P Priority [0-7]: 5
Parental Control	Enter 802.1Q VLAN ID [1-4094]: 2
Quality of Service	
Routing	and and
DNS	Back Next
DSL	



- 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

7TE击W	
LICHY	Language Sel
Device Info Advanced Setup	- Enter information provided to you by your ISP to configure the WAN IP settings. Notice: If "Obtain an IP address automatically" is chosen, DHCP will be enabled for PVC in MER mode. If "Use the following Static IP address" is chosen, enter the WAN IP address, subnet mask and interface gateway.
Layer2 Interface ATM Interface PTM Interface WAN Service LAN	Obtain an IP address automatically     Option 60 Vendor ID:     C Use the following Static IP address:
Vlan Trunk Setting Security Parental Control	WAN IP Address: WAN Subnet Mask: WAN gateway IP Address:
Quality of Service Routing DSL Upnp Certificate	

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

ZTE中兴	
	Routing Default Gateway
Device Info	Select a preferred wan interface as the system default gateway.
Advanced Setup	
Layer2 Interface	Selected WAN Interface pppoe_0_0_1.2/ppp0.2
ATM Interface	
PTM Interface	
WAN Service	
LAN	
Vlan Trunk Setting	
NAT	
Security	a start
Parental Control	Back Next
Quality of Service	
Routing	

12. Click **Next** to enter the interface as shown in Figure 95.

#### FIGURE 95 DNS CONFIGURATION

TTP-LW	
ZIEΨ兴	Language Select: English
	DNS Server Configuration
Device Info	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.
Advanced Setup Layer2 Interface	Obtain DNS info from a WAN interface:
ATM Interface PTM Interface	WAN Interface selected: pppoe_0_0_1.2/ppp0.2 💌
WAN Service	C Use the following Static DNS IP address:
LAN	Primary DNS server:
Vian Trunk Setting NAT	Secondary DNS server:
Security	
Parental Control 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**.

13. Click **Next** to enter the interface as shown in Figure 96.

#### FIGURE 96 NAT CONFIGURATION

<b>ZTE中兴</b>	Language Select: 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 (ANN
Advanced Setup Layer2 Interface ATM Interface PTM Interface	Enable NAT
WAN Service LAN Vlan Trunk Setting	IGMP Multicast
NAT Security Parental Control Quality of Service Routing	Back Next

14. Click **Next** to enter the interface as shown in Figure 94.



FIGURE 97 DEFAULT GATEWAY CONFIGURATION

ZTE中兴	
	Routing Default Gateway
Device Info Advanced Setup Layer2 Interface ATM Interface PTM Interface WAN Service LAN Vlan Trunk Setting NAT Security Parental Control Quality of Service Routing	Select a preferred wan interface as the system default gateway. Selected WAN Interface ipoe_0_0_1.2/ptm0.2 💌

15. Click **Next** to enter the interface as shown in Figure 95.

#### FIGURE 98 DNS CONFIGURATION

ZTE中兴	Language Select. English
	DNS Server Configuration
Device Info Advanced Setun	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.
Layer2 Interface ATM Interface	Obtain DNS info from a WAN interface: WAN Interface selected: [pppoe_0_0_1.2/ppp0.2]
PTM Interface WAN Service LAN	C Use the following Static DNS IP address:
Vlan Trunk Setting NAT	Secondary DNS server:
Security Parental Control 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**.

16. Click **Next** to enter the interface as shown in Figure 99.

WAN Setup - Summ	a <b>ry</b> tings below match the se	ttings provided by your ISP.
Connection Type:	IPOE	1
Service Name:	ince 0.0.1.2	
Comuloo Cotogomuu	1000_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	-
Quality of oct vice.	Enabled	
Click Apply/Save to ha	ve this interface to be eff	ective. Click Back to make any modifications.
		Back Save/Apply
	WAN Setup - Summ. Make sure that the set Connection Type: Service Name: Service Category: IP Address: Service State: NAT: Full Cone NAT: Full Cone NAT: Firewall: IGMP Multicast: Quality Of Service: Click Apply/Save to ha	WAN Setup - Summary Make sure that the settings below match the set Connection Type: IPoE Service Name: poe_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 Apply/Save to have this interface to be effected

#### 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.

ZTE中兴	
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vlan Trunk Setting Security Parental Control	Local Area Network Setup         Configure the DSL Router IP Address and Subnet Mask for LAN Interface.         IP Address:       192.168.1.1         Subnet Mask:       255.255.255.0         Imable IGMP Snooping         Imable DHCP Server         Imable DHCP Server
Quality of Service Routing DSL Upnp Certificate Wireless Diagnostics Management	Start IP Address: 192.168.1.2 End IP Address: 192.168.1.254 Leased Time(hour): 24 Static IP Lease List: (A maximum 10 entries can be configured) MAC Address IP Address Remove Add Remove Add Remove

FIGURE 101 LAN CONFIGURATION OVERVIEW

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.

### **O** Note:

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

3. <u>Table 16</u> is a description of the different options.

	i
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.

#### TABLE 16 LAN CONFIGURATION OPTIONS

- 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 Stat	tic IP address then click .	
MAC Address:	00:19:5B:74:32:72	(e.g 00:19:58:74:32:72)
IP Address:	10.1.1.1	(e.g 192.168.1.100)
		Save

- 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:
 10.1.1.2
 Subnet Mask:
 255.255.0

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

FIGURE 104 VLAN TRUNKING OVERVIEW

 Select Advanced Setup > Vlan Trunk Setting to display the interface as shown in Figure 104.

#### ZTE中兴 vlan Trunk Setting Device Info LAN interface select: eth0 -Advanced Setup Layer2 Interface 🗖 vlan Trunk Enable ATM Interface **PTM Interface** WAN Service LAN Vlan Trunk Setting Security Parental Control **Quality of Service** Routing Save/Apply DSL Upnp

- 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

Window	s Internet Explorer
♪	You cannot enable vlan trunk for this interfce, because no VlanMux wan service existed, you should create an VlanMux wan bridge service first !
	OK

4. Select **Advanced Setup > WAN Service** to display the interface as shown in Figure 106.

#### FIGURE 106 WAN SERVICE OVERVIEW

ZTE中兴									ı	.anguage Se
		Choose A	<b>N</b> .dd, or R	<b>lide Area Ne</b> emove to con	<b>twork (WAN</b> figure a WAN	I <b>) Servic</b> e service o	e Setup ver a selec	ted interfa	ace.	
Device Info										
Advanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
Layer2 Interface	atm0	br 0 8 81	Bridae	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface										
PTM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
WAN Service										
LAN										
Vlan Trunk Setting					Add Remov	(e				
				-						

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

WAN Service Interface Configuration         Select a layer 2 interface for this service         Advanced Setup         Layer2 Interface         ATM Interface         PTM Interface         PTM Interface         WAN Service         Layer 2 Interface         Device Info         Advanced Setup         Note: For PTM Interface, the descriptor string is (portid_high_low)         Where portid=0> DSL Latency PATH0         portid=1> DSL Latency PATH1         portid=4> DSL Latency PATH0         wave Service         low =0> Low PTM Priority not set         low =0> High PTM Priority not set         high =0> High PTM Priority not set         bidth =1> Low PTM Priority not set         bidth =1> Low PTM Priority not set         bidth =1> Low PTM Priority not set
Select a layer 2 interface for this service       Device Info       Advanced Setup       Layer2 Interface       ATM Interface       PTM Interface       PTM Interface       WAN Service       LAN
Device Info         Note: For PTM interface, the descriptor string is (portid_high_low)           Advanced Setup         Where portid=0> DSL Latency PATH0           Layer2 Interface         portid=1> DSL Latency PATH0           ATM Interface         portid=1> DSL Latency PATH0           PTM Interface         low =0> Low PTM Priority not set           WAN Service         low =1> Low PTM Priority not set           LAN         high =0 -> High PTM Priority not set
Advanced Setup     Note: For PTM interface, the descriptor string is (portid_high_low)       Layer2 Interface     Where portId=0> DSL Latency PATH0       ATM Interface     portId=1> DSL Latency PATH0       PTM Interface     low =0> Low PTM Priority not set       WAN Service     low =1> Low PTM Priority not set       LAN     high =0> High PTM Priority not set
Layer2 Interface         Where portId=U> DSL Latency PATHI0           ATM Interface         portId=U> DSL Latency PATHI0           PTM Interface         portId=U> DSL Latency PATHI0           PTM Interface         portId=U> DSL Latency PATHI0           WAN Service         low =0 -> Low PTM Priority not set           LAN         blob =1 -> LOW PTM Priority not set
ATM Interface     portid=4 -> DSL Latency PATH081       PTM Interface     low =0> Low PTM Priority not set       WAN Service     low =1> Low PTM Priority set       LAN     high =0 -> High PTM Priority not set
PTM Interface         Iow =0> Low PTM Priority not set           WAN Service         Iow =1> Low PTM Priority set           LAN         high =0> High PTM Priority not set
WAN Service         low =1> Low PTM Priority set           LAN         high =0> High PTM Priority not set           bigh =1> Link PTM Priority set
LAN high =0> High PTM Priority not set
bidb =1> Hidb PTM Priority cot
Vlan Trunk Setting
NAT ntm0//0_0_11
Security
Parental Control
Quality of Service Back Next
Routing
DNS

6. Click **Next** to enter the interface as shown in Figure 108.

#### FIGURE 108 SELECT WAN SERVICE TYPE

ZTE中兴	
XV	WAN Service Configuration
	Select WAN service type:
Device Info	C PPP over Ethernet (PPPoE)
Advanced Setup	IP over Ethernet
Layer2 Interface	🖸 Bridging
ATM Interface	
PTM Interface	
WAN Service	Service Description:  br_0_0_1
LAN	
Vlan Trunk Setting NAT	Enable VLAN Mux - Supporting Multiple Protocols Over a Single PTM interface
Security	Enter 802.1P Priority [0-7]: 5
Parental Control	Enter 802.1Q VLAN ID [1-4094]; 2
Quality of Service	
Routing	
DNS	Back Next
DSL	
Upnp	
Certificate	

- 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

ZTE中兴			
	WAN Setup - Summa Make sure that the set	<b>ary</b> tings below mate	ch the settlings provided by your ISP.
Device Info			
Advanced Setup	Connection Type:	Bridge	
Layer2 Interface	Service Name:	br_0_0_1.2	
ATM Interface	Service Category:	UBR	
PTM Interface	IP Address:	Not Applicable	
WAN Service	Service State:	Enabled	
LAN Vian Trunk Sotting	NAT:	Disabled	
Man munk secung	Full Cone NAT:	Disabled	
Security	Firowall:	Disabled	
Parental Control	TITEWall.	Mat Angliashia	
Quality of Service	IGMP MULUCASU:	Not Applicable	
Routing	Quality Of Service:	Enabled	
DNS	Click Apply/Save to bar	ve this interface	to be effective. Click Back to make any modifications.
DSL	onex rippi)/ouro a na		Back Save/Apply
Upnp			
Uertificate			
Diagnostics			
Management			

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

ZTE中兴									L	.anguage Sele
			W	/ide Area Ne	twork (WAN	) Service	e Setup			
		Choose A	dd, or R	emove to con	figure a WAN	service o	ver a selec	ted interfa	ace.	
evice Info										
dvanced Setup	Interface	Description	Туре	Vlan8021p	VlanMuxId	ConnId	Igmp	NAT	Firewall	Remove
ayer2 Interface	atmO	br_0_8_81	Bridge	N/A	N/A	N/A	Disabled	Disabled	Disabled	
ATM Interface										
PTM Interface	ipoa0	ipoa_0_8_35	IPoA	N/A	N/A	N/A	Disabled	Enabled	Enabled	
VAN Service	ptm0.2	br_0_0_1.2	Bridge	5	2	N/A	Disabled	Disabled	Disabled	
AN				1						
'lan Trunk Setting										
IAT		Add Remove								
ecurity										
arental Control										

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.



ZTE中兴	je Select: Er
vlan Trunk Setting	
Device Info LAN interface select: eth0  Advanced Setup	
Layer2 Interface 🔽 vlan Trunk Enable	
ATM Interface	
PTM Interface NOTICE: You Can enable the below vian IDs as allowed vian IDs for this interface, except you have choose others will be BLOCKED 1	sed, any
WAN Service Griefs thin be becauld it	
LAN Supported VLAN Number : 1 (0-4)	
Barontal Control Vian ID1: 2/ptm0.2 V	
Routing	
DSL NOTICE: PVID CANNOT be the same as the vlan trunk Id which have been set above !	
Upnp If PVID is set to IV/A, then UNTAGED packets though this interface will be BLUCKED !	
Certificate PVID: 2/ptm0.2 V	
Wireless	
Diagnostics	
Management Save/Apply	

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



- 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.

# Chapter **8**

# **NAT Configuration**

#### **Table of Contents**

Overview	83
Virtual Servers Setup	
Port Triggering	
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.

### O 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.

### **O** 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

7TE由兴	
LILTA	Language Select: English +
	NAT Virtual Servers
Device Info Advanced Setup Layer2 Interface WAN Service	Select the service name, and enter the server IP address and click Apply/Save to forward IP packets for this service to the specified server. NOTE: The Internal Port End cannot be modified directly. Normally, it is set to the same value as External Port End. However, if you modify Internal Port Start , then Internal Port End will be set to the same value as Internal Port Start Remaining number of entries that can be configured:32
LAN	Use Interface pppoe_0_0_35/ppp0 V
Vian Trunk Setting	Service Name:
NAT	Select a Service: Select One
Virtual Servers	C Custom Service:
Port Triggering	
DMZ Host	Server IP Address: 192.168.1.
Security	
Parental Control	
Quality of Service	External Port Start External Port End Protocol Internal Port Start Internal Port End
Routing	
DNS	TCP I
DSL	
Upnp	
Certificate	
Wireless	TCP 💌
Diagnostics	
Management	
Uliveles -	
Wireless	
Management	TCP 💌
management	TCP 💌
wireless	
Diagnostics	
Management	
	Save/Apply

- 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

<b>ZTE中兴</b>										Languag	e Select: E	Inglish
	NAT Port Trigger	ing Setup										
Device Info Advanced Setup Layer2 Interface	Some applications red dynamically opens up party using the 'Trigg application on the LAP	quire that s the 'Open ering Ports Viside using	pecific po Ports' in '. The Ro ; the 'Opi	orts in the fir iuter a en Por	the Router wall when allows the re ts'. A maxin	's firewa i an appl emote pa mum 32	all be o lication arty fro entrie:	pened for access b on the LAN initiate om the WAN side to s can be configured	iy the remo is a TCP/UI i establish t.	ite parties. Port OP connection to new connection	Trigger ) a remote s back to t	e the
WAN Service		Tr	igger		0	lpen						
Vian Trunk Setting	Application Name	Destacol	Port Ra	Range	Dustand	Port R	ange	WAN Interface	Remove			
NAT		PIOLOCOI	Start	End	PIULULUI	Start	End					
Virtual Servers												
Port Triggering	Add Remove											
DMZ Host Security												

2. Click Add to display the interface as shown in Figure 116.

#### FIGURE 116 ADDING PORT TRIGGERING

	Language Select, English
Device Info Advanced Setup Layer2 Interface WAN Service	Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's frewall be opened for access by the applications. You can configure the port settings from this screen by selecting an existing application or creating your own (Custom application) and click Save/Apply to add it. Remaining number of entries that can be configured:32 Use Interface popoe_0_0_35/ppp0 💌
Vian Trunk Cotting	Application Name:
Vian munk security	Select One application : Select One
Vietual Corvore	C Custom application :
Port Triggoring	
DM7 Host	Ingger Port Startlingger Port EndIngger Protocolupen Port Startupen Port Endupen Protocol
Security	
Darental Control	тср 🔽
Duality of Service	
Routing	
DNS	
DSL	
Upnp	тср 🔽
Certificate	
Wireless	
Diagnostics	
Management	

- 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. <u>Table 17</u> is a description of the different 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.

#### TABLE 17 CUSTOM PORT TRIGGERING CONFIGURATION OPTIONS

### **O** 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 combina-tion of these, for example 80, 90-140, 180.

7. 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.

### **D** 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 net work 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.

### O Note:

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

### Adding A DMZ 1. Select Advanced Setup > NAT > DMZ Host to display the interface as shown in Figure 118.

#### FIGURE 118 DMZ HOST CONFIGURATION

ZTE中兴	Language Salect - English 💌
	NAT DMZ Host
Device Info	The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.
Advanced Setup	Enter the computer's IP address and click Apply to activate the DMZ host.
Layer2 Interface WAN Service	Clear the IP address field and click Apply to deactivate the DMZ host.
LAN Vian Trunk Setting	DMZ Host IP Address: 192.168.2.155
NAT	Gave/ánniv
Virtual Servers Port Triggering	and all the full
DMZ Host	

- 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 <u>119</u>.

FIGURE	119	DMZ	Ноѕт	CONFIGURATION	NOTICE

windows Internet Explorer	
Since DMZ is set, the DSL router WEB server port will be moved to 8080, TELNET server port will be moved to 2323, TFTP server port will be mo 6969, SNMP port will be moved to 16116.	red to
OK	

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.

Chapter 9

# **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 Policy	93
Configure MAC Filtering Rule	95
MAC Filtering - Global Policy FORWARDED	96
MAC Filtering - Global Policy BLOCKED	97

# Configure MAC Filtering Policy

Select **Advanced Setup > Security > MAC Filtering** to display the interface as shown in Figure 120.

#### FIGURE 120 MAC FILTERING OVERVIEW

ZTE中兴	Language Select   English 💌
	MAC Filtering Setup
Device Info Advanced Setup Layer2 Interface WAN Service LAN	MAC Filtering is only effective on ATM PVCs or WAN services based on PTM configured in Bridge mode. FORWARDED means that all MAC layer frames will be FORWARDED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table. MAC Filtering Policy For Each Interface: WARNING: Changing from one policy to another of an interface will cause all defined rules for that interface to be REMOVED AUTOWATICALLY! You will need to create new rules for the new policy.
Vlan Trunk Setting	Interface Bolicy Phange
Security	плетасе Ройсу спануе
MAC Filtering	atm0 FORWARD 🔽
Parental Control Quality of Convice	ptm0_1 FORWARD
Routing	
DSL Upnp	Change Policy
Certificate	Choose Add or Remove to configure MAC filtering rules.
Wireless	
Management	Interface Protocol Destination MAC Source MAC Frame Direction Remove
management	Add Remove



### **O** 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 for- warded 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

ZTE中兴	tamman Select English -
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vian Trunk Setting Security MAC Filtering Parental Control Quality of Service Routing DSL Uppp Certificate	MAC Filtering Setup         MAC Filtering is only effective on ATM PVCs or WAN services based on PTM configured in Bridge mode. FORWARDED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules in the following table. BLOCKED means that all MAC layer frames will be BLOCKED except those matching with any of the specified rules for that interface to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.         Interface Policy Change       atmo       BLOCKED       ptm0_1       ptm1       ptm1 <t< th=""></t<>
Wireless Diagnostics Management	Choose Add or Remove to configure MAC filtering rules.           Interface         Protocol         Destination MAC         Source MAC         Frame Direction         Remove           Add         Remove         Remov

### 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 <u>Figure 122</u>.



#### FIGURE 122 ADDING MAC FILTERING RULE

#### 2. <u>Table 19</u> is a description of the different 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.

#### TABLE 19 MAC FILTERING RULE CONFIGURATION OPTIONS

- 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 <u>Figure 123</u>.

ZTE中兴

#### FIGURE 123 REMOVING MAC FILTERING RULE

ZTE中兴								guage Select: Englis
								,,
	MAC Filtering Setup							
vevice Info Advanced Setup Layer2 Interface WAN Service LAN	MAC Filtering is only effe all MAC layer frames will means that all MAC layer MAC Filtering Policy For E WARNING: Changing fr REMOVED AUTOMATICA	tive on ATM PV be FORWARDE frames will be I ach Interface: om one policy ALLY! You will	Cs or WAN services D except those mat BLOCKED except the to another of an i need to create ne	based on PT thing with ar ise matching <b>nterface w</b> w rules for	M configu ny of the s with any <b>ill cause</b> the new	rred in Bridge mode pecified rules in the of the specified rule all defined rules f policy.	FORWAR following t is in the foll	DED means that able, BLOCKED lowing table, terface to be
Vlan Trunk Setting			Interface	Policy	Change	1		
MAC filtering					-			
MAC FILTERING			atmu	BLUCKED				
Parental Control			ptm0_1	FORWARD				
Quality of Service								
Routing								
USL	Change Policy							
upnp Gautificate								
Certificate	Choose Add or Remove t	o configure MAC	; filtering rules.					
vireiess								
agnostics	Inter	face Protoco	Destination MAC	Source M	AC	Frame Direction	Remove	
lanayement	atmO	PPPoE		00:13:20:	9E:0F:10	вотн		
	atmO	PPPoE		00:13:20:	9E:0F:12	LAN_TO_WAN		
			Add	Remove			,	

# 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

<b>ZTE中兴</b>	Language Select. English 👱
	Add MAC filter
Device Info	Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click Apply to save and activate the filter.
Advanced Setup Layer2 Interface	Protocol Type:
WAN Service LAN	Destination MAC Address: eg: 00:00:00:00:00:00 Source MAC Address: 00:13:20:9E:0F:10 eg: 00:00:00:00:00:00
Security MAC Filtering	Frame Direction:
Parental Control Quality of Service	WAN Interfaces (Configured in Bridge mode only)
Routing DSL	br_0_8_81/atm0
Upnp Certificate	Save/Apply
Wireless Diagnostics Management	

- 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

<b>ZTE中</b> 兴	Language Select: English
	Add MAC Filter
Device Info	Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click Apply to save and activate the filter.
Advanced Setup Layer2 Interface	Protocol Type: PPPoE
WAN Service	Destination MAC Address: eg: 00:00:00:00:00:00
Vian Trunk Setting	Source MAC Address: 00:13:20:9E:0F:12 eg; 00:00:00:00:00:00
Security MAC Filtering	Frame Direction: WAN=>LAN -
Parental Control	WAN Interfaces (Configured in Bridge mode only)
Quality of Service Routing DSL	br_0_8_81/atm0 <
Upnp Certificate	Save/Apply
Wireless	
Diagnostics Management	

- 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.

## Chapter 10

# **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 OoS	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

<b>ZTE中兴</b>	
	Language Select: C
	QoS Queue Management Configuration
	If Enable OnS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a
Davias Infe	narticular classifier. Click Anniv/Save hutton to save it
Device Inito	
Advanced Setup	
Layer2 Interface	
WAN Service	Note: If Enable Dos checkbox is not selected, all DoS will be disabled for all interfaces.
LAN	
Vlan Trunk Setting	Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.
Security	
Parental Control	Finale QoS
Quality of Service	
Queue Config	
OoS Classification	Select Default DSCP Mark No Change-1)
Routing	
DSI	
Uppp	Save/Apply
Certificate	
Wireless	
Diagnostics	
nagnosacs .	
Management	

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.

#### 7TF 由兴 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 Device Info Advanced Setup The QoS function has been disabled. Queues would not take effects. Layer2 Interface WAN Service Name Key Interface Precedence DSL Latency PTM Priority Enable Remove LAN Vlan Trunk Setting Add Enable Remove Security Parental Control Quality of Service Queue Config **QoS Classification** Routing DSL Upnp Certificate Wireless Diagnostics Management

#### FIGURE 128 QOS QUEUE CONFIGURATION OVERVIEW

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.



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

ZTE中兴		Language Select: En
	QoS Queue Config	uration
Device Info Advanced Setup Layer2 Interface	configured for a spe appropriately" "Note "Click Apply/Save to	The precedence. The queue entry configured here will be used by the classifier to place in the grades and be the precedence of the place entry configured here will be used by the classifier to place ingress packets to come integer values for precedence imply higher priority for this queue relative to others" save and activate the queue."
WAN Service	Name:	ADSL
Vlan Trunk Setting	Enable:	Enable 💌
Security Parental Control	Interface:	atm0(0_8_81)
Quality of Service Queue Config	Precedence:	1 💌
QoS Classification Routing	DSL Latency:	Path0 -
DSL		
Certificate		Save/Apply
Wireless Diagnostics		
Management		

2. <u>Table 20</u> 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 inter- face. The modem automatically allocates selected network inter- face 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 pri- ority 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

To delete a certain queue, select the queue , click  $\ensuremath{\text{Disable}}$  and then click  $\ensuremath{\text{Remove}}$ .

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



 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

7TC+W		
<b>ZIE</b> Ψ兴		Language Select English 💌
	Add Network Traffic Class Rule	
Device Info Advanced Setup Layer2 Interface	The screen creates a traffic class rule to classify the and optionally overwrite the IP header DSCP byte. A specified conditions in this classification rule must be rule.	upstream traffic,assign queue which defines the precedence and the interface rule consists of a class name and at least one condition below. All of the satisfied for the rule to take effect. Click Save/Apply to save and activate the
WAN Service	Traffic Class Name:	
LAN	Rule Order:	Last
Vlan Trunk Setting	Rule Status:	Disable -
Security Deroptal Control		
Quality of Service Queue Config	Specify Classification Criteria A blank criterion indicates it is not used for classifica	tion.
QoS Classification	Class Interface :	
Routing	Ether Type:	
DSL	Source MAC Address:	
Upnp	Source MAC Mask:	
Lertificate	Destination MáC áddress:	
Diagnostics	Destination M&C Mask:	
Management	Destandar meter mask.	
5	Specify Classification Results Must select a classification queue. A blank mark or t	ag value means no change.
Management	Assian Classification Oueue:	<b>•</b>
	Mark Differentiated Service Code Point (DSCP):	
	Mark 802.1p priority:	
	Tag VLAN ID:	
		Save/Apply
	@ 2000 2009 ZTE Come	All debies of the second

### 3. <u>Table 21</u> is a description of the different 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 modi- fies the original packet IP header if all rules defined within the classification class are matched. (CS - Mark IP Precedence, AF - Assured Forwarding, EF - Expe- dited Forwarding).
Mark 802.1p if 802.1q is enabled	Select an 802.1p priority num- ber that serves as the 802.1p value.

### TABLE 21 QOS CLASSIFICATION CONFIGURATION OPTIONS

- 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 besteffort 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 filed. 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

<b>ZIE</b> 中兴	4200	
		Language Select: English 💌
	Add Network Traffic Class Rule	
Device Info Advanced Setup Layer2 Interface	The screen creates a traffic class rule to classify the u and optionally overwrite the IP header DSCP byte. A r specified conditions in this classification rule must be rule.	upstream traffic,assign queue which defines the precedence and the interface ule consists of a class name and at least one condition below. All of the satisfied for the rule to take effect. Click Save/Apply to save and activate the
WAN Service	Traffic Class Name:	0-32
LAN	Rule Order:	Last
Vian Trunk Setting	Rule Status:	Enable -
Security Barantal Control		
Parental Control Duality of Service	Specify Classification Criteria	
Quality of Service	A blank criterion indicates it is not used for classificati	on.
QoS Classification	Class Interface:	eth
Routing	Class and race.	
DSL	Source MAC Address:	
Upnp	Course MAC Marks	
Certificate	Source MAC Mask:	
Wireless	Destination MAC Address:	
Diagnostics	Destination MAC Mask:	
Management	Specify Classification Results Must select a classification queue. A blank mark or tag	g value means no change.
Management	Assign Classification Queue:	atm0&Prec1&Path0
	Mark Differentiated Service Code Point (DSCP):	CS5(101000)
	Mark 802.1p priority:	7
	Tag VLAN ID:	
		Save/Apply
	@ 2000-2008 ZTE Corpora	ation. 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

ZTE中兴	
Device Info Advanced Setup Layer2 Interface WAN Service LAN	Routing Default Gateway Select a preferred wan interface as the system default gateway. Selected WAN Interface pppoe_0_0_35/ppp0 💌
Vian Trunk Setting Security Parental Control Quality of Service Routing Default Gateway Static Route Policy Routing	Save/Apply

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  $\frac{Figure 136}{2}$ .

### 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

<b>7TF</b> 中兴	
LILIA	Language Select: En
	Routing Static Route Add
Device Info	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.
Advanced Setup Layer2 Interface WAN Service	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.
LAN	
Vlan Trunk Setting	Destination Network Address:
Parental Control	Subnet Mask :
Quality of Service	
Routing Default Gateway	Use Interface pppoe_0_35/ppp0 💌
Static Route	
Policy Routing	
DSL	Save/Appiy

- 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

<b>ZTE中兴</b>	
	Language Select: En
	Routing Static Route Add
Device Info	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.
Advanced Setup Layer2 Interface WAN Service	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.
LAN Vlan Trunk Setting	
Security	Destination Network Address:
Parental Control	Subnet Mask:
Quality of Service	
Routing Default Gateway	Use Interface LAN/br0
Static Route	Use Gateway IP Address
Policy Routing	Crun/Apply
DSL	Sare/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**

 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

ZTE中兴	Language Select   Engli
	Policy Routing Settup Enter the policy name, policies, and WAN interface then click 'Save/Apply' to add the entry to the policy routing table. Note: If selected IPOE as WAN interface, default gateway must be configured, and if selected WAN interface is in VlanMux mode, vlan trunk MIST he set via menu 'Vlan Trunk Setting'.
Newice Into	
Lauora Interface	Policy Name:
WAN Service	
LAN	Physical LAN Port:
Vian Trunk Setting	
NAT	
Security	
Parental Control	Source IP:
Quality of Service	
Routina	
Default Gateway	Default Gateway:
Static Route	
Policy Routing	Save/Annly
PID	

3. <u>Table 22</u> 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 se- lect IPoE as WAN interface, de- fault gateway must be config- ured, and if selected WAN inter-

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

4. 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

<b>ZTE中</b> 兴	Languinge Salect. English
	Routing RIP Configuration
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing Default Gateway Static Route	Interface       Version       Operation       Enabled         interface       Version       Operation
Policy Routing RIP	

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

## Chapter 12

## 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.

 Select Advanced Setup > DNS > DNS Server to display the interface as shown in Figure 142.

<b>ZTE中兴</b>	Language Select English
	DNS Server Configuration Select the configured WAN interface for DNS server information OR enter the static DNS server IP Addresses for single PVC with
Device Info	IPoA, static MER protocol.
Advanced Setup	
Layer2 Interface	Obtain DNS info from a WAN interface:
WAN Service	WAN Interface selected: pppoe 0 0 35/ppp0 🗸
LAN	
Vlan Trunk Setting	O Use the following Static DNS IP address:
NAT	Primary DNS serverr:
Security	Sociedary DNS conver
Parental Control	Securidary Divo server .
Quality of Service	
Routing	
DNS	
DNS Server	
Dynamic DNS	

### 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.

**O** 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

ZTE中兴	Language Select: English 2
	Dynamic DNS
	The Dynamic DNS service allows you to alias a dynamic IP address to a static hostname in any of the many domains, allowing your
Device Info	DSL router to be more easily accessed from various locations on the internet.
Advanced Setup	Chanse Add or Remove to configure Dynamic DNS
Layer2 Interface	Choose waa of Kennove to Configure Dynamic Disp.
WAN Service	Hostnamo Ilsornamo Coruico Interfaco Pomouo
LAN	
Vlan Trunk Setting	Add Remove
NAT	Nau Itemove
Security	
Parental Control	
Quality of Service	
Routing	
DNS	
DNS Server	
Dynamic DNS	

2. Click **Add** to display the interface as shown in Figure 144.

### FIGURE 144 ADDING DYNAMIC DNS

ZTE中兴		
	Add Dynamic DNS	
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vlan Trunk Setting	This page allows you to a D-DNS provider Hostname Interface	dd a Dynamic DNS address from DynDNS.org or TZO.          DynDNS.org         pynDNS.org
NAT Security Parental Control Quality of Service Routing DNS DNS Server Dynamic DNS	<b>DynDNS Settings</b> Username Password	Save/Apply

3. <u>Table 23</u> is a description of the different options.

### TABLE 23 DYNAMIC DNS CONFIGURATION OPTIONS

Field	Description
D-DNS provider	You can add a Dynamic DNS ad- dress 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

<b>ZTE中兴</b>		
	DSL Settings	
Douico Info	Select the modulation below.	Select the profile below.
Advanced Setup	🗹 G.Dmt Enabled	🗹 8a Enabled
Layer2 Interface	🗹 G.lite Enabled	☑ 8b Enabled
WAN Service	T1 413 Enabled	R Enabled
Vian Trunk Setting		
NAT	M ADSL2 Enabled	No so Enabled
Security	MannexL Enabled	IV 12a Enabled
Parental Control	☑ ADSL2+ Enabled	☑ 12b Enabled
Quality of Service Routing	VDSL2 Enabled	🔽 17a Enabled
DNS		US0
DSL		Enabled
Upnp		
Certificate		
wireless Diagnostics		Apply/Save
Management		

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.

## Chapter 14

## **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	
ISAKMP	
IKE	

## 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 ContentsTime RestrictionURL Filter126

## **Time Restriction**

Select **Advanced Setup > Parental Control > Time Restriction** to display the interface as shown in <u>Figure 146</u>.

### FIGURE 146 TIME RESTRICTION OVERVIEW



Click **Add** to display the interface as shown in Figure 147.

ZTE中兴

ZTE中兴	
	Language Select: English Access Time Restriction
Device Info Advanced Setup Layer2 Interface WAN Service	This page adds time of day restriction to a special LAN device connected to the Router. The 'Browser's MAC Address' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the Other MAC Address button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type ipconfig /all.
LAN	User Name
Vlan Trunk Setting	
Security	Browser's MAC Address 00:1e:90:3f:5b:b5
Parental Control	O Other MAC Address
Time Restriction	(oraciae oraciae)
Url Filter	
Quality of Service	Days of the week Mon Tue Wed Thu Fri Sat Sun
Routing	Click to select
DSL	
Upnp	Start Blocking Time (hh:mm)
Certificate	End Blocking Time (hh:mm)
Wireless	Save/Apply
Diagnostics	
Management	
5	

### 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

 Select Advanced Setup > Parental Control > URL Filter to display the interface as shown in Figure 148.

#### FIGURE 148 URL FILTER OVERVIEW

7TE th	
LIE中兴	Language Salect. Englis
	URL Filter Please select the list type first then configure the list entries. Maximum 100 entries can be configured.
ouico Info	Note: URL List Type indicates the filter mode you select, 'Exclude' means the websites in the entries below are blocked while others are allowed
Advanced Setup	and anowed, and 'Include' means that all websites are blocked except those configured in the entries below.
Layer2 Interface WAN Service	You must restart the modem for the configuration to take effect!
LAN Vlan Trunk Setting	URL List Type: C Exclude O Include
Security	
Parental Control Time Restriction	Address Port Remove
Url Filter	Add Remove
Quality of Service Routing	MMM TROTTOYO
DSL	
Upnp	
Vireless	
Diagnostics	
lanagement	

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 al-lowed.
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

<b>ZTE中兴</b>	
	Parental Control URL Filter Add
Device Info Advanced Setup Layer2 Interface	URL Address: (e.g. http://www.zte.com.cn, which means all pages on this website will be filtered )
WAN Service LAN Vlan Trunk Setting Security	Port Number: (Default 80 will be applied if leave blank.)
Parental Control Time Restriction Url Filter	
Quality of Service Routing DSL	
upnp Certificate Wireless Diagnostics	
Management	

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





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



## **UPNP** Configuration

Select **Advanced Setup > Upnp** to display the interface as shown in <u>Figure 150</u>.

FIGURE 150 UPNP CONFIG

ZTE中兴	
	Upnp Configuration
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing DSL Upnp Certificate Wireless	☑ Enable or disnable Upnp protocol Save/Apply
Management	

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.

### **O** 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 forwarding, 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.



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

## Chapter 17

## **Certificate Configuration**

Select **Advanced Setup > Certificate** to display the interface as shown in Figure 151.

### FIGURE 151 LOCAL CERTIFICATE OVERVIEW

ZTE中兴	
	Local Certificates
Device Info Advanced Setup	Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.
Layer2 Interface	Name In Lies Publicat Tump Action
LAN	Name In use Subject Type Action
Vlan Trunk Setting	Create Certificate Request Import Certificate
Security Parental Control	
Quality of Service	
Routing	
Upnp	
Certificate	
Local	
Trusted CA	
Wireless	
Diagnostics	
Management	

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: Eng
	Create new certificate	request	Language Screen
Device Info	To generate a certificate s letter Country Code for the	igning request you need to include Common Name,Organization Name, State/Pi 9 certificate.	rovince Name, and the 2
Advanced Setup	Certificate Name:	mycertificate	
WAN Service	Common Name	zte.com	
LAN	Organization Name:	zte	
Vlan Trunk Setting	- State/Province Name:	shandhai	
Security	Country/region Name:	CN (China)	
Parental Control	oosine //rogiorritemor		
Quality of Service			
Routing			
DSL		Apply	
Upnp			
Certificate			
Trusted CA			
Wireless			
Diagnostics			
Management			
-			

Table 26 is a description of the different options.

Field	Description
Certificate name	Creates an SSL certificate in the specified certificate repository (administrator's or domain's re- pository) by using a private key file and a corresponding certifi- cate 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 char- acters 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).

### TABLE 26 CREATE CERTIFICATE REQUEST CONFIGURATION OPTIONS

Field	Description
State/Province Name	This is the name of the state or province where your organ- ization's head office is located. Please enter the full name of the state or province.
Country/Region Name	This is the two-letter ISO abbre- viation for your country (for ex- ample, GB for the United King- dom).

2. Click **Apply** and wait several seconds, the generated certificate request is displayed as shown in <u>Figure 153</u>.

	Certificate signing r Certificate signing req load the signed certific	Language Select.) E equest uset successfully created. Note a request is not yet functional - have it signed by a Certificate Authority and ate to this device.
Device Info Advanced Setup	Name	mycertificate1
Layer2 Interface WAN Service	Туре	request
LAN	Subject	CN=zte/O=zte/ST=shanghai/C=CN
Security Parental Control Quality of Service Routing DSL Upnp Certificate Local Trusted CA Wireless Diagnostics Management	Signing Request	E EBGIN CERTIFICATE REQUEST TUTTBezCBGUNG41350ABWvcqCTVQVQDEWBGGUCEDDAKERVWBA0TA3p0ZTERMABGAIUE CEBU C2hhbmdOYWscC4JBgWYBAYTARMONIG+MAOCC39G51b3DQEBAQUAAGANACB UKBG0MUUD4/9409UVF73051F+4510MMdotry1Y9173/S3IITWEZEBKX 12/AL7/0UH73AEZra102MMX3Zch02TRE11VbJDR1UM0QvqU3V333B1W96F28 gwddHT3DwrBM0J11F/f1V070291F13M4-C2B0E24KV1YPUDAQBADAAVDVJT K0ZILNCHAQEBCAAD gEASTH014xZ13wrf+ux0UT394953U/F09G5c3MAEAF0/YEdo 5509U//x0F0p1I1c0DJTPt+t+f5L/1tN3y/r/x3ZjH3kBPG8qeEuFQ+XK1YtBG00= END CERTIFICATE REQUEST

### FIGURE 153 GENERATE CERTIFICATE REQUEST

- The certificate request needs to be submitted to a certificate authority, which signs the request.
   The signed certificate needs to be loaded into modem, click
- The signed certificate needs to be loaded into modem, click Load Signed Certificate in Figure 153, or Load Signed in the Local Certificates home page as shown in Figure 154.



#### FIGURE 154 GENERATED CERTIFICATE COMPLETED

TE中兴									r
	L = = = l							Language Select	9
	Local	certificates							
	Add, V	iew or Remove	e certifica	ites from this page. Local certificates are i	used by pe	eers to ver	ify your identity.		
Info	Maxim	um 4 certificate	es can be	e stored.					
ed Setup									
r2 Interface									
Service		Name	In Use	Subject	Туре	Action			L
						1.11-11-11	Land Olavad	[ ]	1
runk Setting		mycertificate		CN=zte.com/O=zte/ST=shanghai/C=CN	request	VIEW	Load Signed	Remove	l
ity									í
ntal Control				Create Certificate Request	Im	oort Certifi	icate		
y of Service									
ng									
ate									
I									
ed CA									
tics									
ment									

5. Paste the signed certificate as shown in Figure 155.

### FIGURE 155 LOAD CERTIFICATE

ZTE中兴	ξ ( La	guage Select: English 💌
	Load certificate	
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vlan Trunk Setting Security Parental Control Quality of Service Routing DSL Upnp Certificate Local Trusted CA Wireless Diagnostics Management	Paste signed certificate. Certificate Name:  constrained to the serve se	X
	Apply	

# Import An Existing Local Certificate

Click  $\ensuremath{\textbf{Import Certificate}}$  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

ZTE中兴			
	Import certificate	Language Select	English 💌
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vian Trunk Setting Security Parental Control Quality of Service Portice	Enter certificate name, paste certificate content and private key. Certificate Name:BEGIN CERTIFICATE <insert certificate="" here="">END CERTIFICATE</insert>		K
DSL Upnp Certificate Local Trusted CA Wireless Diagnostics Management	certificate:		*
Management	BEGIN RSA PRIVATE KEY <insert here="" key="" private=""> END RSA PRIVATE KEY</insert>		×
Management Management	Private Key:		
Management			T
	Apply		_

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.

#### ZTE中兴 Trusted CA (Certificate Authority) Certificates Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates. Maximum 4 certificates can be stored. Device Info Advanced Setup Layer2 Interface WAN Service Name Subject Type Action LAN Vlan Trunk Setting Import Certificate Security Parental Control Quality of Service Routing DSL Upnp Certificate Local Trusted CA Wireless Diagnostics Management

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

#### FIGURE 158 IMPORT CERTIFICATE

ZTE中兴	€	Language Select: English 💌
Device Info Advanced Setup Layer2 Interface WAN Service LAN Vian Trunk Setting Security Parental Control Quality of Service Routing DSL Uppp Certificate Local	Import CA certificate certificate Certificate BEGIN CERTIFICATE <insert bere="" certificate=""> END CERTIFICATE certificate:</insert>	
Wireless Diagnostics Management	Apply	z

#### FIGURE 157 TRUSTED CA CERTIFICATES

## 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.



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 com- puter that acts as a communica- tion hub for users of a wireless de- vice to connect to a wired LAN. APs are important for providing rein- forced wireless security and for ex- tending the physical range of serv- ice 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 wire- less 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 op- erates in Infrastructure mode. It controls network access on the wireless interface in its broadcast area. It allows access to the wire- less network by devices that use the correct SSID after a nego- tiation process takes place. By default, the Guw5.5Z66-5 broad- casts 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 Infra- structure mode allows wireless devices to survey that network and select an access point with which to associate. You may dis- able SSID broadcas

## 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 <u>Table 28</u> below to get some quick information to help you differentiate between the available wireless networking standards.

Standard	Data Rate	Modu- lation Scheme	Security	Pros/Cons & More Info
IEEE802.11	Up to 2 Mbps in the 2.4 GHz band	FHSS or DSSS	WEP & WPA	This speci- fication has been ex- tended into 802.11b.

#### TABLE 28 WIRELESS NETWORKING STANDARDS

Standard	Data Rate	Modu- lation 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 ad- here to this standard are consid- ered "Wi-Fi Certified". Eight avail- able chan- nels. Less potential for RF interfer- ence than 802.11b and 802.11b and 802.11b at supporting multime- dia voice, video and large-image applications in densely populated user envi- ronments. Relatively shorter range than 802.11b. Not intero- perable 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 ad- here to this standard are consid- ered "Wi-Fi Certified". Not intero- perable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high- speed ac- cess to data at up to 300 feet from base sta- tion. 14 channels available in

Standard	Data Rate	Modu- lation 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 ad- here to this standard are consid- ered "Wi-Fi Certified". May replace 802.11b. Improved security enhance- ments over 802.11. Compati- ble 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.

# O 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 WPSenabled 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 hexadecimals. 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 Transmis**sion 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.

ZTE中兴

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 <u>Table 29</u>.

TABLE 29 I	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.

ZTE中兴

FIGURE 162 WIRELESS - BASIC

ZTE中兴	Language Select English 式
	WirelessBasic
Device Info Advanced Setup Wireless Basic Security Advanced Station Info Diagnostics Management	This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, Nod the network form active scans, set the wireless network name (also known as SSID) and restrict the channel set based on country requirements.         Note: Legal SSID can contain 0-9,A-7,a-2,,,, #, #, &.         Click "Apply" to configure the basic wireless options.         Image: Enable Wireless         Hide Access Point         Clients Isolation         Disable WMM Advertise         SSID:       02:10:18:01:00:02         Country/Region:       CHINA         Max Clients:       16
	Enabled     SSID     Hidden     Isolate Clients     Disable WMM Advertise     Max Clients     BSSID       Image: Milloguest1     Image: Milloguest2     Image: Milloguest2

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, Coun- try/Region, Max Clients, Wire- less – 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 scan- ning.

Field	Description
Clients Isolation	When many clients connect to the same access point, they can ac- cess 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 pro- vide high-performance multimedia voice and video data transfers.
SSID	The SSID is the network name shared among all points in a wire- less network. The SSID must be identical for all points in the wire- less 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 se- curity, you should change the de- fault 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 ac- cording 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 vlaue, 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 ac- cess points can be configured.

Click  ${\bf Save}/{\bf Apply}$  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.

TF中兴

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)

7TF由兴	
LILTA	Language Select: English 💌
	Wireless Security
Device Info Advanced Setup Wireless Rasic	This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Prototed Setup(WPS)
Security Advanced Station Info Diagnostics Management	WSC Setup Enable WSC Disabled
	Manual Setup AP 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.
	Select SSID: ZXDSL931VII  Network Authentication: Open
	Save/Apply

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 <b>Open</b> .

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 <u>Figure 164</u>.

FIGURE 164 WIRELESS-SECURITY (64-BIT WEP)

)evice Info \dvanced Setup	This page allows you to con	
Vireless Basic Security Advanced	You may setup configuration OR through WIFI Proteted Setup WSC Setup	figure security features of the wireless LAN interface. I manually p(WPS)
Station Info Diagnostics Aanagement	Enable WSC	Disabled V
	Manual Setup AP	
	You can set the network aut specify whether a network k Click "Save/Apply" when doi	hentication method, selecting data encryption, key is required to authenticate to this wireless network and specify the encryption strength . ne,
	Select SSID:	ZXDSL931WII -
	Network Authentication:	Open 🔽
	WEP Encryption: Encryption Strength: Current Network Key: Network Key 1:	Enabled • 64-bit • 1 •
	Network Key 2:	12345
	Network Key 3: Network Key 4:	12345 12345 Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

Table 32 is the description of the different options.

TABLE 32	WLAN	<b>Security</b>	64-BIT	WEP	ENCRYPTION	CONFIGURATION
<b>OPTIONS</b>						

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

ZTE中兴	
	Wireless Security
Device Info Advanced Setup Wireless Basic Security Advanced Station Info Diagnostics Management	This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WFI Proteted Setup(WPS) WSC Setup Enable WSC Disabled V
	Manual Setup AP         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.         Select SSID:       IXDSL931VII I         Network Authentication:       Image: Im
	WEP Encryption:       Enabled          Encryption Strength:       128-bit          Current Network Key:       1         Network Key 1:       1234567890123         Network Key 3:       1234567890123         Network Key 4:       1234567890123         Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys         Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

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 <b>Open</b> or <b>Shared</b> .
WEP Encryption	Enable WEP Encryption.
Encryption Strength	Set the data security type to <b>128-</b> bit.

Field	Description
Current Network Key	Select one of network key that you set on the <b>Key</b> boxes as the default one.
Network Key 1 to 4	Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit en- cryption 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)

	Wireless Security	
evice Info dvanced Setup fireless Basic	This page allows you to confi You may setup configuration OR through WiFi Protcted Setup(	igure security features of the wireless LAN interface. manually WPS)
Security Advanced Station Info agnostics anagement	WSC Setup Enable WSC	Disabled ×
	Manual Setup AP You can set the network auth	ientication method, selecting data encryption,
	Click "Save/Apply" when done	y is required to advice rocate to this writeless network and specify the end ypoon strength . e.
	Select SSID: Network Authentication:	ZXDSL931WII -
	RADIUS Server IP Address: RADIUS Port:	0.0.0.0 1812
	RADIUS Key: WEP Encryption: Encryption Strength: Current Network Key:	Enabled T 128-bit T
	Network Key 1: Network Key 2:	1234567890123 1234567890123
	Network Key 3: Network Key 4:	123456/390123 123456/390123 Extra 12.1071 characterise on 26 insurance factors for 120 bit accounting laws

Table 34 is the description of the different options.

TABLE 34 WLAN	<b>SECURITY</b>	<b>802.1</b> x	<b>AUTHENTICATION</b>	CONFIGURATION
<b>O</b> PTIONS				

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be <b>802.1x</b> .
Radius Server IP Adress	Enter the IP Address of the au- thentication server.
Radius Port	Enter the port number of the au- thentication server. The default port number is <b>1812</b> .
Radius Key	Enter the same key as that on the Radius server.
WEP Encryption	Enable WEP Encryption. The de- fault 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 <b>key</b> 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 hexadec- imal digits. For a 128-bit encryp- tion 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)

ZTE中兴		Language S	elect: English 💌
	Wireless Security	injure seruirity features of the wireless I AN Interface.	
Device Info Advanced Setup Wireless Basic	You may setup configuration OR through WiFi Proteted Setup(	gano balan () robal do en la ministro den internet. manually (MPS)	
Security Advanced Station Info Diagnostics Management	WSC Setup Enable WSC	Disabled P	
	Manual Setup AP You can set the network auth specify whether a network ke Click "Save/Apply" when don	nentication method, selecting data encryption, ay is required to authenticate to this wireless network and specify the encryption strength . e.	
	Select SSID: Network Authentication:	ZXDSL931WII - WPA -	
	WPA Group Rekey Interval: RADIUS Server IP Address: RADIUS Port: RADIUS Key: WPA Encryption: WEP Encryption:	0 0.0.0.0 1812 TKIP Disabled	
		Save/Apply	

Table 35 is the description of the different options.

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be <b>WPA-PSK</b> .
WPA Group Rekey Interval	Specifies the time interval for which the WPA key remains un- changed. The value 0 indicates that you need not change the WPA key. The change is done automati- cally between the server and the client.
Radius Server IP Adress	Enter the IP address of the authen- tication server.
Radius Port	Enter the port number of the au- thentication server. The default port number is <b>1812</b> .
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 encryp- tion mode means AP auto adjusts to use TKIP or AES according to wireless clients.

### TABLE 35 WLAN SECURITY WPA AUTHENTICATION CONFIGURATION OPTIONS

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)

ZTE中兴	
	English 💌
Device Info Advanced Setup Wireless Basic Security Advanced Station Info Diagnostics	This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WIFI Prototed Setup(WPS) WSC Setup Enable WSC
Management	Manual Setup AP 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.
	Select SSID: IXDSL931WII  Network Authentication: WPA2
	WPA2 Presultentication:     Disable       RADIUS Port:     1812       RADIUS Key:
	Save/Apply

#### Table <u>36</u> 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 <b>WPA2</b> .
WPA2 Preauthentication	Select Enable or Disable.
Network Re-auth Interval	Specifies the time of re-authenti- cation 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 be- tween the server and the client.
Radius Server IP Adress	Enter the IP address of the authen- tication server.
Radius Port	Enter the port number of the authentication server. The default port number is <b>1812</b> .

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 auto- matically 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)

<b>ZIE</b> Ψ兴		Langu	age Select: English 💌
	Wireless Security		
Device Info Advanced Setup Wireless Basic Security Advanced Station Info Diagnostics Management	This page allows you to conf You may setup configuration OR through WFI Protected Setup WSC Setup Enable WSC	ingure security features of the wireless LAN interface. manually (WPS) Disabled T	
	Manual Setup AP You can set the network aut specify whether a network k Click "Save/Apply" when don	nentication method, selecting data encryption, ey is required to authenticate to this wireless network and specify the encryption strengt le,	h .
	Select SSID : Network Authentication :	ZXDSL931WII     WFA-PSK	ß
	WPA Pre-Shared Key: WPA Group Rekey Interval: WPA Encryption: WEP Encryption:	Click here to display       0       TKIP       Disabled	
		Save/Apply	

Table 37 is the description of the different options.

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be <b>WPA-PSK</b> .
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 <u>Table 38</u> for in- structions 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 be- tween 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 auto- matically adjusts to use TKIP or AES according to wireless clients.

## TABLE 37 WLAN SECURITY WPA AUTHENTICATION CONFIGURATION OPTIONS

#### 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)

	Wireless Security		
Device Info Advanced Setup Vireless Rasic	This page allows you to c You may setup configurat OR through WiFi Protcted Se	configure security features of the wireless LAN interface. tion manually http:(WPS)	
Security Advanced Station Info Diagnostics Management	WSC Setup Enable WSC	Disabled <b>T</b>	
	Manual Setup AP You can set the network - specify whether a networ Click "Save/Apply" when	authentication method, selecting data encryption, rk key is required to authenticate to this wireless network and specify the encryption strength . done.	
	Select SSID: Network Authentication:	IXDSL931WII - WPA2 -PSK -	

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 <b>WPA2-PSK</b> .
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 <u>Table 40</u> to for in- structions 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 be- tween 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 auto- matically 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)

<b>ZTE中</b> 兴	Langauge Select. English 🗨
	Wireless Security
Device Info Advanced Setup Wireless Basic	This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protected Setup(WPS)
Security Advanced Station Info Diagnostics Management	WSC Setup Enable WSC Disabled
	Manual Setup AP 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.
	Select SSID: ZXDSL931WII Network Authentication: Mixed WPA2/WPA -FSX
	WPA Pre-Shared Key:     Click here to display       WPA Group Rekey Interval:     0       WPA Encryption:     TKIP+AES       WEP Encryption:     Disabled
	Save/Apply

Table 41 is the description of the different options.

Field	Description
Network Authentication	Select the authentication mode for the selected wireless LAN of SSID to be <b>Mixed WPA2/WPA-PSK</b> .
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 <u>Table 42</u> for in- structions 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 be- tween 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 auto- matically adjusts to use TKIP or AES according to wireless clients.

#### TABLE 41 WIRELESS-SECURITY (WPA-PSK AUTHENTICATION)

#### 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)

<b>7TF</b> 中兴	
	Language Select English
	wireless Security
Device Info Advanced Setup Wireless Basic	This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WIFi Protcted Setup(WPS)
Security	WSC Setup
Station Info Diagnostics Management	Enable WSC Disabled
	Manual Setup AP
	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.
	Select SSID: ZXDSL931WII
	Network Authentication: Mixed WPA2/WPA 💌
	WPA2 Preauthentication:     Disable       Network Re-auth Interval:     96000       WPA Group Rekey Interval:     0       RADIUS Server IP Address:     0.0.0.0       RADIUS Port:     1812       RADIUS Very:     Image: Comparison of the server in the serve

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 <b>Mixed WPA2/WPA</b> .
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 <u>Table 44</u> for in- structions 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 be- tween the server and the client.

Field	Description
Radius Server IP Adress	Enter the IP address of the authen- tication server.
Radius Port	Enter the port number of the au- thentication server. The default port number is <b>1812</b> .
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 auto- matically 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

	Uticalass Advanced	Language Select JEnglish
	wireless Auvanceu	
Device Info	This page allows you to confi operate, force the transmissi	igure advanced features of the wireless LAN interface. You can select a particular channel on which to ion rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup
Advanced Setup	interval for clients in power-s	save mode, set the beacon interval for the access point, set XPress mode and set whether short or
Wireless	Click "apply" to configure the	advanced wireless ontions
Security	onar rippi) ia corrigoro dia	
Advanced	Band:	2.4GHz 💌
Station Info	Channel:	Auto 🔽 Current: 1
Diagnostics	Auto Channel Timer(min)	0
Management	54g™ Rate:	Aut o
	Multicast Rate:	Aut o 💌
	Basic Rate:	Default
	Fragmentation Threshold:	2346
	RTS Threshold:	2347
	DTIM Interval:	1
	Beacon Interval:	100
	Global Max Clients:	16
	XPress™ Technology:	Disabled 💌
	54g™ Mode:	54g Auto
	54g™ Protection:	Auto 💌
	Afterburner Technology:	Disabled Disable WMM for Selection
	Preamble Type:	long 💌
	Transmit Power:	100% -
	WMM(WI-Fi Multimedia):	Enabled 💌
	WMM No Acknowledgement:	Disabled V
	WMM APSD:	Enabled 💌

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 set- tings. The default channel is 11. All devices in your wireless net- work 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 trans- mission should be set depending on the speed of your wireless net- work. You can select from a range of transmission speeds, or you can select <b>Auto</b> to have the 931WII automatically use the fastest pos- sible data rate and enable the Auto-Fallback feature. Auto-Fall- back negotiates the best possible connection speed between the 931WII and a wireless client. The default value is <b>Auto</b> .
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 se- lect from a range of transmission speeds, or you can select <b>Auto</b> to have the 931WII automatically use the fastest possible data rate and enable the Auto-Fallback fea- ture. Auto-Fallback negotiates the best possible connection speed be- tween the 931WII and a wireless client. The default value is <b>Auto</b> .
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 Mes- sage (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 informa- tion 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 bea- con again. The beacon interval is in milliseconds (ms). The default value 100 is recommended.
XPress™ Technology	Select <b>Enabled</b> or <b>Disabled</b> . 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 transmis- sion 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 compat- ibility 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 wire- less clients that connect to the Guw5.5Z66-5 Access Point. If you select it, the preamble type is dis- abled and cannot be set.
	54g Auto: Only stations that are configured in 802.11b/g mode can associate.
	54g Perfomance : Only stations that are configured in 802.11g mode can associate. Similar to 54g LRS, if you select it, the pre- amble type is disabled and cannot be set.

Field	Description
54g <sup>™</sup> 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 Pro- tection as 802.11b device may need to use your wireless net- work. In Auto Mode, the wire- less device uses RTS/CTS to improve 802.11g performance in mixed 802.11g/802.11b net- works. Turn protection OFF to maximize 802.11g throughput under most conditions.
Preamble Type	Preambles are a sequence of bi- nary bits that help the receivers synchronize and ready for re- ceipt 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.
₩ММ	Select whether WMM is enabled or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes re- late 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 Dis- abled, meaning that an acknowl- edge packet is returned for every packet received. This provides a more reliable transmission but increases traffic load, which de- creases performance. Disabling the acknowledgement can be use- ful 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 consump- tion 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 <u>Figure 175</u>.

FIGURE 175 WIRELESS - AUTHENTICATED STATIONS

ZTE中兴							
	Wireless Aut	henticated S	stations.				
Device Info	This page shows	authenticated	wireless static	ons and	l their status.		
Advanced Setup Wireless	MAC Address	Associated	Authorized	SSID	Interface		
Basic Security Advanced					Refre	lish	
Station Info							
Diagnostics Management							

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

This page is intentionally blank.

# Chapter 19

# Diagnostics Configuration

1. Select **Diagnostics** to display the interface as shown in Figure 176.

#### FIGURE 176 DIAGNOSTICS

<b>ZTE中兴</b>	
Device Info Advanced Setup Wireless Diagnostics Management	br_0_8_81 Diagnostics         Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.         Test the connection to your local network         Test your eth0 Connection:       FAIL         Test your eth2 Connection:       FAIL         Help       Test your eth3 Connection:         Test your eth3 Connection:       FAIL         Help       Test your oth3 Connection:         Test your oth3 Connection:       FAIL         Help       Test your oth3 Connection:         Test your oth3 Connection:       FAIL         Help       Test your oth3 Connection:         Test your Soure that connection:       FAIL         Help       Test your oth3 Connection:         Test your Soure to your DSL service provider       Test x0SL Synchronization:
	Test with DAM E5 ATM DAM E5 end-to-end ning: DISABLED Help
	Test With OAM F5 Test With OAM F4

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
--	------------	-----------------	------------



- 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	
TR-069 Client Management	
Internet Time	
Access Control	
Undate Software	
Reboot	

# Settings

### Setting Backup

Select **Management > Settings > Backup** to display the interface as shown in <u>Figure 178</u>.

#### FIGURE 178 BACKUP CONFIG





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

## Setting Update

 Select Management > Settings > Update to display the interface as shown in Figure 179.

#### FIGURE 179 UPDATE CONFIG

ZTE中兴	
Device Info Advanced Setup Wireless Diagnostics Management Settings Backup Update Restore Default System Log SIMP Agent IR-069 Client Internet Time Access Control Update Software Reboot	Tools Update Settings Update DSL router settings. You may update your router settings using your saved files. Settings File Name: Browse Update

- 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

 Select Management > System Log to display the interface as shown in Figure 181.

#### FIGURE 181 SYSTEM LOG

ZTE中兴	
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log SNMP Agent TR-069 Client Internet Time Access Control Update Software Reboot	System Log The System Log dialog allows you to view the System Log and configure the System Log options. Click View System Log to view the System Log. Click Configure System Log to configure the System Log options. View Configure

2. Click **Configure** to display the interface as shown in <u>Figure</u> <u>182</u>.



#### 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 Level:	Debugging	~
Display Level:	Error	~
Mode:	Local 💌	-

Save/Apply	
------------	--

- 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

ZTE 中 <sub></sub>	ŧ
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log TR-069 Client Internet Time Access Control Update Software Save/Reboot	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 dipayed. If the selected mode is 'Remote' or 'Both,' events will be sent the specified IP address and dick 'Save/Apply' to configure the system log options.         Log:       Obselle O Enable         Log Level;       Debugzing         Debugzing       Debugzing         Server UDP Port:       State         Server UDP Port:       State

- 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.

#### ZTE中兴

#### 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

Refresh Close

## **SNMP** Agent

Select **Management > SNMP Agent** to display the interface as shown in Figure 185.

#### FIGURE 185 SNMP AGENT

<b>ZTE中兴</b>	
	Linguage Selection Simple Network Management Protocol (SMMP) allows a management annitration to retrieve statistics and status from the SMMP
Device Info	agent in this device.
Advanced Setup Wireless	Select the desired values and click Apply to configure the SNMP options.
Diagnostics Management	You must restart snmp agent by first disabling and then enabling it for the configuration of Read/Set Community to take effect
Settings	SNMP Agent 🕜 Disable C Enable
System Log SNMP Agent	Read Community: public
TR-069 Client	Set Community: private
Access Control	System Name: ZTE 931WII
Update Software	System Location : Shanghai
Reboot	System Contact: [2] E Trap Manager IP: [192.168.2.2
	Save/Apply

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.

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 con- tact the maintenance personnel if the system fails.
Trap Manager IP	Define NMS server IP address to receive system SNMP trap reports.

#### TABLE 46 SNMP AGENT CONFIGURATION OPTIONS

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

### **O** 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 <u>Figure 186</u>.

#### FIGURE 186 PROTOCOL STACK

CPE/ACS Management Application		
RPC Methods		
SOAP		
нтр		
SSUTLS		
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 appli- cation 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 pro- cedure calls. Specifically SOAP 1.1.
НТТР	HTTP 1.1.
SSL/TLS	The standard Internet transport layer security protocols. Specifi- cally, 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

<b>ZTE中兴</b>		Language Salect, English 💌
	TR-069 client - Configuration	
Device Info Advanced Setup	WAN Management Protocol (TR-069) and diagnostics to this device.	allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection,
Wireless Diagnostics Managament	Inform	© Disable C Enable
Settings System Log	Inform Interval: ACS URI :	300
SNMP Agent TR-069 Client	ACS User Name: ACS Password:	admin
Internet Time Access Control Update Software	WAN Interface used by TR-069 client	Any_WAN
Reboot	Display SOAP messages on serial con	sole @ Disable C Enable
	Connection Request User Name:	admin
	Connection Request Password: Connection Request URL:	•••••
		Save/Apply GetRPCMethods

Table 48 is a description of the different options.

#### TABLE 48 TR-069 CLIENT CONFIGURATION OPTIONS

Field	Description
Inform	If the <b>Enable</b> option is selected, the CPE accepts the commands from ACS. If the <b>Disable</b> option is selected, the CPE does not accept the commands from ACS.
Inform Interval	The seconds between two at- tempts 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 cli- ent:	Define the WAN interface used to transfer TR-069 messaage, <b>Any_WAN, LAN</b> , and <b>Loopback</b> .
Display SOAP messages on serial console	When <b>Enable</b> is selected, the SOAP information is displayed on the serial console, when <b>Disable</b> is selected, the information is not displayed.
Connection Request Authentica- tion	If this checkbox is selected, you need to enter the <b>Connection Re-quest</b> , <b>User Name</b> , and the <b>Connection Request Password</b> . 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  $\ensuremath{\textbf{GetRPCMethods}}$  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

ZTE中兴	
Device Info Advanced Setup Wireless Diagnostics Management Settings System Log SWMP Agent TR-069 Client Internet Time Access Control Update Software Reboot	Time settings         This page allows you to the modem's time configuration.         Automatically synchronize with Internet time servers         Save/Apply

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 <u>Figure 190</u>.

#### FIGURE 190 INTERNET TIME SETUP

ZTE中兴	
	Time settings
	This page allows you to the modem's time configuration.
Device Info Advanced Setup	☑ Automatically synchronize with Internet time servers
Wireless Diagnostics	First NTP time server: time.nist.gov
Management	Second NTP time server: ntp1.tummy.com
Settings	Third NTP time server: None
System Log	Fourth NTP time server: None
SNMP Agent	Fifth NTP time server: None
Internet Time Access Control	Time zone offset: (GMT+08:00) Beijing, Chongquing, Hong Kong, Urumqi
Update Software Reboot	Save/Apply

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

<b>ZTE中兴</b>	Lasenare Select. English V
	Access Control Passwords
	Access to your DSL router is controlled through two user accounts: admin and user.
Device Info	The user name admin has unrestricted across to change and view configuration of your DSL Router
Advanced Setup	The deer hame during hard an obtained access to change and hew comparation of your book reader.
Wireless	The user name user can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.
Diagnostics	
Management	Use the fields below to enter up to 128 characters sand click Apply to change or create passwords. Note: Legal password can
Settings	Luntain U=9,R=2,a=2,,@, #,\$;0
System Log	Isername: admin
SNMP Agent	
TR-069 Client	
Internet Time	New Password:
Access Control	Confirm Password:
Passwords	
Update Software	Save/Apply
Reboot	

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 <u>Figure 192</u>.

#### FIGURE 192 UPDATE SOFTWARE

ZTE中兴	
	Tools Update Software
XX 1/2	Step 1: Obtain an updated software image file from your ISP.
Device Info	
Advanced Setup	Step 2: Enter the path to the image hie location in the box below or click the "Browse" button to locate the image hie.
Wireless	Step 3: Click the button once to upload the new image file.
Diagnostics	
Management	NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot.
Settings	
System Log	Software Hie Name: Browse
SNMP Agent	
TR-069 Client	Update
Internet Time	
Access Control	
Update Software	
Reboot	

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

F中兴



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	
Figure 5 IP and DNS Configuration	19
Figure 6 Web-based Management - Home Page	21
Figure 7 Web-based Management - Login Authentication	า
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	
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	
Figure 25 DNS Configuration	
Figure 26 EOA PPPoE WAN Connection Setup Summary.	37
Figure 27 EOA PPPoE WAN Connection Configuration	
Completed	37
Figure 28 ADSL PVC Configuration Overview	
Figure 29 Adding EOA PVC	
Figure 30 EOA PVC Configuration Completed	
Figure 31 WAN Service Overview	
Figure 32 Select Layer2 Interface	40

Figure 33 Select WAN Service Type40
Figure 34 WAN IP Configuration40
Figure 35 NAT Configuration41
Figure 36 Default Gateway Configuration41
Figure 37 DNS Configuration42
Figure 38 EOA IPoE WAN Connection Setup Summary42
Figure 39 EOA IPoE WAN Connection Configuration
Completed43
Figure 40 ADSL PVC Configuration Overview43
Figure 41 Adding EOA PVC44
Figure 42 EOA PVC Configuration Completed45
Figure 43 WAN Service Overview45
Figure 44 Select Layer2 Interface46
Figure 45 Select WAN Service Type46
Figure 46 EOA Bridge WAN Connection Setup Summary47
Figure 47 EOA Bridge WAN Connection Configuration
Completed47
Figure 48 ADSL PVC Configuration Overview48
Figure 49 Adding PPPoA PVC48
Figure 50 PPPoA PVC Configuration Completed49
Figure 51 WAN Service Overview49
Figure 52 Select Layer2 Interface50
Figure 53 WAN Service Configuration50
Figure 54 PPPoA Configuration50
Figure 55 Default Gateway Configuration51
Figure 56 DNS Configuration
Figure 57 PPPoA WAN Connection Setup Summary52
Figure 58 PPPoA WAN Connection Configuration Completed53
Figure 59 ADSL PVC Configuration Overview53
Figure 60 Adding IPoA PVC54
Figure 61 IPoA PVC Configuration Completed54
Figure 62 WAN Service Overview55
Figure 63 Select Layer2 Interface55
Figure 64 WAN Service Configuration56
Figure 65 WAN IP Configuration56
Figure 66 NAT Configuration56
Figure 67 Default Gateway Configuration57
Figure 68 DNS Configuration
Figure 69 IPoA WAN Connection Setup Summary58
Figure 70 IPoA WAN Connection Configuration Completed58

Figure 71 VDSL2 PTM Interface Configuration Overview59
Figure 72 Adding PTM Interface59
Figure 73 WAN Service Overview60
Figure 74 Select Layer2 Interface60
Figure 75 Select WAN Service Type61
Figure 76 PPPoE Configuration61
Figure 77 Default Gateway Configuration62
Figure 78 DNS Configuration63
Figure 79 PTM Interface PPPoE WAN Connection Setup
Summary63
Figure 80 PTM Interface PPPoE WAN Connection Configuration
Completed64
Figure 81 VDSL2 PTM Interface Configuration Overview64
Figure 82 Adding PTM Interface65
Figure 83 WAN Service Overview65
Figure 84 Select Layer2 Interface66
Figure 85 Select WAN Service Type66
Figure 86 PTM Interface Bridge WAN Connection Setup
Summary67
Figure 87 PTM Interface Bridge WAN Connection
Configuration Completed67
Figure 88 VDSL2 PTM Interface Configuration Overview68
Figure 89 Adding PTM Interface68
Figure 90 WAN Service Overview69
Figure 91 Select Layer2 Interface69
Figure 92 Select WAN Service Type69
Figure 93 WAN IP Configuration70
Figure 94 Default Gateway Configuration
igure y i benaute eaternaly configuration internal inte
Figure 95 DNS Configuration
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       73         Figure 100 PTM Interface IPoE WAN Connection Configuration       73         Figure 101 LAN Configuration Overview       75
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       73         Figure 100 PTM Interface IPoE WAN Connection Configuration       73         Figure 101 LAN Configuration Overview       75         Figure 102 Adding DHCP Static IP Lease       76
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       73         Figure 100 PTM Interface IPoE WAN Connection Configuration       73         Figure 101 LAN Configuration Overview       75         Figure 103 Configure Second IP Address       76

Figure 105	VLAN Trunking Notice79	
Figure 106	WAN Service Overview80	
Figure 107	Select Layer2 Interface80	
Figure 108	Select WAN Service Type81	
Figure 109	PTM Interface Bridge WAN Connection Setup	
	Summary81	
Figure 110	PTM Interface Bridge WAN Connection	
	Configuration Completed82	
Figure 111	VLAN Trunking Configuration82	
Figure 112	Virtual Server85	
Figure 113	Virtual Servers Overview86	
Figure 114	Adding Virtual Servers87	
Figure 115	Port Triggering Overview	
Figure 116	Adding Port Triggering88	
Figure 117	DMZ host90	
Figure 118	DMZ host Configuration91	
Figure 119	DMZ Host Configuration Notice91	
Figure 120	MAC Filtering Overview93	
Figure 121	MAC Filtering Change Policy94	
Figure 122	Adding MAC Filtering Rule95	
Figure 123	Removing MAC Filtering Rule96	
Figure 124	Adding MAC filtering - Forwarded96	
Figure 125	Adding MAC filtering - Blocked97	
Figure 126	Quality of Service99	
Figure 127	Enable QoS 100	
Figure 128	QoS Queue Configuration Overview101	
Figure 129	QoS Queue Configuration102	
Figure 130	QoS Queue Configuration - Completed 103	
Figure 131	QoS Classification	
Figure 132	QoS Classification Overview104	
Figure 133	QoS Classification Configuration105	
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 Overview112	
Figure 140	Adding Policy Routing 112	
Figure 141	RIP Configuration114	
Figure 142	DNS Server Configuration Overview115	

Figure 143 Dynamic DNS Configuration Overview116
Figure 144 Adding Dynamic DNS117
Figure 145 DSL Configuration 119
Figure 146 Time Restriction Overview125
Figure 147 Time Restriction Config126
Figure 148 URL Filter Overview127
Figure 149 URL Filter Config127
Figure 150 UPNP Config129
Figure 151 Local Certificate Overview131
Figure 152 Create New Certificate Request132
Figure 153 Generate Certificate Request
Figure 154 Generated Certificate Completed134
Figure 155 Load Certificate134
Figure 156 Import Certificate135
Figure 157 Trusted CA Certificates136
Figure 158 Import Certificate136
Figure 159 Client Mode138
Figure 160 Ad Hoc Mode138
Figure 161 Typical Wireless Network Topology139
Figure 162 Wireless - Basic148
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)
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 - Advanced165
Figure 175 Wireless - Authenticated Stations169
Figure 176 Diagnostics171
Figure 177 Troubleshooting Procedures172
Figure 178 Backup Config173
Figure 179 Update Config174
Figure 180 Restore Default Config175

Figure 181 System Log 175
Figure 182 Enabling System Log176
Figure 183 Log Server Config 176
Figure 184 System Event Logs 177
Figure 185 SNMP Agent177
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
Figure 190 Internet Time Setup182
Figure 191 Access Control
Figure 192 Update Software 183
Figure 193 Reboot

# **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

### ZTE中兴

Table 33 WLAN Security 128-bit WEP Encryption
Configuration Options152
Table 34 WLAN Security 802.1x Authentication Configuration
Options154
Table 35 WLAN Security WPA Authentication Configuration
Options156
Table 36 WLAN Security WPA2 Authentication Configuration
Options157
Table 37 WLAN Security WPA Authentication Configuration
Options159
Table 38 WPA Pre-Shared Key 159
Table 39 WLAN Security WPA2 Authentication Configuration
Options160
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 Options165
Table 46 SNMP Agent Configuration Options    178
Table 47 Protocol Layer Summary    179
Table 48 TR-069 Client Configuration Options    180