

6219-X1 ADSL2+ 4-Port Router Users Guide

Document Part Number: 830-02072-02
February 2010



Z H O N E .

Zhone Technologies, Inc.
@ Zhone Way
7001 Oakport Street
Oakland, CA 94621
USA
510.777.7000
www.zhone.com
info@zhone.com

COPYRIGHT ©2000-2010 Zhone Technologies, Inc. All rights reserved.

This publication is protected by copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission from Zhone Technologies, Inc.

Bitstorm, EtherXtend, IMACS, MALC, MXK, Raptor, SLMS, Z-Edge, Zhone, ZMS, zNID and the Zhone logo are trademarks of Zhone Technologies, Inc.

Zhone Technologies makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability, non infringement, or fitness for a particular purpose. Further, Zhone Technologies reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Zhone Technologies to notify any person of such revision or changes.

This product may contain copyrighted software that is licensed under the GNU General Public License ("GPL"), a copy of which is available at www.gnu.org/licenses. You may obtain a copy of such software, in source code form, from Zhone for a period of three years after our last shipment of the product by following the instructions at www.zhone.com/gplinfo.



Important Safety Instructions

1. Read and follow all warning notices and instructions marked on the product or included in the manual.
2. Slots and openings in the housing are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.
3. Do not allow anything to rest on the power cord and do not locate the product where persons will walk on the power cord.
4. Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.
5. General purpose cables are used with this product for connection to the network. Special cables, which may be required by the regulatory inspection authority for the installation site, are the responsibility of the customer. Use a UL Listed, CSA certified, minimum No. 24 AWG line cord for connection to the Digital Subscriber Line (DSL) network.
6. When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.
7. A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are interconnected, the voltage potential may cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action prior to interconnecting the products.
8. Input power to this product must be provided by one of the following: (1) a UL Listed/CSA certified power source with a Class 2 or Limited Power Source (LPS) output for use in North America, or (2) a certified transformer, with a Safety Extra Low Voltage (SELV) output having a maximum of 240 VA available, for use in the country of installation.
9. In addition, since the equipment is to be used with telecommunications circuits, take the following precautions:
 - Never install telephone wiring during a lightning storm.
 - Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
 - Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
 - Use caution when installing or modifying telephone lines.
 - Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
 - Do not use the telephone to report a gas leak which is in the vicinity of the leak.

CE Marking

When the product is marked with the CE mark on the equipment label, a supporting Declaration of Conformity may be downloaded from the Zhone World Wide Web site at www.zhone.com.

FCC Part 15 Declaration

An FCC Declaration of Conformity may be downloaded from the Zhone World Wide Web site at www.zhone.com.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by the responsible party.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Notice to Users of the United States Telephone Network

The following notice applies to versions of the modem that have been FCC Part 68 approved.

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council for Terminal Attachment (ACTA). On the bottom side of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the Telephone Company.

This equipment is intended to connect to the Public Switched Telephone Network through a Universal Service Order Code (USOC) type RJ11C jack. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It has been designed to be connected to a compatible modular jack that is also compliant.

If the modem causes harm to the telephone network, the Telephone Company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the Telephone Company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The Telephone Company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the Telephone Company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service. If trouble is experienced with the modem, refer to the repair and warranty information in this document.

If the equipment is causing harm to the telephone network, the Telephone Company may request that you disconnect the equipment until the problem is resolved.

The user may make no repairs to the equipment.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

If the site has specially wired alarm equipment connected to the telephone line, ensure the installation of the modem does not disable the alarm equipment. If you have questions about what will disable alarm equipment, consult your Telephone Company or a qualified installer.

Notice to Users of the Canadian Telephone Network

NOTICE: This equipment meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation IC before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

If your equipment is in need of repair, contact your local sales representative, service representative, or distributor directly.

▲CANADA - EMI NOTICE:

This Class B digital apparatus meets all requirements of the Canadian interference-causing equipment regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du règlement sur le matériel brouilleur du Canada.

Japan Notices

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

Table of Contents

Important Safety Instructions.....	3
CE Marking	3
FCC Part 15 Declaration.....	3
About This Guide.....	11
Style and notation conventions	11
Typographical conventions	12
Acronyms	12
Contacting Global Service and Support.....	14
Chapter 1 Introduction	15
System Requirements	15
Package Contents	16
Safety Instructions.....	16
Front Panel.....	17
Back Panel	18
Chapter 2 Hardware Installation and PC Setup	19
Overview	19
Connecting your hardware	19
Mounting the Router.....	20
Standing the Router Vertically	20
Configuring Your Computer	21
Windows 2000	21
Windows XP.....	22
Chapter 3 The Web User Interface	23
Log in to the Router.....	23
Summary	24
WAN Info	25
LAN Statistics	25
WAN Statistics.....	26
ATM Interface Statistics.....	26
ADSL Statistics	27
ADSL BER Test	28
Route.....	29
ARP	29
DHCP	30

Chapter 4	Advanced Setup	31
WAN		31
Create a New WAN Connection — ATM PVC Configuration		32
Connection Type PPPoA		33
Connection Type PPPoE		36
Connection Type MAC Encapsulation Routing		39
Connection Type IP over ATM		42
Connection Type Bridging		44
Remove Function		46
Finish Function		47
LAN Local Area Network (LAN) Setup		48
Ethernet Mode		50
NAT		51
Virtual Servers		51
Port Triggering		53
DMZ Host		54
MAC Filtering		55
Parental Control		57
URL Filter		58
Quality of Service		59
Queue Config		59
QoS Classification		60
Routing		62
Default Gateway		62
Static Route		63
Policy Route		64
DSL		65
Modulation Methods		65
Capability		66
DSL Advanced Settings		66
Interface Group		68
IPSec		70
Certificate		72
Local		72
Trusted CA		74

Chapter 5	Wireless	75
Basic		75
Security		77
MAC Filter		81
Wireless Bridge		82
Advanced		84
Station Info		85
Diagnostics		86
Management		87
Settings		87
Backup Settings		87
Update or Restore User Settings		88
Restore Default		88
System Log		89
Configure System Log		90
SNMP		91
TR-069 Client		91
Access Control		92
Services		92
IP Addresses		93
Passwords		94
Update Software		95
Reboot Router		96
Chapter 6	Troubleshooting	97
The Router Is Not Functional		97
You Cannot Connect to the Router		97
LEDs Blink in a Sequential Pattern		97
The Status LED Continues to Blink		97
The Status LED is Always Off		98
Diagnosing Problems using IP Utilities		98
Ping		98
Nslookup		99
Appendix A	Glossary	101

About This Guide

This guide is intended for use by installation technicians, system administrators, and network administrators. It explains how to install the 1611-A3 router.

Style and notation conventions

The following conventions are used in this document to alert users to information that is instructional, warns of potential damage to system equipment or data, and warns of potential injury or death. Carefully read and follow the instructions included in this document.



Caution: A caution alerts users to conditions or actions that could damage equipment or data.



Note: A note provides important supplemental or amplified information.



Tip: A tip provides additional information that enables users to more readily complete their tasks.



WARNING! A warning alerts users to conditions or actions that could lead to injury or death.

Typographical conventions

The following typographical styles are used in this guide to represent specific types of information.

Bold	Used for names of buttons, dialog boxes, icons, menus, profiles when placed in body text, and property pages (or sheets). Also used for commands, options, parameters in body text, and user input in body text.
Fixed	Used in code examples for computer output, file names, path names, and the contents of online files or directories.
Fixed Bold	Used in code examples for text typed by users.
<i>Fixed Bold Italic</i>	Used in code examples for variable text typed by users.
<i>Italic</i>	Used for book titles, chapter titles, file path names, notes in body text requiring special attention, section titles, emphasized terms, and variables.
PLAIN UPPER CASE	Used for environment variables.
Command Syntax	Brackets [] indicate optional syntax. Vertical bar indicates the OR symbol.

Acronyms

The following acronyms are related to Zhone products and may appear throughout this manual:

Table 1: Acronyms and their descriptions

Acronym	Description
ADSL	Asymmetrical Digital Subscriber Line
AP	Access Point
ACS	Auto Configuration Server
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EFM	Ethernet in the First Mile
MALC	Multi-Access Line Concentrator
MIB	Management Information Bases
NAT	Network Address Translation
NMS	Network Management System
PVC	Permanent Virtual Circuit

RADIUS	Remote Authentication Dial In User Service
SHDSL	Symmetric High-bit-rate Digital Subscriber Line
SLMS	Single Line Multi-Service
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
VoIP	Voice over IP
VoWi-Fi	Voice-over-Wifi
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity (IEEE 802.11 wireless networking)
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
ZMS	Zhone Management System

Contacting Customer Service and Technical Support

Customer service and technical support for this Zhone device are provided by your Internet Service Provider.

Chapter 1 Introduction

The 6219-X1 ADSL 2+ 4 port WiFi is an easily installed router which delivers the performance needed for multimedia applications

This User's Guide will show you how to set up the router, and how to customize its configuration to get the most out of this product.

The 6219-X1 provides the following features:

- **Built-in ADSL modem which offers G.dmt, G.lite, T1.413, ADSL2, Annex L, and ADSL2+ to meet different linking speeds from your ISP**
- **Four 10/100BaseT Ethernet ports to provide Internet connectivity to all computers on your LAN**
- **Wireless Access Point with 802.11b/g with 200mW antenna power for extended WiFi reach and performance**
- **Easy-to-use configuration program accessible through a standard web browser**

This User Guide will show you how to connect your 6219-X1 and how to customize its configuration to get the most out of your new product.

System Requirements

In order to use your 6219-X1 ADSL router for Internet access, you must have the following:

- **ADSL service subscription from your ISP**
- **A PC with:**
 - **An Ethernet 10/100BaseT network interface card**
 - **A processor equivalent to or faster than a Pentium II 133 MHz**
 - **32 MB RAM or greater**
 - **Windows 95b, 98, 98SE, 2000, ME, NT, or XP (Note: Windows 95 requires the installation of the Winsock program, not included.)**
- **(Optional) An Ethernet hub or switch, if you are connecting the device to several computers on an Ethernet network.**
- **For system monitoring or configuration using the supplied web interface, a web browser such as Internet Explorer Version 6.0 or later. Netscape is not supported.**

Package Contents

In addition to this document, your package should arrive containing the following:

- **6219-X1 ADSL 2+ 4 port router**
- **12V 1 A power adapter**
- **RJ-11 telephone cable**
- **RJ-45 Ethernet cable**
- **User Manual / Quick Guide**

Safety Instructions

Place your modem on a flat surface close to the cables in a location with sufficient ventilation.

To prevent overheating, do not obstruct the ventilation openings of the device.

Plug the device into a surge protector to reduce the risk of damage from power surges and lightning strikes.

Operate this equipment only from an electrical outlet with the correct power source as indicated on the adapter.

Do not open the cover of the device. Opening the cover will void any warranties on the equipment.

Do not use another power adapter except for the one which accompanies the unit.

Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid / aerosol cleaners or magnetic / static cleaning devices.

Front Panel




LED	Mode	INDICATION
Power	Solid green	Boot-up successful
	Solid red	Router is booting up or there is problem with internal Power On Self Test (POST)diagnostic
	No light	The router may not be turned on. Check if the power adapter is connected to the modem and plugged in
Alarm	Solid	DSL is not connected
	No light	DSL is linked successfully
LAN 1-4	Solid on green	Ethernet interface is successfully connected to a device through the LAN port
	Flashing	The router is sending or receiving data over Ethernet
	Off	No LAN Link
WIFI	Solid	Wireless access point option is enabled
	No light	Wireless access point is disabled
	Blinking	Wireless traffic activity
DSL	Solid	Connection established. The router is able to communicate with your ISP via ADSL
	Flashing	The router is attempting to connect to your ISP
	Solid	ADSL is connected
Internet	No light	ADSL is not connected. The ALARM LED will be red
	Blinking	The router is connected to the LAN

Back Panel



NOTE: The below port descriptions are listed as they appear on the back panel from left to right.

Port	Description
Phone	RJ-11 cable connects to telephone (no external splitter necessary; unit has internal splitter).
Line	RJ-11 cable connects between telephone and the LINE port using a splitter (not included) if needed.
LAN1 – LAN4	RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
Reset / Default	<p>Restart—press the button for less than 4 seconds.</p> <p>Default settings—press the button for 4 seconds or longer.</p> <p> Warning : pressing the RESET button may erase the configuration your service provider has loaded in the modem and may cause service disruption.</p>
Power	Connects to a 12V 1A power adapter.

Chapter 2 Hardware Installation and PC Setup

Overview

This chapter provides basic instructions for connecting the router to a computer or a LAN and to the Internet using DSL. The first part provides instructions to set up the hardware, and the second part describes how to prepare your PC for use with the router. Refer to Chapter 3, Using the Web Interface for configuration instructions.

It is assumed that you have already subscribed to DSL service with your telephone company or other Internet service provider (ISP).

Connecting your hardware

Shut down your PC before connecting the router. To connect your modem:

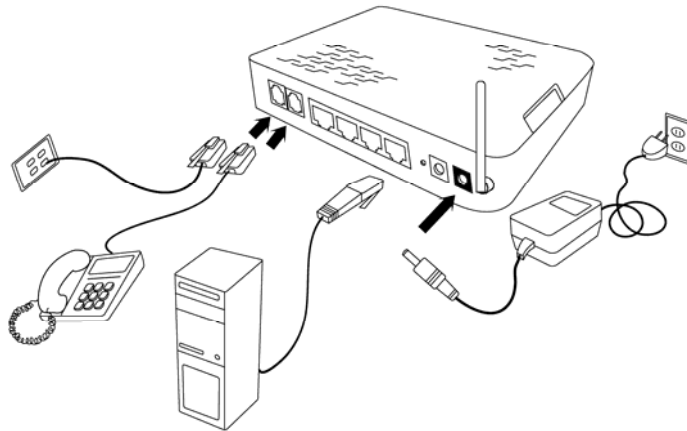
1. Connect the ADSL Line and Telephone

Connect one end of an RJ-11 cable from your ADSL connection and the other end to the LINE port of the modem.

Use a second RJ-11 cable to connect between a telephone and the PHONE port of the modem.

2. Connect the PC to the Router

To use the Ethernet connection, connect the Ethernet cable from the computer directly to the router. Connect one end of the Ethernet cable to one of the four ports labelled LAN on the back of the router and attach the other end to the Ethernet port of your computer.

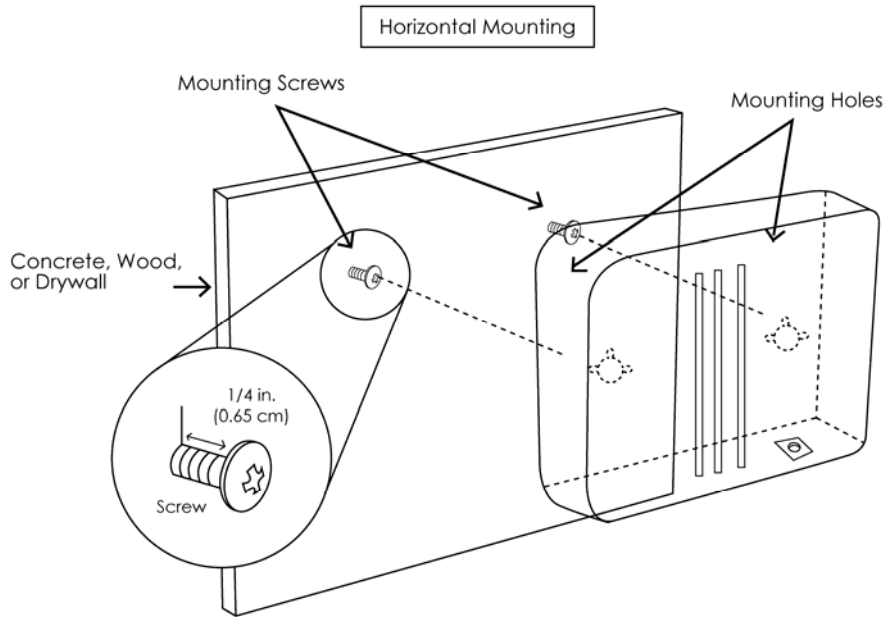


3. Connect the Power Adapter

Complete the process by connecting the AC power adapter to the POWER connector on the back of the device and plug the adapter into a wall outlet or power strip. Then turn on and boot up your PC and any LAN devices, such as hubs or switches, and any computers connected to them.

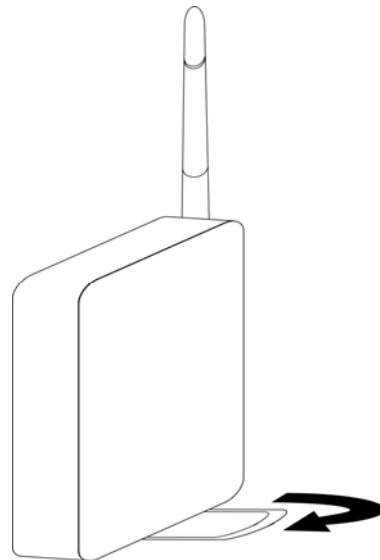
Mounting the Router

The router can be mounted on the wall with two screws. Mounting can be done on wall material including concrete, wood, or drywall. Select an appropriate location free from obstructions or any possible interference. Make sure the cables can be easily attached to the router without strain. The illustration below shows how to mount the router horizontally on a wall.



Standing the Router Vertically

The router can be set vertically on the desktop or other surface. On the right side of the unit as it sits horizontally is a foot which can be rotated.



Configuring Your Computer

Prior to accessing the router through the LAN or the USB port, note the following necessary configurations—

- Your PC's TCP/IP address: 192.168.1.___(the last number is any number between 2 and 254)
- The router's default IP address: 192.168.1.1
- Subnet mask: 255.255.255.0

Below are the procedures for configuring your computer. Follow the instructions for the operating system that you are using.

If you used the Ethernet cable to connect your router and PC, you do not need any specific driver installation.

Windows 2000

1. *In the Windows taskbar, click the Start button and point to **Settings, Control Panel, and Network and Dial-up Connections** (in that order).*
2. *Click **Local Area Connection**. When you have the **Local Area Connection Status** window open, click **Properties**.*
3. *Listed in the window are the installed network components. If the list includes **Internet Protocol (TCP/IP)**, then the protocol has already been enabled, and you can skip to Step 10.*
4. *If Internet Protocol (TCP/IP) does not appear as an installed component, then click **Install**.*
5. *In the **Select Network Component Type** window, click on protocol and then the **Add** button.*
6. *Select **Internet Protocol (TCP/IP)** from the list and then click on **OK**.*
7. *If prompted to restart your computer with the new settings, click **OK**.*
8. *After your computer restarts, click the **Network and Dial-up Connections** icon again, and right click on the **Local Area Connection** icon and then select **Properties**.*
9. *In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)** and then click **Properties**.*
10. *In the **Internet Protocol (TCP/IP) Properties** dialog box, click the radio button labelled **Use the following IP address** and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.*
11. *Click **OK** twice to save your changes and then close the **Control Panel**.*

Windows XP

1. In the Windows taskbar, click the **Start** button and point to **Settings** and then click **Network Connections**.
2. In the **Network Connections** window, right click on the **Local Area Connection** icon and click on **Properties**.
3. Listed in the **Local Area Connection** window are the installed network components. Make sure the box for **Internet Protocol (TCP/IP)** is checked and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the radio button labelled **Use the following IP address** and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.
5. Click **OK** twice to save your changes and then close the **Control Panel**.

Chapter 3 The Web User Interface

The 6219-X1 combination modem/router has a Wide Area Network (WAN) connection which connects to your phone line. This connects to your Internet Service Provider (ISP) via the phone line. The four Local Area Network (LAN) connections are where you plug in your local computers to the router. The 6219-X1 also has a wireless interface. The router is normally configured to automatically provide all the PCs on your network with Internet addresses.

To set up your router with a basic configuration, from the top navigation bar, select **Advanced Setup** from the left hand navigation bar. Setup has two main subsections underneath **Advanced Setup** — **WAN** and **LAN**. Setup instructions are covered in Chapter 4, Advanced Setup.

If you connected a PC (rather than a hub or a switch) directly to the router, your LAN consists of that PC. You may also create connections for various protocol options by creating new connections.

To configure your router you will first need to log in to the router.

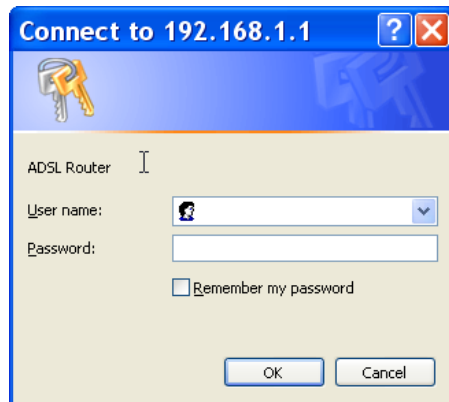
Note: Before configuring your router, make sure you have followed the instructions in Chapter 2 Hardware Installation and PC Setup. You should have your PCs configured for DHCP mode (if your router will be), and have proxies disabled on your browser. If you see a login redirection screen when you access the web interface, verify that JavaScript support is enabled in your browser. Also, if you do not get the screen shown below, you may need to delete your temporary Internet files.

Log in to the Router

This section will explain how to log in to your router.

1. *Launch your web browser.*
2. *Enter the URL <http://192.168.1.1> in the address bar and press Enter.*

A login screen like the one below will be displayed after you connect to the user interface.



3. *Enter your user name and password, and then click on **OK** to display the user interface.*

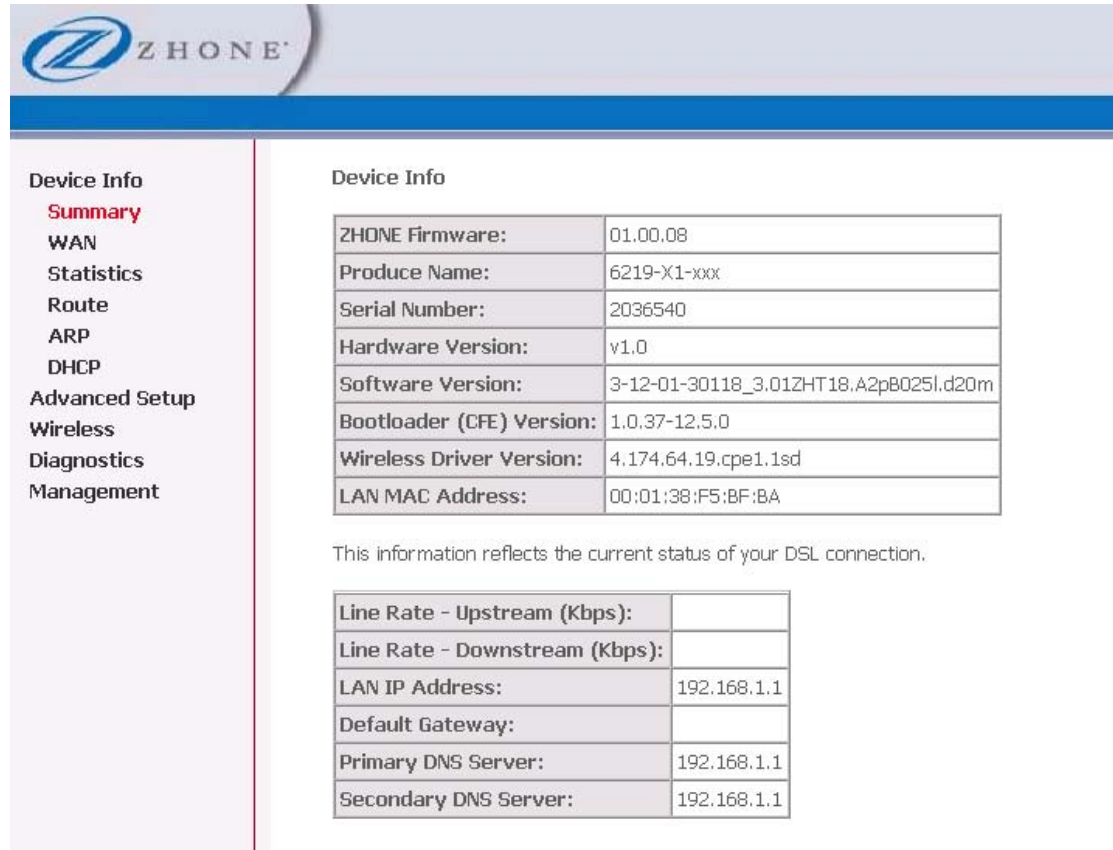
The user name / password are admin / admin and both are case sensitive.



Note: There are two default user name and password combinations. The user / user name and password combination can display device status, but cannot change or save configurations. The admin / admin combination can perform all functions. Passwords can be changed at any time.

Summary

Access the general information of the router by clicking **Summary** under **Device Info**. This screen shows details of the router such as the version of the software, bootloader, LAN IP address, etc. It also displays the current status of your DSL connection as shown below—



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

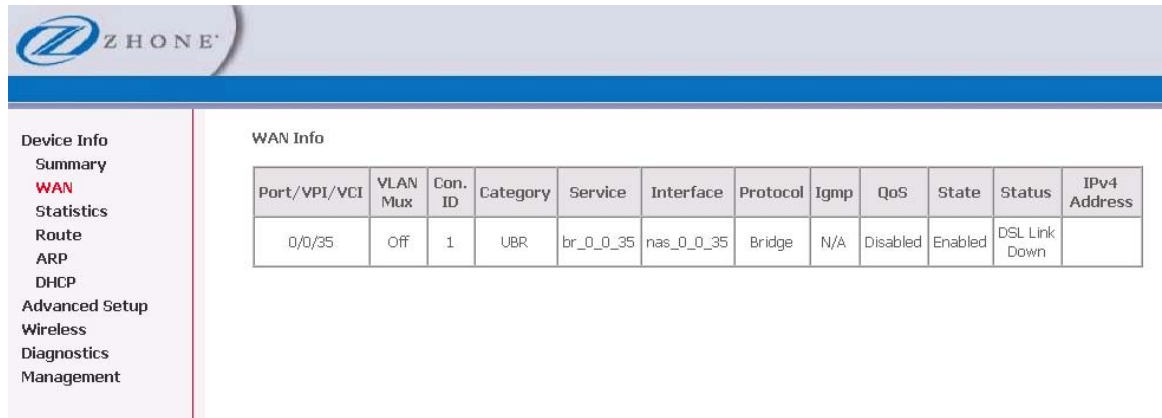
ZHONE Firmware:	01.00.08
Produce Name:	6219-X1-xxx
Serial Number:	2036540
Hardware Version:	v1.0
Software Version:	3-12-01-30118_3_01ZHT18.A2pB025l.d20m
Bootloader (CFE) Version:	1.0.37-12.5.0
Wireless Driver Version:	4.174.64.19.cpe1.1sd
LAN MAC Address:	00:01:38:F5:BF:BA

Below this table, it states: "This information reflects the current status of your DSL connection." Below that is another table with the following information:

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

WAN Info

Display the WAN status report from the router by clicking **WAN** under **Device Info**. The graphic below shows the screen when a WAN connection is set up.

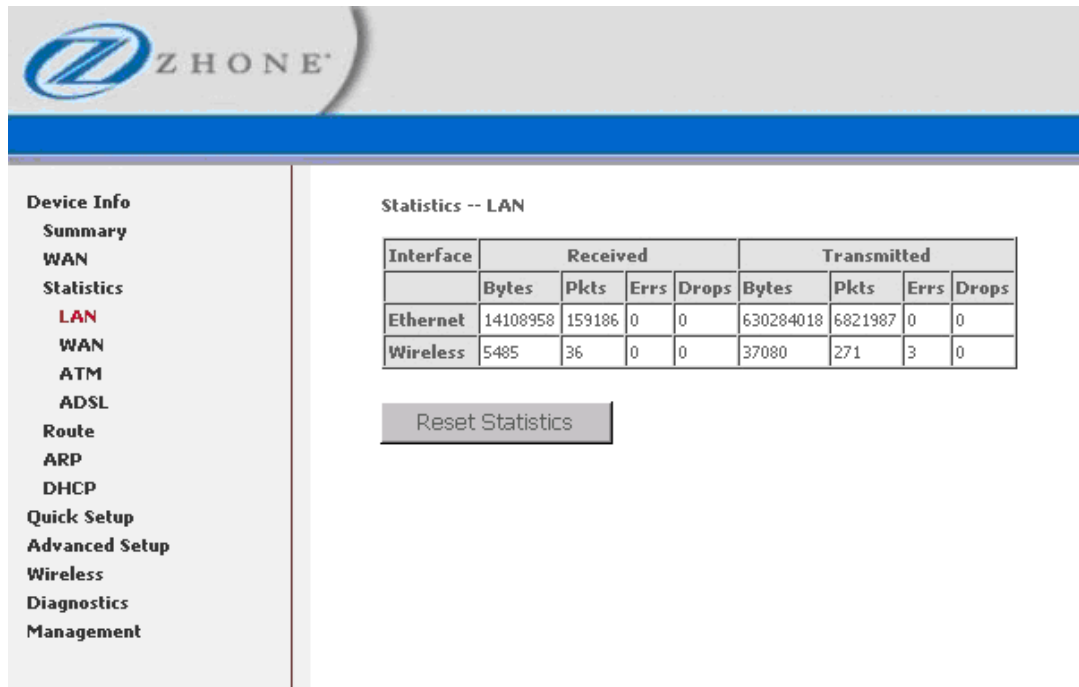


The screenshot shows the Zhone router's web interface. On the left is a navigation menu with options: Device Info, Summary, WAN (highlighted in red), Statistics, Route, ARP, DHCP, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "WAN Info" and contains a table with the following data:

Port/VPI/VCI	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Status	IPv4 Address
0/0/35	Off	1	UBR	br_0_0_35	nas_0_0_35	Bridge	N/A	Disabled	Enabled	DSL Link Down	

LAN Statistics

Display LAN statistics by clicking **LAN** under **Statistics**



The screenshot shows the Zhone router's web interface. On the left is a navigation menu with options: Device Info, Summary, WAN, Statistics (highlighted), LAN (highlighted in red), WAN, ATM, ADSL, Route, ARP, DHCP, Quick Setup, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Statistics -- LAN" and contains a table with the following data:

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Ethernet	14108958	159186	0	0	630284018	6821987	0	0
Wireless	5485	36	0	0	37080	271	3	0

Below the table is a button labeled "Reset Statistics".

The reset statistics button zeros out the counters so that you can more easily determine if the errors are still occurring.

WAN Statistics

Display WAN statistics by clicking **WAN** under **Statistics**.

Statistics -- WAN

Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
mer_0_0_35	0/0/35	MER	nas_0_0_35	447044141	401709	0	0	13453459	152493	0	0
br_0_0_36	0/0/36	Bridge	nas_0_0_36	2147483647	6267914	0	0	16870	241	0	0
pppoa_0_0_40_1	0/0/40	PPPoA	ppp_0_0_40_1	0	0	0	0	0	0	0	0
br_0_0_41	0/0/41	Bridge	nas_0_0_41	0	0	0	0	0	0	0	0
ipoa_0_0_42	0/0/42	IPoA	ipa_0_0_42	0	0	0	0	0	0	0	0

[Reset Statistics](#)

The reset statistics button zeros out the counters so that you can more easily determine if the errors are still occurring.

ATM Interface Statistics

Display ATM statistics by clicking **ATM** under **Statistics**.

ATM Interface Statistics

In Octets	Out Octets	In Errors	In Unknown	In Hec Errors	In Invalid Vpi Vci Errors	In Port Not Enable Errors	In PTI Errors	In Idle Cells	In Circuit Type Errors	In OAM RM CRC Errors	In GFC Errors
397358359	13500868	0	0	0	0	0	0	0	0	0	0

AAL5 Interface Statistics

In Octets	Out Octets	In Ucast Pkts	Out Ucast Pkts	In Errors	Out Errors	In Discards	Out Discards
397358359	13500868	6637911	153010	1565	0	0	0


AAL5 VCC Statistics

VPI/VCI	CRC Errors	SAR Timeouts	Oversized SDUs	Short Packet Errors	Length Errors
0/35	1516	0	0	0	0
0/36	1516	0	0	0	0
0/40	1516	0	0	0	0
0/41	1516	0	0	0	0
0/42	1516	0	0	0	0

[Reset](#) [Close](#)

ADSL Statistics

Display ADSL statistics by clicking **ADSL** under **Statistics**. Information contained in this screen is useful for troubleshooting and diagnostics of connection problems.



Device Info

- Summary
- WAN
- Statistics
 - LAN
 - WAN
 - ATM
 - ADSL
- Route
- ARP
- DHCP
- Advanced Setup
- Wireless
- Diagnostics
- Management

Statistics -- ADSL

Mode:	G.DMT	
Type:	Fast	
Line Coding:	Trellis On	
Status:	No Defect	
Link Power State:	L0	
	Downstream	Upstream
SNR Margin (dB):	12.9	13.0
Attenuation (dB):	42.5	17.0
Output Power (dBm):	11.9	19.7
Attainable Rate (Kbps):	7808	1100
Rate (Kbps):	6016	768
K (number of bytes in DMT frame):	189	25
R (number of check bytes in RS code word):	0	0
S (RS code word size in DMT frame):	1	1
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	14395	14335
Super Frame Errors:	0	0
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	0	0
DCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	3472665	0
Data Cells:	2613	0
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	18	0

ADSL BER Test

Reset Statistics

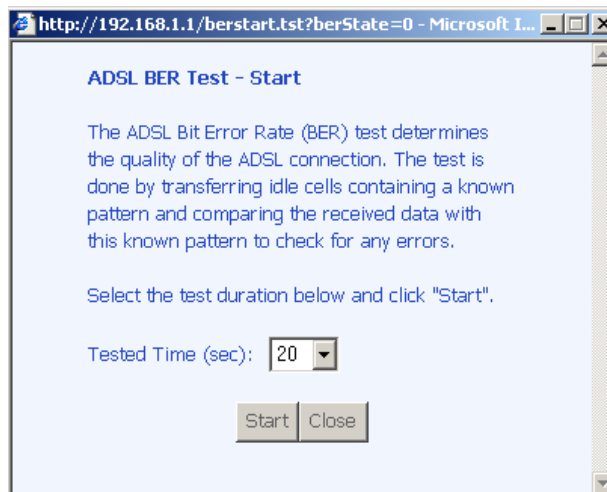
ADSL BER Test

The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is performed by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors. The **BER Test** reflects the ratio of error bits to the total number transmitted.

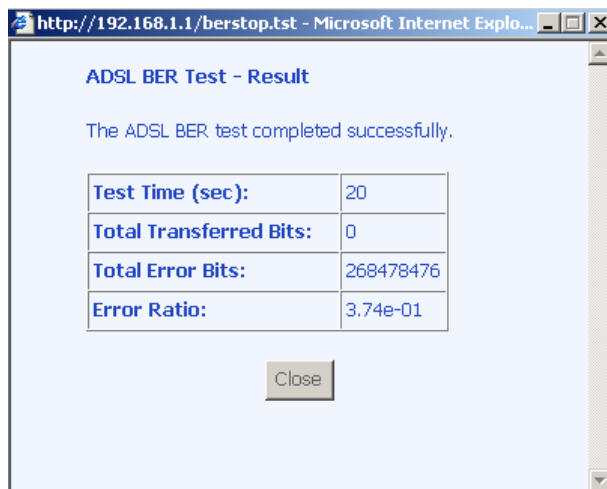
If you click on the **ADSL BER Test** button at the bottom of the ADSL Statistics page, the following pop-up screen will appear allowing you to set the tested time and to begin the test.

To run a BER test:

1. On the bottom of the **ADSL statistics** page, click **ADSL BER Test**
2. In the **Tested Time (sec)** drop down, select the test duration, and then click **Start**.

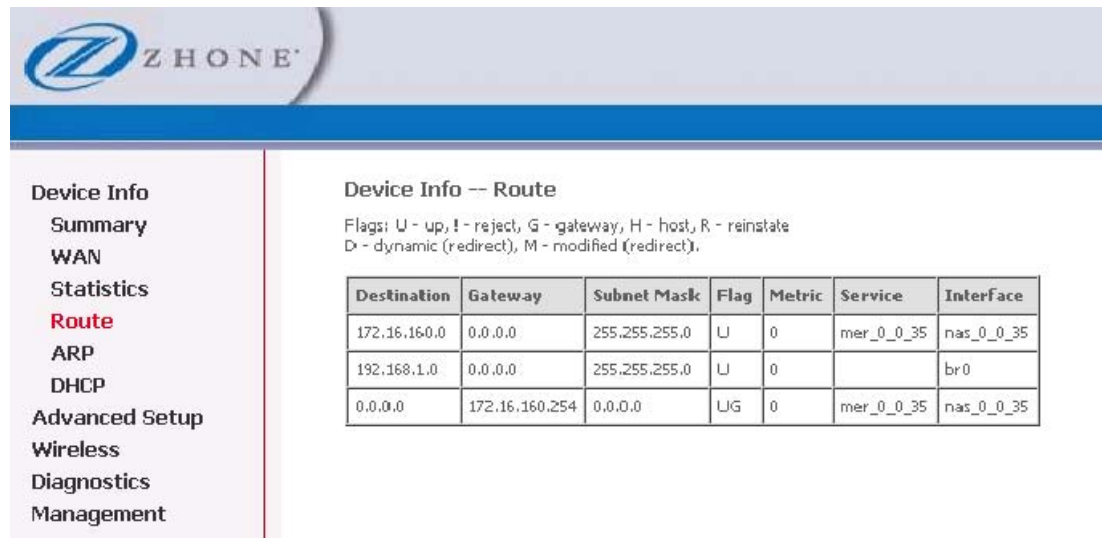


3. Check the results.



Route

Access the routing status report from the router by clicking **Route** under **Device Info**.



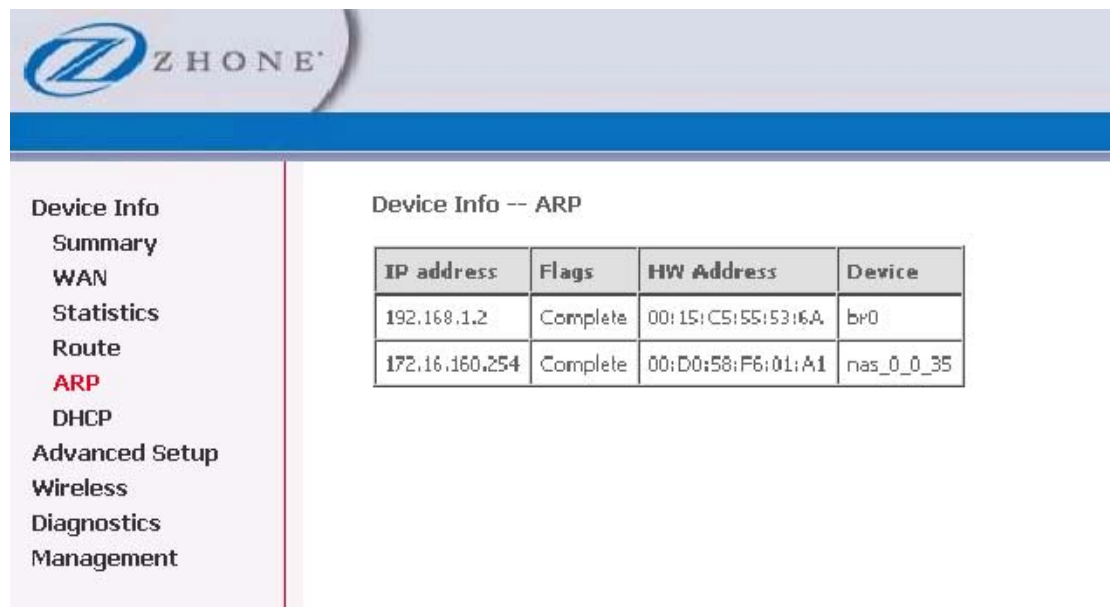
The screenshot shows the Zhone router's web interface. The top header features the Zhone logo. On the left, a navigation menu lists various sections: Device Info, Summary, WAN, Statistics, Route (highlighted in red), ARP, DHCP, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info -- Route" and includes a legend for flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect). Below the legend is a table with the following data:

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
172.16.160.0	0.0.0.0	255.255.255.0	U	0	mer_0_0_35	nas_0_0_35
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	172.16.160.254	0.0.0.0	UG	0	mer_0_0_35	nas_0_0_35

ARP

Display the ARP status report by clicking **ARP** under **Device Info**.

ARP (Address Resolution Protocol) maps the IP address to the physical address, labeled **HW Address** (the MAC address) and identifies computers on the LAN.



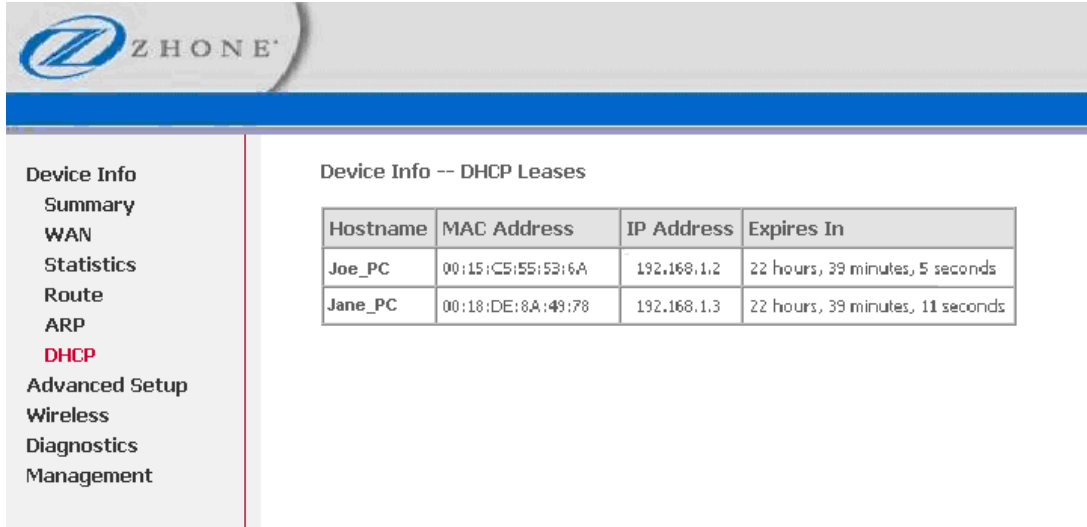
The screenshot shows the Zhone router's web interface. The top header features the Zhone logo. On the left, a navigation menu lists various sections: Device Info, Summary, WAN, Statistics, Route, ARP (highlighted in red), DHCP, Advanced Setup, Wireless, Diagnostics, and Management. The main content area is titled "Device Info -- ARP" and contains a table with the following data:

IP address	Flags	HW Address	Device
192.168.1.2	Complete	00:15:C5:55:53:6A	br0
172.16.160.254	Complete	00:D0:58:F6:01:A1	nas_0_0_35

DHCP

Access the DHCP Leases screen by clicking **DHCP** under **Statistics**.

This page shows the computers, identified by the hostname and MAC address that have acquired IP addresses by the DHCP server with the time that the lease for the IP address is up.



Device Info -- DHCP Leases

Hostname	MAC Address	IP Address	Expires In
Joe_PC	00:15:C5:55:53:6A	192.168.1.2	22 hours, 39 minutes, 5 seconds
Jane_PC	00:18:DE:8A:49:78	192.168.1.3	22 hours, 39 minutes, 11 seconds

Chapter 4 Advanced Setup

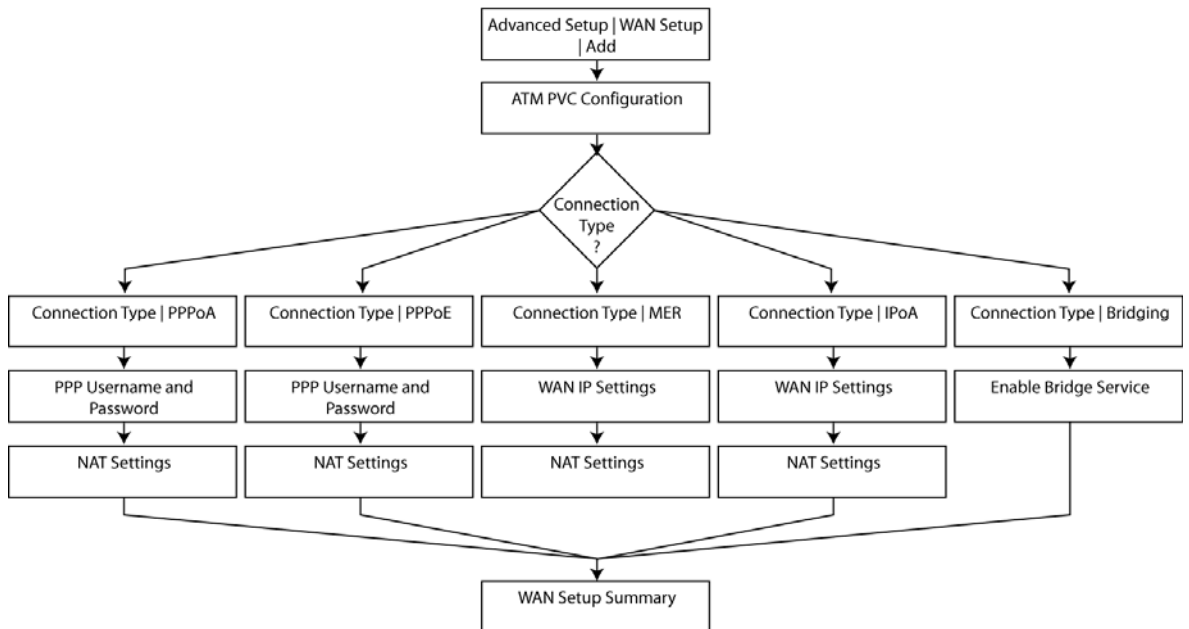
This section contains advanced setup settings.

WAN

Configure the WAN settings as provided by your ISP. For each type of WAN connection, you create a new ATM Permanent Virtual Channel (PVC) identifier. The PVC is made up of a Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI).

The default settings for the 6219-X1 has a bridge configured. If you are not going to use the bridge, delete it before proceeding to configure a new WAN connection.

When you click **Add** you begin creating a new WAN connection. The command tree for creating a WAN connection depends on the connection type selected.



Create a New WAN Connection — ATM PVC Configuration

To add a new connection for the WAN interface, click **Add**.

The ATM PVC Configuration screen follows as seen below. The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.

The screenshot shows the 'ATM PVC Configuration' screen in a Zhone web interface. On the left is a navigation menu with categories like Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Virtual Servers, Port Triggering, DMZ Host, Security, Parental Control, Quality of Service, Routing, DSL, Interface Group, IPsec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled 'ATM PVC Configuration' and contains the following elements:

- A description: 'This screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category. Otherwise choose an existing interface by selecting the checkbox to enable it.'
- Input fields: 'VPI: [0-255]' with a value of 0, and 'VCI: [32-65535]' with a value of 35.
- A checkbox: 'VLAN Mux - Enable Multiple Protocols Over a Single PVC' which is unchecked.
- A dropdown menu for 'Service Category' with 'UBR Without PCR' selected. A tooltip is visible over the dropdown showing options: 'UBR Without PCR', 'UBR With PCR', 'CBR', 'Non Realtime VBR', and 'Realtime VBR'.
- Text: 'Enabling packet le... Realtime VBR. Q...' followed by a description: '...ves performance for selected classes of applications. QoS cannot be set for CBR and Realtime VBR. Q... purposes; therefore the number of PVCs will be reduced. Use **Advanced Setup/Quality of Service** to assign priorities for the applications.'
- A checkbox: 'Enable Quality Of Service' which is unchecked.
- Buttons: 'Back' and 'Next'.

Find out the following values from your ISP before you change them:

- **VPI : Virtual Path Identifier.** The valid range is 0 to 255.
- **VCI : Virtual Channel Identifier.** The valid range is 32 to 65535.
- **Service Category :** Five classes of traffic:
 - **UBR Without PCR (*Unspecified Bit Rate without Peak Cell Rate*)**—UBR service is suitable for applications that can tolerate variable delays and some cell losses. Applications suitable for UBR service include text/data/image transfer, messaging, distribution, and retrieval and also for remote terminal applications such as telecommuting.
 - **UBR With PCR (*Unspecified Bit Rate with Peak Cell Rate*)**
 - **CBR (*Constant Bit Rate*)**—used by applications that require a fixed data rate that is continuously available during the connection time. It is commonly used for uncompressed audio and video information such as videoconferencing, interactive audio (telephony), audio / video distribution (e.g. television, distance learning, and pay-per-view), and audio / video retrieval (e.g. video-on-demand and audio library).
 - **Non Realtime VBR (*Non-Real-time Variable Bit Rate*)**—can be used for data transfers that have critical response-time requirements such as airline reservations, banking transactions, and process monitoring.
 - **Realtime VBR (*Real-time Variable Bit Rate*)**—used by time-sensitive applications such as real-time video. Rt-VBR service allows the network more flexibility than CBR.

Connection Type | PPPoA

Point to Point Protocol over ATM (PPPoA) Point-to-Point Protocol is a protocol for serial data transmission that is used to carry IP data between your ISP and your computer. PPPoA encapsulates PPP frames for ATM Adaption Layer 5 (AAL5). PPPoA offers authentication, encryption and compression.

1. *Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use, then click **Next***
2. *In the Connection Type page, select **PPP over ATM (PPPoA)**, then click **Next***

The screenshot shows the Zhone router's web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup (WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DSL, Interface Group, IPSec, Certificate), Wireless, Diagnostics, and Management. The main content area is titled "Connection Type" and contains the instruction: "Select the type of network protocol for IP over Ethernet as WAN interface:". Below this are five radio button options: "PPP over ATM (PPPoA)" (selected), "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)", "IP over ATM (IPoA)", and "Bridging". There is an "Encapsulation Mode" dropdown menu set to "VC/MUX". At the bottom right are "Back" and "Next" buttons.

3. *In the **PPP Username and Password** page, enter a username and password and change other parameters as directed by your ISP, and then click **Next**.*

The screenshot shows the Zhone router's web interface for the "PPP Username and Password" configuration page. The left sidebar is the same as in the previous screenshot. The main content area is titled "PPP Username and Password" and contains the instruction: "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.". Below this are several input fields and checkboxes: "PPP Username:" (text box), "PPP Password:" (text box), "Authentication Method:" (dropdown menu set to "AUTO"), "PPP MTU [128-1492]:" (text box set to "1492"), and five checkboxes: "Dial on demand (with idle timeout timer)", "PPP IP extension", "Use Static IP Address", "Retry PPP password on authentication error", and "Enable PPP Debug Mode". At the bottom right are "Back" and "Next" buttons.

4. In the **Network Address Translation Settings** page, make changes as directed by your ISP, and then click **Next**.

Network Address Translation Settings

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

Enable NAT

Enable Fullcone NAT

Public IP of NAT:

Enable Firewall

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

When the settings are complete, the next screen shows a **WAN Setup – Summary** screen displaying the WAN configurations made.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

- Make sure that the settings on the **WAN Setup - Summary** screen match the settings provided by your ISP. If all settings are correct, click **Save** to save these settings; if not, click **Back** to make any modifications. If you want to change any item after saving, click **Edit** to make any modifications.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 0 / 35
Connection Type:	PPPoA
Service Name:	pppoa_0_0_35_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.

NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

[Back](#) [Save](#)

- Click **Save** to save the settings.

After the settings are saved, the below screen will follow displaying the WAN settings that you made with the option to **Add** or **Remove** any of the connections that you have made.

The screenshot shows the Zhone router's WAN Setup Summary screen. On the left is a navigation menu with options like Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DSL, Interface Group, IPsec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled 'Wide Area Network (WAN) Setup' and includes instructions: 'Choose Add, Edit, or Remove to configure WAN interfaces. Choose Save/Reboot to apply the changes and reboot the system.' Below this is a table with the following data:

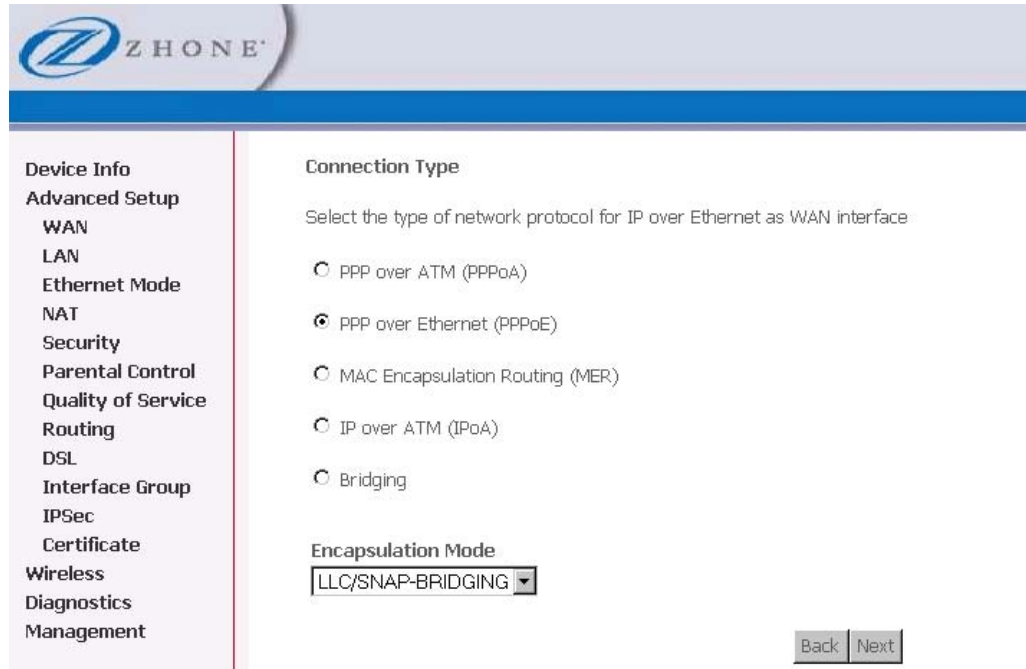
Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoa_0_0_35_1	ppp_0_0_35_1	PPPoA	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit

At the bottom of the table are three buttons: [Add](#), [Remove](#), and [Save/Reboot](#).

Connection Type | PPPoE

Point to Point Protocol over Ethernet (PPPoE) encapsulates PPP frames in Ethernet frames.

1. *Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use, then click **Next***
2. *In the Connection Type page, select **PPP over Ethernet (PPPoE)**, then click **Next***



The screenshot shows the Zhone router configuration interface. The top header features the Zhone logo and the text 'Z H O N E'. Below the header is a navigation menu on the left with the following items: Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DSL, Interface Group, IPsec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled 'Connection Type' and contains the instruction: 'Select the type of network protocol for IP over Ethernet as WAN interface'. There are five radio button options: 'PPP over ATM (PPPoA)', 'PPP over Ethernet (PPPoE)' (which is selected), 'MAC Encapsulation Routing (MER)', 'IP over ATM (IPoA)', and 'Bridging'. Below these options is a section for 'Encapsulation Mode' with a dropdown menu currently set to 'LLC/SNAP-BRIDGING'. At the bottom right of the configuration area are two buttons: 'Back' and 'Next'.

3. *In the **PPP Username and Password** page, enter a username and password and change other parameters as directed by your ISP, and then click **Next**.*

Z H O N E

Device Info
 Advanced Setup
 WAN
 LAN
 Ethernet Mode
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 DSL
 Interface Group
 IPSec
 Certificate
 Wireless
 Diagnostics
 Management

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

PPP Username:
 PPP Password:
 PPPoE Service Name:
 Authentication Method:
 PPP MTU [128-1492]:

Dial on demand (with idle timeout timer)

PPP IP extension

Use Static IP Address

Retry PPP password on authentication error

Enable PPP Debug Mode

Bridge PPPoE Frames Between WAN and Local Ports (Default Enabled)

4. In the **Network Address Translation Settings** page, make changes as directed by your ISP, and then click **Next**.

Z H O N E

Device Info
 Advanced Setup
 WAN
 LAN
 Ethernet Mode
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 DSL
 Interface Group
 IPSec
 Certificate
 Wireless
 Diagnostics
 Management

Network Address Translation Settings

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

Enable NAT

Enable Fullcone NAT

Public IP of NAT:

Enable Firewall

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast


Enable WAN Service

Service Name:

Enable MAC Clone

Enable MAC Clone

When the settings are complete, the next screen shows a **WAN Setup – Summary** screen displaying the WAN configurations made.



Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

WAN Setup - Summary

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


PORT / VPI / VCI:	0 / 3 / 38
Connection Type:	PPPoE
Service Name:	pppoe_0_3_38_1
Service Category:	UBR
IP Address:	Automatically Assigned
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

[Back](#) [Save](#)

5. Make sure that the settings on the **WAN Setup - Summary** screen match the settings provided by your ISP. If all settings are correct, click **Save** to save these settings; if not, click **Back** to make any modifications. If you want to change any item after saving, click **Edit** to make any modifications.
6. Click **Save** to save the settings.

After the settings are saved, the below screen will follow displaying the WAN settings that you made with the option to **Add** or **Remove** any of the connections that you have made.



Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoa_0_0_35_1	ppp_0_0_35_1	PPPoA	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/3/38	Off	1	UBR	pppoe_0_3_38_1	ppp_0_3_38_1	PPPoE	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit

[Add](#) [Remove](#) [Save/Reboot](#)

Connection Type | MAC Encapsulation Routing

MAC Encapsulation Routing (MER) allows the router to have routing on the LAN, but have bridging on the WAN connection to the ISP.

1. Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use, then click **Next**
2. In the Connection Type page, select **MAC Encapsulation Routing (MER)**, then click **Next**

The screenshot shows the Zhone router's web interface. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL), Interface Group (IPSec, Certificate), Wireless, Diagnostics, and Management. The main content area is titled "Connection Type" and contains the instruction: "Select the type of network protocol for IP over Ethernet as WAN interface". There are five radio button options: "PPP over ATM (PPPoA)", "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)" (which is selected), "IP over ATM (IPoA)", and "Bridging". Below these is an "Encapsulation Mode" dropdown menu set to "LLC/SNAP-BRIDGING". At the bottom right are "Back" and "Next" buttons.

3. In the **WAN IP Settings** page, change parameters as directed by your ISP, and then click **Next**.

The screenshot shows the Zhone router's web interface for the "WAN IP Settings" page. The left navigation menu is the same as in the previous screenshot. The main content area is titled "WAN IP Settings" and includes a notice: "Enter information provided to you by your ISP to configure the WAN IP settings. Notice: DHCP can be enabled for PVC in MER mode or IP over Ethernet as WAN interface if 'Obtain an IP address automatically' is chosen. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from DHCP or other WAN connection. If you configure static default gateway over this PVC in MER mode, you must enter the IP address of the remote gateway in the 'Use IP address'. The 'Use WAN interface' is optional." There are three main radio button options: "Obtain an IP address automatically", "Use the following IP address:" (selected), and "Obtain default gateway automatically". Under "Use the following IP address:", there are input fields for "WAN IPv4 Address" (192.2.1.1) and "WAN Subnet Mask" (255.255.255.0). Under "Obtain default gateway automatically", there are two radio button options: "Use the following default gateway:" (selected) and "Obtain DNS server addresses automatically". The "Use the following default gateway:" option has sub-options for "Use IPv4 Address:" (input field) and "Use WAN Interface:" (dropdown menu showing "mer_0_5_42/"). The "Obtain DNS server addresses automatically" option has sub-options for "Primary DNS server:" and "Secondary DNS server:" (input fields). At the bottom right are "Back" and "Next" buttons.

- In the **Network Address Translation Settings** page, make changes as directed by your ISP, and then click **Next**.

Network Address Translation Settings

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

Enable NAT

Enable Fullcone NAT

Public IP of NAT:

Enable Firewall

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

Enable MAC Clone

Enable MAC Clone

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

When the settings are complete, the next screen shows a **WAN Setup – Summary** screen displaying the WAN configurations made.

WAN Setup - Summary

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

PORT / VPI / VCI:	0 / 5 / 42
Connection Type:	MER
Service Name:	mer_0_5_42
Service Category:	UBR
IP Address:	192.2.1.1
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

[Back](#) [Save](#)

- Make sure that the settings on the **WAN Setup - Summary** screen match the settings provided by your ISP. If all settings are correct, click **Save** to save these settings; if not, click **Back** to make any modifications. If you want to change any item after saving, click **Edit** to make any modifications.
- Click **Save** to save the settings.

After the settings are saved, the below screen will follow displaying the WAN settings that you made with the option to **Add** or **Remove** any of the connections that you have made.

- Device Info
- Advanced Setup
- WAN
- LAN
- Ethernet Mode
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DSL
- Interface Group
- IPSec
- Certificate
- Wireless
- Diagnostics
- Management

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoa_0_0_35_1	ppp_0_0_35_1	PPPoA	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/3/38	Off	1	UBR	pppoe_0_3_38_1	ppp_0_3_38_1	PPPoE	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/5/42	Off	1	UBR	mer_0_5_42	nas_0_5_42	MER	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit

Connection Type | IP over ATM

Internet Protocol over ATM (IPoA) supports extending across classic IP subnet boundaries using IP routing and IP forwarding.

1. Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use, then click **Next**
2. In the Connection Type page, select **IP over ATM (IPoA)**, then click **Next**

The screenshot shows the Zhone router's web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DNS, DSL, Interface Group, IPSec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled "Connection Type" and contains the following text: "Select the type of network protocol for IP over Ethernet as WAN interface". Below this text are five radio button options: "PPP over ATM (PPPoA)", "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)", "IP over ATM (IPoA)", and "Bridging". The "IP over ATM (IPoA)" option is selected. Below the radio buttons is a section titled "Encapsulation Mode" with a dropdown menu set to "LLC/SNAP-BRIDGING". At the bottom right of the page are "Back" and "Next" buttons.

3. In the **WAN IP Settings** page, change parameters as directed by your ISP, and then click **Next**.

The screenshot shows the Zhone router's web interface for the "WAN IP Settings" page. The left sidebar is the same as in the previous screenshot. The main content area is titled "WAN IP Settings" and contains the following text: "Enter information provided to you by your ISP to configure the WAN IP settings." Below this is a notice: "Notice: DHCP is not supported in IPoA mode. Changing the default gateway or the DNS effects the whole system. Configuring them with static values will disable the automatic assignment from other WAN connection." The configuration fields are: "WAN IP Address:" with a text box containing "192.2.1.1"; "WAN Subnet Mask:" with a text box containing "255.255.255.0"; a checkbox "Use the following default gateway:" which is unchecked; a sub-section "Use IP Address:" with a text box; a sub-section "Use WAN Interface:" with a dropdown menu set to "ipoa_0_7_45/ipa_0_7_45"; a checkbox "Use the following DNS server addresses:" which is unchecked; "Primary DNS server:" with a text box; and "Secondary DNS server:" with a text box. At the bottom right of the page are "Back" and "Next" buttons.

- In the **Network Address Translation Settings** page, make changes as directed by your ISP, and then click **Next**.

Z HONE

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

Network Address Translation Settings

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

Enable NAT

Enable Fullcone NAT

Public IP of NAT:

Enable Firewall

Enable IGMP Multicast, and WAN Service

Enable IGMP Multicast

Enable WAN Service

Service Name:

Enable MAC Clone

Enable MAC Clone

When the settings are complete, the next screen shows a **WAN Setup – Summary** screen displaying the WAN configurations made.

Z HONE

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

WAN Setup - Summary


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

PORT / VPI / VCI:	0 / 7 / 45
Connection Type:	IPoA
Service Name:	ipoa_0_7_45
Service Category:	UBR
IP Address:	192.2.1.1
Service State:	Enabled
NAT:	Disabled
Firewall:	Disabled
IGMP Multicast:	Enabled
Quality Of Service:	Disabled

Click "Save" to save these settings. Click "Back" to make any modifications.
NOTE: You need to reboot to activate this WAN interface and further configure services over this interface.

- Make sure that the settings on the **WAN Setup - Summary** screen match the settings provided by your ISP. If all settings are correct, click **Save** to save these settings; if not, click **Back** to make any modifications. If you want to change any item after saving, click **Edit** to make any modifications.
- Click **Save** to save the settings.

After the settings are saved, the below screen will follow displaying the WAN settings that you made with the option to **Add** or **Remove** any of the connections that you have made.



Device Info
Advanced Setup
WAN
 LAN
 Ethernet Mode
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 DSL
 Interface Group
 IPSec
 Certificate
 Wireless
 Diagnostics
 Management


Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
 Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Igmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	pppoa_0_0_35_1	ppp_0_0_35_1	PPPoA	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/3/38	Off	1	UBR	pppoe_0_3_38_1	ppp_0_3_38_1	PPPoE	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/5/42	Off	1	UBR	mer_0_5_42	nas_0_5_42	MER	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit
0/7/45	Off	1	UBR	ipoa_0_7_45	ipa_0_7_45	IPoA	Enabled	Disabled	Enabled	<input type="checkbox"/>	Edit

Connection Type | Bridging

1. Select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use, then click **Next**
2. In the Connection Type page, select **Bridging**, then click **Next**



Device Info
Advanced Setup
WAN
 LAN
 Ethernet Mode
 NAT
 Security
 Parental Control
 Quality of Service
 Routing
 DNS
 DSL
 Interface Group
 IPSec
 Certificate
 Wireless
 Diagnostics
 Management

Connection Type

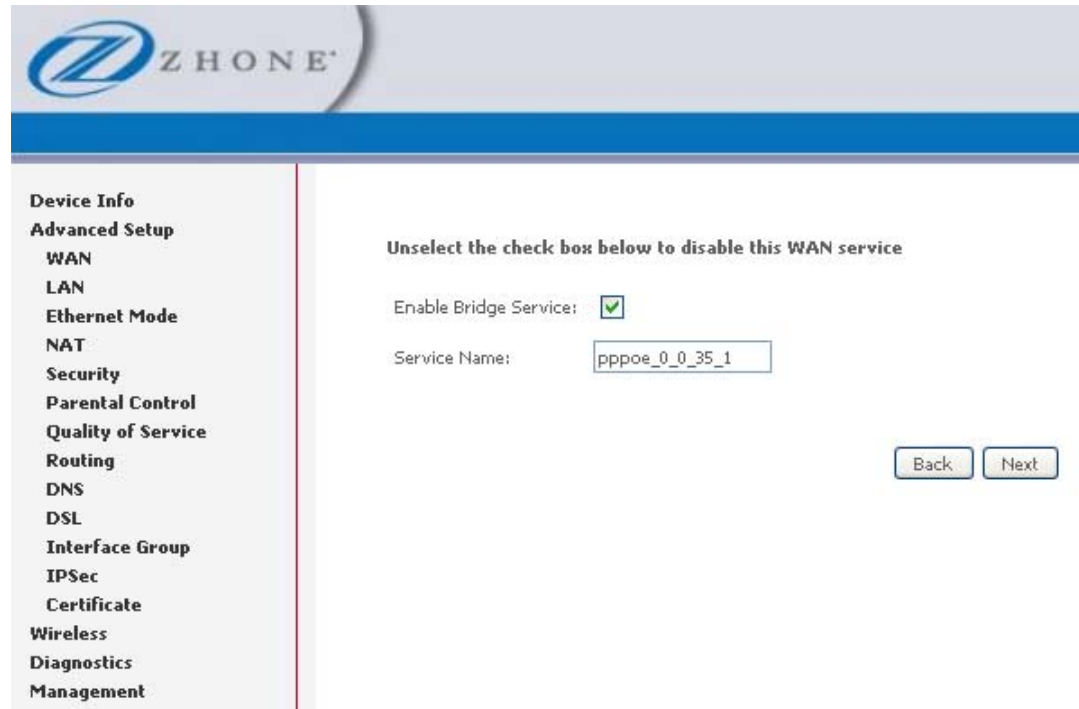
Select the type of network protocol for IP over Ethernet as WAN interface

PPP over ATM (PPPoA)
 PPP over Ethernet (PPPoE)
 MAC Encapsulation Routing (MER)
 IP over ATM (IPoA)
 Bridging

Encapsulation Mode

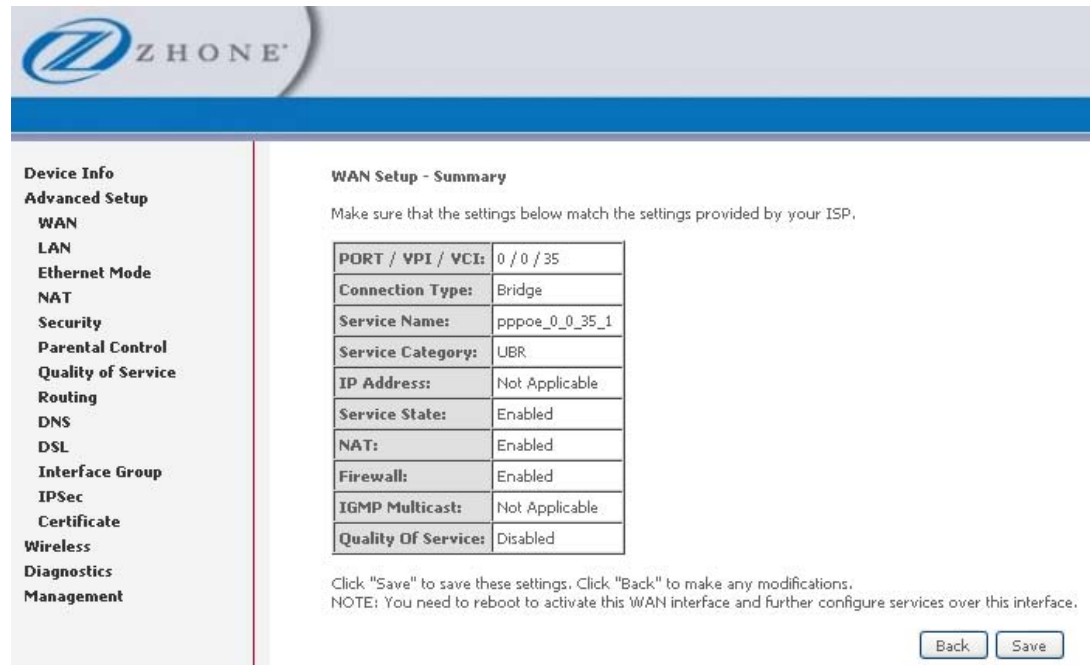
LLC/SNAP-BRIDGING ▾

The Bridge Service screen appears allowing you to disable bridge service if desired.



3. Check or uncheck **Enable Bridge Service**, and then click **Next**.

When the settings are complete, the next screen shows a **WAN Setup – Summary** screen displaying the WAN configurations made.



4. Click **Save** to save the settings.

After the settings are saved, the below screen will follow displaying the WAN settings that you made with the option to **Add** or **Remove** any of the connections that you have made.

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Icmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	br_0_0_35	nas_0_0_35	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit
0/3/38	Off	1	UBR	br_0_3_38	nas_0_3_38	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit

Add Remove Save/Reboot

Remove Function

If you want to delete a connection from the listed WAN setup, click the **Remove** check box next to the item, then click **Remove**.

Wide Area Network (WAN) Setup

Choose Add, Edit, or Remove to configure WAN interfaces.
Choose Save/Reboot to apply the changes and reboot the system.

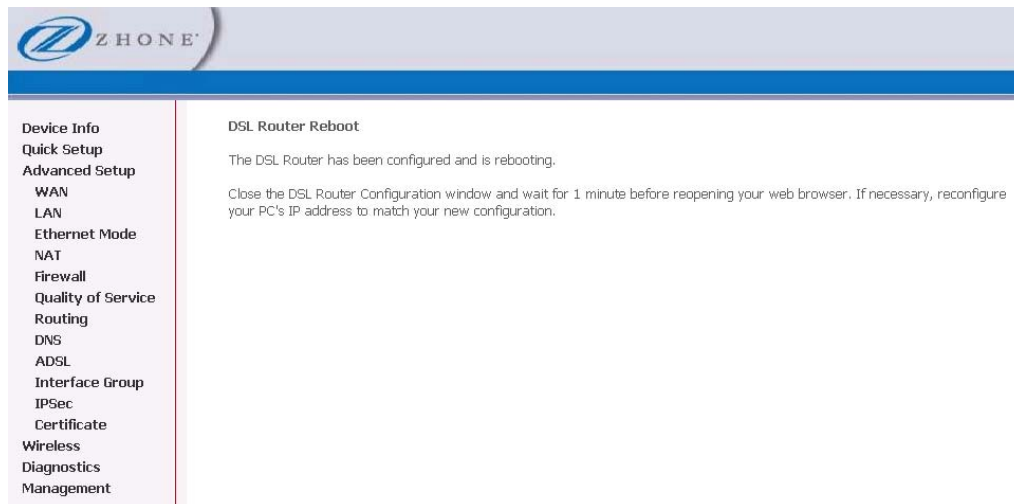
Port/Vpi/Vci	VLAN Mux	Con. ID	Category	Service	Interface	Protocol	Icmp	QoS	State	Remove	Edit
0/0/35	Off	1	UBR	br_0_0_35	nas_0_0_35	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit
0/3/38	Off	1	UBR	br_0_3_38	nas_0_3_38	Bridge	N/A	Disabled	Enabled	<input type="checkbox"/>	Edit

Add Remove Save/Reboot

Finish Function

When satisfied with the settings click **Finish**.

After selecting the **Finish** button, the **DSL Router Reboot** screen will appear. At this point, the router will reboot to save the changes made.



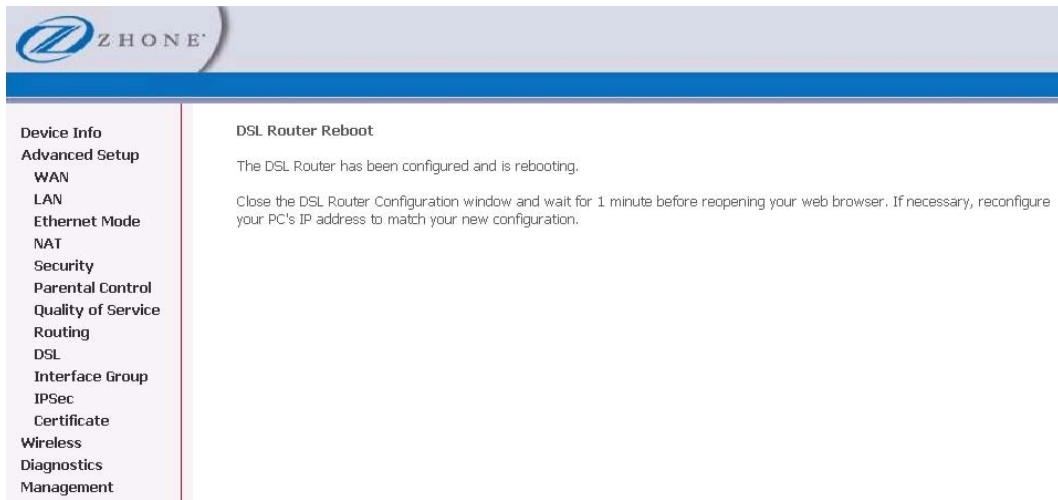
LAN Local Area Network (LAN) Setup

You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond to your LAN's IP Subnet. If you want the DHCP server to automatically assign IP addresses, then enable the DHCP server and enter the range of IP addresses that the DHCP server can assign to your computers. Disable the DHCP server if you would like to manually assign IP addresses.

The **Save** button only saves the LAN configuration data, but does not apply the configurations. Select the **Save/Reboot** button to save the LAN configuration data and reboot the router and apply the new configurations.

The screenshot shows the Zhone DSL Router web interface. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, WAN, LAN (highlighted in red), Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DSL, Interface Group, IPsec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled "Local Area Network (LAN) Setup". Below the title, there is a descriptive paragraph: "Configure the DSL Router IP Address and Subnet Mask for LAN interface. Save button only saves the LAN configuration data. Save/Reboot button saves the LAN configuration data and reboots the router to make the new configuration effective." The configuration fields are as follows: IP Address: 192.168.1.1; Subnet Mask: 255.255.255.0. There are three radio button options: "Enable IGMP Snooping" (checked), "Standard Mode" (selected), and "Blocking Mode". Below these are two radio button options for the DHCP server: "Disable DHCP Server" and "Enable DHCP Server" (selected). The "Enable DHCP Server" section includes fields for Start IP Address (192.168.1.2), End IP Address (192.168.1.254), Subnet Mask (255.255.255.0), and Leased Time (hour) (24). A note states: "Static IP Lease List: Please click on Save/Reboot button to make the new configuration effective. (A maximum 32 entries can be configured)". Below this note is a table with three columns: MAC Address, IP Address, and Remove. There are two buttons: "Add Entries" and "Remove Entries". At the bottom of the DHCP section, there is a radio button for "Enable DHCP Server Relay" with a corresponding "DHCP Server IP Address" field. At the very bottom, there is a checkbox for "Configure the second IP Address and Subnet Mask for LAN interface" and two buttons: "Save" and "Save/Reboot".

The following DSL Router Reboot screen appears after **Save / Reboot** is clicked.



Z H O N E

- Device Info
- Advanced Setup
 - WAN
 - LAN
- Ethernet Mode
- NAT
- Security
- Parental Control
- Quality of Service
- Routing
- DSL
- Interface Group
- IPSec
- Certificate
- Wireless
- Diagnostics
- Management

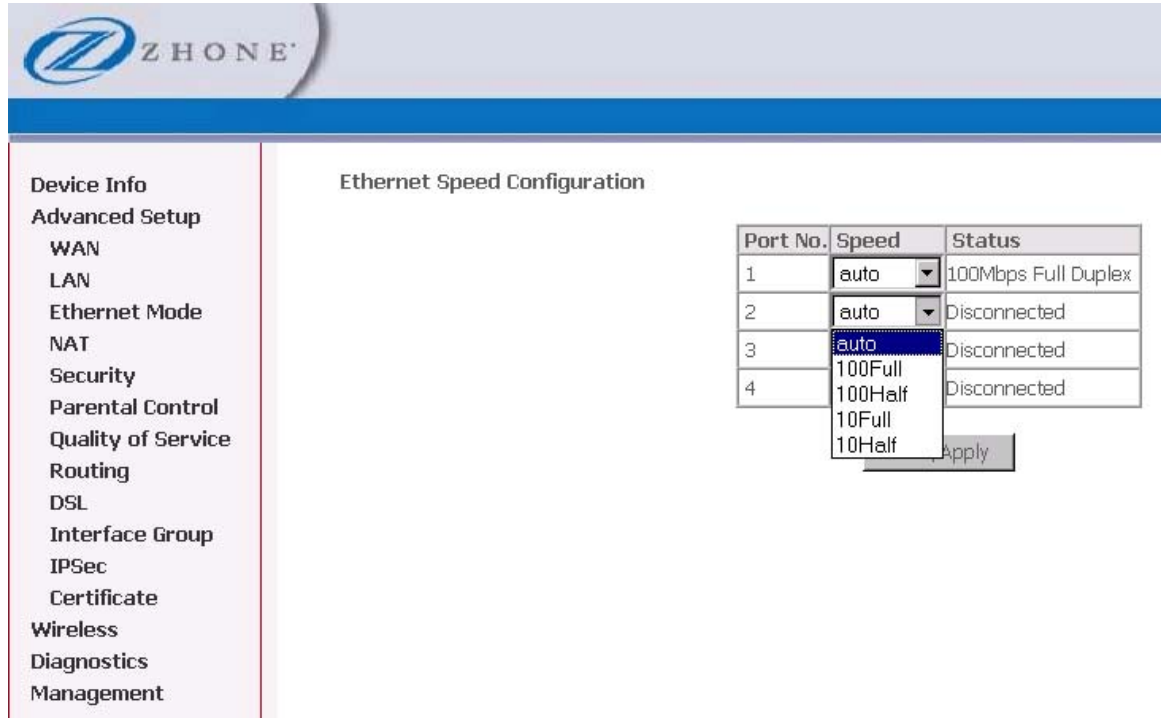
DSL Router Reboot

The DSL Router has been configured and is rebooting.

Close the DSL Router Configuration window and wait for 1 minute before reopening your web browser. If necessary, reconfigure your PC's IP address to match your new configuration.

Ethernet Mode

Ethernet mode allows you to select the speed of your Ethernet connection. Modes include—auto, 100 full, 100 half, 10 full and 10 half. If you select **auto** then the router will use the common mode with which all the connected interfaces can operate.



The screenshot displays the 'Ethernet Speed Configuration' page in the Zhone router's web interface. On the left is a navigation menu with options like Device Info, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DSL, Interface Group, IPsec, Certificate, Wireless, Diagnostics, and Management. The main content area shows a table with the following data:

Port No.	Speed	Status
1	auto	100Mbps Full Duplex
2	auto	Disconnected
3	auto	Disconnected
4	auto	Disconnected

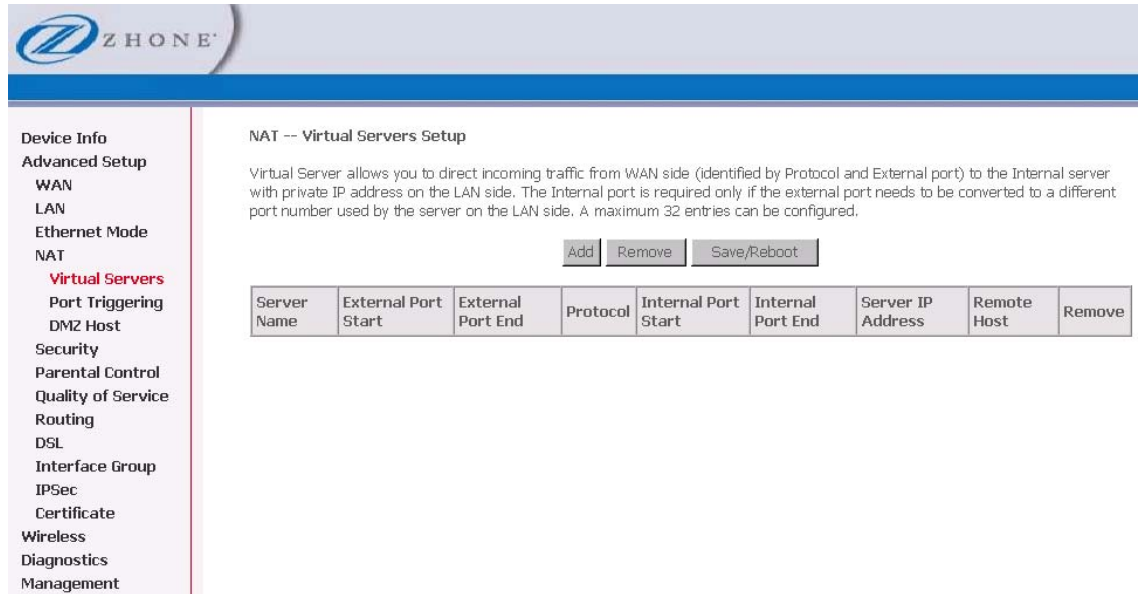
A dropdown menu is open for Port 3, showing the following options: auto, 100Full, 100Half, 10Full, and 10Half. An 'Apply' button is located below the table.

NAT

You can configure Virtual Servers, Port Triggering, and DMZ Host when NAT (Network Address Translation) is enabled.

Virtual Servers

A virtual server allows you to direct incoming traffic from the WAN side to a specific IP address on the LAN side. The following figure shows the screen that allows you to configure your virtual server(s).



To direct incoming traffic from a service (or other server):

1. Click **Add** to configure a virtual server.

2. Either select a service (by using the **Select a Service** dropdown) or select a custom server (by entering the IP address of the server in the **Custom Server** text box).

You can select a Service or make a new one.

3. Enter the IP address of the LAN side PC in the **Server IP Address** text box.
4. Click **Save / Apply** to submit the configuration.

The **NAT – Virtual Servers Setup** screen appears after you save your selection. To add additional virtual servers, click **Add**. If you need to remove any of the server names, select the check box and click on the **Remove** button.

Port Triggering

Click **Add** to add Port Triggering to your Internet application.

NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application	Trigger		Open		Remove		
	Name	Protocol	Port Range	Protocol		Port Range	
			Start	End	Start	End	

The **NAT – Port Triggering** screen appears when you click **Add** allowing you to select the application that you want to set the port settings for. After a selection has been made, click **Save / Apply** to save your settings.

NAT -- Port Triggering


Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall 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

Application Name:
 Select an application:
 Custom application:

Trigger Port	Start	Trigger	Open Port	Start	Open Port	End	Open Protocol
							TCP
							TCP
							TCP
							TCP
							TCP
							TCP
							TCP
							TCP
							TCP

The **NAT – Port Triggering Setup** screen appears after you save your selections. You will be able to add or remove selections made by clicking on the **Add** and **Remove** buttons.



Device Info
Advanced Setup
 WAN
 LAN
Ethernet Mode
 NAT
 Virtual Servers
Port Triggering
 DMZ Host
 Security
 Parental Control
 Quality of Service
 Routing
 DSL
 Interface Group
 IPSec
 Certificate
 Wireless
 Diagnostics
 Management


NAT -- Port Triggering Setup

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Application	Trigger		Open			Remove	
Name	Protocol	Port Range		Protocol	Port Range		
		Start	End		Start	End	
Aim Talk	TCP	4099	4099	TCP	5191	5191	<input type="checkbox"/>

DMZ Host

You can define the IP address of the DMZ Host on this screen. Enter the IP address and click **Save / Apply**.



Device Info
Advanced Setup
 WAN
 LAN
Ethernet Mode
 NAT
 Virtual Servers
Port Triggering
DMZ Host
 Security
 Parental Control
 Quality of Service
 Routing
 DSL
 Interface Group
 IPSec
 Certificate
 Wireless
 Diagnostics
 Management

NAT -- DMZ Host

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.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

DMZ Host IP Address:

MAC Filtering

MAC filtering can forward or block traffic by MAC address. You can change the policy or add settings to the MAC filtering table in the **MAC Filtering Setup** screen.

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
MAC Filtering
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

MAC Filtering Setup

MAC Filtering Global Policy: **FORWARDED**

MAC Filtering is only effective on ATM PVCs 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.

Choose Add or Remove to configure MAC filtering rules.

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Remove
---------	----------	-----------------	------------	-----------------	--------

If you click **Change Policy**, a confirmation dialog allows you to verify your change.

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
MAC Filtering
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

Change MAC Filtering Global Policy

WARNING: Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Are you sure you want to change MAC Filtering Global Policy from **FORWARDED** to **BLOCKED** ?

To add a setting to the MAC filtering table, enter the **Source** and **Destination MAC** address, and select protocol type, frame direction, and WAN interface. Click **Save/Apply** to save the MAC filter.

ZHONE

Device Info
Advanced Setup
 WAN
 LAN
 Ethernet Mode
 NAT
Security
 MAC Filtering
 Parental Control
 Quality of Service
 Routing
 DSL
 Interface Group
 IPSec
 Certificate
Wireless
 Diagnostics
 Management

Add MAC Filter

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.

Protocol Type:

Destination MAC Address:

Source MAC Address:

Frame Direction:

WAN Interfaces (Configured in Bridge mode only)

Select All
 br_0_0_35/nas_0_0_35

When you **Save / Apply** the IP filter, the **MAC Filtering Setup** screen appears. The **MAC Filtering Setup** screen lists the MAC filters, including filters which were added from the previous screen.

You can view, add or delete MAC filters. The **Remove** button appears only when you have an existing IP filter already set up.

Parental Control

Use the Parental Control feature to restrict the days and times a particular device is allowed to access the Internet.

To setup parental controls

1. Click **Add** to set up the restrictions.

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
URL Filter
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

Time of Day Restrictions -- A maximum 16 entries can be configured.

Username	MAC	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start	Stop	Remove
----------	-----	-----	-----	-----	-----	-----	-----	-----	-------	------	--------

The **Add Parental Control** screen appears.

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
URL Filter
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

Time of Day Restriction

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".

User Name

Browser's MAC Address
 Other MAC Address
(xx:xx:xx:xx:xx:xx)

Days of the week Mon Tue Wed Thu Fri Sat Sun
Click to select

Start Blocking Time (hh:mm)
End Blocking Time (hh:mm)

2. Enter a **User Name** to identify the target of the restrictions.
3. Enter the MAC address of the network adapter to be restricted, and, optionally, another MAC address.
4. Select the days of the week the restriction is in force.
5. Specify the start and end times the restriction is in force. Use the form hh:mm, where 23:59, for example, is one minute before midnight.
6. Click **Save / Apply** to save the settings and to continue.

URL Filter

Access to websites can be blocked by creating a URL filter. Two types of lists can be created, either an exclude or include list.

1. Click **Add** to continue to the next screen to enter the URL address.

The screenshot shows the Zhone router's web interface. The left sidebar contains a menu with the following items: Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, **URL Filter** (highlighted in red), Quality of Service, Routing, DSL, Interface Group, IPSec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled "URL Filter -- A maximum 100 entries can be configured." Below the title, there are two radio buttons for "URL List Type": "Exclude" and "Include". To the right, there are three buttons: "Address", "Port", and "Remove". Below these, there are two buttons: "Add" and "Remove".

2. In **URL Address** enter the URL address; in **Port Number** enter the port number and click **Save / Apply**.

If no port number is entered, the the default 80 port will be applied. Continue this process until all the necessary websites are entered.

The screenshot shows the Zhone router's web interface for adding a URL filter. The left sidebar is the same as in the previous screenshot, with "URL Filter" highlighted. The main content area is titled "Parental Control -- URL Filter Add". Below the title, there is a text prompt: "Enter the URL address and port number then click 'Save/Apply' to add the entry to the URL filter." There are two input fields: "URL Address:" and "Port Number:". Below the "Port Number:" field, there is a note: "(Default 80 will be applied if leave blank.)". At the bottom right, there is a "Save/Apply" button.

Quality of Service

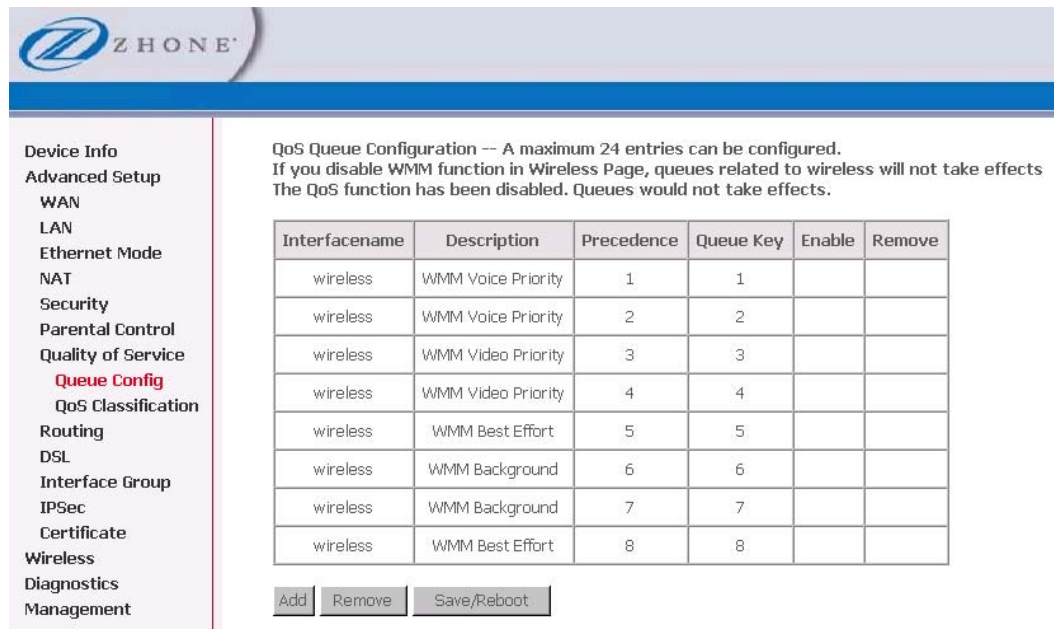
You can configure the Quality of Service to apply different priorities to traffic on the router.

Queue Config

In the Queue Config page you can enable a queue for a network interface. Each interface associated with QoS is allocated three queues. Lower Queue Precedence values denote a higher priority for the queue, so “1” has higher priority than “2.”

To associate an interface with QoS:

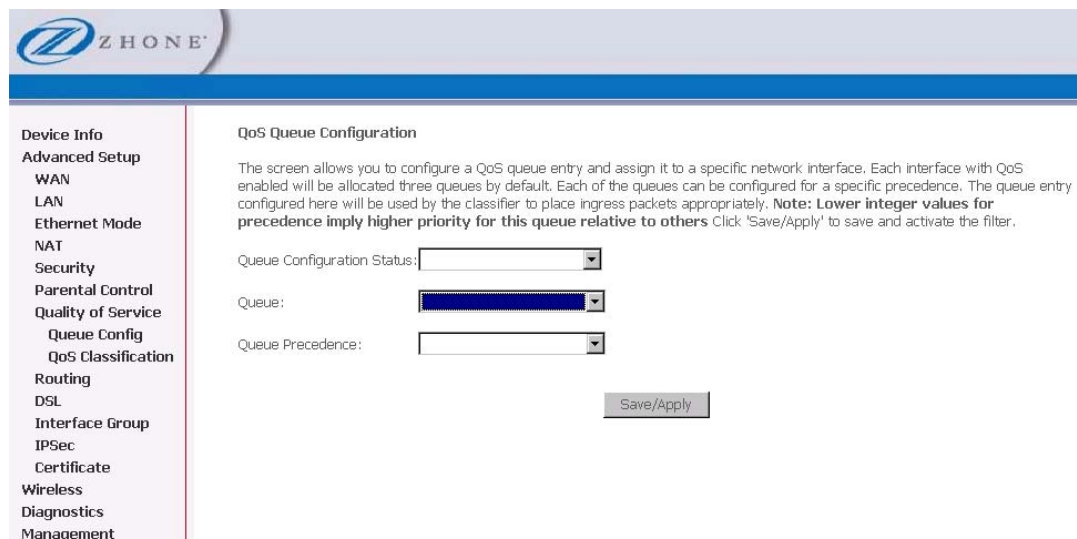
1. From the **Queue Config** page, click **Add**.



The screenshot shows the Zhone Queue Configuration page. On the left is a navigation menu with options like Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Queue Config (highlighted), QoS Classification, Routing, DSL, Interface Group, IPSec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled "QoS Queue Configuration -- A maximum 24 entries can be configured. If you disable WMM function in Wireless Page, queues related to wireless will not take effects. The QoS function has been disabled. Queues would not take effects." Below this is a table with columns: Interfacename, Description, Precedence, Queue Key, Enable, and Remove. The table contains 8 entries for the "wireless" interface, with descriptions ranging from "WMM Voice Priority" to "WMM Best Effort" and precedence values from 1 to 8. At the bottom of the table are buttons for "Add", "Remove", and "Save/Reboot".

Interfacename	Description	Precedence	Queue Key	Enable	Remove
wireless	WMM Voice Priority	1	1		
wireless	WMM Voice Priority	2	2		
wireless	WMM Video Priority	3	3		
wireless	WMM Video Priority	4	4		
wireless	WMM Best Effort	5	5		
wireless	WMM Background	6	6		
wireless	WMM Background	7	7		
wireless	WMM Best Effort	8	8		

2. In the Add QoS Queue page enable the queue by selecting **Enable** from the **Queue Configuration Status** drop down.



The screenshot shows the Zhone Add QoS Queue page. The navigation menu is the same as in the previous screenshot. The main content area is titled "QoS Queue Configuration" and contains a paragraph explaining the configuration process. Below the text are three dropdown menus: "Queue Configuration Status:", "Queue:", and "Queue Precedence:". A "Save/Apply" button is located at the bottom right of the configuration area.

3. Select the interface from the **Queue** drop down.
4. Set the priority for the queue from the **Queue Precedence** drop down
5. Click **Save/Apply**.

QoS Classification

You can configure the Quality of Service to apply different priorities to traffic on the router.

Quality of Service Setup

Choose Add or Remove to configure network traffic classes.

If you disable WMM function in Wireless Page, classification related to wireless will not take effects
The QoS function has been disabled. Classification rules would not take effects.

MARK				TRAFFIC CLASSIFICATION RULES										
Class Name	DSCP Mark	Queue ID	802.1P Mark	Lan Port	Protocol	DSCP	Source Addr./Mask	Source Port	Dest. Addr./Mask	Dest. Port	Source MAC Addr./Mask	Destination MAC Addr./Mask	802.1P	Ord
<input type="button" value="Add"/> <input type="button" value="Save/Apply"/>														

The **Add Network Traffic Class Rule** screen allows you to add a network traffic class rule.

To add a rule:

1. *In the **Quality of Service—QoS Classification** screen, click **Add**.*

Add Network Traffic Class Rule

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

Traffic Class Name:
Rule Order:
Rule Status:

Assign ATM Priority and/or DSCP Mark for the class
If non-blank value is selected for 'Assign Differentiated Services Code Point (DSCP) Mark', the corresponding DSCP byte in the IP header of the upstream packet is overwritten by the selected value.

Assign Classification Queue:
Assign Differentiated Services Code Point (DSCP) Mark:
Mark 802.1p if 802.1q is enabled:

Specify Traffic Classification Rules
Enter the following conditions either for IP level, SET-1, or for IEEE 802.1p, SET-2.

SET-1
Physical LAN Port:
Protocol:
Differentiated Services Code Point (DSCP) Check:
 IP Address
Source Subnet Mask:
UDP/TCP Source Port (port or port:port):
Destination IP Address:
Destination Subnet Mask:
UDP/TCP Destination Port (port or port:port):
Source MAC Address:
Source MAC Mask:
Destination MAC Address:
Destination MAC Mask:

SET-2
802.1p Priority:

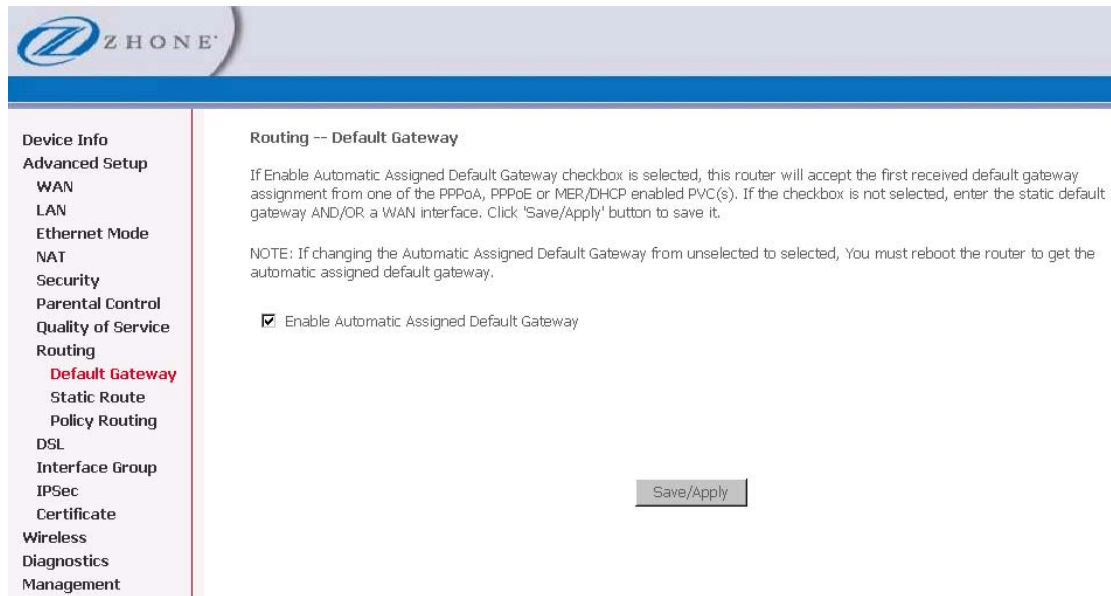
2. *In the **Add Network Traffic Class Rule** screen give a name to this traffic class.*
3. *Assign a priority level—low, medium, and high—to this traffic class.*
4. *Select an IP precedence from the 0-7 range.*
5. *Enter an IP Type of Service from the following selections—*
 - **Normal Service**
 - **Minimize Cost**
 - **Maximize Reliability**
 - **Maximize Throughput**
 - **Minimize Delay**
6. *Enter the traffic conditions for the class such as the protocol (TCP / UDP, TCP, UDP, or ICMP) to be used.*
7. *Click **Save / Apply** to save the settings.*

Routing

Under the Routing heading you assign a default gateway, create a routing table (in Static Route), create routing policy rules, and activate Routing Information Protocol (RIP) on the device.

Default Gateway

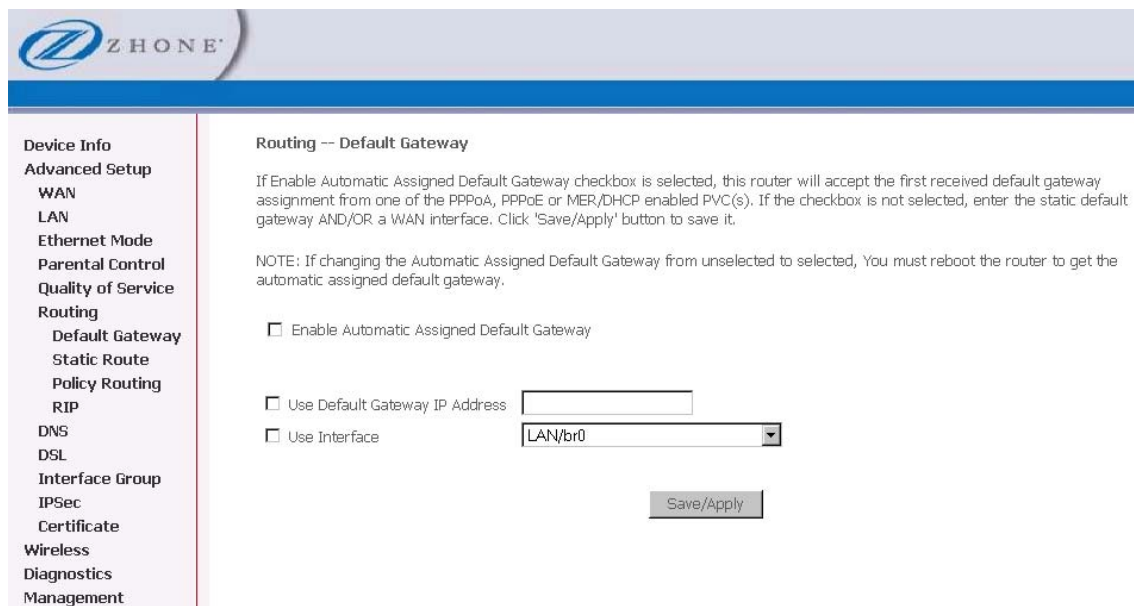
You can enable automatic assigned default gateway on the Routing – Default Gateway screen. By default, the **Enable Automatic Assigned Default Gateway** checkbox is checked.



The screenshot shows the Zhone web interface. On the left is a navigation menu with categories: Device Info, Advanced Setup (WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing), DSL, Interface Group, IPSec, Certificate, Wireless, Diagnostics, and Management. Under the 'Routing' category, 'Default Gateway' is highlighted in red. The main content area is titled 'Routing -- Default Gateway'. It contains a paragraph explaining that if the 'Enable Automatic Assigned Default Gateway' checkbox is selected, the router will accept the first received default gateway assignment from one of the PPPoA, PPPoE or MER/DHCP enabled PVC(s). A note states that if this checkbox is changed from unselected to selected, the router must be rebooted. The checkbox 'Enable Automatic Assigned Default Gateway' is checked. A 'Save/Apply' button is located at the bottom right of the configuration area.

To enable **Automatic Assigned Default Gateway** leave the checkbox checked. To disable **Automatic Assigned Default Gateway** uncheck the checkbox.

If you change the automatic assigned default gateway address, you must reboot the router to be assigned a new default gateway IP address.

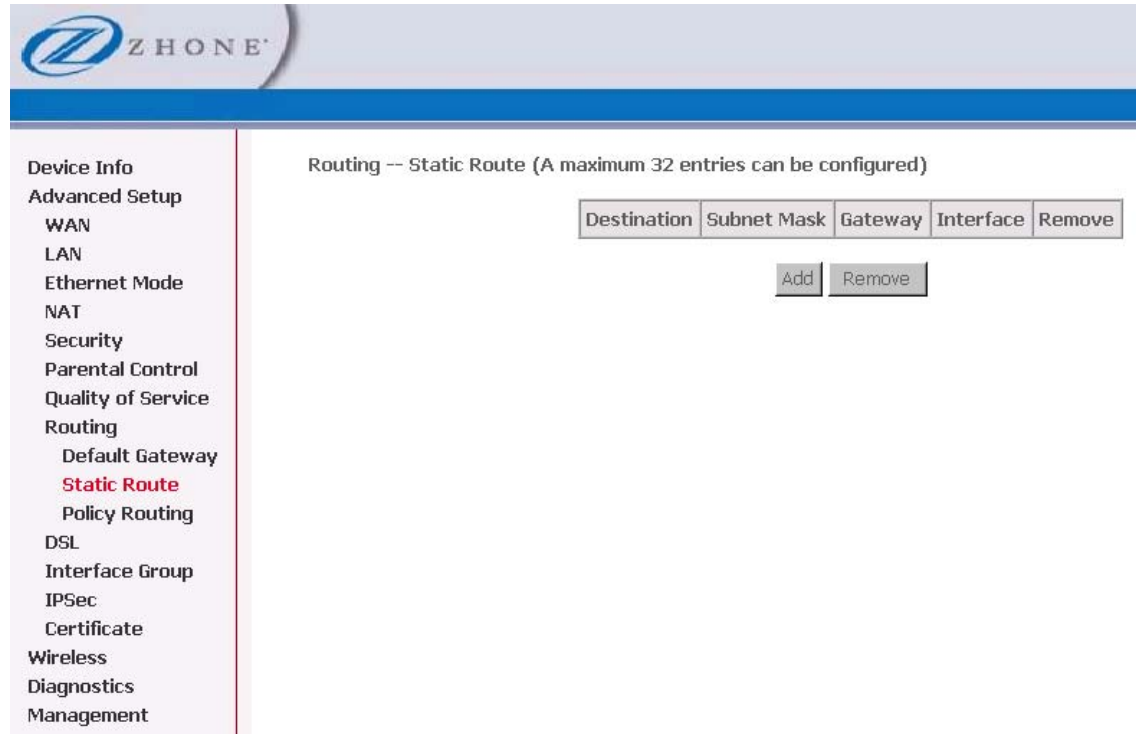


This screenshot shows the same Zhone web interface as the previous one, but with different settings. The 'Enable Automatic Assigned Default Gateway' checkbox is now unchecked. Below it, the 'Use Default Gateway IP Address' checkbox is also unchecked, and the 'Use Interface' checkbox is checked. A text input field is present next to 'Use Default Gateway IP Address', and a dropdown menu next to 'Use Interface' is set to 'LAN/br0'. The 'Save/Apply' button remains at the bottom right.

Static Route

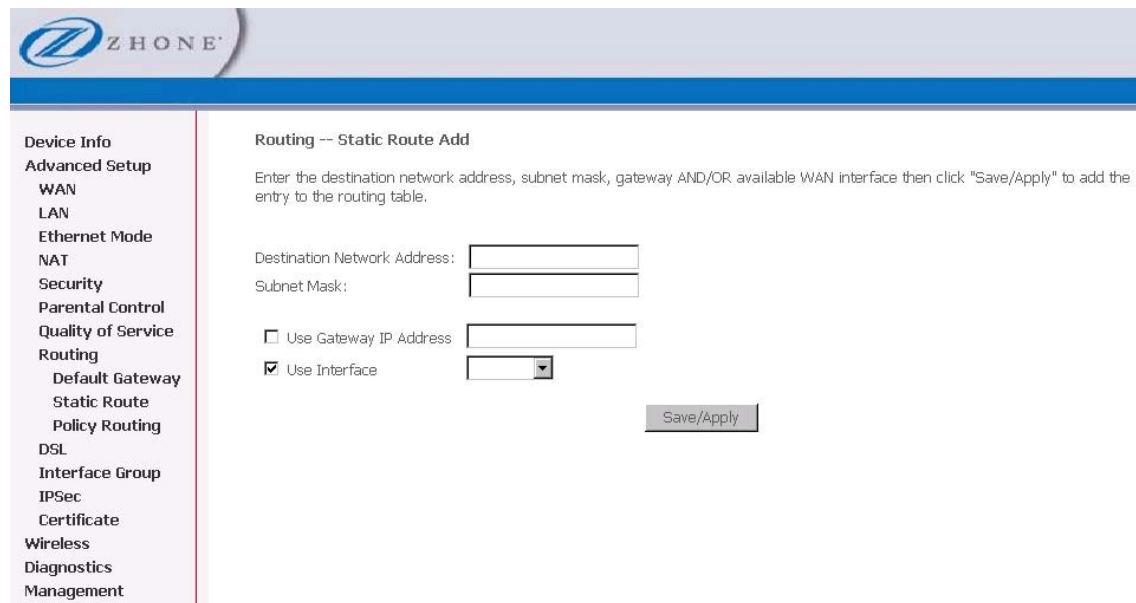
To add a routing table use the Static Route page. A maximum of 32 entries can be configured.

Click **Add**.



The screenshot shows the Zhone router configuration interface. The left sidebar contains a menu with the following items: Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing (highlighted), Default Gateway, Static Route (highlighted in red), Policy Routing, DSL, Interface Group, IPSec, Certificate, Wireless, Diagnostics, and Management. The main content area is titled "Routing -- Static Route (A maximum 32 entries can be configured)". It features a table with columns: Destination, Subnet Mask, Gateway, Interface, and Remove. Below the table are two buttons: "Add" and "Remove".

Enter the route information and then save and apply your configurations.



The screenshot shows the Zhone router configuration interface for adding a static route. The left sidebar is identical to the previous screenshot, with "Static Route" highlighted in red. The main content area is titled "Routing -- Static Route Add". It contains the following text: "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." Below this text are four input fields: "Destination Network Address:" (text box), "Subnet Mask:" (text box), " Use Gateway IP Address" (checkbox with text box), and " Use Interface" (checkbox with dropdown menu). A "Save/Apply" button is located at the bottom right of the form.

Policy Route

The policy routing feature allows the administrator to have more control over how packets should flow through the modem and into their networks. The feature allows administrator to route IP packets according to their Source Interface; Source/Destination IP address/subnets; IP Protocols; Source/Destination Ports to specific Gateway address and/or Gateway Interfaces.

Policy Routing Setting -- A maximum 8 entries can be configured.

Policy Name	Source Interface	Protocol	Source Address / Mask	Source Port	Dest. Address / Mask	Dest. Port	Gateway Address	Gateway Interface	Remove
-------------	------------------	----------	-----------------------	-------------	----------------------	------------	-----------------	-------------------	--------

To add a policy routing rule:

1. **Click Add.**

Routing -- Policy Route Add

Enter the policy name, policies, and WAN interface then click "Save/Apply" to add the entry to the policy routing table.
Note: If selected "MER" as WAN interface, gateway IP address must be configured.

Policy Name:

Source Interface:

Protocol:

Source IP Address:

Source Subnet Mask:

UDP/TCP Source Port (port or port:port):

Destination IP Address:

Destination Subnet Mask:

UDP/TCP Destination Port (port or port:port):

Gateway IP Address:

Gateway Interface:

2. **Enter a unique name for the rule in the *Rule Name* text box.**
3. **Select the interface to associate with the rule from the *Source Interface* drop down**

4. Select the appropriate protocol and define other parameters for the routing rule:
 - **Source and/or Destination address and/or Subnet Mask**
 - **UDP/TCP Source or Destination port.**
 - **Gateway address or Interface (These can be Active PVCs or Port Mapping Groups)**
5. Click **Save/Apply**.

DSL

The DSL settings page contains sections—modulation and capability—that should be specified by your ISP. Consult with your ISP to select the correct settings for each.

Click **Save / Apply** if you are finished or click on **Advanced Settings** if you want to configure more advanced settings.

Modulation Methods

The following modulation methods are supported by the 6219-X1 router:

- **G.dmt Enabled**
- **G.lite Enabled**
- **T1.413 Enabled**
- **ADSL Enabled**
- **Annex L Enabled**
- **ADSL2+ Enabled.**

Do not change this setting unless so directed by your ISP.

Capability

The following are included under Capability:

- **Bitswap Enable**
- **SRA Enable** (Seamless Rate Adaptation)

Do not change these settings unless so directed by your ISP.

DSL Advanced Settings

Do not change the **DSL Advanced Settings** unless so directed by your ISP.

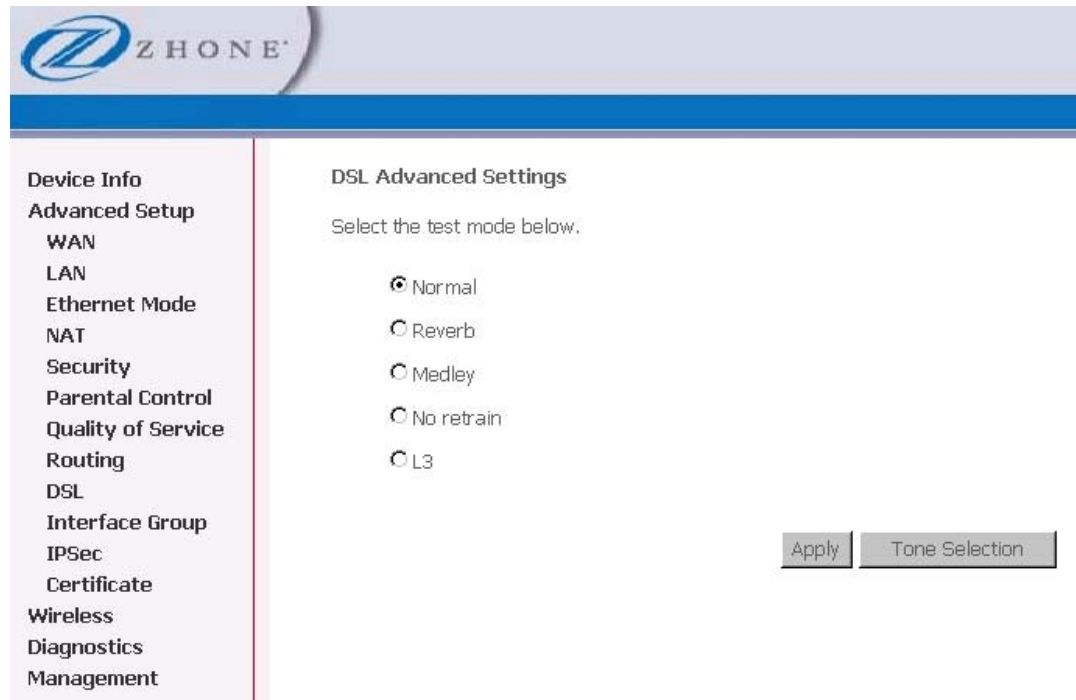
To view the DSL Advanced Settings screen, click **Advanced Settings** button on the **DSL Settings** screen.

The test mode can be selected from the DSL Advanced Settings page. There are five test modes between the router and your ISP:

- **Normal test:** Puts the router in a test mode in which it only sends a Normal signal.
- **Reverb test:** Puts the router in a test mode in which it only sends a Reverb signal.
- **Medley test:** Puts the router in a test mode in which it only sends a Medley signal.
- **No Retrain:** In this mode the router will try to establish a connection as in normal mode, but once the connection is up it will not retrain if the signal is lost.
- **L3:** Puts the router into the L3 power state.

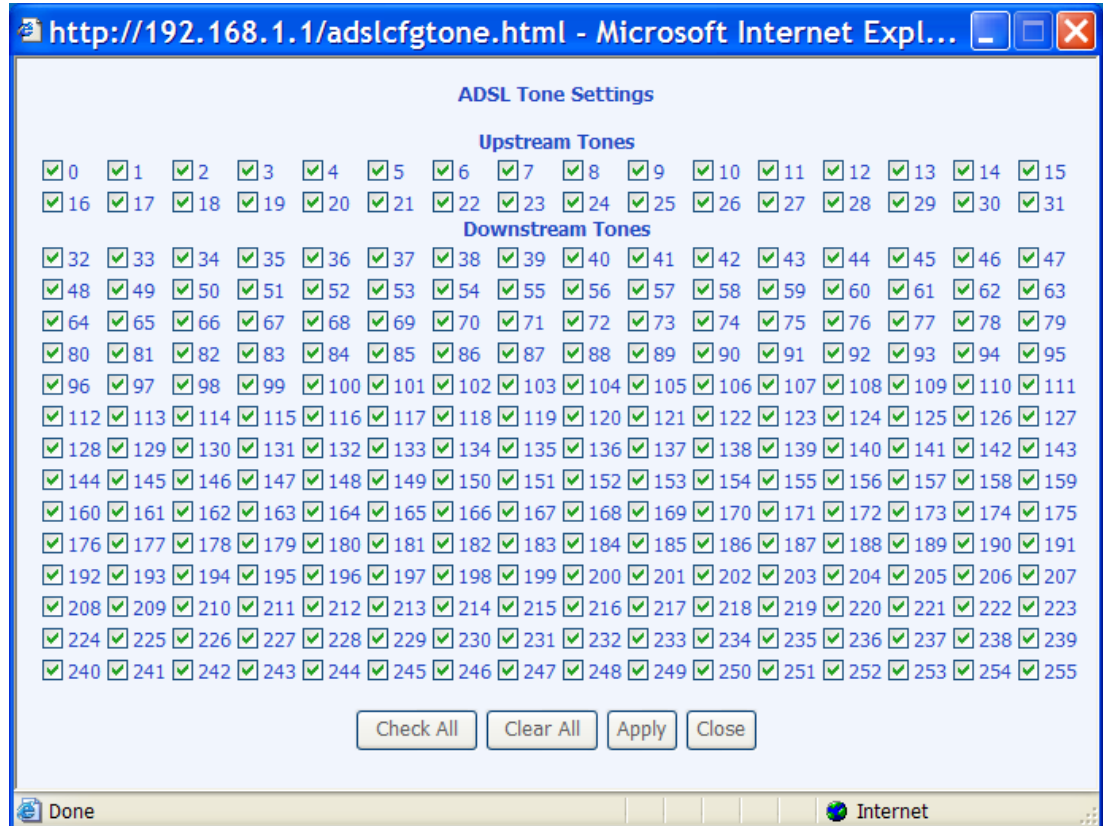
To run a test:

1. Select a test mode and click **Apply**.



2. **Click Tone Selection.**

The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart. With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream. Do not change these settings unless directed by your ISP.

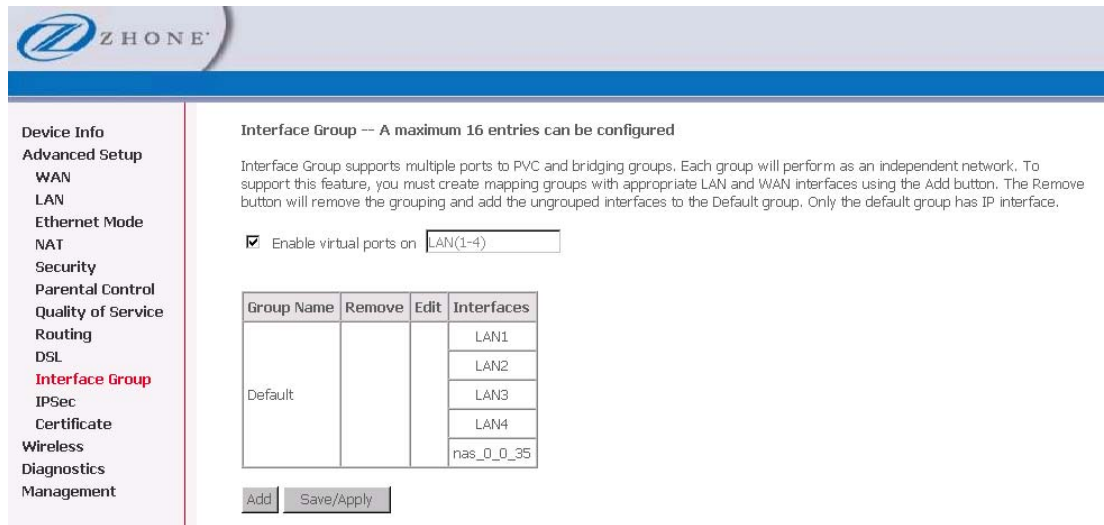


Interface Group

The interface group feature allows you to open ports to allow certain Internet applications on the WAN side to pass through the firewall and enter your LAN. To use this feature, mapping groups should be created.

To create a new mapping group:

1. Click **Add** button



Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Wireless
Diagnostics
Management

Interface Group -- A maximum 16 entries can be configured

Interface Group supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

Enable virtual ports on

Group Name	Remove	Edit	Interfaces
Default			LAN1
			LAN2
			LAN3
			LAN4
			nas_0_0_35

If you need to edit an entry, then click **Edit** for that group.

After clicking the **Add** button, the **Port Mapping Configuration** screen appears

2. Enter a unique Group name.

Interface Group Configuration

To create a new interface group:

1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.
2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses
3. Click Save/Apply button to make the changes effective immediately

Note that the selected interfaces will be removed from their existing groups and added to the new group.

IMPORTANT If a vendor ID is configured for a specific client device, please **REBOOT** the client device attached to the modem to allow it to obtain an appropriate IP address.

Group Name:

Grouped Interfaces **Available Interfaces**

LAN1
LAN2
LAN3
LAN4
nas_0_0_35

->
<-

Automatically Add Clients With the following DHCP Vendor IDs

3. Select interfaces from the available interface list and add them to the grouped interface list using the arrow buttons to create the required mapping of the ports.
4. Click **Save/Apply**.

IPSec

Internet Protocol Security (IPSec) allows you to set up secure tunnel access between two IP addresses. Encryption and key exchange make this a secure way to access remote networks. Contact your ISP for the necessary information to correctly configure this connection.

The screenshot shows the Zhone router's web interface. The top header features the Zhone logo. On the left is a navigation menu with options: Device Info, Advanced Setup, WAN, LAN, Ethernet Mode, NAT, Security, Parental Control, Quality of Service, Routing, DSL, Interface Group, **IPSec**, Certificate, Wireless, Diagnostics, and Management. The main content area is titled "IPSec Tunnel Mode Connections" and includes the instruction: "Add, edit or remove IPSec tunnel mode connections from this page." Below this is a table with columns: Enable, Connection Name, Remote Gateway, Local Addresses, and Remote Addresses. A button labeled "Add New Connection" is positioned below the table.

Click **Add New Connection** to access the IPSec Settings screen to enter your configurations.

The screenshot shows the "IPSec Settings" configuration page. The left navigation menu is identical to the previous page, with "IPSec" highlighted. The main content area is titled "IPSec Settings" and contains the following fields and options:

- IPSec Connection Name:
- Remote IPSec Gateway Address:
- Tunnel access from local IP addresses: (dropdown)
- IP Address for VPN:
- IP Subnetmask:
- Tunnel access from remote IP addresses: (dropdown)
- IP Address for VPN:
- IP Subnetmask:
- Key Exchange Method: (dropdown)
- Authentication Method: (dropdown)
- Pre-Shared Key:
- Perfect Forward Secrecy: (dropdown)

At the bottom of the settings area are two buttons: "Show Advanced Settings" and "Save / Apply".

The **Show Advanced Settings** button at the bottom of the screen provides additional encryption settings.

ZHONE

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Local
Trusted CA
Wireless
Diagnostics
Management

IPSec Settings

IPSec Connection Name: new connection
Remote IPSec Gateway Address: 0.0.0.0

Tunnel access from local IP addresses: Subnet
IP Address for VPN: 0.0.0.0
IP Subnetmask: 255.255.255.0

Tunnel access from remote IP addresses: Subnet
IP Address for VPN: 0.0.0.0
IP Subnetmask: 255.255.255.0

Key Exchange Method: Auto(IKE)
Authentication Method: Pre-Shared Key
Pre-Shared Key: key
Perfect Forward Secrecy: Disable

Advanced IKE Settings: Hide Advanced Settings

Phase 1
Mode: Main
Encryption Algorithm: 3DES
Integrity Algorithm: MD5
Select Diffie-Hellman Group for Key Exchange: 1024bit
Key Life Time: 3600 Seconds

Phase 2
Encryption Algorithm: 3DES
Integrity Algorithm: MD5
Select Diffie-Hellman Group for Key Exchange: 1024bit
Key Life Time: 3600 Seconds

Save / Apply

Certificate

Use the Certificate screen to add, view, or remove a certificate for use by a peer to verify your identity. A maximum of four certificates can be stored. You can add a certificate either by creating a new one or importing an existing one from a location where one is stored.



Note: Certificates are used with TR-069. Firmware that does not support TR-069 will not support certificates..

Local

A local certificate identifies your device over the network.

To apply for a certificate:

1. Click **Create Certificate Request**

Device Info
Advanced Setup
WAN
LAN
Ethernet Mode
NAT
Security
Parental Control
Quality of Service
Routing
DSL
Interface Group
IPSec
Certificate
Local
Trusted CA
Wireless
Diagnostics
Management

Local Certificates

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity. Maximum 4 certificates can be stored.

Name	In Use	Subject	Type	Action
------	--------	---------	------	--------

Create Certificate Request Import Certificate

If you have an existing certificate, click on **Import Certificate** to retrieve it.

The Create new certificate request screen allows you to request a new certificate request.

2. *Follow the screens that appear to configure a new certificate.*
3. *Click **Apply** to submit the request.*

If you have a certificate already, you can simply import the certificate by pasting the certificate content and private key into the space provided. Click **Apply** to submit the request to import the certificate.

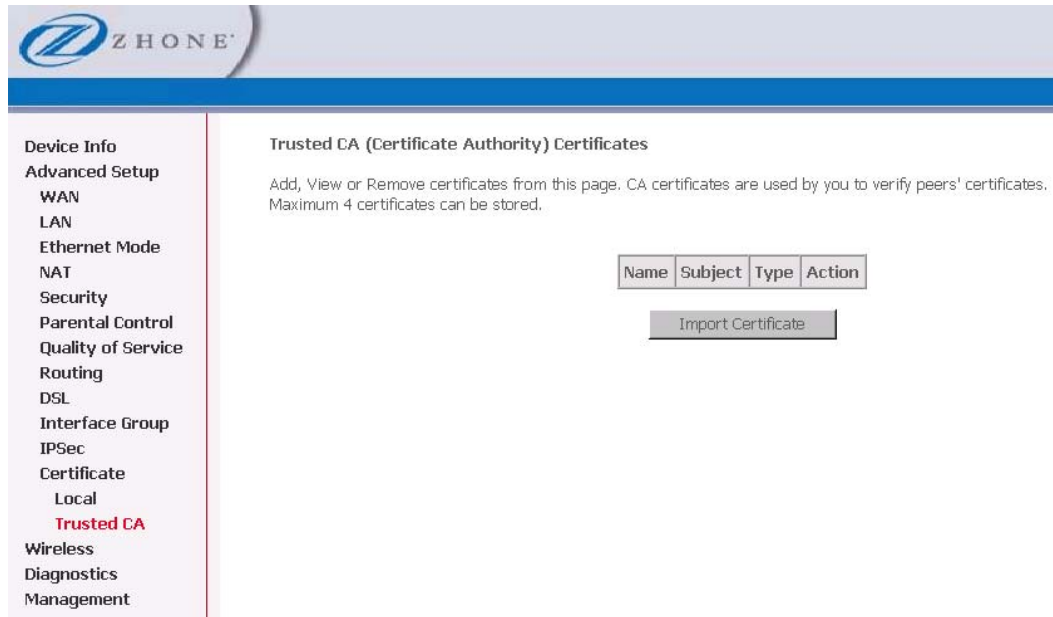
Trusted CA

The trusted certificate authority (CA) allows you to verify the certificates of your peers.

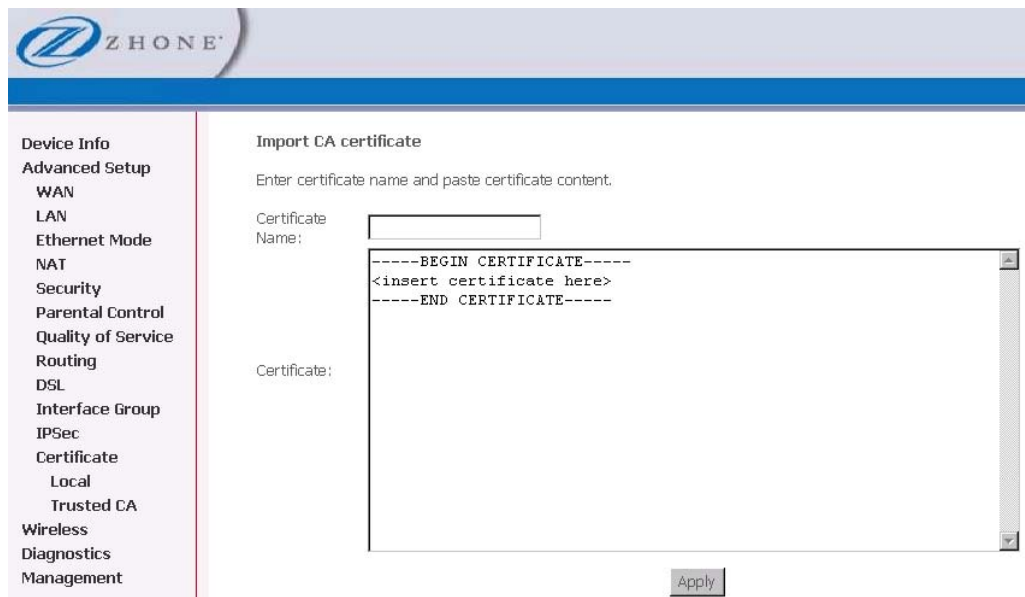
The **Trusted CA (Certificate Authority) Certificates** screen also allows you to view certificates. You can store up to 4 certificates.

To Import a certificate

1. Click on **Import Certificate**



2. Enter the certificate name in the Certificate text box.



3. In the Certificate text window paste the content of the certificate.
4. Click **Apply**.

Chapter 5 Wireless

The router's wireless feature can be configured to your needs. Sections covered under the wireless section include

- **Basic**
- **Security**
- **MAC filter**
- **Wireless bridge**
- **Advanced**
- **Quality of service and station info.**

Basic

The **Wireless – Basic** screen allows you to enable or disable wireless functionality. You can also hide the access point so others cannot see your ID on the network. If you enable wireless, be sure to enter an SSID, your wireless network name and select the country that you are in.

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN 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. Click "Apply" to configure the basic wireless options.

Enable Wireless

Disable Wireless If DSL Line is Down

Hide Access Point

Clients Isolation

Disable WMM Advertise

SSID:

BSSID:

Country:

Max Clients:

If you select **Wireless disabled is DSL link is down** (which is disabled by default) when **Enable Wireless** is selected, the wireless connection will automatically be disabled if the DSL WAN link goes down.

Hide Access Point does not allow others to see your ID. The router is hidden from active scans.

With **Clients Isolation** selected wireless clients will be isolated from one another and are not allowed to share information over the LAN.

With **Disable WMM Advertise** selected, the wireless router does not advertise for 802.11b/g devices to connect for voice over WiFi services. When WMM (WiFi Multi-media) advertise is

enabled (the selection is unchecked) the access point sends out WPA-PSK information for WiFi handsets.

When you enable a wireless bridge, you can also see the other wireless bridges by SSID and BSSID (MAC address).

Z H O N E

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Save/Apply" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Security

The **Wireless – Security** screen allows you to select the network authentication method and to enable or disable WEP encryption.

Note that depending on the network authentication that is selected, the screen will change accordingly so additional fields can be configured for the specific authentication method.

Network authentication methods include the following—

- **Open** — anyone can access the network. The default is a disabled WEP encryption setting

The screenshot shows the Zhone Wireless Security configuration page. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Wireless (selected), Basic, Security (highlighted in red), MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area is titled "Wireless -- Security" and includes the following text: "This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually." Below this is the "Manual Setup AP" section, which states: "You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click 'Save/Apply' when done." The configuration fields are: "Select SSID:" with a dropdown menu set to "wireless"; "Network Authentication:" with a dropdown menu set to "Open"; and "WEP Encryption:" with a dropdown menu set to "Disabled". A "Save/Apply" button is located at the bottom of the form.

- **Shared** — WEP encryption is enabled and encryption key strength of 64-bit or 128-bit needs to be selected. Click on Set Encryption Keys to manually set the network encryption keys. Up to 4 different keys can be set and you can come back to select which one to use at anytime.

The screenshot shows the Zhone Wireless Security configuration page for the Shared authentication method. The left sidebar is identical to the previous screenshot, with "Security" highlighted in red. The main content area is titled "Wireless -- Security" and includes the same introductory text. The "Manual Setup AP" section is also present. The configuration fields are: "Select SSID:" with a dropdown menu set to "wireless"; "Network Authentication:" with a dropdown menu set to "Shared"; "WEP Encryption:" with a dropdown menu set to "Enabled"; "Encryption Strength:" with a dropdown menu set to "128-bit"; and "Current Network Key:" with a dropdown menu set to "1". Below these are four empty text input fields labeled "Network Key 1:", "Network Key 2:", "Network Key 3:", and "Network Key 4:". At the bottom, there is a "Save/Apply" button and a note: "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."

- **802.1X** — requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is also enabled and the encryption strength must also be selected.

The screenshot shows the 'Wireless -- Security' configuration page on a Zhone router. The left sidebar contains a navigation menu with 'Wireless' selected. The main content area is titled 'Wireless -- Security' and includes a description: 'This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually'. Below this is the 'Manual Setup AP' section, which explains that users can set the network authentication method, select data encryption, and specify the encryption strength. The configuration fields are as follows:

- Select SSID: wireless
- Network Authentication: 802.1X
- RADIUS Server IP Address: 0.0.0.0
- RADIUS Port: 1812
- RADIUS Key: (empty)
- WEP Encryption: Enabled
- Encryption Strength: 128-bit
- Current Network Key: 2
- Network Key 1: (empty)
- Network Key 2: (empty)
- Network Key 3: (empty)
- Network Key 4: (empty)

At the bottom, there are instructions: 'Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys' and 'Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys'.

- **WPA (Wi-Fi Protected Access)** — usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses 128-bit dynamic session keys (per user, per session, and per packet keys).

The screenshot shows the 'Wireless -- Security' configuration page on a Zhone router, similar to the previous one but with WPA settings. The left sidebar is the same. The main content area is titled 'Wireless -- Security' and includes the same description. Below is the 'Manual Setup AP' section, which explains that users can set the network authentication method, select data encryption, and specify the encryption strength. The configuration fields are as follows:

- Select SSID: wireless
- Network Authentication: WPA
- WPA Group Rekey Interval: 0
- RADIUS Server IP Address: 0.0.0.0
- RADIUS Port: 1812
- RADIUS Key: (empty)
- WPA Encryption: TKIP
- WEP Encryption: Disabled

At the bottom, there is a 'Save/Apply' button.

- **WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key)** — WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise environment. The main

difference is that the password is entered manually. A group re-key interval time is also required.

The screenshot shows the Zhone Wireless Security configuration page. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area is titled "Wireless -- Security" and includes the following text: "This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually." Below this is the "Manual Setup AP" section, which states: "You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click 'Save/Apply' when done." The configuration fields are: "Select SSID:" with a dropdown menu set to "wireless"; "Network Authentication:" with a dropdown menu set to "WPA-PSK"; "WPA Pre-Shared Key:" with an empty text input field and a link "Click here to display"; "WPA Group Rekey Interval:" with a text input field containing "0"; "WPA Encryption:" with a dropdown menu set to "TKIP"; and "WEP Encryption:" with a dropdown menu set to "Disabled". A "Save/Apply" button is located at the bottom of the form.

- **WPA2** (Wi-Fi Protected Access 2) — second generation WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method. Network re-authorization interval is the time in which another key needs to be dynamically issued.

The screenshot shows the Zhone Wireless Security configuration page. The left sidebar contains a navigation menu with the following items: Device Info, Advanced Setup, Wireless, Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info, Diagnostics, and Management. The main content area is titled "Wireless -- Security" and includes the following text: "This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually." Below this is the "Manual Setup AP" section, which states: "You can set the network authentication method, selecting data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength. Click 'Save/Apply' when done." The configuration fields are: "Select SSID:" with a dropdown menu set to "wireless"; "Network Authentication:" with a dropdown menu set to "WPA2"; "WPA2 Preauthentication:" with a dropdown menu set to "Disabled"; "Network Re-auth Interval:" with a text input field containing "36000"; "WPA Group Rekey Interval:" with a text input field containing "0"; "RADIUS Server IP Address:" with a text input field containing "0.0.0.0"; "RADIUS Port:" with a text input field containing "1812"; "RADIUS Key:" with an empty text input field; "WPA Encryption:" with a dropdown menu set to "AES"; and "WEP Encryption:" with a dropdown menu set to "Disabled". A "Save/Apply" button is located at the bottom of the form.

- **WPA2-PSK** (Wi-Fi Protected Access 2 – Pre-Shared Key) — suitable for home and SOHO environments, it also uses AES encryption and requires you to enter a password and a re-key interval time.

The screenshot shows the 'Wireless -- Security' configuration page on a Zhone router. The left sidebar contains a navigation menu with 'Wireless' selected. The main content area has a title 'Wireless -- Security' and a description: 'This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually'. Below this is the 'Manual Setup AP' section, which explains that users can set the network authentication method, select data encryption, and specify whether a network key is required. The configuration fields are as follows:

- Select SSID: wireless
- Network Authentication: WPA2-PSK
- WPA Pre-Shared Key: [text input] [Click here to display](#)
- WPA Group Rekey Interval: 0
- WPA Encryption: AES
- WEP Encryption: Disabled

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

- **Mixed WPA2 / WPA** — useful during transitional times for upgrades in the enterprise environment, this mixed authentication method allows “upgraded” and users not yet “upgraded” to access the network via the router. RADIUS server information must be entered for WPA and as well as a group re-key interval time. Both TKIP and AES are used.

The screenshot shows the 'Wireless -- Security' configuration page on a Zhone router, specifically for the 'Mixed WPA2/WPA' authentication method. The left sidebar is the same as in the previous screenshot. The main content area has the same title and description. The 'Manual Setup AP' section explains that users can set the network authentication method, select data encryption, and specify whether a network key is required. The configuration fields are as follows:

- Select SSID: wireless
- Network Authentication: Mixed WPA2/WPA
- WPA2 Preauthentication: Disabled
- Network Re-auth Interval: 36000
- WPA Group Rekey Interval: 0
- RADIUS Server IP Address: 0.0.0.0
- RADIUS Port: 1812
- RADIUS Key: [text input]
- WPA Encryption: TKIP+AES
- WEP Encryption: Disabled

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

- **Mixed WPA2 / WPA-PSK** — useful during transitional times for upgrades in the home or SOHO environment, a pre-shared key must be entered along with the group re-key interval time. Both TKIP and AES are also used.

MAC Filter

The MAC filter screen allows you to manage MAC address filters.

Add the MAC addresses that you want to manage and then select the mode that you want to use to manage them. You can disable this feature or you can allow or deny access to the MAC addresses that you add to the list.

To add a MAC Filter:

1. *In the Wireless — MAC Filter page, select the SSID for the*

- From one of the **MAC Restrict Mode** radio buttons, select **Disabled, Allow** or **Deny**.
- Click **MAC Address** to add the MAC address; enter the MAC address in the **MAC Address** text box, then click **Save/Apply**.

Wireless Bridge

In the **Wireless — Wireless Bridge** screen, you can select the mode for the router, either access point or wireless bridge. If you enable the bridge restrict option, then proceed to enter the MAC addresses of the remote bridges.

To restrict a wireless bridge:

- In the **Wireless — Wireless Bridge** screen select the access point mode from the **AP Mode** dropdown.

AP Mode options are

- Access Point**
- Wireless Bridge**

- From the **Bridge Restrict** dropdown select to enable, disable or refresh

3. If you have chosen to enable access point, in the **Remote Bridges MAC Address** text box(es) MAC address(es) for the bridge(s).
4. If you have chosen access point **Refresh only allowed...**

Z H O N E

Device Info
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management

Wireless -- Bridge

This page allows you to configure wireless bridge features of the wireless LAN interface. You can select Wireless Bridge (also known as Wireless Distribution System) to disable access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled(Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Click "Refresh" to update the remote bridges. Wait for few seconds to update. Click "Save/Apply" to configure the wireless bridge options.

AP Mode:

Bridge Restrict:

Remote Bridges MAC Address:

Advanced

The Advanced page configures advanced features of the wireless LAN interface.

Wireless -- Advanced

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

Band: 2.4GHz
Channel: 11 Current: 1
Auto Channel Timer(min): 0
54g™ Rate: Auto
Multicast Rate: Auto
Basic Rate: Default
Fragmentation Threshold: 2346
RTS Threshold: 2347
DTIM Interval: 1
Beacon Interval: 100
Global Max Clients: 128
XPress™ Technology: Disabled
54g™ Mode: 54g Auto
54g™ Protection: Auto
Preamble Type: long
Transmit Power: 100%
Transmit Power Mode(mW): 400

Save/Apply

Advanced features include:

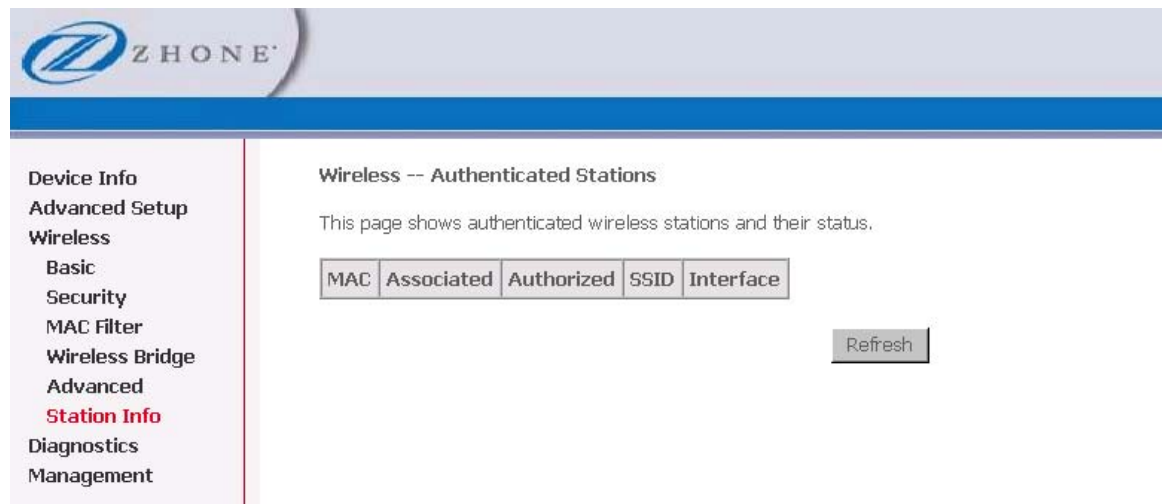
- **Band** — a default setting at 2.4GHz – 802.11g
- **Channel** — 802.11b and 802.11g use channels to limit interference from other devices. If you are experiencing interference with another 2.4Ghz device such as a baby monitor, security alarm, or cordless phone, then change the channel on your router.
- **Auto Channel Timer** — a timer that rescans and finds the best available channel for use on your wireless network.
- **54g Rate** — rate at which information will be transmitted and received on your wireless network.
- **Multicast Rate** — the rate at which a message is sent to a specified group of recipients.
- **Basic Rate** — the set of data transfer rates that all the stations will be capable of using to receive frames from a wireless medium.
- **Fragmentation Threshold** — used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.
- **RTS Threshold (Request to Send Threshold)** — determines the packet size of a transmission through the use of the router to help control traffic flow.
- **DTIM Interval** — sets the Wake-up interval for clients in power-saving mode.
- **Beacon Interval** — a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).
- **Xpress Technology** — a technology that utilizes standards based on frame bursting to achieve higher throughput. With Xpress Technology enabled, aggregate throughput (the sum of the

individual throughput speeds of each client on the network) can improve by up to 25% in 802.11g only networks and up to 75% in mixed networks comprised of 802.11g and 802.11b equipment.

- **54g Mode** — 54g is a Broadcom Wi-Fi technology.
- **54g Protection** — the 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without “speaking” at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS (Request to Send / Clear to Send) to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.
- **Preamble Type** — this information relates to wireless communication based
- **Transmit Power** — select from 20%, 40%, 60%, 80% and 100%. The default value is 100% but can be changed.
- **WMM (Wi-Fi Multimedia)** — prioritizes traffic from different applications such as voice, audio and video applications under different environments and conditions.
- **WMM No Acknowledgement** — the acknowledgement policy used on the MAC level. Enabling no-acknowledgement can result in efficient throughput but higher error rates in a noisy Radio Frequency (RF) environment.
- **WMM APSD** — APSD (Automatic Power Save Delivery). APSD manages radio usage for battery-powered devices to allow battery life in certain conditions. APSD allows a longer beacon interval until an application—VoIP for example—requiring a short packet exchange interval starts. Only if the wireless client supports APSD does APSD affect radio usage and battery life.

Station Info

The Station Info page shows stations that have been authorized access to the router through its wireless function.



The screenshot displays the Zhone router's web interface. The top header features the Zhone logo. A left-hand navigation menu lists various settings: Device Info, Advanced Setup, Wireless (selected), Basic, Security, MAC Filter, Wireless Bridge, Advanced, Station Info (highlighted in red), Diagnostics, and Management. The main content area is titled "Wireless -- Authenticated Stations" and includes the text "This page shows authenticated wireless stations and their status." Below this is a table with the following columns: MAC, Associated, Authorized, SSID, and Interface. A "Refresh" button is positioned to the right of the table.

Diagnostics

The diagnostics screen allows you to run diagnostic tests to check your DSL connection. The outcome will show test results of three connections—

- **Connection to your local network**
- **Connection to your DSL service provider**
- **Connection to your Internet service provider**

There are two buttons at the bottom of the page—**Test** and **Test with OAM F4**—which allow you to retest if necessary.

ZHONE

Device Info
Advanced Setup
Wireless
Diagnostics
Management

br_0_0_35 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 LAN1 Connection:	PASS	Help
Test your LAN2 Connection:	FAIL	Help
Test your LAN3 Connection:	FAIL	Help
Test your LAN4 Connection:	FAIL	Help
Test your Wireless Connection:	DOWN	Help

Test the connection to your DSL service provider

Test ADSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	FAIL	Help
Test ATM OAM F5 end-to-end ping:	FAIL	Help

Test Test With OAM F4

Management

The Management section gives you access to certain setups for the purpose of maintaining the system, including backing up the configurations, viewing system log, maintaining access control, updating software, etc.

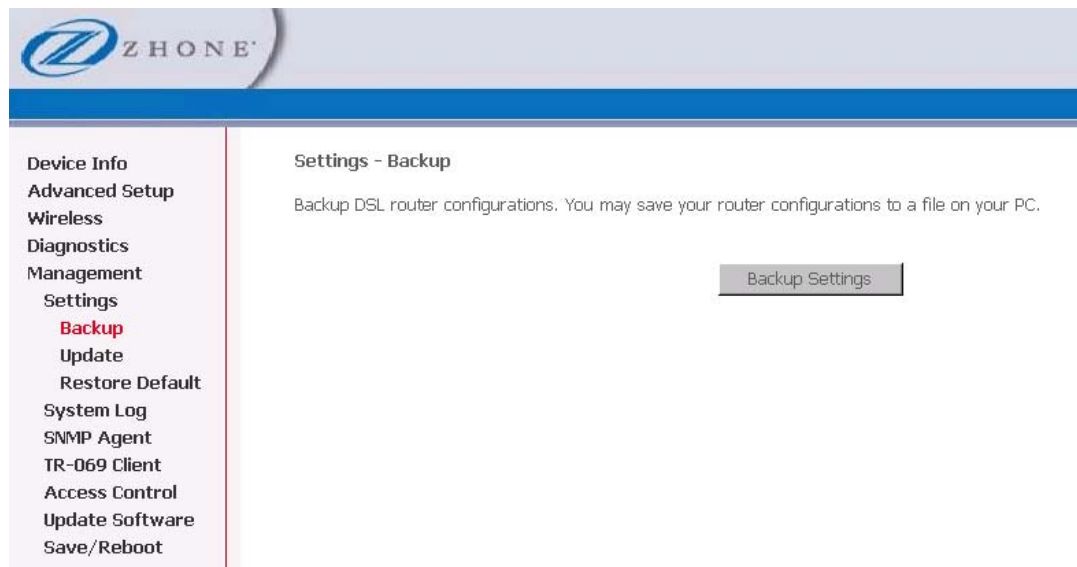
Settings

The page options under Settings provide you with the ability to save configurations to a file, restore configurations from a file and to restore the factory default configuration.

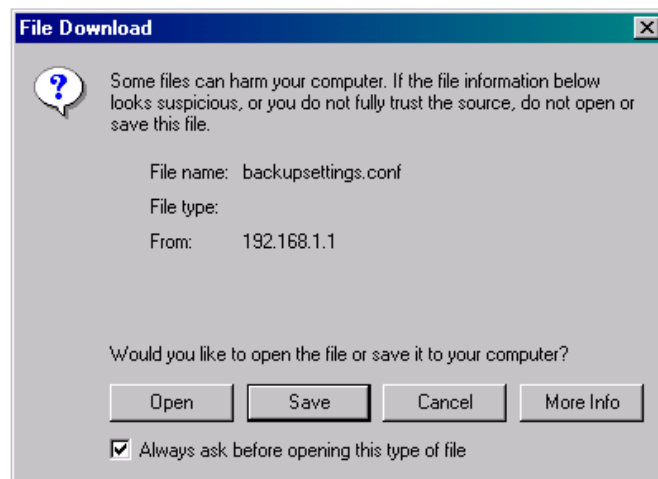
Backup Settings

To save a copy of the configurations that you have made on your router:

1. From the Settings – Backup page click **Backup Settings**.



The below pop-up screen will appear with a prompt to open or save the file to your computer.

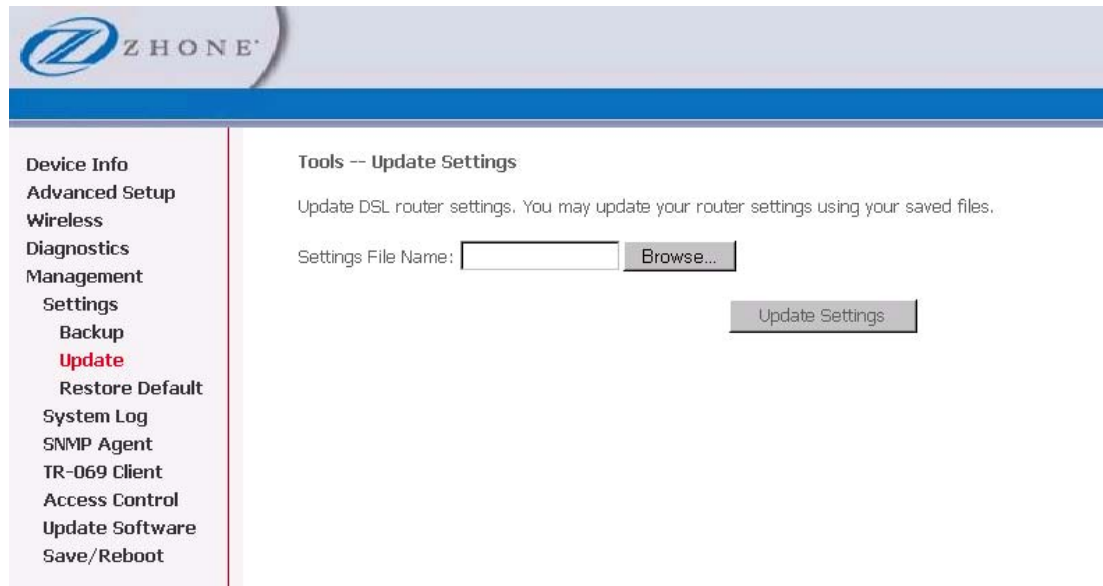


2. Click **Save**.

Update or Restore User Settings

To load a previously saved configuration file onto your router:

1. From the **Settings – Update Settings** page, click **Browse** to find the file on your computer.
2. Click **Update Settings**.



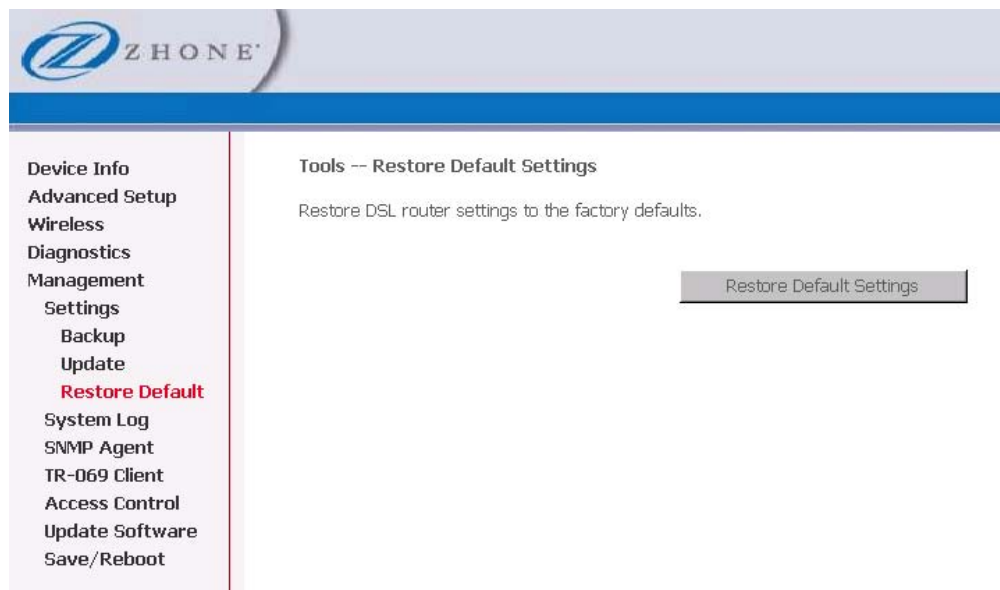
The router will restore settings and reboot to activate the restored settings.

Restore Default

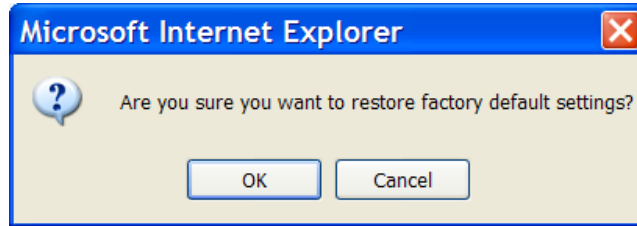
Restore Default will delete all current settings and restore the router to factory default settings.

To restore the factory defaults:

1. From the **Settings – Restore Default Settings** page click **Restore Default Settings**.



2. Click **OK** when the pop-up window appears confirming that you want to restore factory default settings to your router.



The router will restore the default settings and reboot.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options. To view the System Log click **View System Log** to check the log file.

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 System Log](#) [Configure System Log](#)

The **System Log** page shows the date and time of the recorded event, which facility captured the event, the severity of the event and a message which describes the event.

System Log

Date/Time	Facility	Severity	Message
Jan 1 04:52:48	syslog	emerg	BCM96345 started: BusyBox v1.00 (2005.04.12-18:11+0000)
Jan 1 04:52:48	user	crit	kernel: eth0 Link UP.
Jan 1 04:52:48	user	crit	kernel: ADSL G.994 training
Jan 1 04:52:48	user	crit	kernel: ADSL G.992 started
Jan 1 04:52:48	user	crit	kernel: ADSL G.992 channel analysis
Jan 1 04:52:48	user	crit	kernel: ADSL link up, interleaved, us=800, ds=7616
Jan 1 04:52:51	daemon	crit	pppd[358]: PPP LCP UP.
Jan 1 04:52:52	daemon	err	pppd[358]: User name and password authentication failed.
Jan 1 04:52:58	daemon	crit	pppd[358]: PPP LCP UP.
Jan 1 04:52:59	daemon	err	pppd[358]: User name and password authentication failed.
Jan 1 04:53:05	daemon	crit	pppd[358]: PPP LCP UP.
Jan 1 04:53:06	daemon	err	pppd[358]: User name and password authentication failed.

[Refresh](#) [Close](#)

Configure System Log

If the log is enabled, the system will log selected events based on their level. The log levels are

- **Emergency**
- **Alert**
- **Critical**
- **Error**
- **Warning**
- **Notice**
- **Informational**
- **Debugging.**

All events above or equal to the selected log level will be logged and displayed.

System Log -- Configuration

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

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

Log: Disable Enable

Log Level:

Display Level:

Mode:

If the selected mode is **Remote** or **Both**, events will be sent to the specified IP address and UDP port of a remote system log 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** button to configure the system log.

SNMP

SNMP (Simple Network Management Protocol) provides a means to monitor status and performance as well as set configuration parameters. It enables a management station to configure, monitor and receive trap messages from network devices.

SNMP - Configuration

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP Agent Disable Enable

Read Community:

Set Community:

System Name:

System Location:

System Contact:

Trap Manager IP:

TR-069 Client

The router includes a TR-069 client WAN management protocol with default values configured.

To enable the TR-069 client protocol:

1. **Select *Enable*.**

TR-069 client - Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

Inform Disable Enable

Inform Interval:

ACS URL:

ACS User Name:

ACS Password:

Display SOAP messages on serial console Disable Enable

Connection Request Authentication

Connection Request User Name:

Connection Request Password:

2. **Click on the *Save/Reboot* button for the change to take place.**

Access Control

You can enable or disable some services of your router by LAN or WAN. If no WAN connection is defined, only the LAN side can be configured.

Services

Services that can be enabled or disabled on the LAN/WAN are

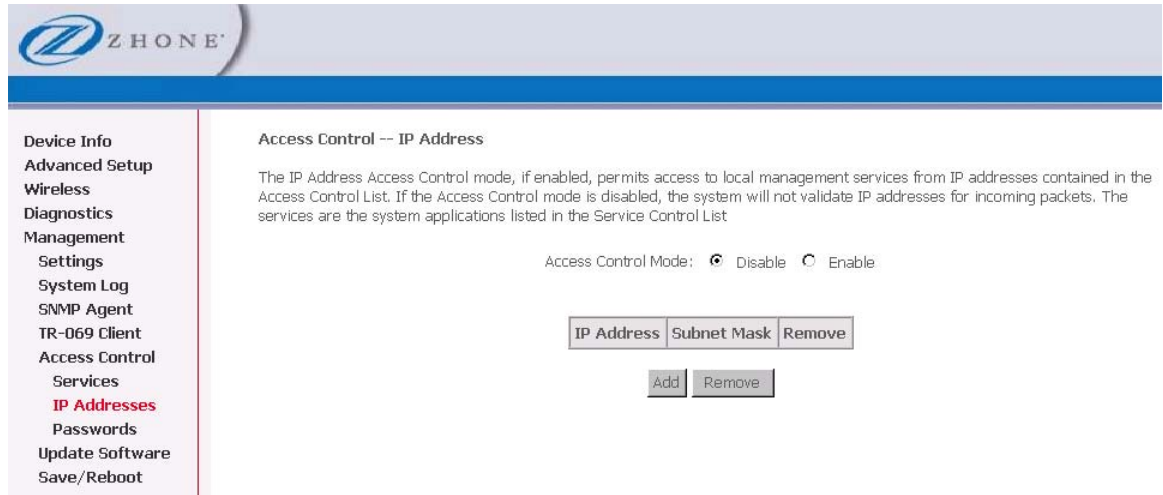
- FTP
- HTTP
- ICMP
- SNMP
- SSH
- Telnet
- TFTP.

The screenshot shows the Zhone router's web interface. The top header features the Zhone logo. A left-hand navigation menu lists various system settings, with 'Services' highlighted under the 'Access Control' section. The main content area is titled 'Access Control -- Services' and contains a descriptive sentence: 'A Service Control List ("SCL") enables or disables services from being used.' Below this is a table with two columns: 'Services' and 'LAN'. The table lists eight services: FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP. Each service has a checkbox in the 'LAN' column, all of which are checked. Below the table is a 'Save/Apply' button.

Services	LAN
FTP	<input checked="" type="checkbox"/> Enable
HTTP	<input checked="" type="checkbox"/> Enable
ICMP	<input type="checkbox"/> Enable
SNMP	<input checked="" type="checkbox"/> Enable
SSH	<input checked="" type="checkbox"/> Enable
TELNET	<input checked="" type="checkbox"/> Enable
TFTP	<input checked="" type="checkbox"/> Enable

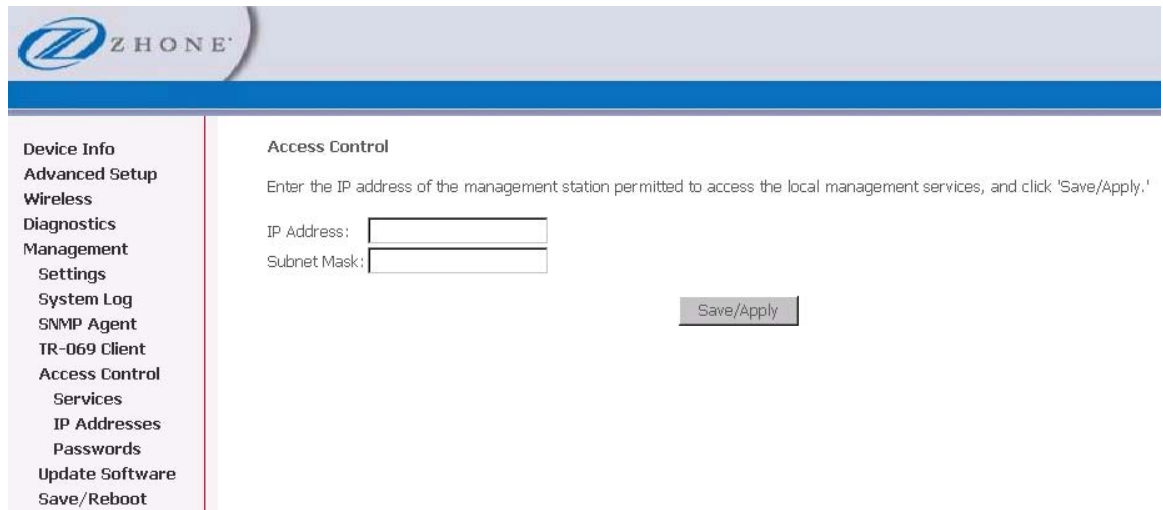
IP Addresses

Web access to the router may be limited when Access Control Mode is enabled.



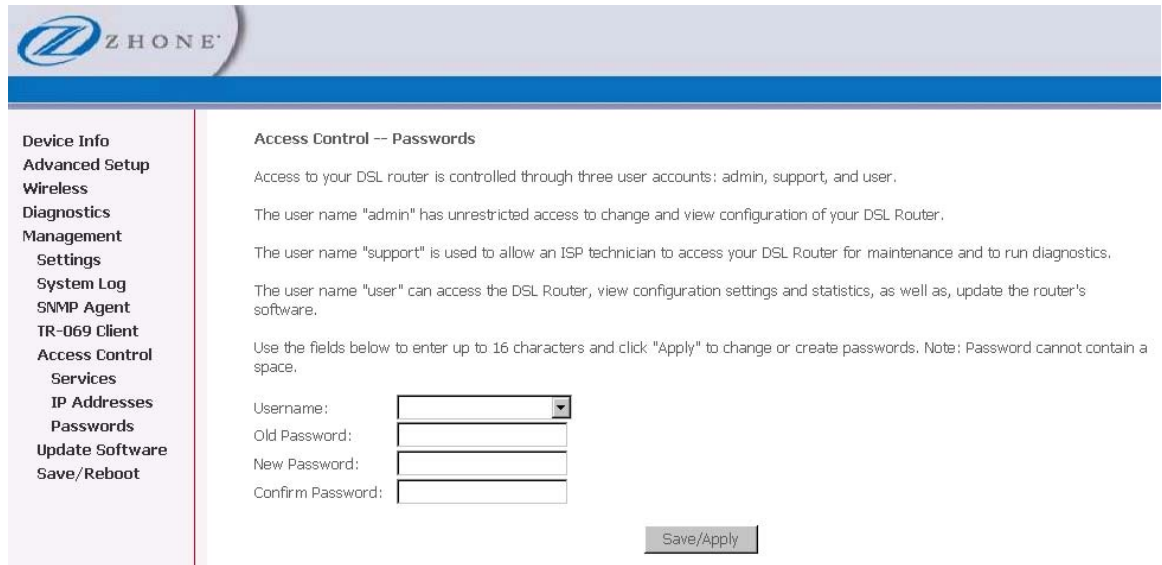
To add the IP address to the IP address list:

1. Click **Add**.
2. Select **Enabled** to enable Access Control Mode.
3. To assign the IP address of the management station that is permitted to access the local management services, enter the IP address in the **IP Address** text box.
4. Enter the **Subnet Mask**.
5. Click **Save / Apply**.



Passwords

Access the **Passwords** screen under the **Access Control** section to change a password. Select an account and enter the current password and the new password and then click on the **Save / Apply** button.



The screenshot shows the Zhone router's web interface. At the top left is the Zhone logo. A left-hand navigation menu lists various settings categories, with 'Access Control' and 'Passwords' highlighted. The main content area is titled 'Access Control -- Passwords' and contains explanatory text about three user accounts: 'admin', 'support', and 'user'. Below the text are four input fields: a dropdown menu for 'Username', and three text boxes for 'Old Password', 'New Password', and 'Confirm Password'. A 'Save/Apply' button is located at the bottom right of the form area.

Zhone

Access Control -- Passwords

Access to your DSL router is controlled through three user accounts: admin, support, and user.

The user name "admin" has unrestricted access to change and view configuration of your DSL Router.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as, update the router's software.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

Username:

Old Password:

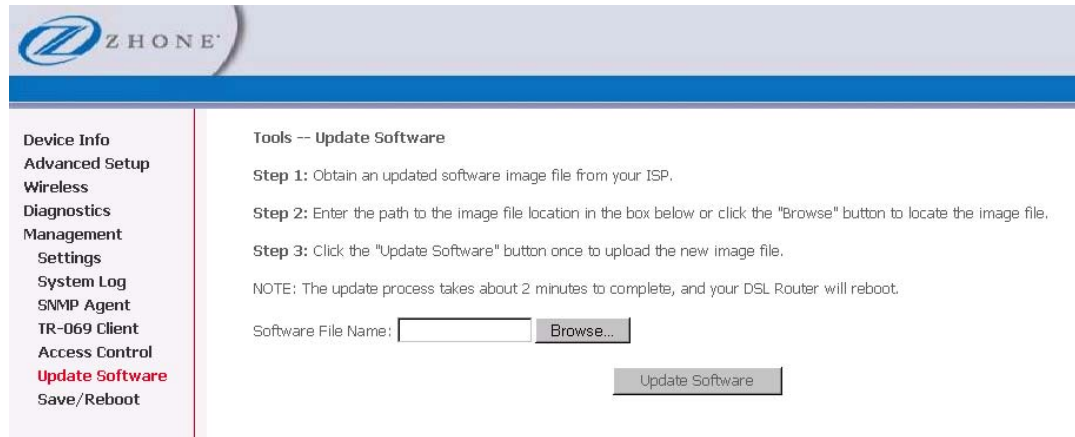
New Password:

Confirm Password:

Update Software

If your ISP releases new software for your router, follow these steps to perform an upgrade:

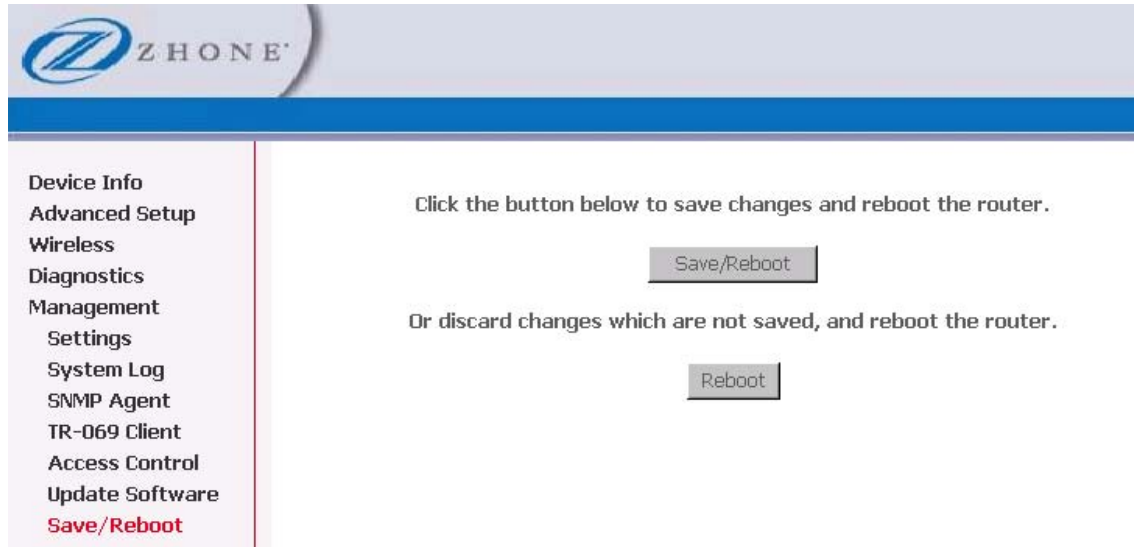
1. Obtain an updated software image file from your ISP.
2. Enter the path to the image file location or click on the **Browse** button to locate the image file.
3. Click **Update Software** once (and only once) to upload the new image file.



The screenshot shows the Zhone router's web interface for updating software. The header features the Zhone logo. A left-hand navigation menu lists various system settings, with 'Update Software' highlighted in red. The main content area is titled 'Tools -- Update Software' and provides three numbered steps: Step 1 is to obtain the software image; Step 2 is to enter the file path or use the 'Browse...' button; Step 3 is to click 'Update Software'. A note indicates the process takes about 2 minutes and causes a reboot. At the bottom, there is a text input field for the 'Software File Name', a 'Browse...' button, and a large 'Update Software' button.

Reboot Router

Clicking **Save/Reboot** saves all the configurations you have made, then reboots the router using the new configuration information.



The screenshot shows the Zhone router configuration interface. At the top left is the Zhone logo. A vertical navigation menu on the left lists various settings: Device Info, Advanced Setup, Wireless, Diagnostics, Management, Settings, System Log, SNMP Agent, TR-069 Client, Access Control, Update Software, and **Save/Reboot** (highlighted in red). The main content area contains two instructions and buttons:

- Click the button below to save changes and reboot the router.
- Or discard changes which are not saved, and reboot the router.

Chapter 6 Troubleshooting

The Router Is Not Functional

1. *Check to see that the power LED is green and the network cables are installed correctly. Refer to the quick start guide for more details.*
2. *Check to see that the LAN and Status LEDs are green.*
3. *Check the settings on your PC. Again, refer to the quick start guide for more details*
4. *Check the router's settings.*
5. *From your PC, can you ping the router? Assuming that the router has DHCP enabled and your PC is on the same subnet as the router, you should be able to ping the router.*
6. *Can you ping the WAN? Your ISP should have provided the IP address of their server. If you can ping the router and your protocols are configured correctly, you should be able to ping the ISP's network. If you cannot ping the ISP's network, make sure you are using the correct protocols with the correct VPI/VCI values.*
7. *Make sure NAT is enabled if you are using private addresses on the LAN ports.*

You Cannot Connect to the Router

1. *Check to see that the power LED is green and that the network cables are installed correctly.*
2. *Make sure you are not connecting the USB and the Ethernet port to the same PC at the same time.*
3. *Make sure that your PC and the router are on the same network segment. The router's default IP address is 192.168.1.1. If you are running a Windows-based PC, type `ipconfig /all` (or `windowsipcfg /all` on Windows 95, 98, or ME) at a command prompt to determine the IP address of your network adapter. Make sure that it is within the same 192.168.1.x subnet. Your PC's subnet mask must match the router's subnet mask. The router has a default subnet mask of 255.255.255.0.*
4. *Make sure NAT is enabled if you are using private addresses on the LAN ports.*

LEDs Blink in a Sequential Pattern

This typically means that either the kernel or flash file system is corrupted. Notify your service representative.

The Status LED Continues to Blink

This means that the DSL line is trying to train but for some reason it cannot establish a valid connection. The likely cause of this is that you are too far away from the central office. Contact your DSL service provider for further assistance.

The Status LED is Always Off

1. *Make sure you have DSL service. You should receive notification from your ISP that DSL service is installed. You can usually tell if the service is installed by listening to the phone line: you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.*
2. *Verify that the phone line is connected directly to the wall and to the line input on the router. If the phone line is connected to the phone side of the router or you have a splitter installed on the phone line, the DSL light will not come on.*

Diagnosing Problems using IP Utilities

Ping

Ping is a command you can use to check whether your PC can recognize other computers on your network and the Internet. A ping command sends a message to the computer you specify. If the computer receives the message, it sends messages in reply. To use it, you must know the IP address of the computer with which you are trying to communicate.

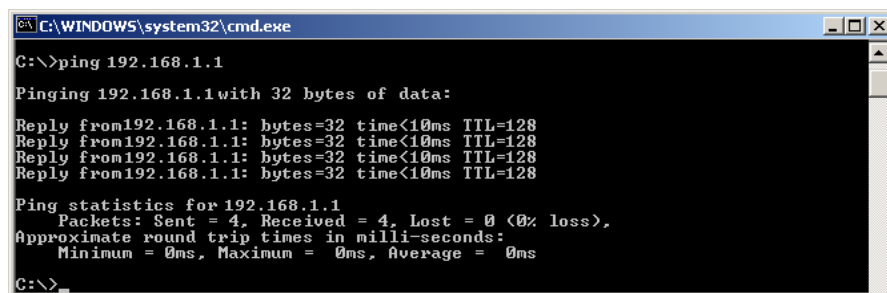
On Windows-based computers, you can execute a ping command from the Start menu.

3. *Click the **Start** button, and then click **Run**. In the Open text box, type a statement such as the following:*

ping 192.168.1.1 or the IP address you have changed

4. *Click **OK**. You can substitute any private IP address on your LAN or a public IP address for an Internet site, if known.*

If the target computer receives the message, a Command Prompt window is displayed:



```
C:\WINDOWS\system32\cmd.exe
C:\>ping 192.168.1.1
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Reply from 192.168.1.1: bytes=32 time<10ms TTL=128
Ping statistics for 192.168.1.1
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

If the target computer cannot be located, you will receive the message “Request timed out.”

Using the ping command, you can test whether the path to the device is working (using the preconfigured default LAN IP address 192.168.1.1) or another address you assigned.

You can also test whether access to the Internet is working by typing an external address, such as that for www.yahoo.com (216.115.108.243). If you do not know the IP address of a particular Internet location, you can use the nslookup command, as explained in the following section.

From most other IP-enabled operating systems, you can execute the same command at a command prompt or through a system administration utility.

Nslookup

You can use the nslookup command to determine the IP address associated with an Internet site name. You specify the common name, and the nslookup command looks up the name in on your DNS server (usually located with your ISP). If that name is not an entry in your ISP's DNS table, the request is then referred to another higher-level server, and so on, until the entry is found. The server then returns the associated IP address.

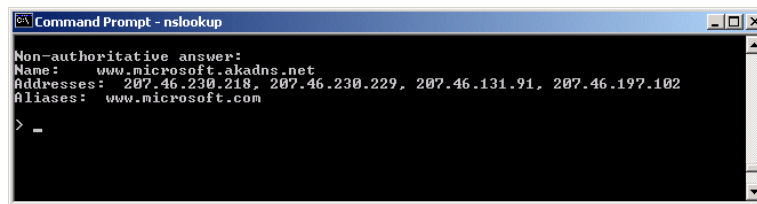
On Windows-based computers, you can execute the nslookup command from the Start menu.

5. Click the **Start** button, and then click **Run**. In the Open text box, type the following:

```
Nslookup
```

6. Click **OK**. A Command Prompt window displays with a bracket prompt (>). At the prompt, type the name of the Internet address that you are interested in, such as www.microsoft.com.

The window will display the associate IP address, if known, as shown below:



```
Command Prompt - nslookup
Non-authoritative answer:
Name:    www.microsoft.akadns.net
Addresses: 207.46.230.218, 207.46.230.229, 207.46.131.91, 207.46.197.102
Aliases: www.microsoft.com

> -
```

There may be several addresses associated with an Internet name. This is common for web sites that receive heavy traffic; they use multiple, redundant servers to carry the same information.

7. To exit from the nslookup utility, type **exit** and press **[Enter]** at the command prompt.

Appendix A – Glossary

Term	Description
802.11	A family of specifications for wireless LANs developed by a working group of the IEEE. This wireless Ethernet protocol, often called Wi-Fi.
10BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 10 Mbps. Also known as Category 3 (CAT 3) wiring. See data rate, Ethernet.
100BASE-T	A designation for the type of wiring used by Ethernet networks with a data rate of 100 Mbps. Also known as Category 5 (CAT 5) wiring. See data rate, Ethernet.
ADSL	Asymmetric Digital Subscriber Line The most commonly deployed “flavor” of DSL for home users is asymmetrical DSL. The term asymmetrical refers to its unequal data rates for downloading and uploading (the download rate is higher than the upload rate). The asymmetrical rates benefit home users because they typically download much more data from the Internet than they upload.
Analog	An analog signal is a signal that has had its frequency modified in some way, such as by amplifying its strength or varying its frequency, in order to add information to the signal. The voice component in DSL is an analog signal. See digital.
ATM	Asynchronous Transfer Mode A standard for high-speed transmission of data, text, voice, and video, widely used within the Internet. ATM data rates range from 45 Mbps to 2.5 Gbps. See data rate.
Authenticate	To verify a user’s identity, such as by prompting for a password.
Binary	The “base two” system of numbers that uses only two digits, 0 and 1, to represent all numbers. In binary, the number 1 is written as 1, 2 as 10, 3 as 11, 4 as 100, etc. Although expressed as decimal numbers for convenience, IP addresses in actual use are binary numbers; e.g., the IP address 209.191.4.240 is 11010001.10111111.00000100.11110000 in binary. See bit, IP address, network mask.
Bit	Short for “binary digit,” a bit is a number that can have two values, 0 or 1. See binary.
Bps	bits per second
Bridging	Passing data from your network to your ISP and vice versa using the hardware addresses of the devices at each location. Bridging contrasts with routing which can add more intelligence to data transfers by using network addresses instead. The device can perform both routing and bridging. Typically, when both functions are enabled, the device routes IP data and bridges all other types of data. See routing.

Broadband	A telecommunications technology that can send different types of data over the same medium. DSL is a broadband technology.
Broadcast	To send data to all computers on a network.
DHCP	Dynamic Host Configuration Protocol DHCP automates address assignment and management. When a computer connects to the LAN, DHCP assigns it an IP address from a shared pool of IP addresses; after a specified time limit, DHCP returns the address to the pool.
DHCP relay	Dynamic Host Configuration Protocol relay A DHCP relay is a computer that forwards DHCP data between computers that request IP addresses and the DHCP server that assigns the addresses. Each of the device's interfaces can be configured as a DHCP relay. See DHCP.
DHCP server	Dynamic Host Configuration Protocol server A DHCP server is a computer that is responsible for assigning IP addresses to the computers on a LAN. See DHCP.
Digital	Of data, having a form based on discrete values expressed as binary numbers (0's and 1's). The data component in DSL is a digital signal. See analog.
DNS	Domain Name System The DNS maps domain names into IP addresses. DNS information is distributed hierarchically throughout the Internet among computers called DNS servers. For example, www.yahoo.com is the domain name associated with IP address 216.115.108.243. When you start to access a web site, a DNS server looks up the requested domain name to find its corresponding IP address. If the DNS server cannot find the IP address, it communicates with higher-level DNS servers to determine the IP address. See domain name.
Domain name	A domain name is a user-friendly name used in place of its associated IP address. Domain names must be unique; their assignment is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN). Domain names are a key element of URLs, which identify a specific file at a web site. See DNS.
Download	To transfer data in the downstream direction, i.e., from the Internet to the user.
DSL	Digital Subscriber Line A technology that allows both digital data and analog voice signals to travel over existing copper telephone lines.
Encryption keys	See network keys
Ethernet	The most commonly installed computer network technology, usually using twisted pair wiring. Ethernet data rates are 10 Mbps and 100 Mbps. See also 10BASE-T, 100BASE-T, twisted pair.
Firewall	A firewall is protection between the Internet and your local network. It acts as the firewall in your car does, protecting the interior of the car from the engine. Your car's firewall has very small opening that allow desired connections from the engine into the cabin (gas pedal connection, etc),

but if something happens to your engine, you are protected.

The firewall in the router is very similar. Only the connections that you allow are passed through the firewall. These connections normally originate from the local network, such as users web browsing, checking e-mail, downloading files, and playing games. However, you can allow incoming connections so that you can run programs like a web server.

FTP	<p>File Transfer Protocol</p> <p>A program used to transfer files between computers connected to the Internet. Common uses include uploading new or updated files to a web server, and downloading files from a web server.</p>
Gbps	<p>Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.</p>
Host	<p>A device (usually a computer) connected to a network.</p>
HTTP	<p>Hyper-Text Transfer Protocol</p> <p>HTTP is the main protocol used to transfer data from web sites so that it can be displayed by web browsers. See web browser, web site.</p>
Hub	<p>A hub is a place of convergence where data arrives from one or more directions and is forwarded out in one or more directions. It connects an Ethernet bridge/router to a group of PCs on a LAN and allows communication to pass between the networked devices.</p>
ICMP	<p>Internet Control Message Protocol</p> <p>An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.</p>
IEEE	<p>The Institute of Electrical and Electronics Engineers is a technical professional society that fosters the development of standards that often become national and international standards.</p>
Internet	<p>The global collection of interconnected networks used for both private and business communications.</p>
Intranet	<p>A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.</p>
IP	<p>See TCP/IP.</p>
IP address	<p>Internet Protocol address</p> <p>The address of a host (computer) on the Internet, consisting of four numbers, each from 0 to 255, separated by periods, e.g., 209.191.4.240. An IP address consists of a network ID that identifies the particular network the host belongs to, and a host ID uniquely identifying the host itself on that network. A network mask is used to define the network ID and the host ID. Because IP addresses are difficult to remember, they usually have an associated domain name that can be specified instead. See domain name, network mask.</p>
ISP	<p>Internet Service Provider</p> <p>A company that provides Internet access to its customers, usually for a fee.</p>

LAN	Local Area Network. A network limited to a small geographic area, such as a home or small office.
LED	Light Emitting Diode An electronic light-emitting device. The indicator lights on the front of the device are LEDs.
MAC address	Media Access Control address The permanent hardware address of a device, assigned by its manufacturer. MAC addresses are expressed as six pairs of hex characters, with each pair separated by colons. For example; NN:NN:NN:NN:NN:NN.
Mask	See network mask.
Mbps	Abbreviation for Megabits per second, or one million bits per second. Network data rates are often expressed in Mbps.
NAT	Network Address Translation A service performed by many routers that translates your network's publicly known IP address into a private IP address for each computer on your LAN. Only your router and your LAN know these addresses; the outside world sees only the public IP address when talking to a computer on your LAN.
Network	A group of computers that are connected together, allowing them to communicate with each other and share resources, such as software, files, etc. A network can be small, such as a LAN, or very large, such as the Internet.
Network keys	(Also known as encryption keys.) 64-bit and 128-bit encryption keys used in WEP wireless security schemes. The keys encrypt data over the WLAN, and only wireless PCs configured with WEP keys that correspond to the keys configured on the device can send/receive encrypted data.
Network mask	A network mask is a sequence of bits applied to an IP address to select the network ID while ignoring the host ID. Bits set to 1 mean "select this bit" while bits set to 0 mean "ignore this bit." For example, if the network mask 255.255.255.0 is applied to the IP address 100.10.50.1, the network ID is 100.10.50, and the host ID is 1. See binary, IP address, subnet.
NIC	Network Interface Card An adapter card that plugs into your computer and provides the physical interface to your network cabling. For Ethernet NICs this is typically an RJ-45 connector. See Ethernet, RJ-45.
Packet	Data transmitted on a network consists of units called packets. Each packet contains a payload (the data), plus overhead information such as where it came from (source address) and where it should go (destination address).
Ping	Packet Internet (or Inter-Network) Groper A program used to verify whether the host associated with an IP address is online. It can also be used to reveal the IP address for a given domain name.
Port	A physical access point to a device such as a computer or router, through which data flows into and out of the device.

PPP	<p>Point-to-Point Protocol</p> <p>A protocol for serial data transmission that is used to carry IP (and other protocol) data between your ISP and your computer. The WAN interface on the device uses two forms of PPP called PPPoA and PPPoE. See PPPoA, PPPoE.</p>
PPPoA	<p>Point-to-Point Protocol over ATM</p> <p>One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoE. You can define only one PPPoA interface per VC.</p>
PPPoE	<p>Point-to-Point Protocol over Ethernet</p> <p>One of the two types of PPP interfaces you can define for a Virtual Circuit (VC), the other type being PPPoA. You can define one or more PPPoE interfaces per VC.</p>
Protocol	<p>A set of rules governing the transmission of data. In order for a data transmission to work, both ends of the connection have to follow the rules of the protocol.</p>
Remote	<p>In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.</p>
RIP	<p>Routing Information Protocol</p> <p>The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.</p>
RJ-11	<p>Registered Jack Standard-11</p> <p>The standard plug used to connect telephones, fax machines, modems, etc. to a telephone port. It is a 6-pin connector usually containing four wires.</p>
RJ-45	<p>Registered Jack Standard-45</p> <p>The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.</p>
Routing	<p>Forwarding data between your network and the Internet on the most efficient route, based on the data's destination IP address and current network conditions. A device that performs routing is called a router.</p>
SDNS	<p>Secondary Domain Name System (server)</p> <p>A DNS server that can be used if the primary DSN server is not available. See DNS.</p>
Subnet	<p>A subnet is a portion of a network. The subnet is distinguished from the larger network by a subnet mask that selects some of the computers of the network and excludes all others. The subnet's computers remain physically connected to the rest of the parent network, but they are treated as though they were on a separate network. See network mask.</p>
Subnet mask	<p>A mask that defines a subnet. See network mask.</p>
TCP	<p>See TCP/IP.</p>
TCP/IP	<p>Transmission Control Protocol/Internet Protocol</p> <p>The basic protocols used on the Internet. TCP is responsible for dividing data up into packets for delivery and reassembling them at the destination, while IP is responsible for delivering the packets from source to destination. When TCP and IP are bundled with higher-level applications such as HTTP, FTP, Telnet, etc., TCP/IP refers to this whole</p>

suite of protocols.

Telnet	An interactive, character-based program used to access a remote computer. While HTTP (the web protocol) and FTP only allow you to download files from a remote computer, Telnet allows you to log into and use a computer from a remote location.
TFTP	Trivial File Transfer Protocol A protocol for file transfers, TFTP is easier to use than File Transfer Protocol (FTP) but not as capable or secure.
TKIP	Temporal Key Integrity Protocol (TKIP) provides WPA with a data encryption function. It ensures that a unique master key is generated for each packet, supports message integrity and sequencing rules and supports re-keying mechanisms.
Triggers	Triggers are used to deal with application protocols that create separate sessions. Some applications, such as NetMeeting, open secondary connections during normal operations, for example, a connection to a server is established using one port, but data transfers are performed on a separate connection. A trigger tells the device to expect these secondary sessions and how to handle them. Once you set a trigger, the embedded IP address of each incoming packet is replaced by the correct host address so that NAT can translate packets to the correct destination. You can specify whether you want to carry out address replacement, and if so, whether to replace addresses on TCP packets only, UDP packets only, or both.
Twisted pair	The ordinary copper telephone wiring used by telephone companies. It contains one or more wire pairs twisted together to reduce inductance and noise. Each telephone line uses one pair. In homes, it is most often installed with two pairs. For Ethernet LANs, a higher grade called Category 3 (CAT 3) is used for 10BASE-T networks, and an even higher grade called Category 5 (CAT 5) is used for 100BASE-T networks. See 10BASE-T, 100BASE-T, Ethernet.
Unnumbered interfaces	An unnumbered interface is an IP interface that does not have a local subnet associated with it. Instead, it uses a router-id that serves as the source and destination address of packets sent to and from the router. Unlike the IP address of a normal interface, the router-id of an unnumbered interface is allowed to be the same as the IP address of another interface. For example, the WAN unnumbered interface of your device uses the same IP address of the LAN interface (192.168.1.1). The unnumbered interface is temporary – PPP or DHCP will assign a 'real' IP address automatically.
Upstream	The direction of data transmission from the user to the Internet.
VC	Virtual Circuit A connection from your DSL router to your ISP.
VCI	Virtual Circuit Identifier Together with the Virtual Path Identifier (VPI), the VCI uniquely identifies a VC. Your ISP will tell you the VCI for each VC they provide. See VC.
VDSL	Very High Speed Digital Subscriber Line It provides faster transmission rate and is capable of supporting high bandwidth applications like IPTV and bandwidth consumed applications.

VPI	<p>Virtual Path Identifier</p> <p>Together with the Virtual Circuit Identifier (VCI), the VPI uniquely identifies a VC. Your ISP will tell you the VPI for each VC they provide. See VC.</p>
WAN	<p>Wide Area Network</p> <p>Any network spread over a large geographical area, such as a country or continent. With respect to the device, WAN refers to the Internet.</p>
Web browser	<p>A software program that uses Hyper-Text Transfer Protocol (HTTP) to download information from (and upload to) web sites, and displays the information, which may consist of text, graphic images, audio, or video, to the user. Web browsers use Hyper-Text Transfer Protocol (HTTP). Popular web browsers include Netscape Navigator and Microsoft Internet Explorer. See HTTP, web site, WWW.</p>
Web page	<p>A web site file typically containing text, graphics and hyperlinks (cross-references) to the other pages on that web site, as well as to pages on other web sites. When a user accesses a web site, the first page that is displayed is called the home page. See hyperlink, web site.</p>
Web site	<p>A computer on the Internet that distributes information to (and gets information from) remote users through web browsers. A web site typically consists of web pages that contain text, graphics, and hyperlinks. See hyperlink, web page.</p>
WEP	<p>Wired Equivalent Privacy (WEP) encrypts data over WLANs. Data is encrypted into blocks of either 64 bits length or 128 bits length. The encrypted data can only be sent and received by users with access to a private network key. Each PC on your wireless network must be manually configured with the same key as your device in order to allow wireless encrypted data transmissions. Eavesdroppers cannot access your network if they do not know your private key. WEP is considered to be a low security option.</p>
Wireless	<p>Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. See wireless LAN.</p>
Wireless LAN	<p>A wireless LAN (WLAN) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs.</p>
WPA	<p>Wi-Fi Protected Access</p> <p>WPA is an initiative by the IEEE and Wi-Fi Alliance to address the security limitations of WEP. WPA provides a stronger data encryption method (called Temporal Key Integrity Protocol (TKIP)). It runs in a special, easy-to-set-up home mode called Pre-Shared Key (PSK) that allows you to manually enter a pass phrase on all the devices in your wireless network. WPA data encryption is based on a WPA master key. The master key is derived from the pass phrase and the network name (SSID) of the device. It provides improved data encryption and stronger user authentication. The mode of WPA supported on your device is called Pre-Shared Key (PSK), which allows you to manually enter a type of key called a pass phrase.</p>
WWW	<p>World Wide Web</p> <p>Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.</p>