1511-A1 (1-Port)
1512-A1 (4-Port)
1518-A1 (4-Port with WiFi)

ADSL2+ Router
Users Guide

Document Part Number: 830-02114-02
September, 2010

ZHONE™

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 disclaim 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.

The Ringer Equivalence Number (REN) is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not

exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local Telephone Company.

The REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point. For example, 03 represents a REN of 0.3.

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.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is labelled on the equipment. The REN assigned to each terminal piece of equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

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

NOTICE: This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de classe B est conforme à la norme Canadienne NMB-003.

⚠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 matérial brouilleur du Canada.

NOTICE: This device complies with RSS-210,IC ID:8609A-1518A1NA

Operation is subject to the following two conditions:

1) This device may not cause interference and

2) This device must accept any interference, including interference that may cause undesired operation of the device.

Table of Contents

Important Safety Instructions....3
CE Marking....4
FCC Part 15 Declaration....4
Table of Contents....7
About This Guide....10
Style and Notation Conventions....10
Typographical Conventions....11
Acronyms....11
Contacting Customer Service and Technical Support....12

Chapter 1 Introduction 13
System Requirements....13
Package Contents....13
Safety Instructions....13
Front Panel....14
1518-A1 Front Panel....14
1512-A1 Front Panel....14
1511-A1 Front Panel....14
LED descriptions....15
Back Panel....16

Chapter 2 Hardware Installation and PC Setup 17
Overview....17
Connecting Your Hardware....17
Mounting the Router....18
Unit dimensions....18
Configuring Your Computer....19
Windows 2000....19
Windows XP....20
Windows 7....20

Chapter 3 The Web User Interface 21
Log in to the Router....21
Summary....22
WAN....23
LAN Statistics....23
WAN Statistics....24
xTM Statistics....24
xDSL Statistics....25
ADSL BER Test....26
Route....27
ARP....27
DHCP....28

Chapter 4 Quick Setup 29
Quick Setup with Automatic Configuration....29
Quick Setup with Automatic Configuration Disabled....30

Chapter 5 Advanced Setup 35
Configuration Types....35

Add a Layer 2 Interface....35
Add a Bridge WAN Service....36
Add a PPPoE WAN Service....37
Add an IPoE WAN Service....39
Add a PPPoA WAN Service....40
Add an IPoA WAN Service....42
Remove a Connection....44
Edit a Connection....44
Ethernet Mode....44
LAN Local Area Network (LAN) Setup....45
IGMP snooping....45
NAT....46
Virtual Servers....46
Port Triggering....49
DMZ Host....50
ALG....51
Security....51
IP Filtering—Outgoing....51
IP Filtering—Incoming....52
MAC Filtering....55
Parental Control....57
Time Restriction....57
URL Filter....58
Quality of Service....60
Queue Config....60
QoS Classification....62
Routing....63
Default Gateway....63
Static Route....64
Policy Route....65
RIP....66
DNS....67
Dynamic DNS....67
DSL....68
Modulation Methods....69
Capability....69
DSL Advanced Settings....69
UPnP....71
DNS Proxy....71
Interface Grouping....72
LAN Ports....73
IPSec....74
Certificate....77
Local....77
Trusted CA....79
Multicast....80
Wireless....80
Basic....80
Security....82
MAC Filter....88
Wireless Bridge....89
Advanced....91
Station Info....93
Diagnostics....94
Management....95
Settings....95
Backup Settings....95
Update Settings....96

Restore Default....96
System Log....97
Configure System Log....99
SNMP Agent....100
TR-069 Client....100
Internet Time....101
Access Control....102
Services....102
Passwords....103
IP Addresses....104
Update Software....105
Reboot....105
Tools....106

Chapter 6 Troubleshooting 108
The Router Is Not Functional....108
You Cannot Connect to the Router....108
The DSL LED Continues to Blink....108
The DSL LED is Always Off....109
The Internet LED is Always Off....109
Diagnosing Problems using IP Utilities....109
Ping....109
Tracert....110
Nslookup....110

Appendix A – Glossary 113

About This Guide

This guide is intended for use by installation technicians, system administrators, and network administrators. It explains how to install and configure the 1511-A1, 1512-A1 and 1518-A1 routers.

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.
`Fixed Bold Italic`	Used in code examples for variable text typed by users.
Italic	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
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

The1518-A1 (four port with WiFi), 1512-A1 (four port), and 1511 (one port) ADSL 2+ routers are easily installed routers which deliver the performance needed for multimedia applications

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

The 15xx-A1 family provides the following features:

- ADSL2+ modem which supports ANSI T1.413 ISSUE 2, ITU G.992.1 (G.DMT), ITU G.992.2 (G.LITE), ITU G992.3, ITU G992.5, and ADSL2+ to meet different linking speeds from your ISP
- 802.11 b/g WiFi LAN port (1518 only)
- Four 10/100BaseT Ethernet ports to provide Internet connectivity to all computers on your LAN (1518 and 1512) The 1511 has one 10/100BaseT Ethernet port
- Easy-to-use configuration program accessible through a standard web browser

System Requirements

In order to use your 15xx-A1 family 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, XP, Vista or Windows 7. (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:

- 1518-A1, 1512-A1, or 1511-A1 ADSL 2+ router
- 12V 700 mA 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.

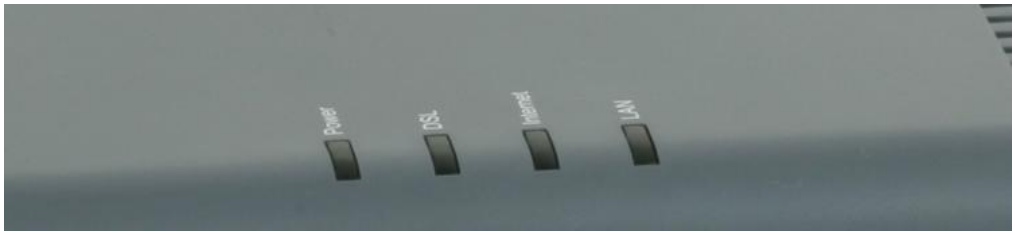
Unplug equipment first before cleaning. A damp cloth can be used to clean the equipment. Do not use liquid / aerosol cleaners or magnetic / static cleaning devices.

Front Panel

1518-A1 Front Panel

1512-A1 Front Panel

1511-A1 Front Panel

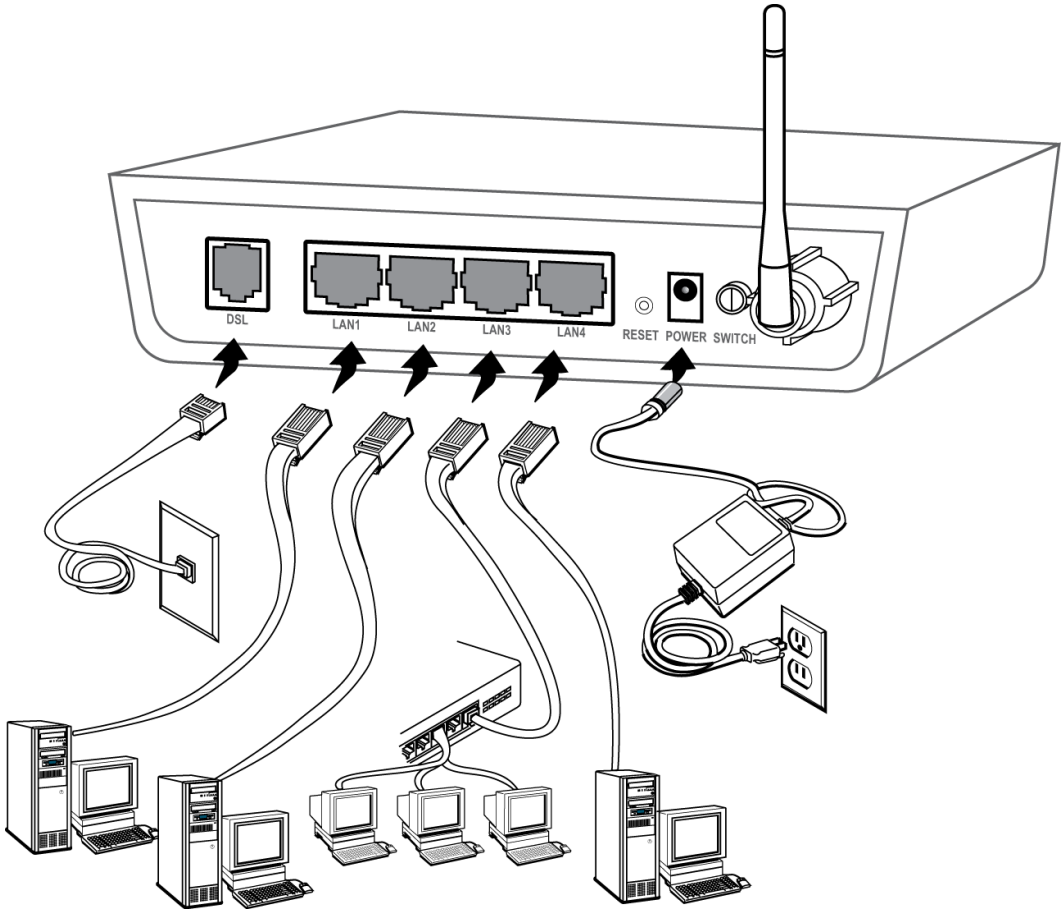


LED descriptions

LED	Mode	INDICATION
Power	Solid green	Boot-up successful
	Solid red	Router is booting up
	No light	The router may not be turned on. Check if the power adapter is connected to the modem, the modem is plugged in and the power switch button is in the on (pushed in) state.
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
Internet	Solid	ADSL is connected
	No light	ADSL is not connected. The ALARM LED will be red
	Blinking	The router is connected to the LAN
LAN 1-4 (1511 has one LAN port)	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
Wireless (1518 only)	Solid	Wireless is enabled
	No light	Wireless is disabled
	Blinking	Wireless traffic activity

NOTE: The 1512 and 1511 do not have the wireless LED. The 1511 has one LAN LED.

Back Panel



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

Port	Description
DSL	RJ-11 cable connects to incoming DSL line
LAN1 – LAN4	RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
Reset / Default	***Restart***—press the button for less than 4 seconds. ***ISP settings***—press the button for 4 seconds or longer. **Factor y Default settings** – press the button for 60 seconds or longer
Power	Connects to a 12V 700 mA power adapter.
Switch	Power on (depressed) or power off for the router.

NOTE: The 1512 and 1511 do not have the wireless antenna. The 1511 has one LAN port.

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

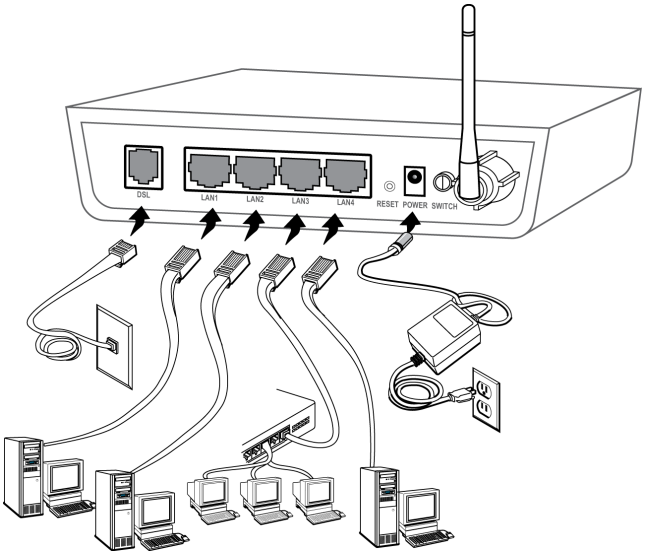
Shut down your PC before connecting the router. To connect your modem:

1. *Connect the ADSL Line*

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



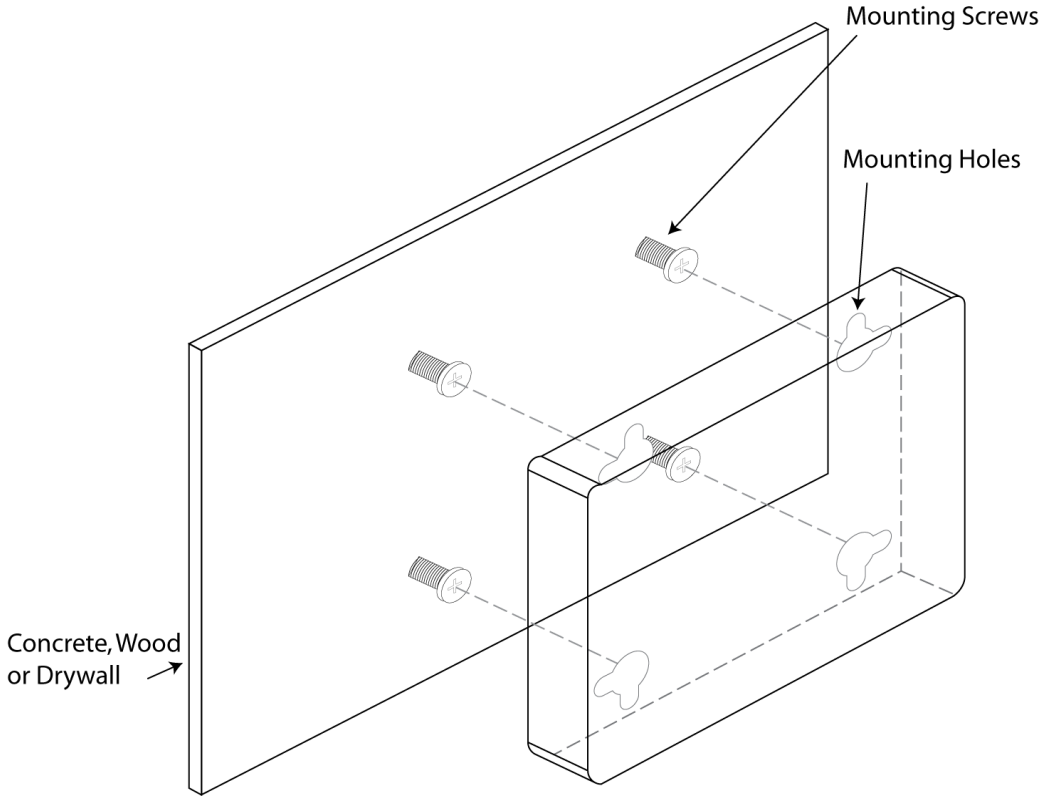
3. *Connect the Power Adapter*

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.

NOTE: Mount the router with the cables facing up, the LEDs facing down.



Unit dimensions

Model	Unit Dimensions	Mounting Holes
1511-A1	1.30"(33 cm) high x 5.67"(144mm) wide x 4.25"(108mm) deep	2 holes- 3.375" (86mm) apart
1512-A1	1.75" (4.4cm) High x 6.56" (14.1cm) Wide x 5.125" (13cm) Deep	4 holes 3.25" (83mm) apart (horizontal) by 4.125" (105mm) apart (vertical)
1518-A1	1.75" (4.4cm) High x 6.56" (14.1cm) Wide x 5.125" (13cm) Deep	4 holes 3.25" (83mm) apart (horizontal) by 4.125" (105mm) apart (vertical)

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**.*

Windows 7

1. *In the Windows taskbar, click the **Start** button and point to **Control Panel** and then click **Network and Internet**.*

2. *In the **Network and Internet** window, click **Network and Sharing Center.***

3. *In the left panel click **Change adapter settings**.*

4. *In the **Network Connections** screen, right click **Local Area Connection** and select **Properties**.*

5. *Listed in the **Local Area Connection** window are the installed network components. Select **Internet Protocol Version 4 (TCP/IP v4)** is checked and then click **Properties**.*

6. *In the **Internet Protocol Version 4 (TCP/IP v4)** 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.*

7. *Click **OK** the **Close** to save your changes and then close the **Control Panel**.*

Chapter 3 The Web User Interface

The 15xx-A1 family of combination modem/routers have 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 Local Area Network (LAN) connections are where you plug in your local computers to the router. The 1518-A1 also has a wireless interface. The router is normally configured to automatically provide all the PCs on your network with Internet addresses.

Your router may be pre-configured with your ISP configuration to ease your installation. Please contact your ISP if you need information on how to connect the modem to your ISP. To set up your router with a basic configuration required by your service provider, you can use the Quick Setup form the top of the navigation bar. In order for this to work, all other WAN services must first be removed. To remove services, from the top navigation bar select **Quick 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.

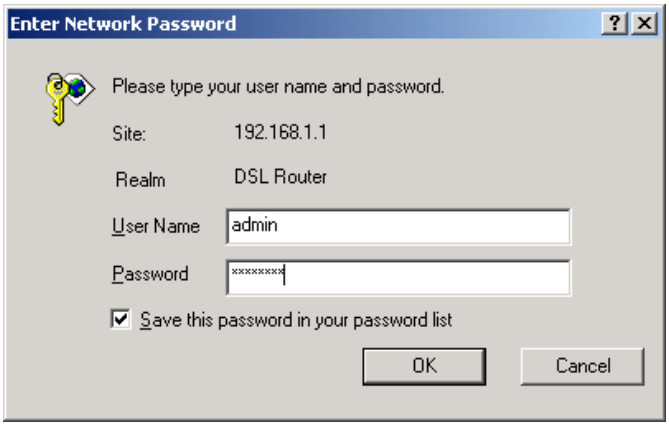
Log in to the Router

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.

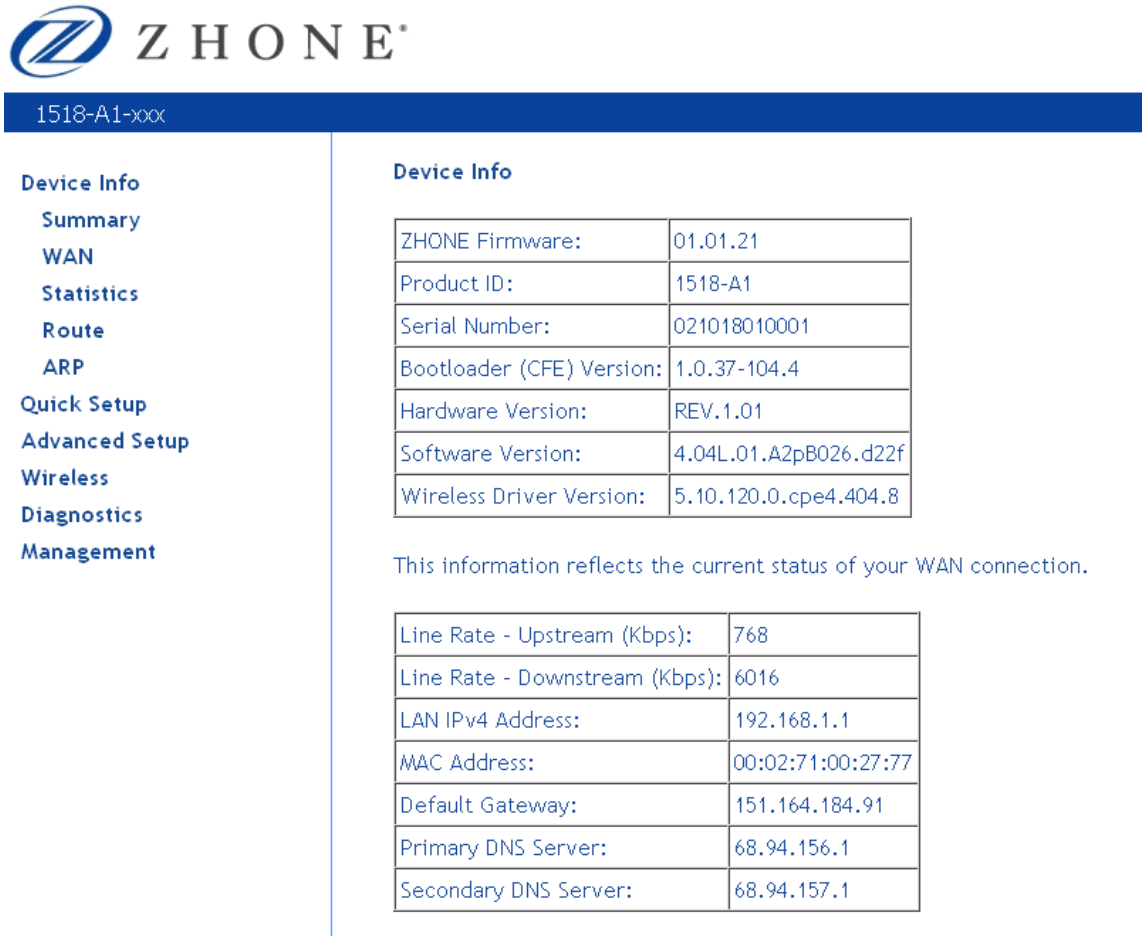
   Note: For security reasons you should change your password as soon as possible.

Note: There are three default user name and password combinations; Admin, Support, and User. 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.

For information about password administration, see *Passwords* on page 103.

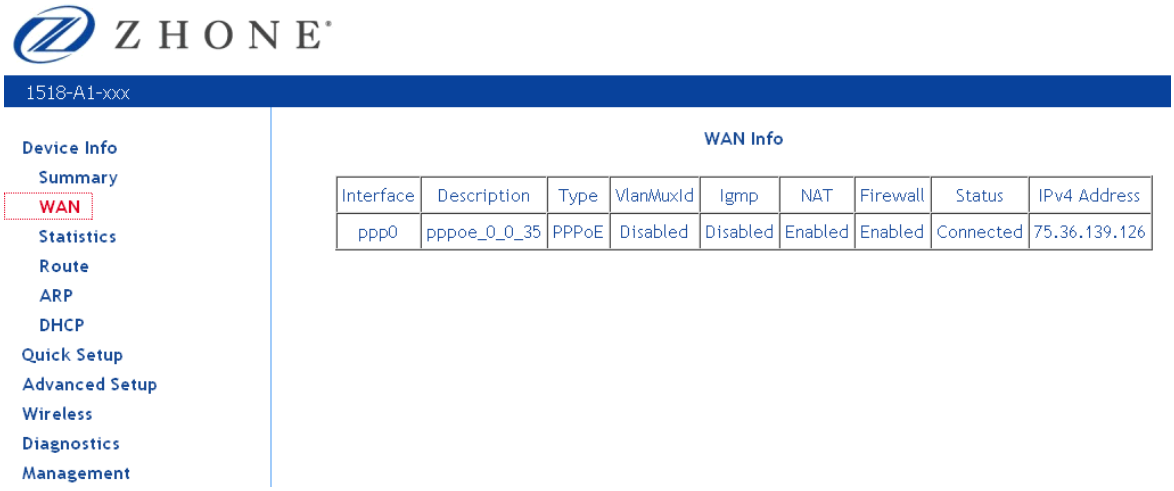
Summary

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.



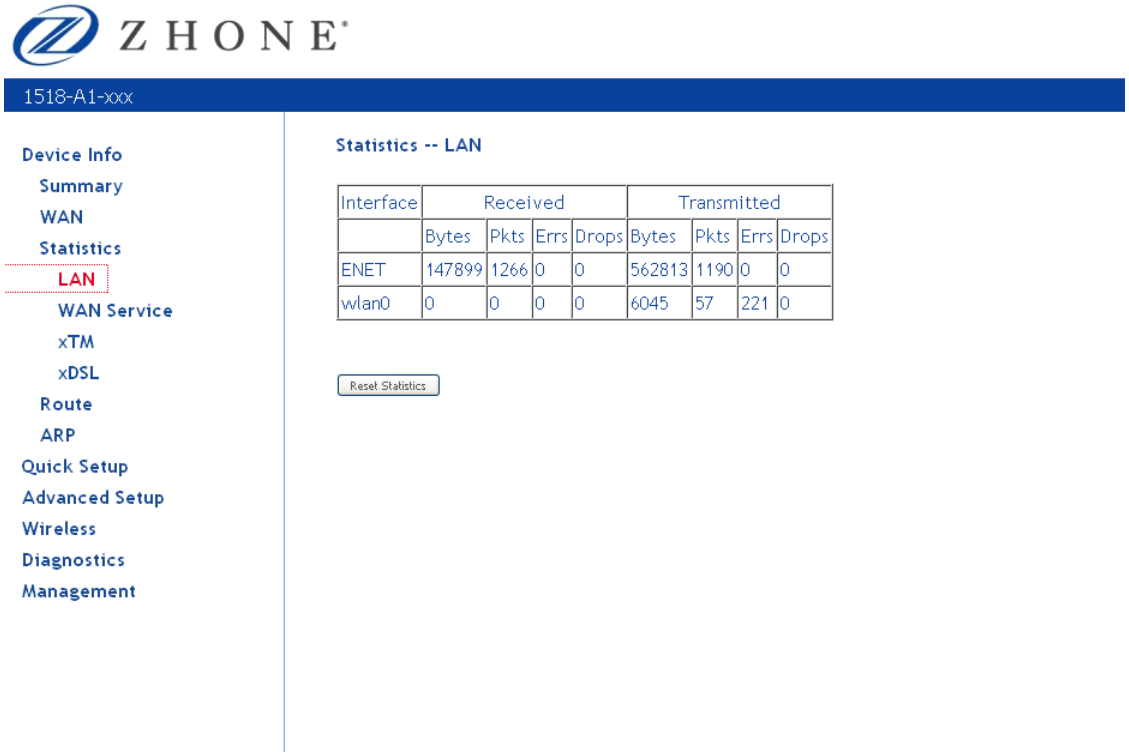
WAN

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.



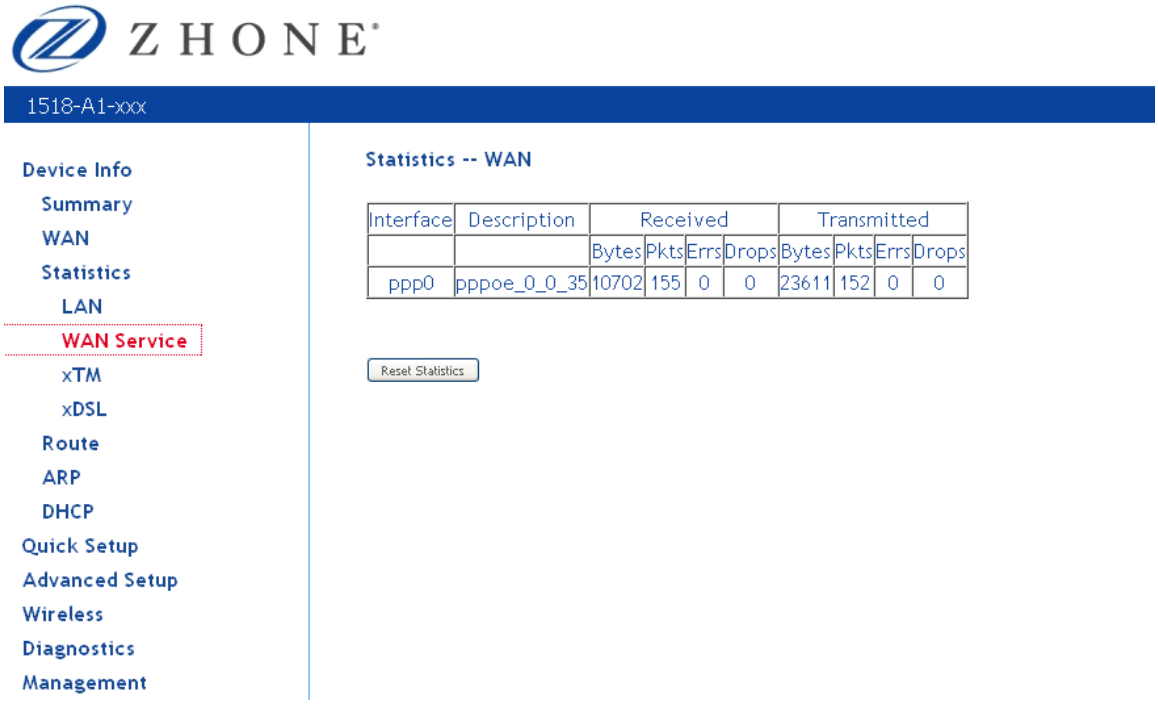
LAN Statistics

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



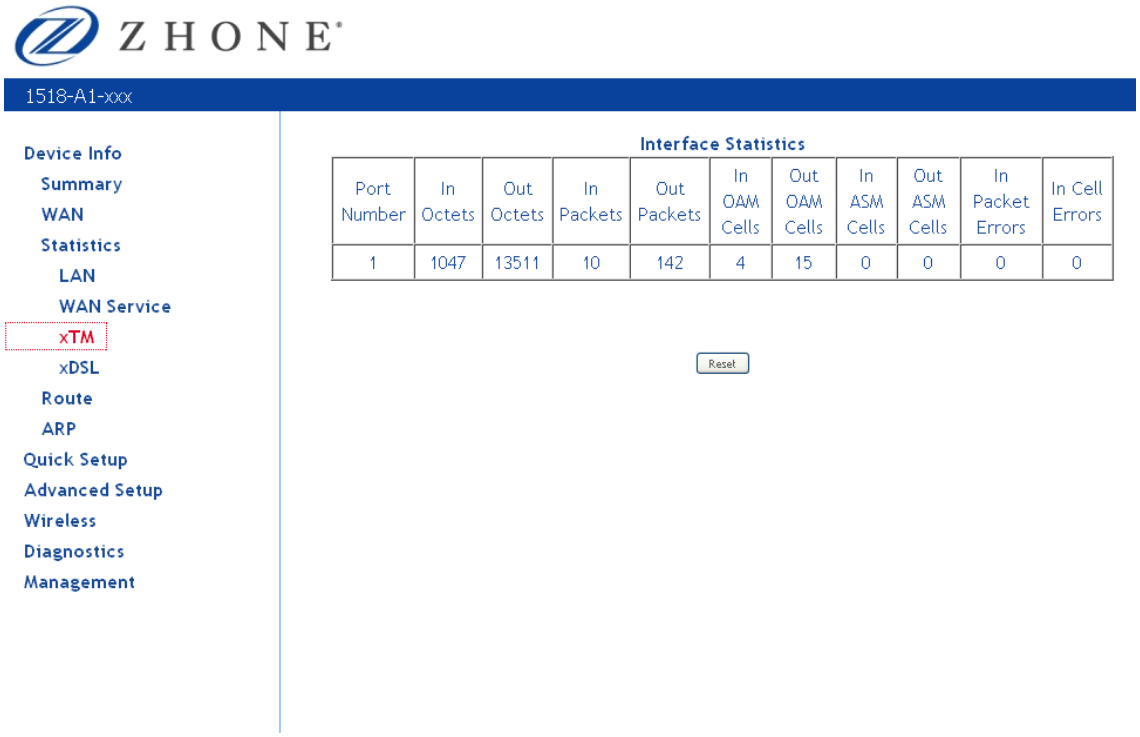
WAN Statistics

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



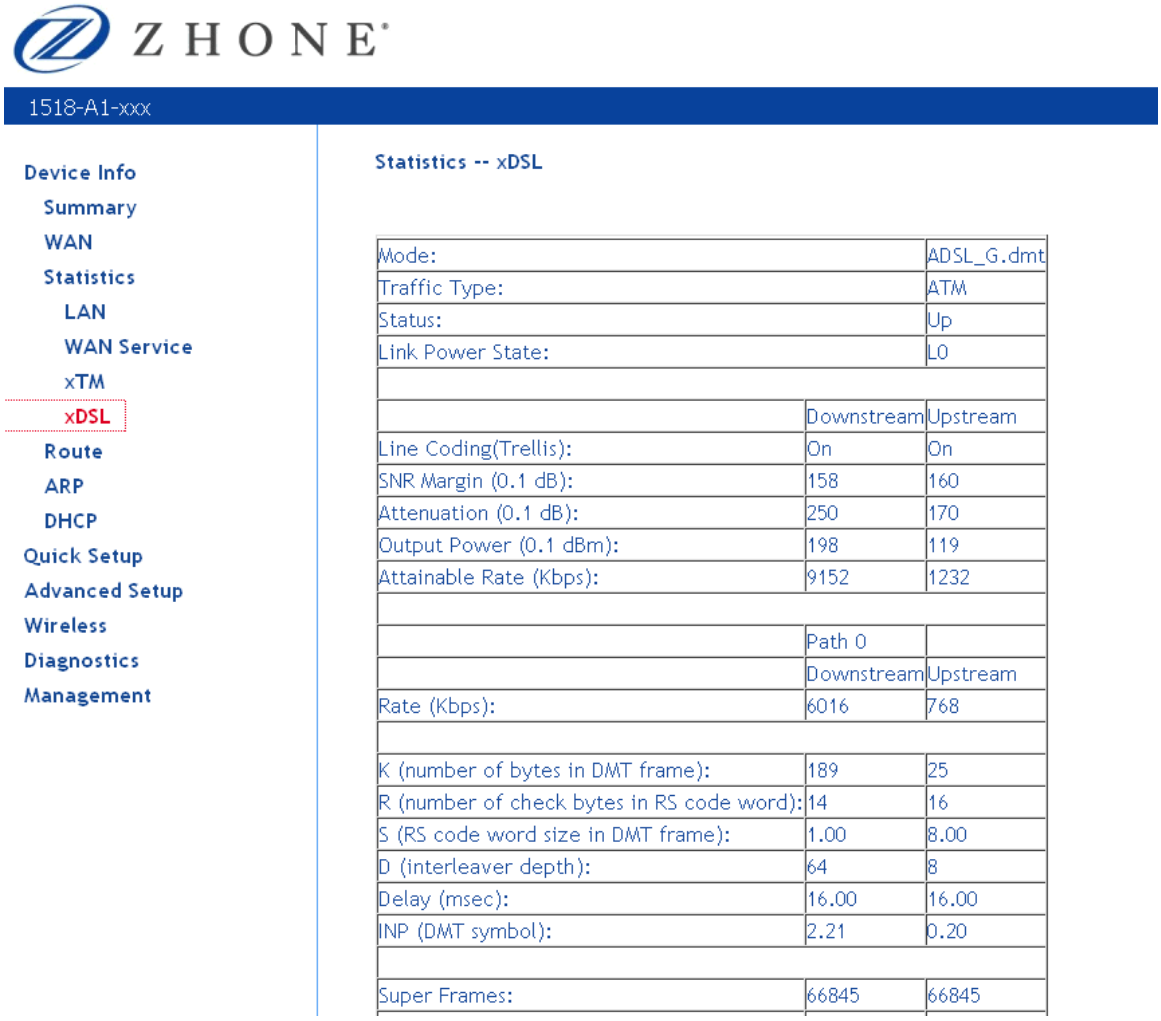
xTM Statistics

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



xDSL Statistics

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



Mode:		ADSL_G.dmt
Traffic Type:		ATM
Status:		Up
Link Power State:		L0
	Downstream	Upstream
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	158	160
Attenuation (0.1 dB):	250	170
Output Power (0.1 dBm):	198	119
Attainable Rate (Kbps):	9152	1232
	Path 0	
	Downstream	Upstream
Rate (Kbps):	6016	768
K (number of bytes in DMT frame):	189	25
R (number of check bytes in RS code word):	14	16
S (RS code word size in DMT frame):	1.00	8.00
D (interleaver depth):	64	8
Delay (msec):	16.00	16.00
INP (DMT symbol):	2.21	0.20
Super Frames:	66845	66845

ADSL BER Test

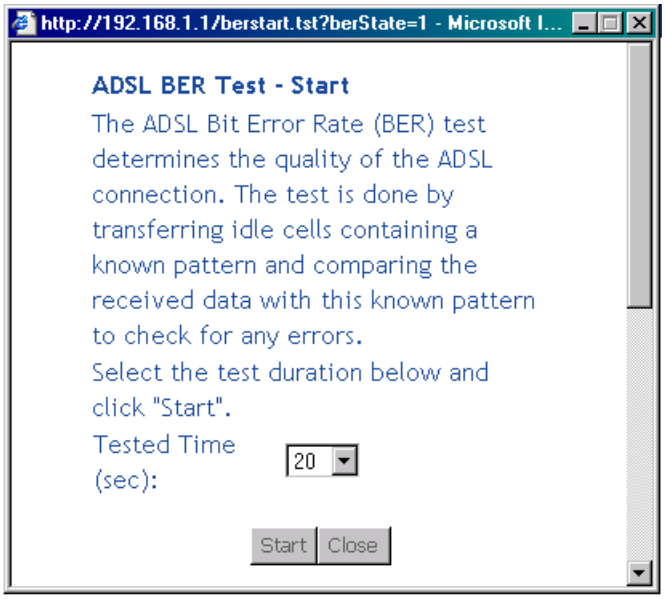
The ADSL Bit Error Rate (BER) test determines the quality of the ADSL connection. The test is performed by transferring idle cells containing a known pattern and comparing the received data with this known pattern to check for any errors The **BER Test** reflects the ratio of error bits to the total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

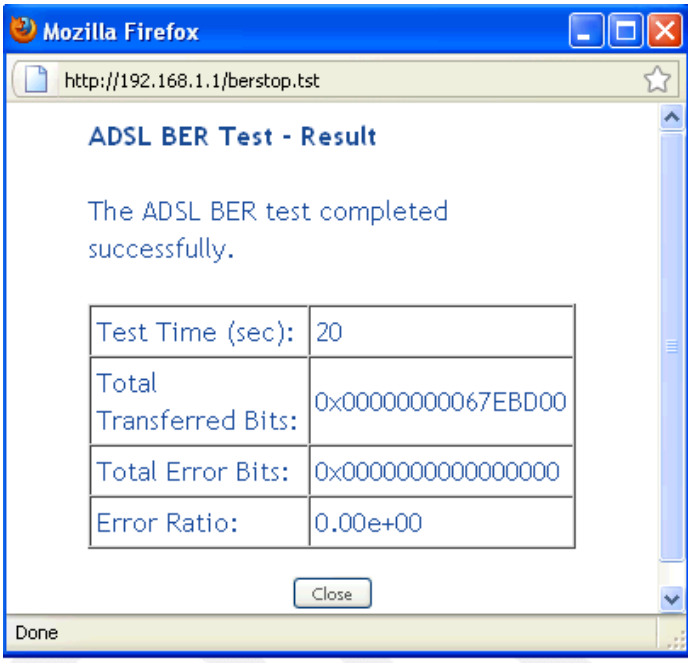
To run a BER test:

1. *On the bottom of the **xDSL statistics** page, click **xDSL BER Test***

2. *In the **Tested Time (sec)** drop down, select the test duration, and then click **Start**.*

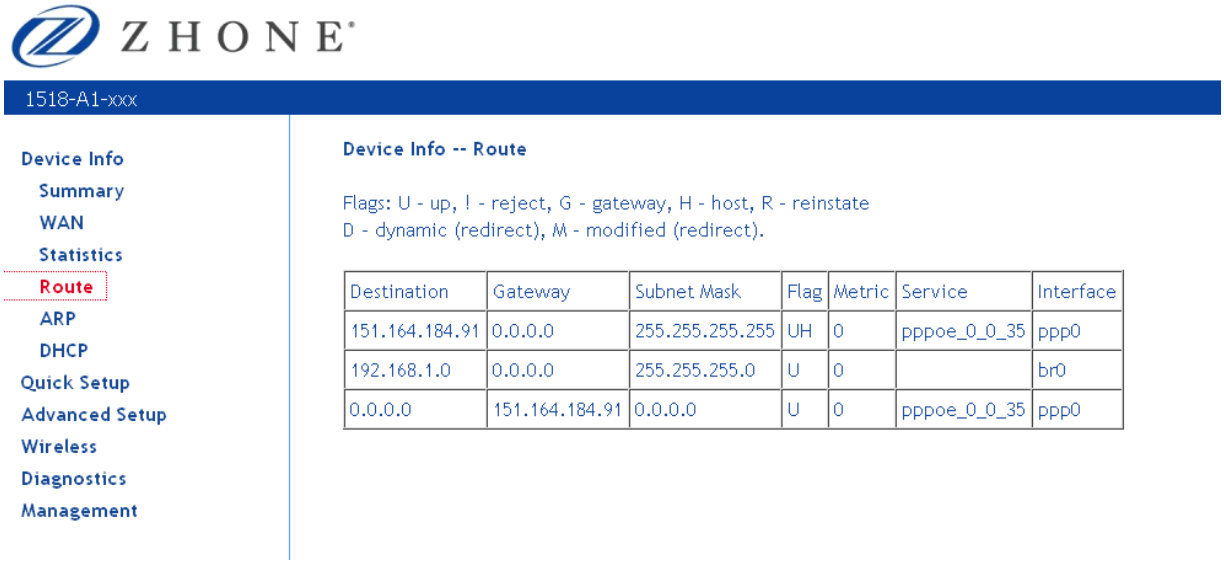


3. *Check the results.*



Route

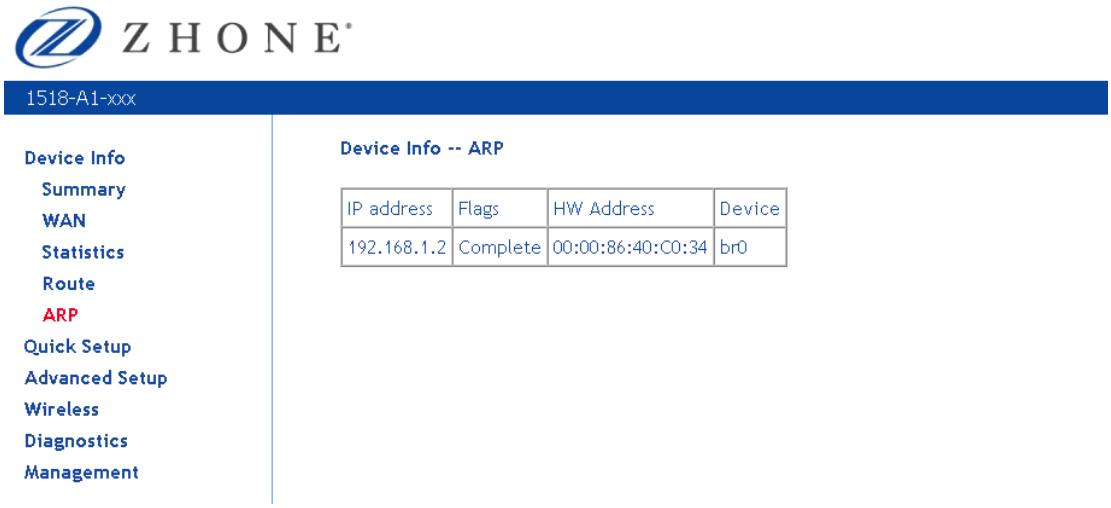
Access the routing status report from the router by clicking **Route** under **Device Info**.



ARP

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

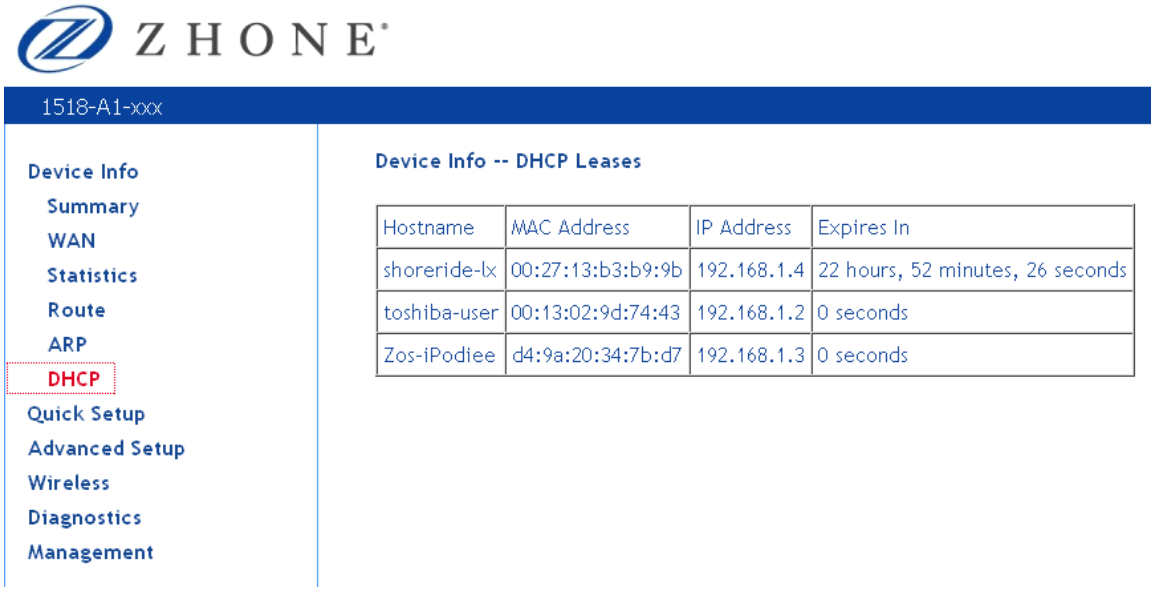
ARP (Address Resolution Protocol) maps the IP address to the physical address, labelled *HW Address* (the MAC address) and identifies computers on the LAN.



DHCP

Display the DHCP lease information by clicking **DHCP** under **Device Info**.

DHCP (Dynamic Host Control Protocol) allows the modem to automatically assign IP addresses, to connected devices. By default, your modem is set up to assign devices addresses from 192.168.1.2 to 192.168.1.254.



Chapter 4 Quick Setup

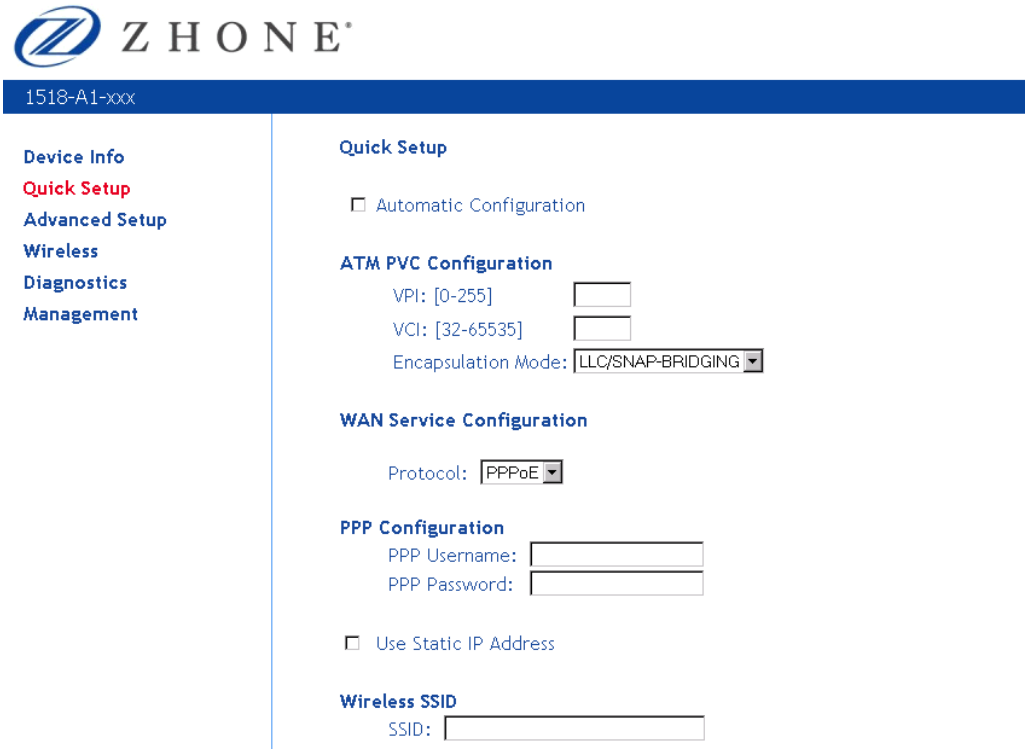
The Automatic Configuration feature will automatically detect the first usable PVC and automatically detect PPPoE, PPPoA, and Bridge Protocol (with DHCP Server available). To use the Automatic Configuration feature you check the **Automatic Configuration** option.

Note: In order for the automatic configuration to work, all previously defined WAN configurations must be removed.

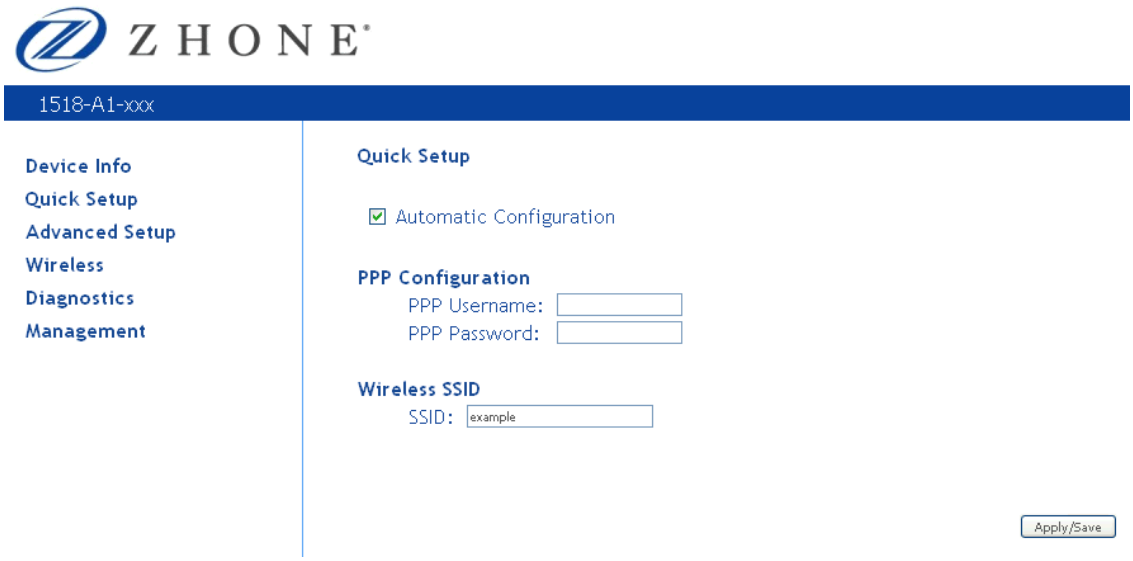
Quick Setup with Automatic Configuration

To enable the Automatic Configuration feature:

1. *From the navigation pane on the left select **Quick Setup**.*



2. *Enter a check in the box labelled **Automatic Configuration**.*

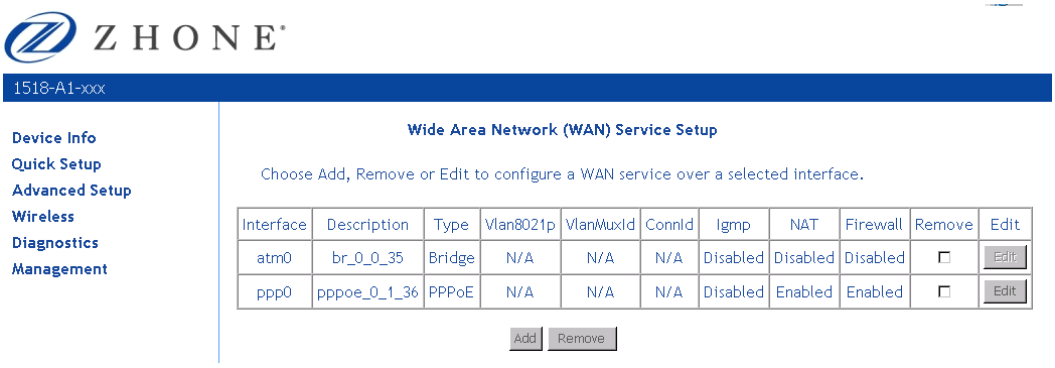


3. *Enter the SSID.*

4. *Click **Apply/Save**.*

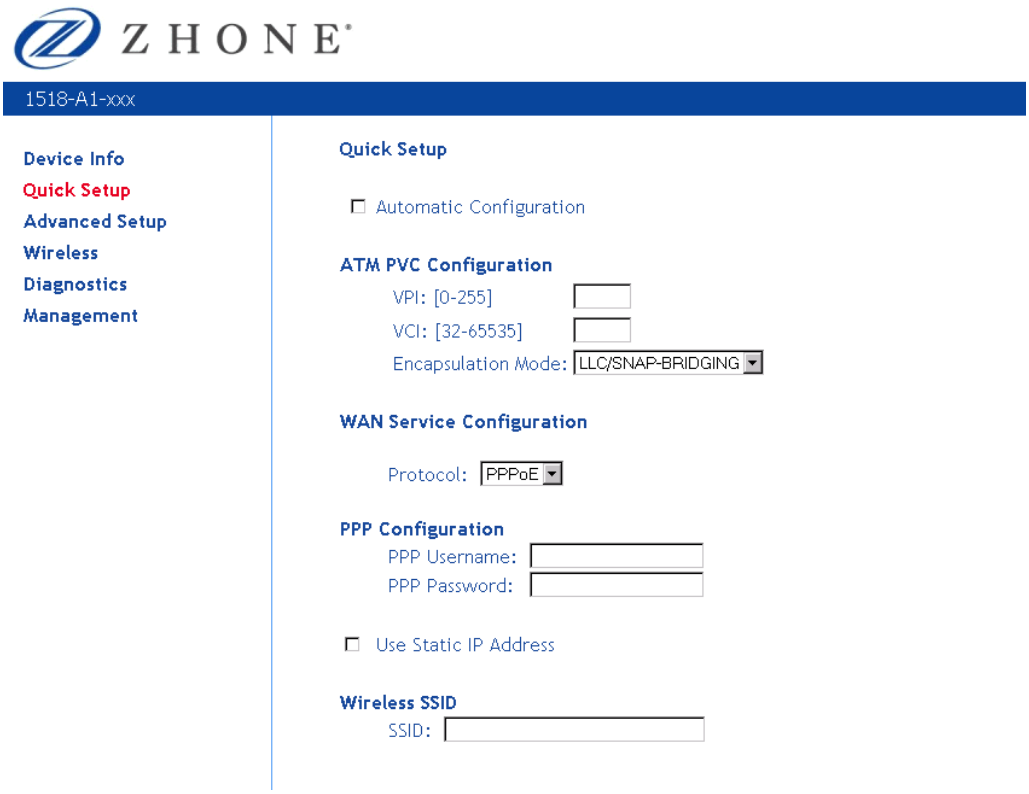
You will see a progress screen

When the connection is complete you will see the Service Setup summary screen.



Quick Setup with Automatic Configuration Disabled

1. *From the navigation pane on the left select **Quick Setup**.*



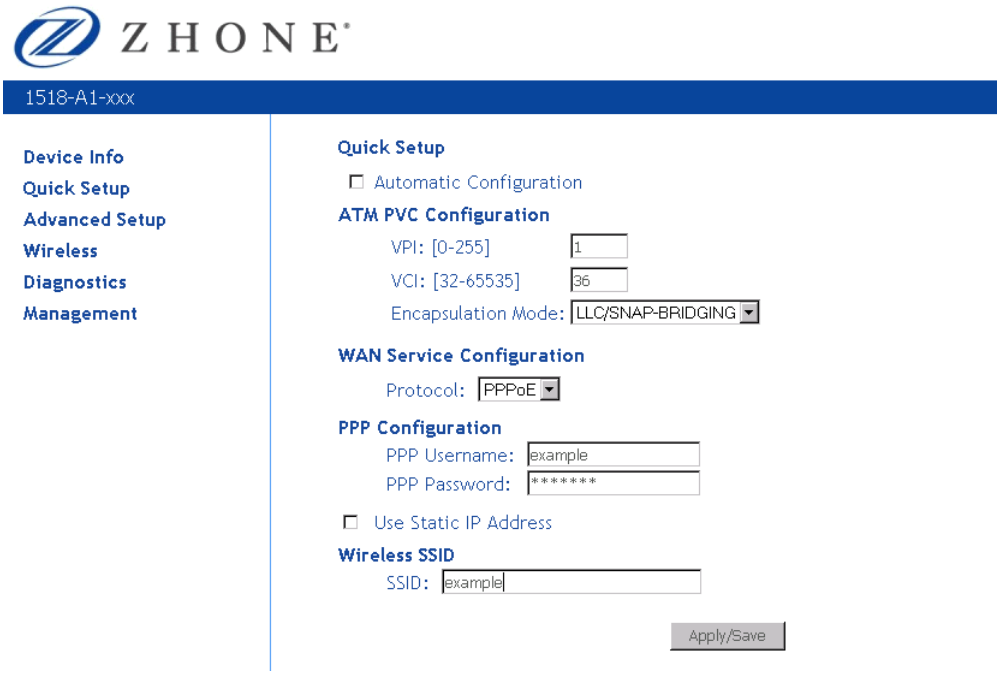
2. *Specify VPI and VCI as directed by your ISP.*

3. *Select the **Encapsulation Mode** as directed by your ISP.*

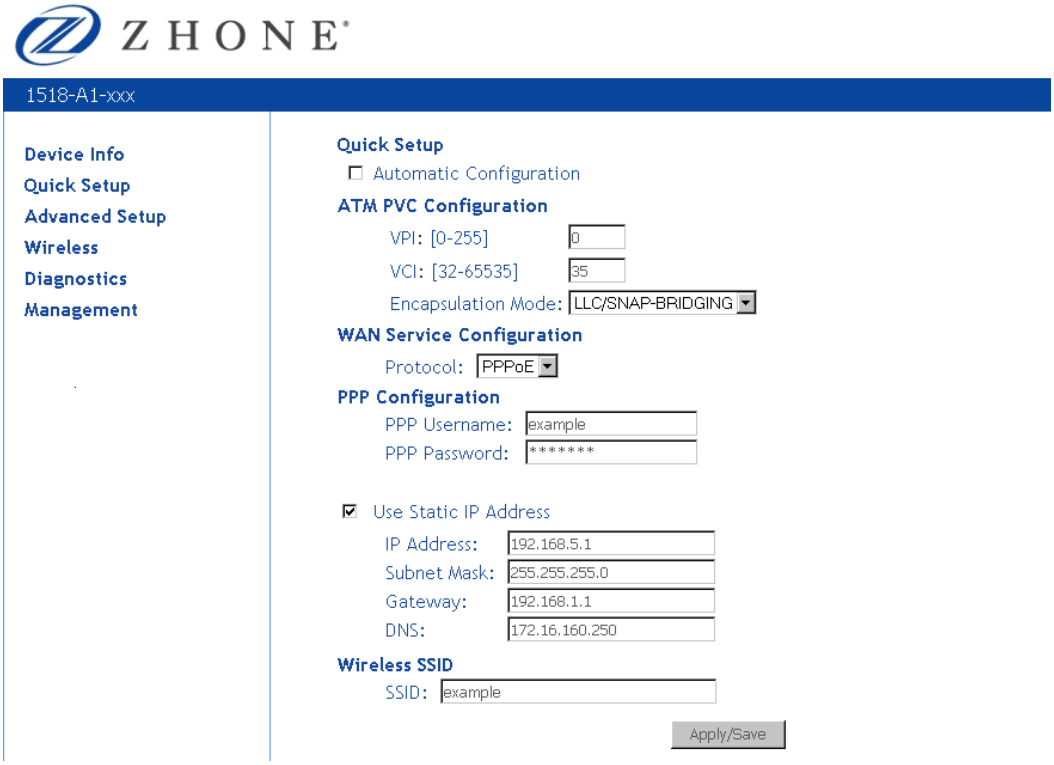
4. *Under **WAN Service Configuration** select the protocol for the WAN connection from the **Protocol** dropdown as directed by your ISP.*

Depending on the protocol selected further parameters are presented. For example, if you selected PPPoE or PPPoA, the PPP Username and Password option appears.

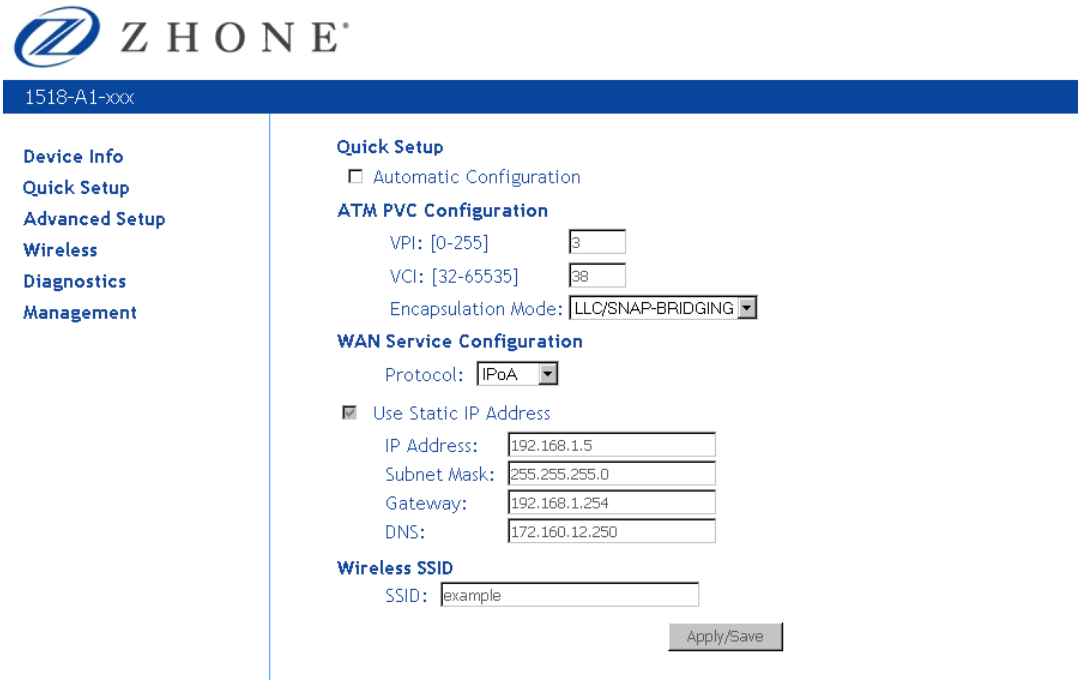
PPPoE and **PPPoA**: You will need to enter the PPP username and password as provided by your ISP.



For PPPoE, if desired, the DSL Router can be configured with a static IP address and Subnet Mask for the LAN interface to correspond to your LAN's IP Subnet. To use a static IP address check the Use Static IP Address option, then enter the **IP Address**, **Subnet Mask**, Default **Gateway** and **DNS** server.

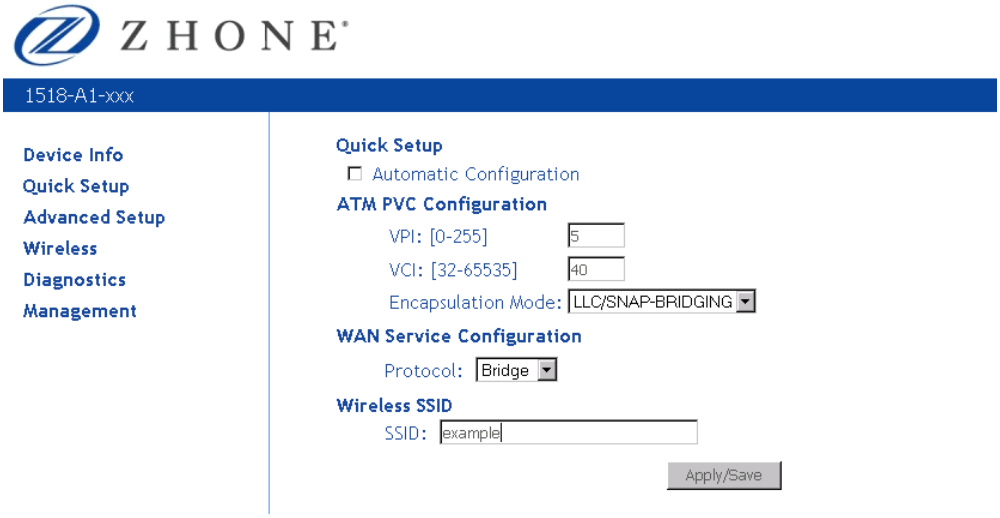


IPoA: For IPoA your ISP will supply information for **IP Address**, **Subnet Mask**, Default **Gateway** and **DNS** server.

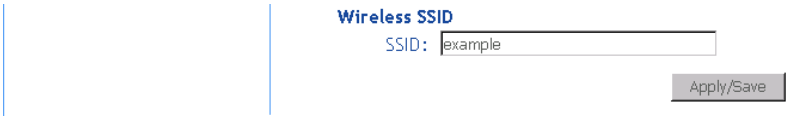


DHCP: With DHCP you need not set any other options.

Bridge: With the Bridge option you do not set any other options.

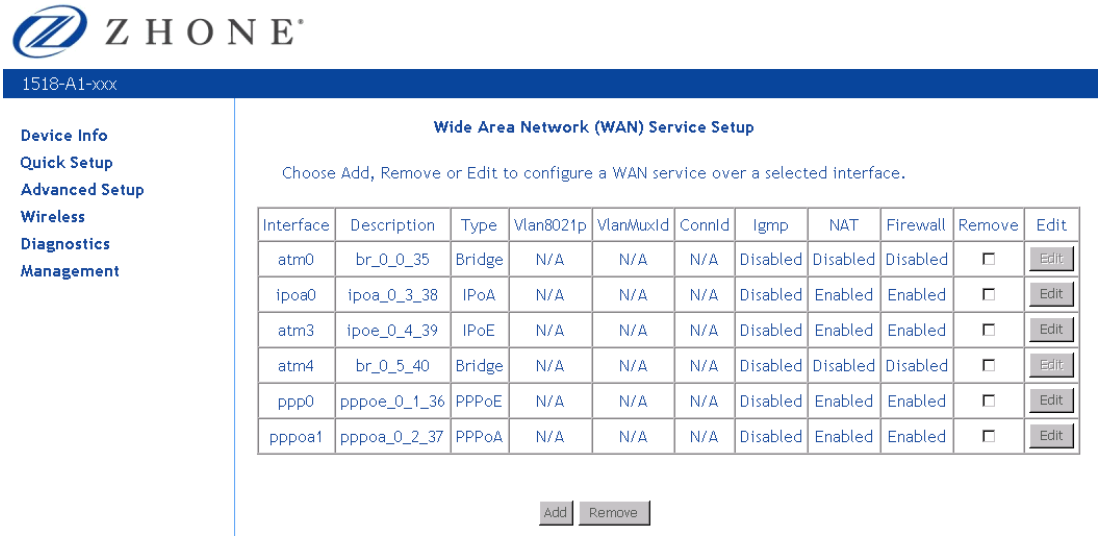


5. *With Quick Setup the router's wireless option is automatically set up and you will need to enter the SSID.*



6. *Click **Apply/Save** to save your settings.*

7. *Upon completion the summary page will be displayed.*



Chapter 5 Advanced Setup

This section contains advanced setup settings. To create a connection you need to define the Layer 2 interface and the WAN service.

Configuration Types

ADSL is an ATM based technology. The 15xx family of routers support Bridging and Ethernet over ATM (EoA) configurations and ATM based configurations:

- Bridging

  Bridging (Layer 2 MAC addressing); uses Ethernet frames.

- PPPoE

  Point to Point Protocol over Ethernet; encapsulates PPP packet in Ethernet. (RFC 2516)

- IPoE

  IP over Ethernet (Layer 3 Internet Protocol addressing in Ethernet frames)

- PPPoA

  Point to Point Protocol over ATM, encapsulates PPP frames in ATM adaption layer 5 (AAL5) packets.

- IPoA

  IP over ATM (Layer 3 Internet Protocol addressing in AAL5 packets

To configure a connection, you first configure the connection type. EoA, PPPoA, or IPoA.

1. *Add a Layer 2 interface and select the connection type.*

   EoA is used for PPPoE, IPoE and Bridge connections. PPPoA and IPoA are AAL5 based connections

2. *Set the WAN interface*

   The WAN interface options to select are determined by the Layer 2 interface type.

Add a Layer 2 Interface

1. *In the left hand menu pane, click **Advanced Setup**.*

2. *Under Advanced Setup, click Layer2 Interface then ATM Interface, then click the **Add** button.*

3. *In the **VPI** and **VCI** text boxes enter appropriate VPI/VCI numbers.*

   VPI/VCI (Virtual Path Identifier/Virtual Circuit Identifier) values essentially define the “pipe” which sends data from the upstream device to the modem/router. The VPI/VCI values will be given to you by your ISP.

4. *Under **Select DSL Link Type** select the appropriate DSL link type:*

5. *For the EoA options you may select a connection mode:*

   Default Mode: a single service over the one connection

   VLAN MUX Mode: multiple VLAN services over the one connection

   MSC Mode: multiple services over one connection. With the MSC Mode setting a single PVC layer 2 interface is created upon which multiple WAN services may be created

6. *From the **Encapsulation Mode** drop down select the appropriate option**:***

   For **EoA** options (PPPoE, IPoE, Bridge) select **LLC/SNAP BRIDGING**

   For **PPPoA** select **VC/MUX**

   For **IPoA** select **LLC/SNAP ROUTING**

7. *From the **Service Category** drop down select the type of service*

   The service category selection will be provided by your ISP. The service category defines 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).
     - Specify a Peak cell Rate Peak cell rate is 1-3442 (cells / sec).
   - **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).
     - Specify a Peak cell Rate. The Peak Cell Rate is rate is 1-3442 (cells / sec).
   - **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.
     - Specify a Peak cell Rate. 1-3442 (cells / sec).
     - Sustainable Cell Rate. 1-3442 (cells / sec).
     - Maximum Burst Size. The maximum number of contiguous cells that can be sent at the Peak Cell Rate. 1-1000000 (cells / sec)
   - **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.
     - Specify a Peak cell Rate. 1-3442 (cells / sec).
     - Sustainable Cell Rate. 1-3442 (cells / sec).
     - Maximum Burst Size. The maximum number of contiguous cells that can be sent at the Peak Cell Rate. 1-1000000 (cells / sec)

   If Quality of Service (QoS) prioritization of IP traffic is needed, select **Enable IP QoS**

8. *Click **Apply/Save** to add the appropriate WAN service*

Add a Bridge WAN Service

1. *Add an EoA Layer 2 interface as described above (**Add a Layer 2 Interface**).*

2. *Under Advanced Setup click WAN Service then click **Add**.*

3. *On the **WAN Service Interface Configuration** page, select the DSL link associated with the bridge interface from the drop down, then click **Next***

4. *On the **WAN Service Configuration** page, select **Bridging***

5. *On the **WAN Service Configuration** page, enter a name if you wish to customize the description shown for the service, then click **Next**.*

6. *In the **WAN Setup – Summary** page, review the settings for this interface. Click **Apply/Save** to accept the settings.*

   If you made a mistake on the configuration and want to make changes to it, select the **Remove** check box and click the **Remove** button.

   In the **Wide Area Network (WAN) Service Setup** page, you will see the new WAN interface added.

Add a PPPoE WAN Service

1. *Add an EoA Layer 2 interface as described above (**Add a Layer 2 Interface**).*

2. *Under **Advanced Setup** click **WAN Service** then click **Add***

3. *On the **WAN Service Interface Configuration** page, select the DSL link associated with the PPPOE interface from the drop down, then click **Next***

4. *On the **WAN Service Configuration** page, select **PPP over Ethernet (PPPoE).***

5. *On the **WAN Service Configuration** page, enter a name if you wish to customize the description shown for the service, then click **Next**.*

6. *On the **PPP Username and Password** page you will need the following information:*

   - **PPP Username**: Your account from ISP to access Internet.
   - **PPP Password:** The password assigned by your ISP.

   Note: If you set the username/password to default/default, the modem will redirect the user to a web page within the modem to change their password when they first log on.

   - **PPPoE Service Name**: Server name of network ISP. No need to set.
   - **Authentication Method**: Authentication mode of network ISP. Default is AUTO
   - **Enable Fullcone NAT**: RFC 3489 defines four types of Network Address Translation (NAT). Fullcone NAT. As with other types of NAT there is a mapping from a public IP address to a private IP address. The external public IP address is extended with the external port. With Fullcone NAT once the mapping is created any external host may send packets to the private IP address by sending to the external IP address and port. Other types of NAT have restrictions such as the sending IP address must initially have had packets sent from the private IP address and port regardless of the external port, or from the private IP address and the external port.

     Enable NAT must be checked for Fullcone NAT to be used.
   - **MAC Clone**: Clicking the **Clone the PC MAC Address** button will use the MAC address from the connected PC for the MAC address of the router.
   - **Dial on demand**: When this mode is selected, the connection that has no traffic within assigned disconnect timeout (e.g. 1 minute) will be automatically disconnected. The connection will be activated again when traffic arrives. This function is advantageous for

users who are charged with online time. It should be noticed that some programs automatically link to Internet. Computer will send data to network when infected by virus. Connection will not be disconnected under these data streams.

- **Inactivity Timeout**: When **Dial on demand** is selected, this input box indicates that after how long the connection will be disconnected in the absence of traffic. If the value is 0, connection will not be disconnected.
- **MTU**: the Maximum transmission unit (MTU) value may be set for your needs. Higher MTU can provide for a more efficient link because each packet will carry more data while the overhead in the packet such as header information does not get larger with the size of the packet. So the bulk throughput on the link will go up. Generally a large packet size can occupy the time on the link, so the higher MTU can increase lag time and minimum latency which is not appropriate for all applications.
- **Manual Connect**: connect/disconnect PPPoE connection manually
- **PPP IP extension**: Allows only one PC on the LAN. The public IP address assigned by the remote using the PPP/IPCP protocol is actually not used on the WAN PPP interface. Instead, it is forwarded to the PC's LAN interface through DHCP.

  Only one PC on the LAN can be connected to the remote since the DHCP server within the ADSL gateway has only a single IP address to assign to a LAN device. NAT and firewall are disabled when this option is selected. The ADSL gateway becomes the default gateway and DNS server to the PC through DHCP using the LAN interface IP address. The ADSL gateway extends the IP subnet at the remote service provider to the LAN PC. That is, the PC becomes a host belonging to the same IP subnet. The ADSL gateway bridges the IP packets between WAN and LAN ports, unless the packet is addressed to the gateway's LAN IP address.
- **Enable NAT**: To define NAT services in the **Advanced Setup | NAT** screens, NAT must be enabled.
- **NAT Public Address** (available if NAT is enabled). **Automatic** means the modem will use pubic IP addresses provided by the network; **Menu IP addresses** means that the modem will use the addresses you specify.
- **Enable Firewall**: Enables Firewall.
- **Use Static IPv4 Address**: Defines a static IP address (v4) which you enter in the **IPv4 Address** text box which is displayed when the **Use Static IPv4 Address** check box is selected.
- **Enable PPP Debug Mode**: Used to debug PPPoE issues. Use only when instructed by your ISP.
- **Enable KeepAlive**: Enables/disables TCP keep alive packets.
- **Bridge PPPoE Frames Between WAN and Local Ports**: By default the bridge PPPoE frame between WAN and local ports is on. This allows a PC behind the modem to be the PPPoE termination point. PPPoE authentication is passed on to the PC instead of to the router. If there are multiple PCs then, each one will have a PPPoE authentication. Note that this option is not applicable for PPPoA.
- **Enable IGMP Multicast Proxy**: Configures the router for IGMP snooping so the router can keep limit multicast traffic.

7. *Click **Next**.*

8. *On the **Routing — Default Gateway** page set the priority of WAN interfaces used as default gateways then click **Next***

If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected Default Gateway Interfaces** window. Top is the highest priority; bottom the lowest.

Change the priority order by removing all items from the **Selected Default Gateway Interfaces** window by selecting them, then clicking the right arrow button. Select the items in

the priority order, then click the left arrow to move them into the **Selected Default Gateway Interfaces** window.

9. *On the **DNS Server Configuration** page set the priority of WAN interfaces to be used as DNS server interfaces, or specify a static DNS Primary and Secondary server, then click **Next.***

   If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected DNS Server Interfaces** window. Top is the highest priority; bottom the lowest.

   Change the priority order by removing all items from the **Selected DNS Server Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected DNS Server Interfaces** window.

   For a **Static DNS IP Address**, enter a primary and secondary DNS server for your modem,

10. *On the **WAN Setup – Summary** page, review your settings and click **Apply/Save** to accept the settings. To change your settings, click the **Back** button on the **WAN Setup – Summary** page (do not click the browser Back button).*

    In the **Wide Area Network (WAN) Service Setup** page, you will see the new WAN interface added.

Add an IPoE WAN Service

1. *Add an EoA Layer 2 interface as described above (**Add a Layer 2 Interface**).*

2. *Under **Advanced Setup** click **WAN Service** then click **Add***

3. *On the **WAN Service Interface Configuration** page, select the DSL link associated with the IPoE interface from the drop down, then click **Next***

4. *On the **WAN Service Configuration** page, select **IP over Ethernet**.*

5. *On the **WAN Service Configuration** page, enter a name if you wish to customize the description shown for the service, then click **Next**.*

6. *On the **WAN IP Settings** page you will need to enter information provided by your ISP, then click **Next**.*

7. *On the **Network Address Translation Settings** you will need to enter information provided by your ISP, then click **Next.***

   - **Enable NAT** must be checked for Fullcone NAT to be used.
   - **Enable Fullcone NAT**: RFC 3489 defines four types of Network Address Translation (NAT). Fullcone NAT. As with other types of NAT there is a mapping from a public IP address to a private IP address. The external public IP address is extended with the external port. With Fullcone NAT once the mapping is created any external host may send packets to the private IP address by sending to the external IP address and port. Other types of NAT have restrictions such as the sending IP address must initially have had packets sent from the private IP address and port regardless of the external port, or from the private IP address and the external port.
   - **Enable Firewall**: Enables Firewall.
   - **Enable IGMP Multicast**: Configures the router for IGMP snooping so the router can keep limit multicast traffic.

8. *On the **Routing — Default Gateway** page set the priority of WAN interfaces used as default gateways then click **Next***

   *If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected Default Gateway Interfaces** window. Top is the highest priority; bottom the lowest.*

   Change the priority order by removing all items from the **Selected Default Gateway Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected Default Gateway Interfaces** window.

9. *On the **DNS Server Configuration** page set the priority of WAN interfaces to be used as DNS server interfaces, or specify a static DNS Primary and Secondary server, then click **Next.***

   *If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected DNS Server Interfaces** window. Top is the highest priority; bottom the lowest.*

   Change the priority order by removing all items from the **Selected DNS Server Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected DNS Server Interfaces** window.

   For a **Static DNS IP Address**, enter a primary and secondary DNS server for your modem,

10. *On the **WAN Setup – Summary** page review your settings and click **Apply/Save** to accept the settings. To change your settings, click the **Back** button on the **WAN Setup – Summary** page (do not click the browser Back button).*

    *In the **Wide Area Network (WAN) Service Setup** page, you will see the new WAN interface added.*

Add a PPPoA WAN Service

1. *Add a PPPoA Layer 2 interface as described above (**Add a Layer 2 Interface**).*

2. *Under **Advanced Setup** click **WAN Service** then click **Add***

3. *On the **WAN Service Interface Configuration** page, select the DSL link associated with the PPOA interface from the drop down, then click **Next***

4. *On the **WAN Service Configuration** page, enter a name if you wish to customize the description shown for the service, then click **Next**.*

5. *On the **PPP Username and Password** page you will need to enter information provided by your ISP. When you are done, click **Next**.*

   - **PPP Username**: Your account from ISP to access Internet.
   - **PPP Password**: The password assigned by your ISP.
   - **Authentication Method**: Authentication mode of network ISP. Default is AUTO.
   - **Enable Fullcone NAT**: RFC 3489 defines four types of Network Address Translation (NAT). Fullcone NAT. As with other types of NAT there is a mapping from a public IP address to a private IP address. The external public IP address is extended with the external port. With Fullcone NAT once the mapping is created any external host may send packets to the private IP address by sending to the external IP address and port.

Other types of NAT have restrictions such as the sending IP address must initially have had packets sent from the private IP address and port regardless of the external port, or from the private IP address and the external port.

Enable NAT must be checked for Fullcone NAT to be used.

- **Dial on demand**: When this mode is selected, the connection that has no traffic within assigned disconnect timeout (e.g. 1 minute) will be automatically disconnected. The connection will be activated again when traffic arrives. This function is advantageous for users who are charged with online time. It should be noticed that some programs automatically link to Internet. Computer will send data to network when infected by virus. Connection will not be disconnected under these data streams.
- **Inactivity Timeout**: When "Dial on demand" is selected, this input box indicates that after how long the connection will be disconnected in the absence of traffic. If the value is 0, connection will not be disconnected.
- **Enable manual MTU set**: the Maximum transmission unit (MTU) value may be set for your needs. Higher MTU can provide for a more efficient link because each packet will carry more data while the overhead in the packet such as header information does not get larger with the size of the packet. So the bulk throughput on the link will go up. Generally a large packet size can occupy the time on the link, so the higher MTU can increase lag time and minimum latency which is not appropriate for all applications.
- **Manual Connect**: connect/disconnect PPPoE connection manually
- **Enable NAT**: To define NAT services in the **Advanced Setup | NAT** screens, NAT must be enabled.
- **Enable Firewall**: Enables Firewall.
- **Use Static IPv4 Address**: Defines a static IP address (v4) which you enter in the **IPv4 Address** text box which is displayed when the **Use Static IPv4 Address** check box is selected.
- **Enable PPP Debug Mode**: Used to debug PPPoE issues. Use only when instructed by your ISP.
- **Enable KeepAlive**: Enables/disables TCP keep alive packets
- **Enable IGMP Multicast Proxy**: Configures the router for IGMP snooping so the router can keep limit multicast traffic.

6. *On the **Routing — Default Gateway** page set the priority of WAN interfaces used as default gateways then click **Next***

If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected Default Gateway Interfaces** window. Top is the highest priority; bottom the lowest.

Change the priority order by removing all items from the **Selected Default Gateway Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected Default Gateway Interfaces** window.

7. *On the **DNS Server Configuration** page set the priority of WAN interfaces to be used as DNS server interfaces then click **Next***

*If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected DNS Server Interfaces** window. Top is the highest priority; bottom the lowest.*

Change the priority order by removing all items from the **Selected DNS Server Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected DNS Server Interfaces** window.

For a **Static DNS IP Address**, enter a primary and secondary DNS server for your modem,

8. *On the **WAN Setup – Summary** page review your settings and click **Apply/Save** to accept the settings. To change your settings, click the **Back** button on the **WAN Setup – Summary** page (do not click the browser Back button).*

   *In the **Wide Area Network (WAN) Service Setup** page, you will see the new WAN interface added.*

Add an IPoA WAN Service

1. *Add a PPPoA Layer 2 interface as described above (Add a Layer 2 Interface).*

2. *Under Advanced Setup click WAN Service then click Add*

3. ***WAN Service Interface Configuration** page, select the DSL link associated with the IPoA interface from the drop down, then click **Next***

4. *On the **WAN Service Configuration** page, enter a name if you wish to customize the description shown for the service, then click **Next**.*

5. *On the **WAN IP Settings** page enter a WAN IP address and WAN subnet mask as instructed by your ISP, then click **Next**.*

6. *On the **Network Address Translation Settings** you will need to enter information provided by your ISP, then click **Next.***

   - **Enable NAT** must be checked for Fullcone NAT to be used.
   - **Enable Fullcone NAT**: RFC 3489 defines four types of Network Address Translation (NAT). Fullcone NAT. As with other types of NAT there is a mapping from a public IP address to a private IP address. The external public IP address is extended with the external port. With Fullcone NAT once the mapping is created any external host may send packets to the private IP address by sending to the external IP address and port. Other types of NAT have restrictions such as the sending IP address must initially have had packets sent from the private IP address and port regardless of the external port, or from the private IP address and the external port.
   - **Enable Firewall**: Enables Firewall.
   - **Enable IGMP Multicast**: Configures the router for IGMP snooping so the router can keep limit multicast traffic.

7. *On the **Routing — Default Gateway** page set the priority of WAN interfaces used as default gateways then click **Next***

   If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected Default Gateway Interfaces** window. Top is the highest priority; bottom the lowest.

   Change the priority order by removing all items from the **Selected Default Gateway Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected Default Gateway Interfaces** window.

8. *On the **DNS Server Configuration** page set the priority of WAN interfaces to be used as DNS server interfaces then click **Next***

   If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected DNS Server Interfaces** window. Top is the highest priority; bottom the lowest.

Change the priority order by removing all items from the **Selected DNS Server Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected DNS Server Interfaces** window.

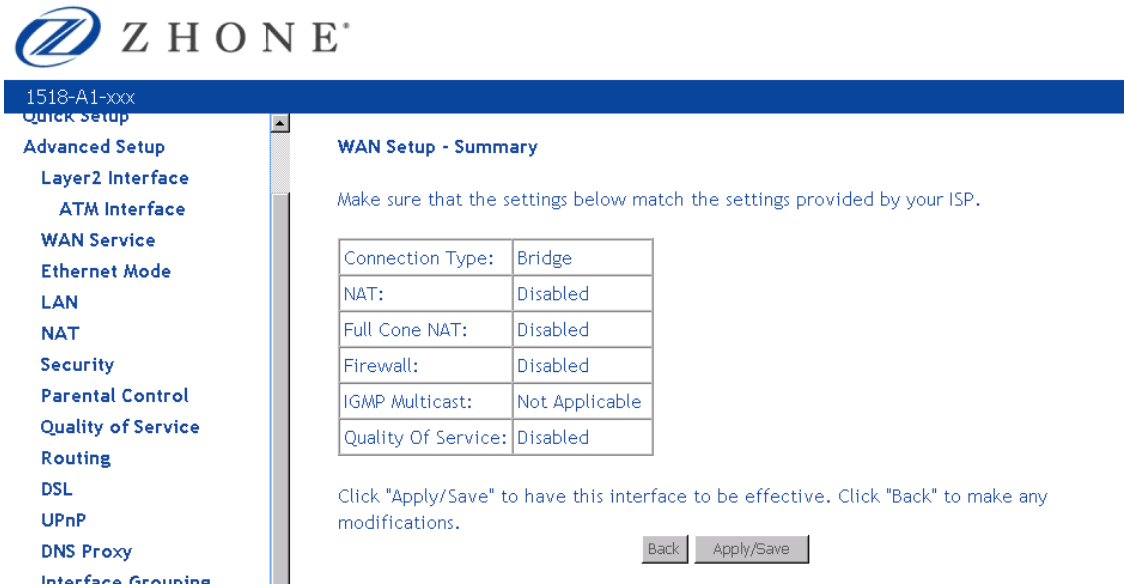
9. *For a **Static DNS IP Address**, enter a primary and secondary DNS server for your modem,*

10. *On the **WAN Setup – Summary** page review your settings and click **Apply/Save** to accept the settings. To change your settings, click the **Back** button on the **WAN Setup – Summary** page (do not click the browser Back button).*

    In the **Wide Area Network (WAN) Service Setup** page, you will see the new WAN interface added.

WAN Setup — Summary

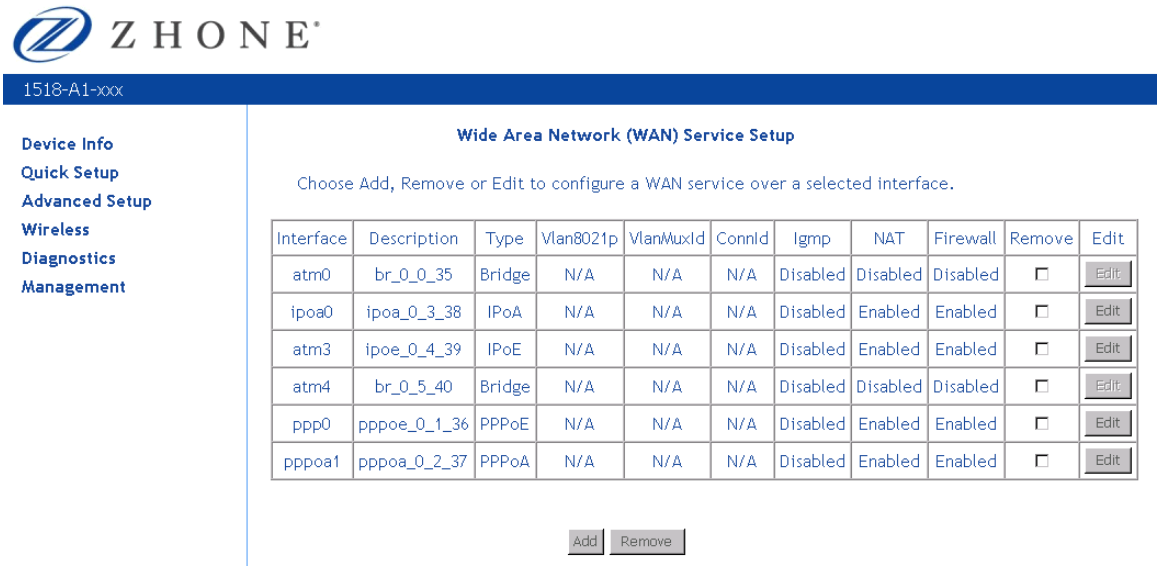
When the settings are complete, the next screen shows a **WAN Setup – Summary** screen displaying the WAN configurations made.



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

2. *Click **Apply/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.



Remove a Connection

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

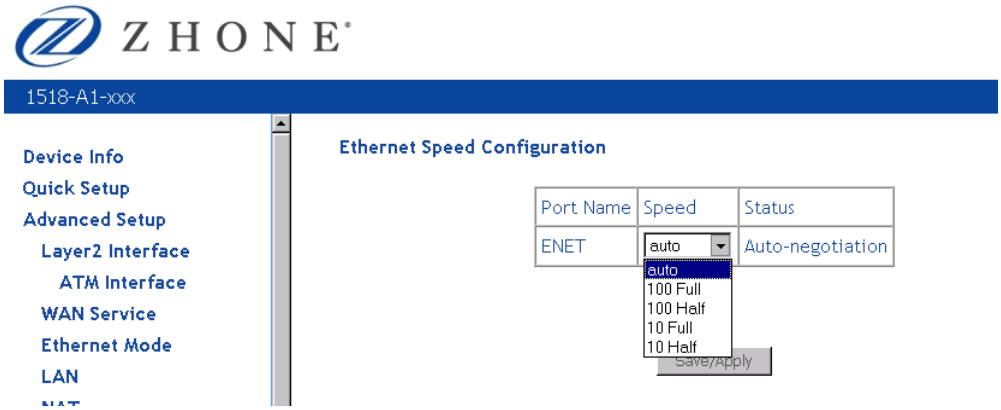
Edit a Connection

If you want to modify a connection from the listed WAN setup, click the **Edit** button next to the connection.

NOTE: Some connection settings cannot be edited after they have been created. You will need to delete and re-add the connection to change some settings.

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 that all the connected interfaces can operate at.



LAN Local Area Network (LAN) Setup

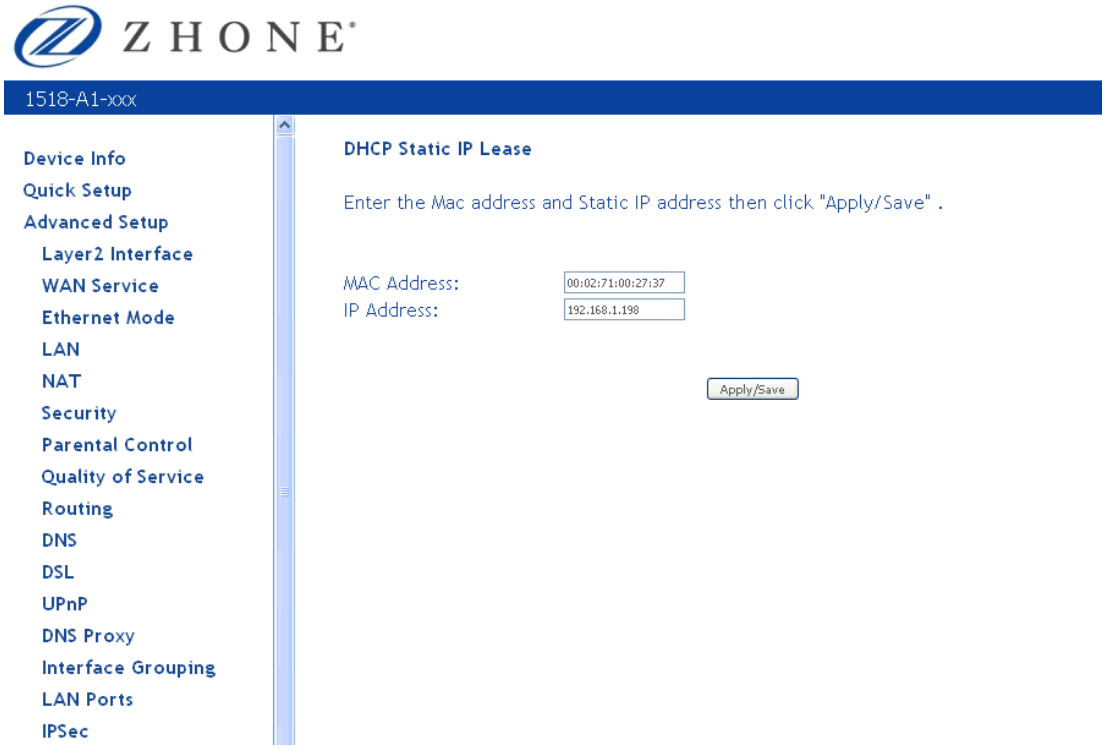
You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond to your LAN's IP Subnet. .Changing the IP address here may cause your browser to be disconnected from the modem. You will need to set your PC to the same subnet as the modem's IP address to access the router again.

IGMP snooping

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.

Default–the default LAN configuration is based on your router's IP address.

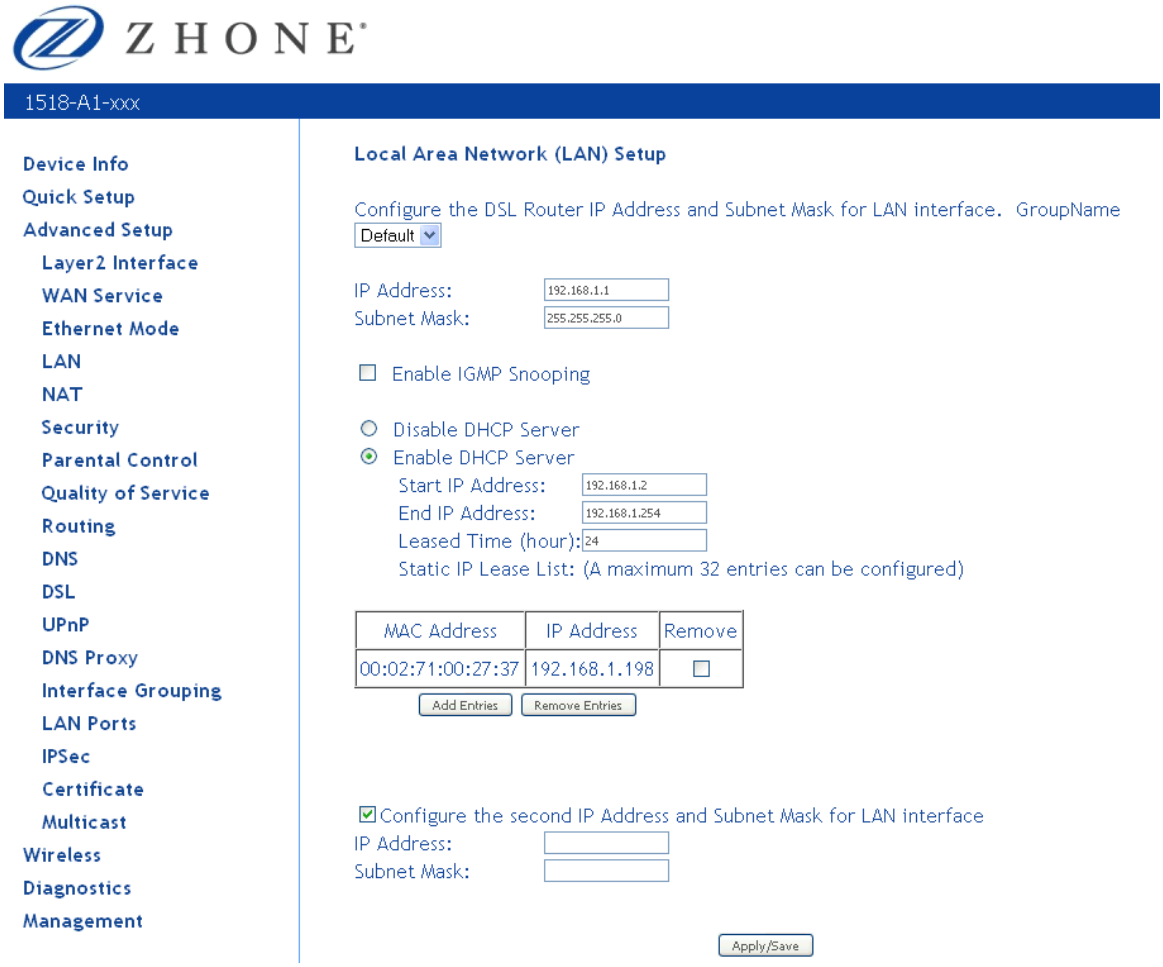
Static IP Lease list – you can configure the DHCP server to set aside up to 32 static IP addresses based on the MAC addresses of the device connected to the router by clicking on the add entries button.



To remove the Static IP address, click the check box next to the MAC address and click **Remove Entries**.

You may be able to assign a second IP address for the modem. To do that, click the check box **Configure the second IP Address** and enter the IP address and subnet mask.

Click the **Apply/Save** button to save the LAN configuration data.



NAT

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

Virtual Servers

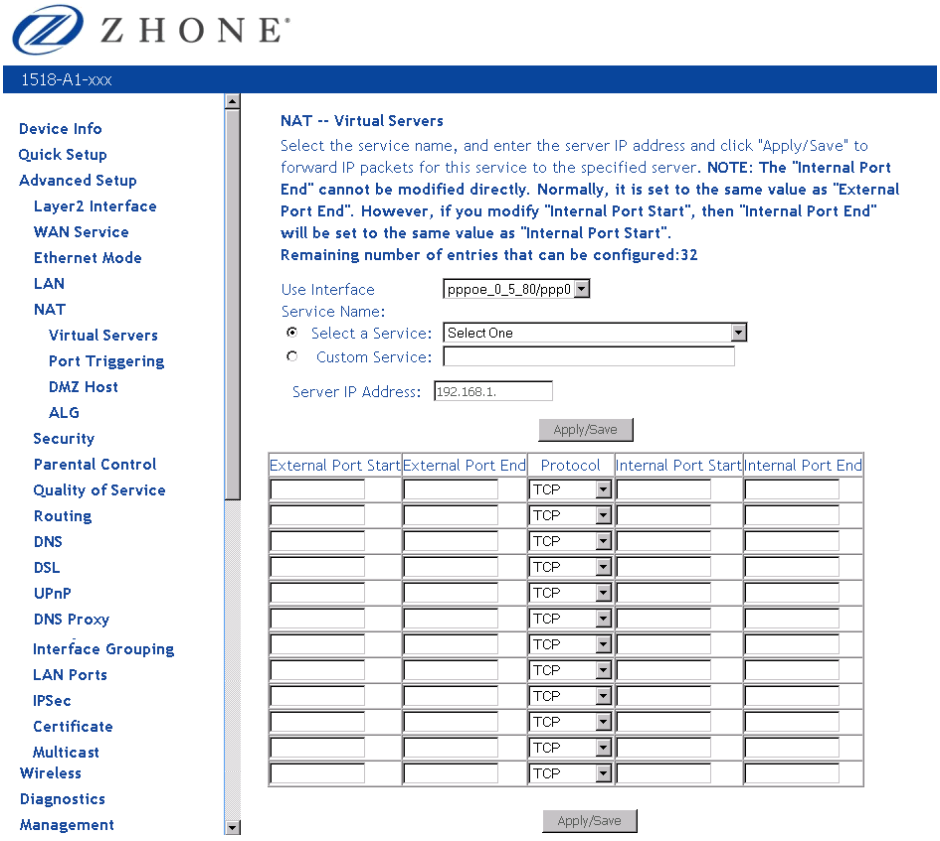
A virtual server allows you to direct incoming traffic from the WAN side to a specific IP address on the LAN side. The following figure shows the screen that allows you to configure your virtual server(s).

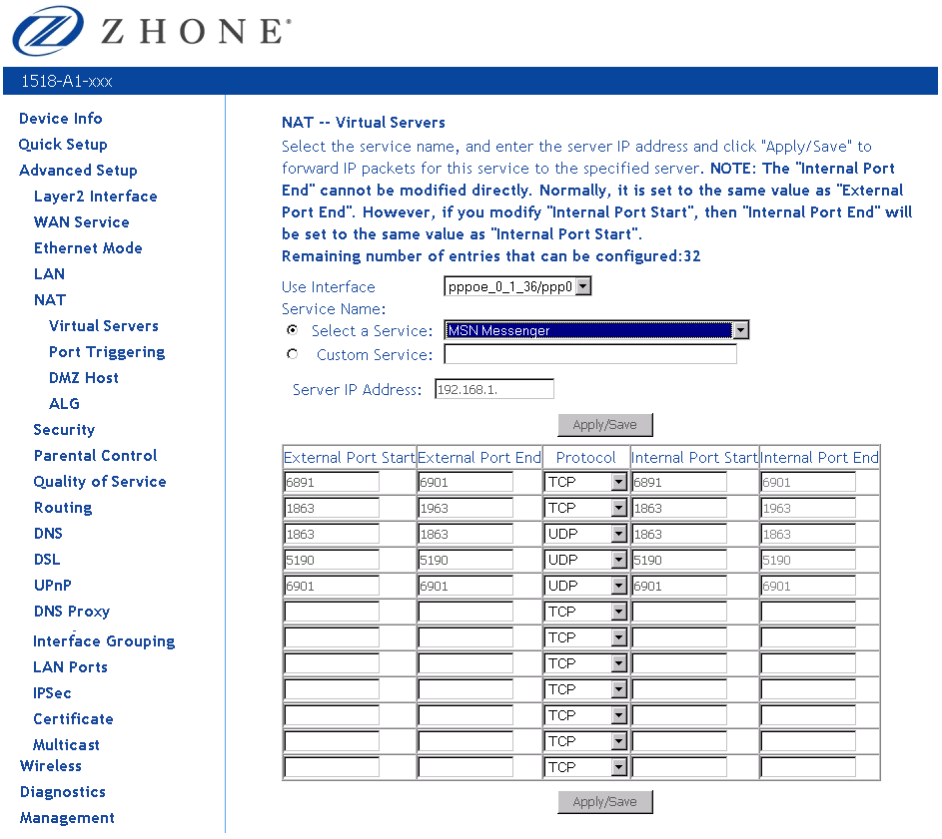
To direct incoming traffic from a service (or other server):

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.





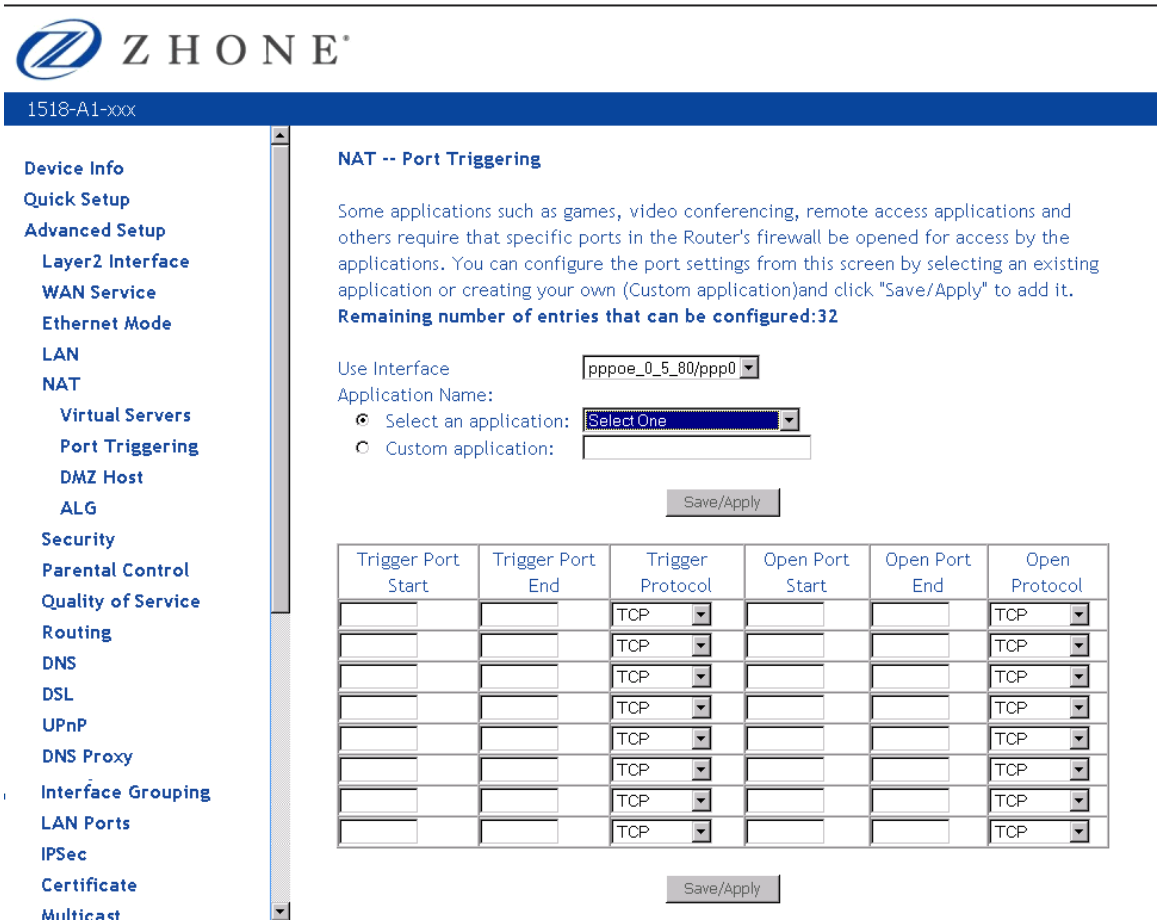
3. *Enter the IP address of the LAN side PC in the **Server IP Address** text box.*

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 for the item and click **Remove**.

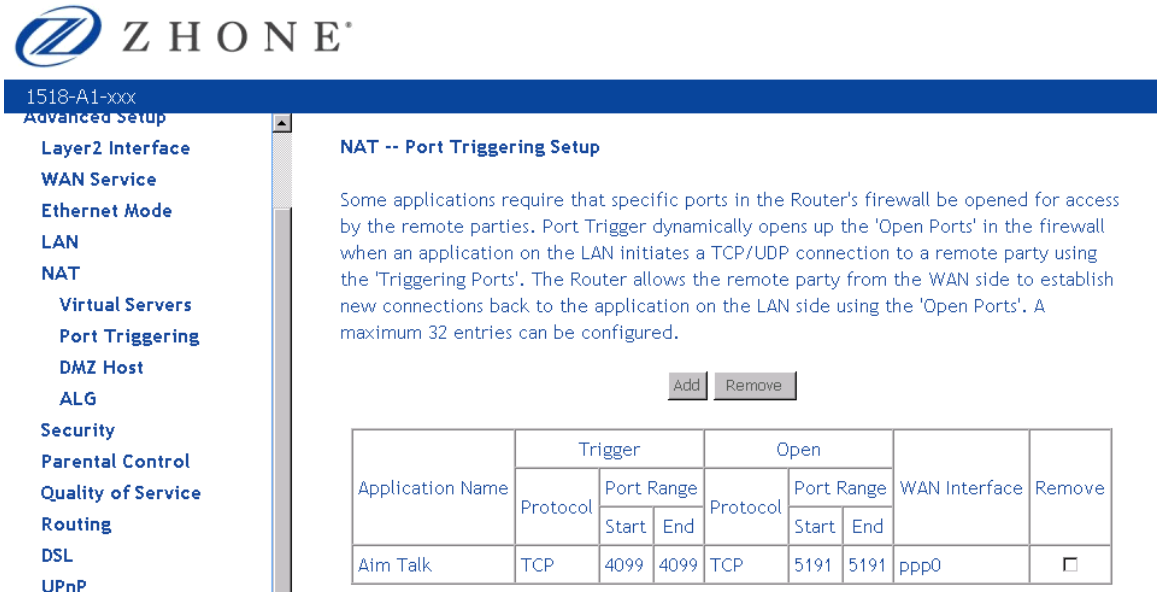
Port Triggering

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



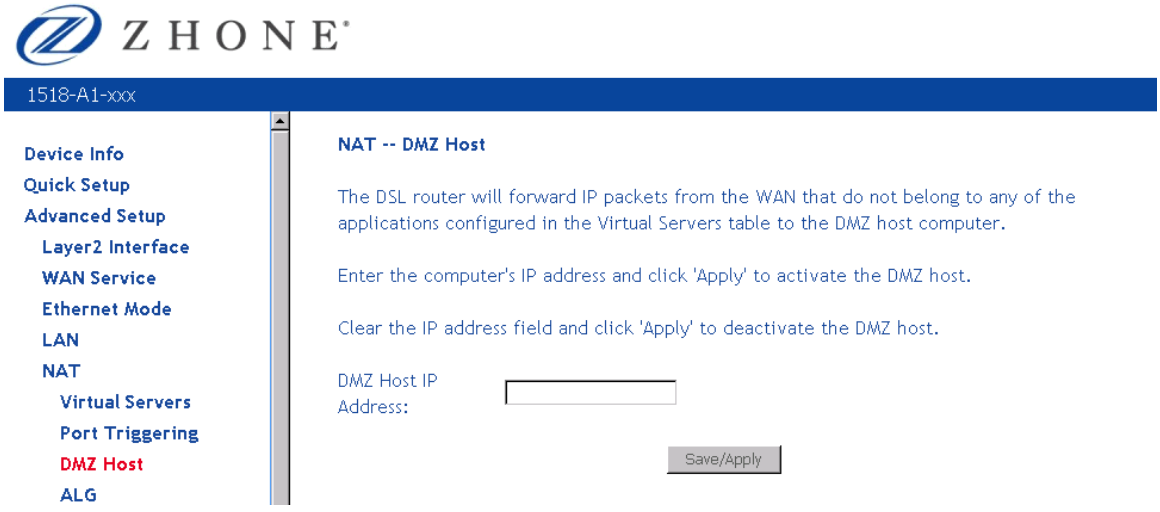
The **NAT – Port Triggering** screen appears when you click **Add** allowing you to select the application that you want to set the port settings for. After a selection has been made, click **Save / Apply** to save your settings.

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.



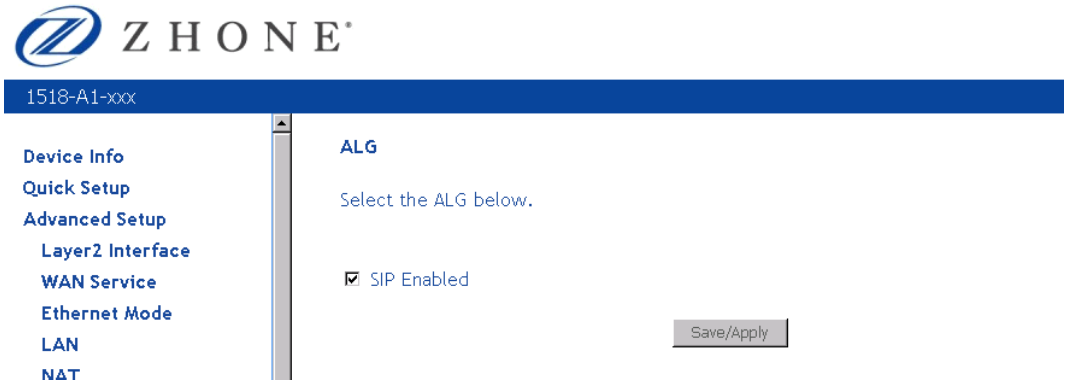
DMZ Host

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



ALG

ALG, Application Layer Gateway can be used to allow firewall traversal with SIP. To enable voice packets to successfully pass through firewalls and NAT, click on the SIP enabled checkbox.

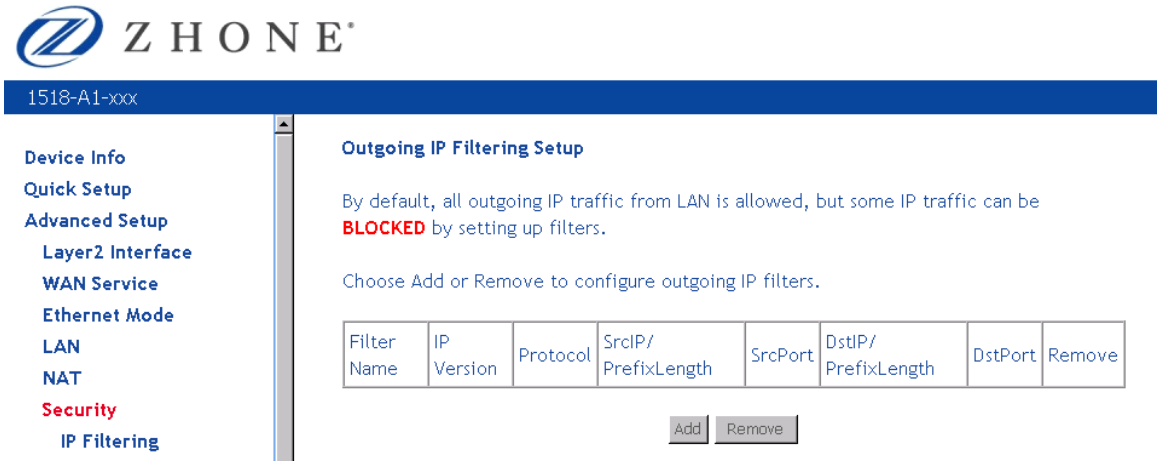


Security

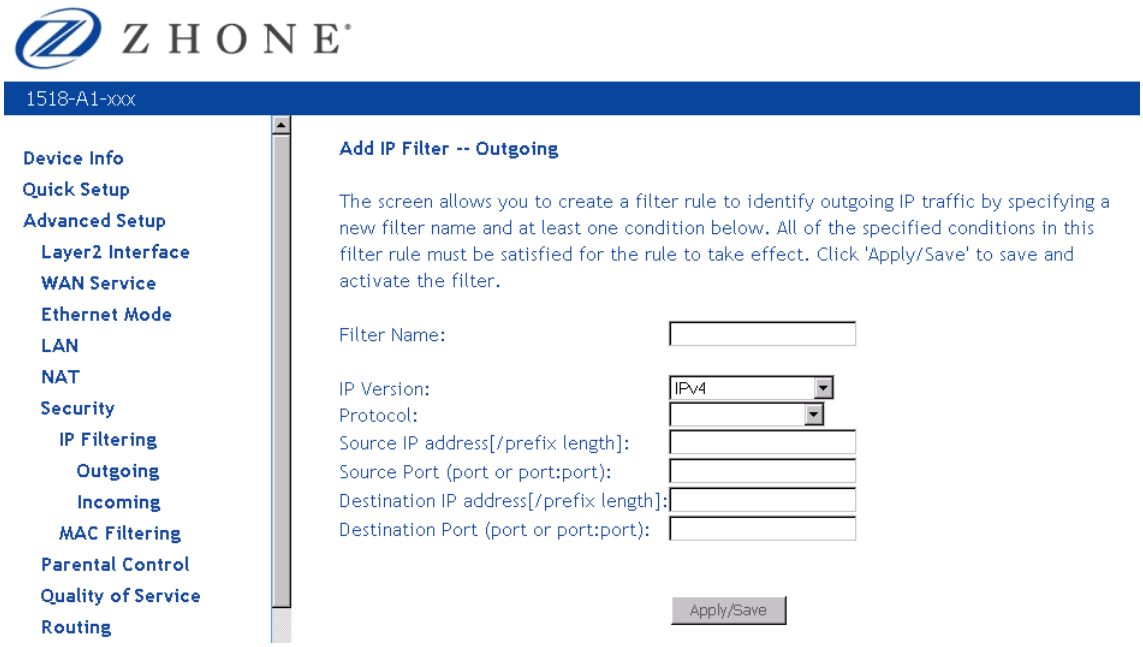
For security reasons, firewall options can be configured only from the LAN side of the router.

IP Filtering—Outgoing

Outgoing IP filters block LAN traffic from entering the WAN side. The **Outgoing IP Filtering Setup** screen will show all outgoing IP filters. Click **Add** to create filters.

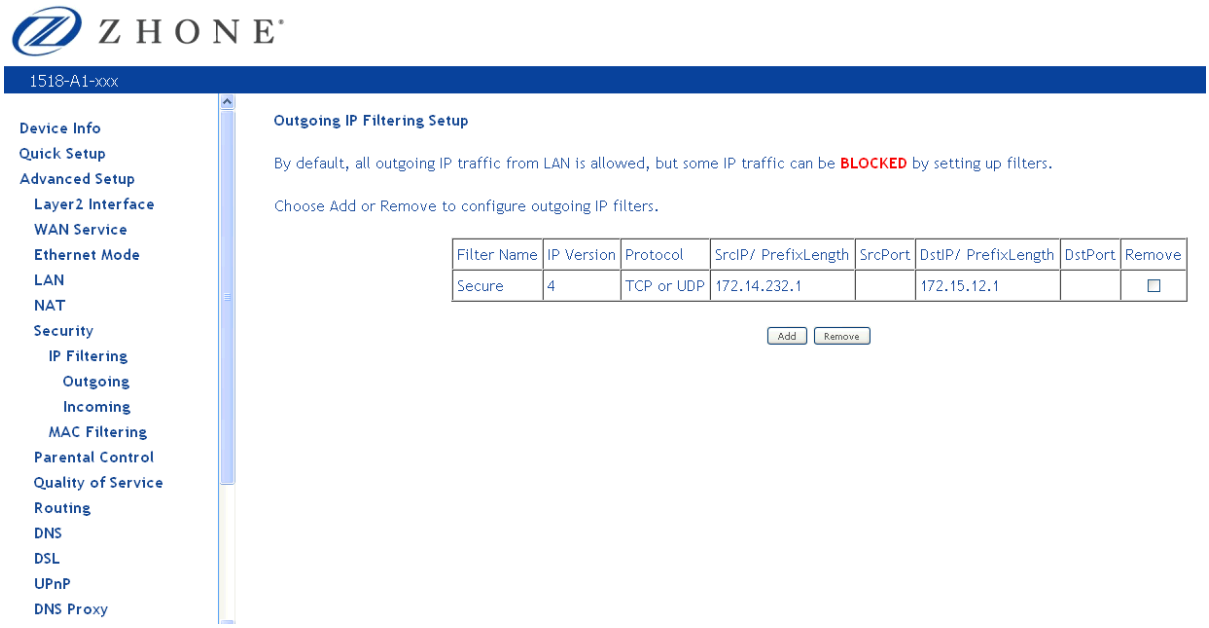


The **Add IP Filter -- Outgoing** screen will appear. Add the filter name, source information (from the LAN side), and destination information (from the WAN side). Then click **Save / Apply**.



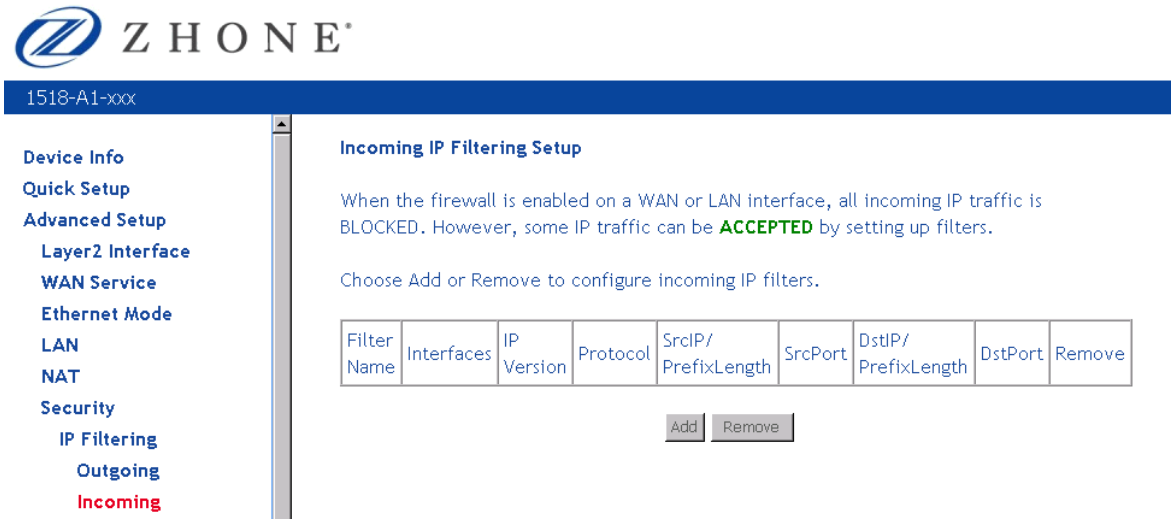
When you **Save / Apply** the IP filter, the **Outgoing IP Filtering Setup** screen appears. The **Outgoing IP Filtering Setup** screen lists the outgoing IP filters, including filters which were added from the previous screen.

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



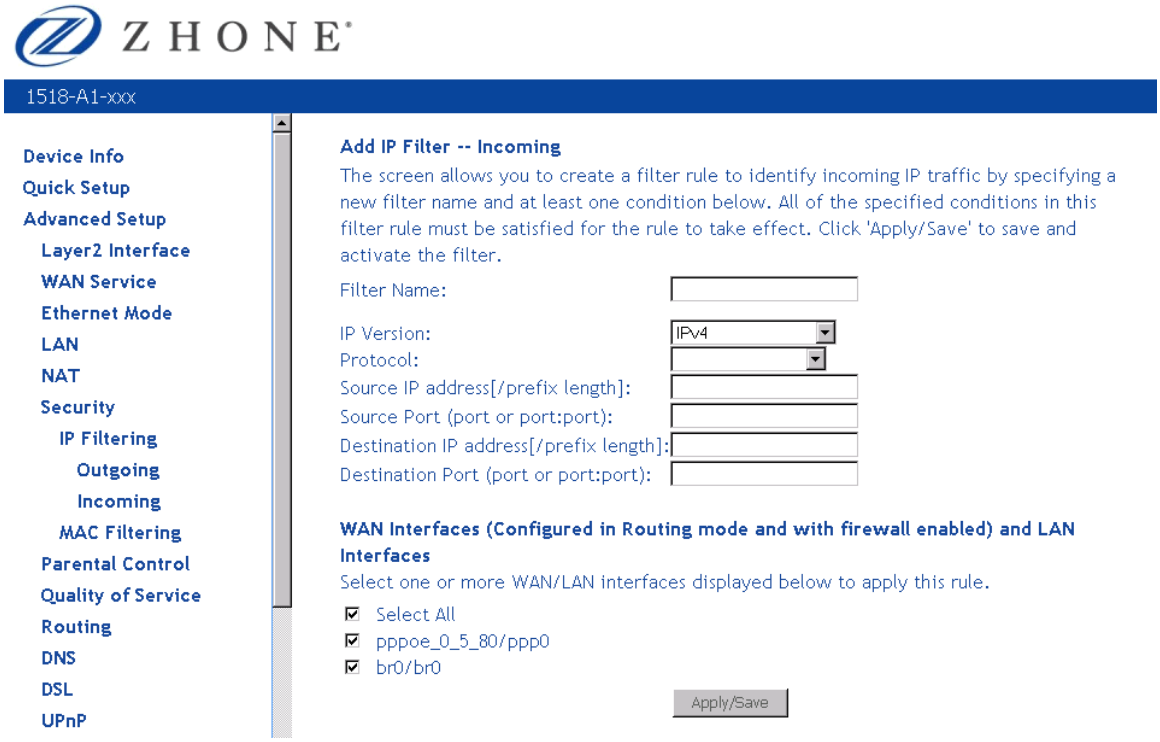
IP Filtering—Incoming

Incoming IP filter filters the WAN traffic to the LAN side. Click **Add** to add incoming filter settings.



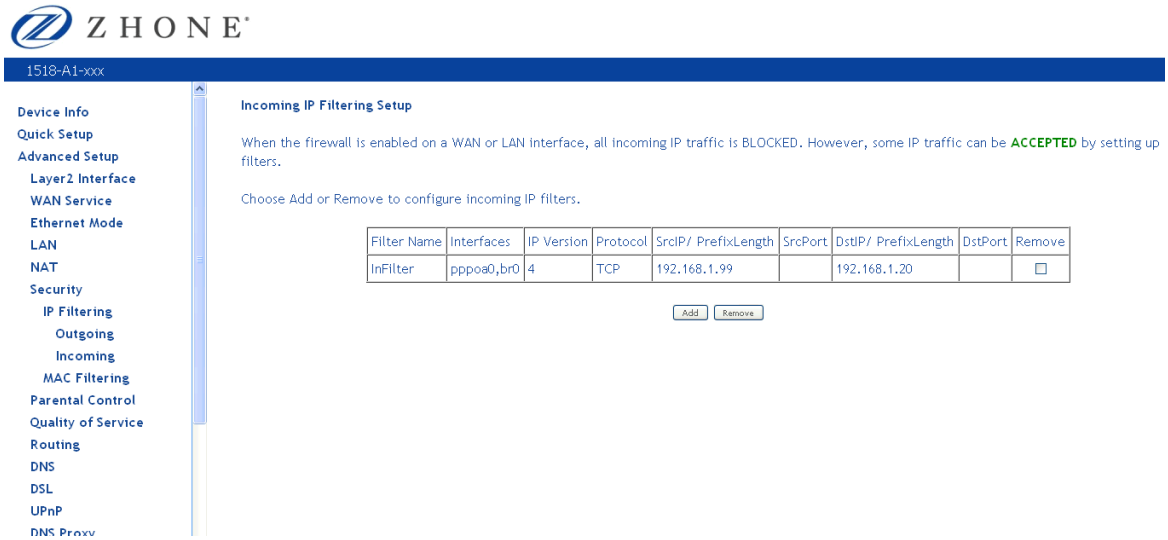
Enter a filter name, information about the source address (from the WAN side), and information about the destination address (to the LAN side). Select the protocol and WAN interface, then click **Save/Apply** to add the setting.

You can view and delete the incoming filter settings in the **Add Ip Filter -- Incoming** screen.



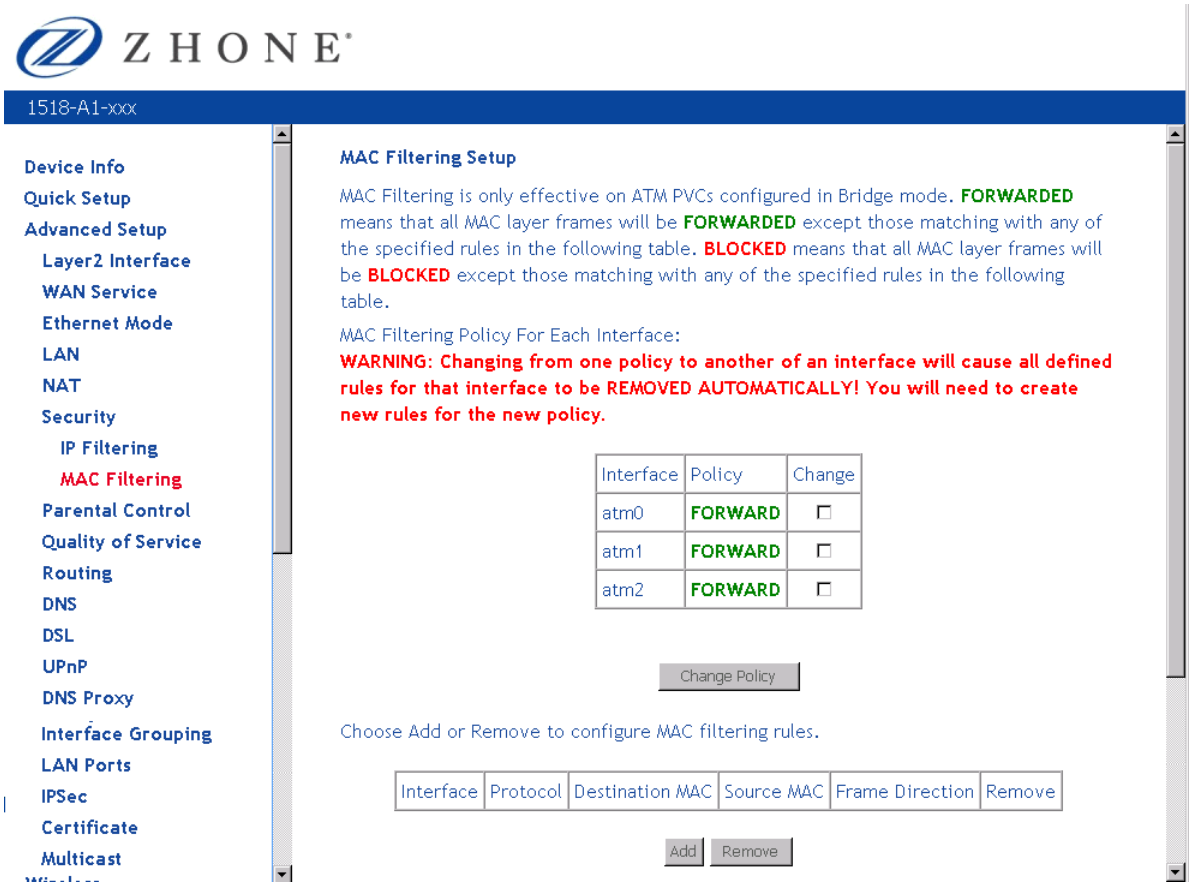
When you **Save / Apply** the IP filter, the **Incoming IP Filtering Setup** screen appears. The **Incoming IP Filtering Setup** screen lists the incoming IP filters, including filters which were added from the previous screen.

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



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.

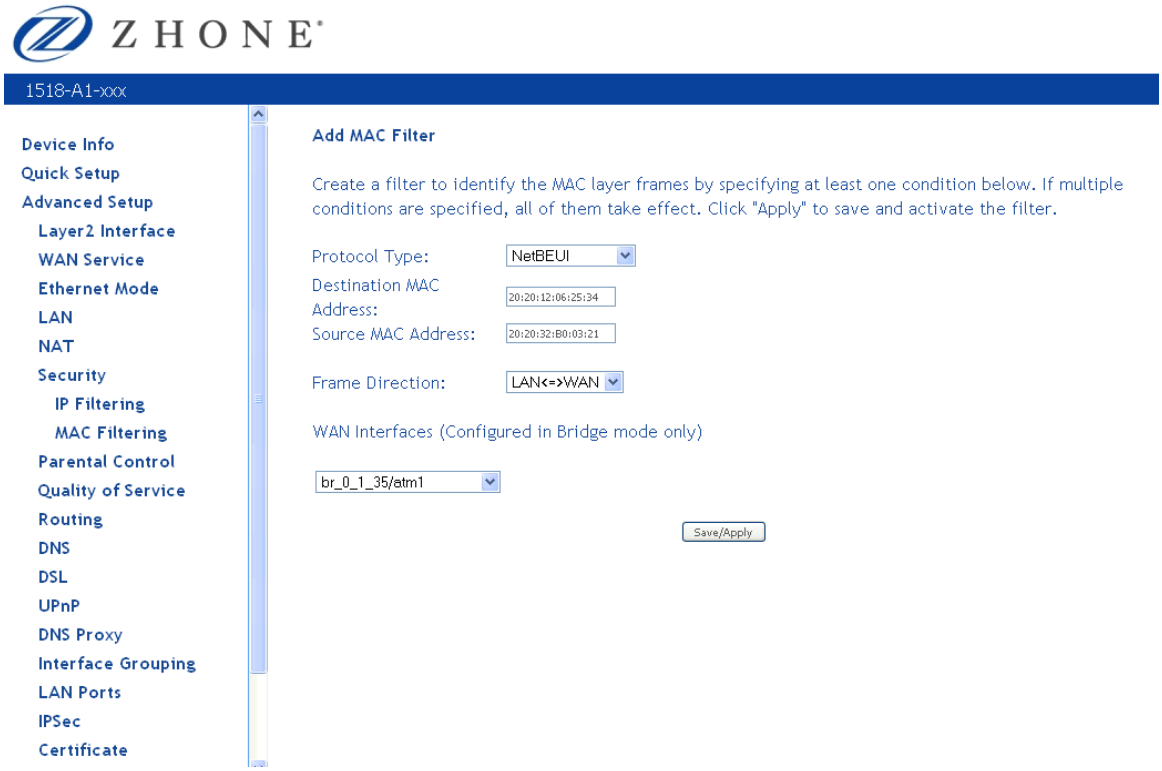


To add a setting to the MAC filtering table, then click **Add** to access the **Add MAC Filter** screen, then configure the MAC filter.

- **Protocol type**: Type of protocol to filter.
  - PPPoE
  - IPv4
  - IPv6
  - AppleTalk
  - IPX
  - NetBEUI
  - IGMP
- **Destination MAC Address**: the destination MAC address you want to filter
- **Source MAC Address**: define the source MAC address
- **Frame Direction**: You can define the direction of the filter. Options are
  - LAN TO WAN and WAN TO LAN
  - WAN to LAN
  - LAN to WAN

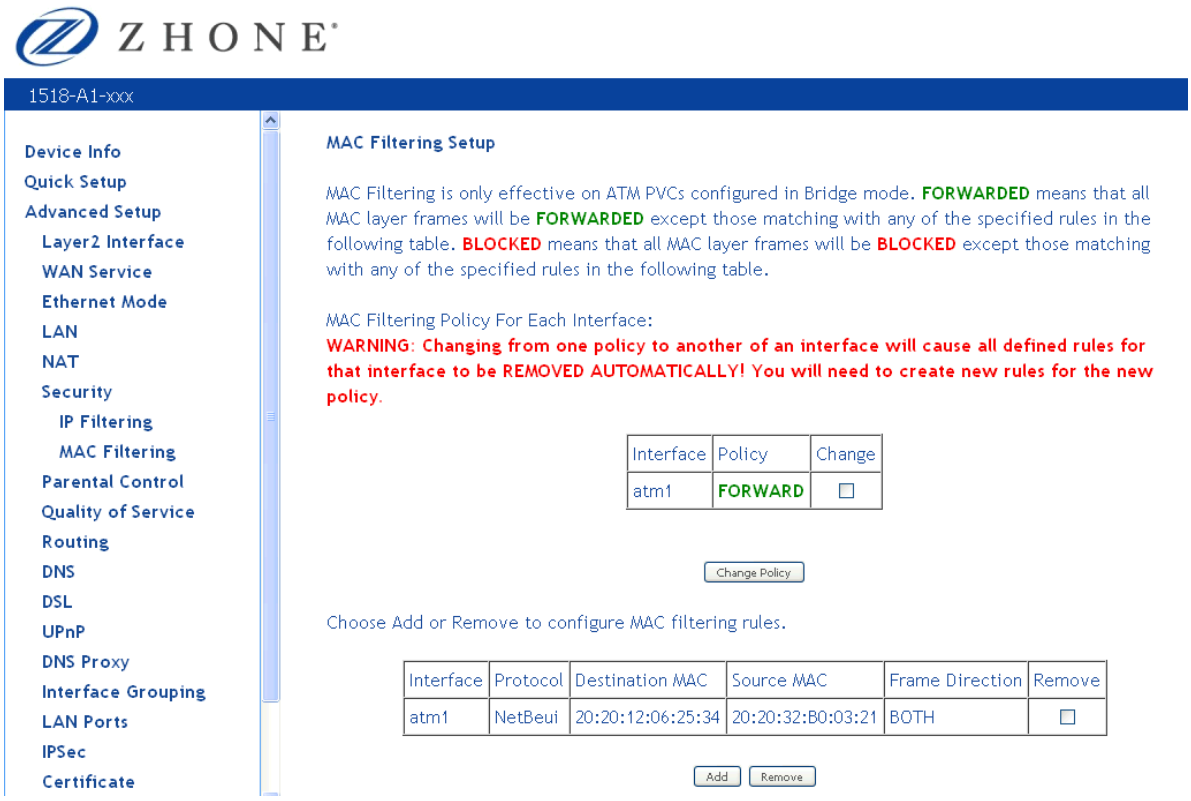
- **WAN Interfaces**: defines the WAN interface for this filter. This drop down list will show all the available WAN interfaces.

Click **Save/Apply** to save the MAC filter.



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.



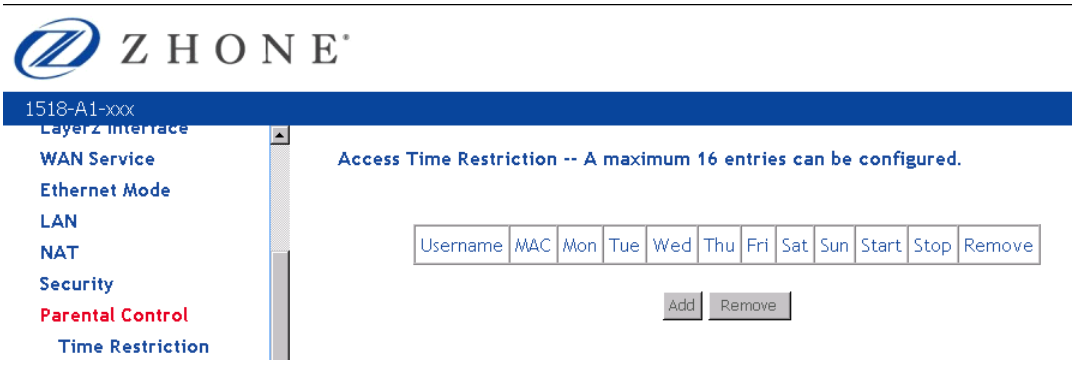
Parental Control

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

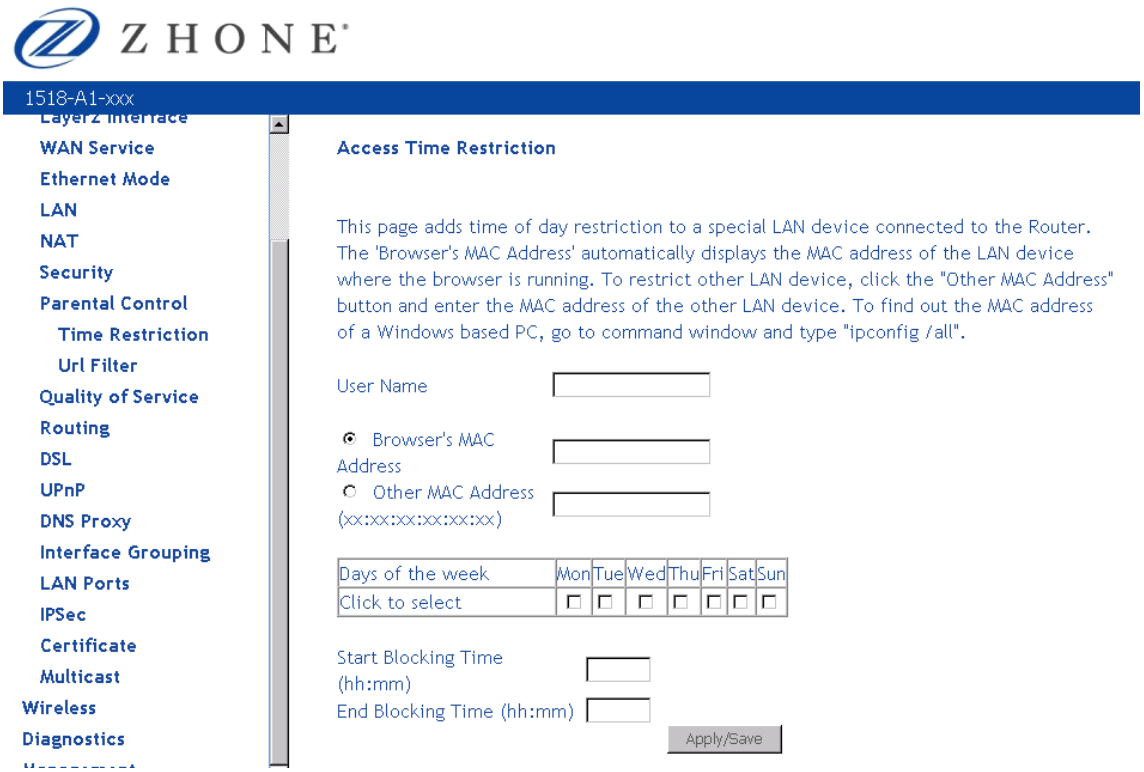
Time Restriction

To setup parental controls:

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



The **Add Parental Control** screen appears.



2. *Enter a **User Name** to identify the target of the restrictions. . This is equivalent to the host name of the IP clients (refer to the **DHCP status** screen check to see the host names)*

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.*

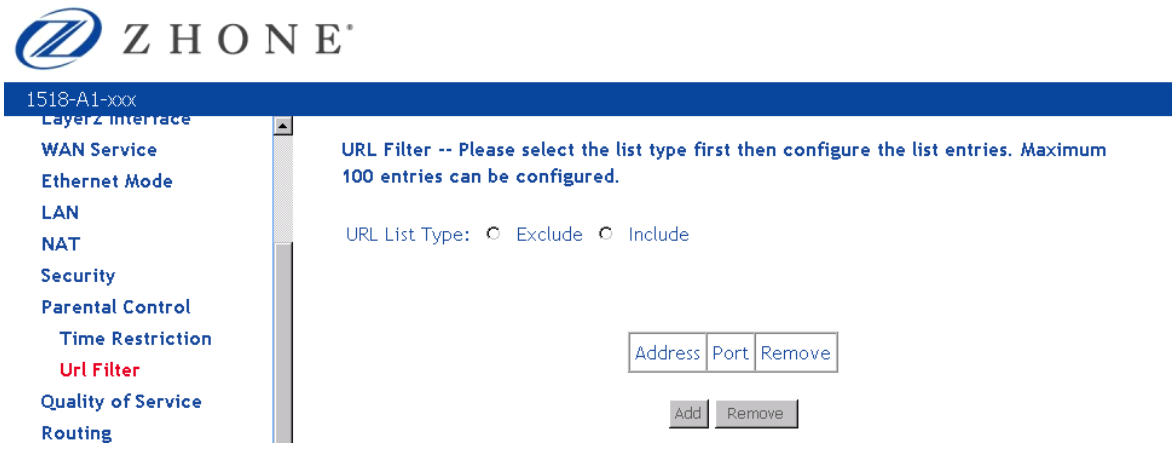
6. *Click **Save / Apply** to save the settings and to continue.*

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.

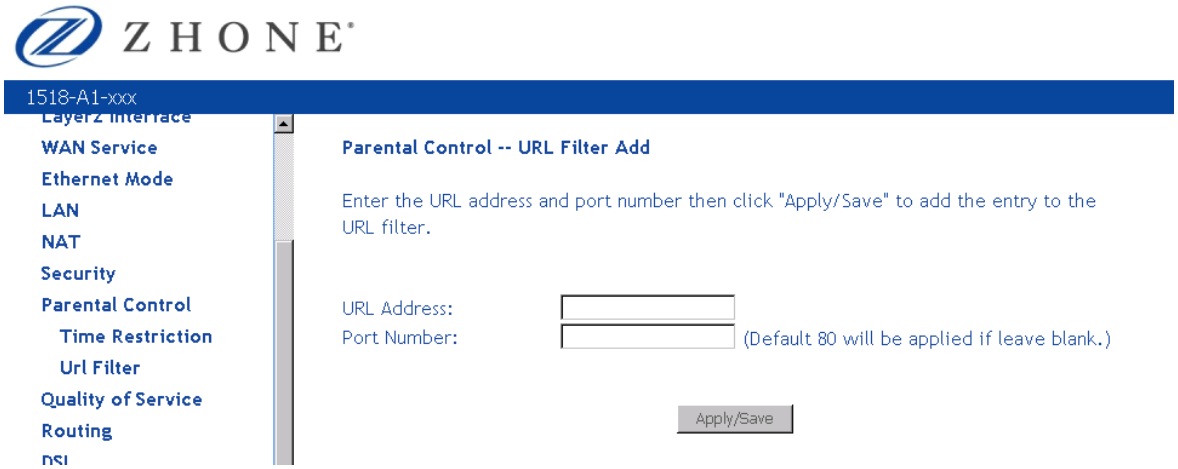
1. *Select the **Exclude** button or **Include** button to specify the web sites you want to block or allow access.*

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



3. *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 default 80 port will be applied. Continue this process until all the necessary websites are entered.

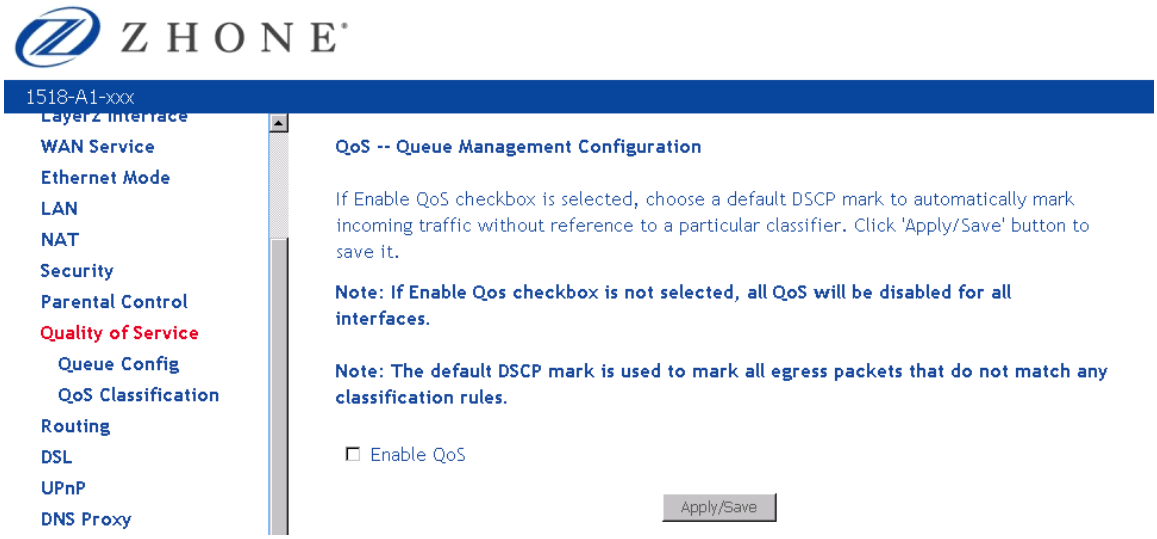


Quality of Service

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

Queue Config

In the **QoS -- Queue Management Configuration** 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 enable QoS:

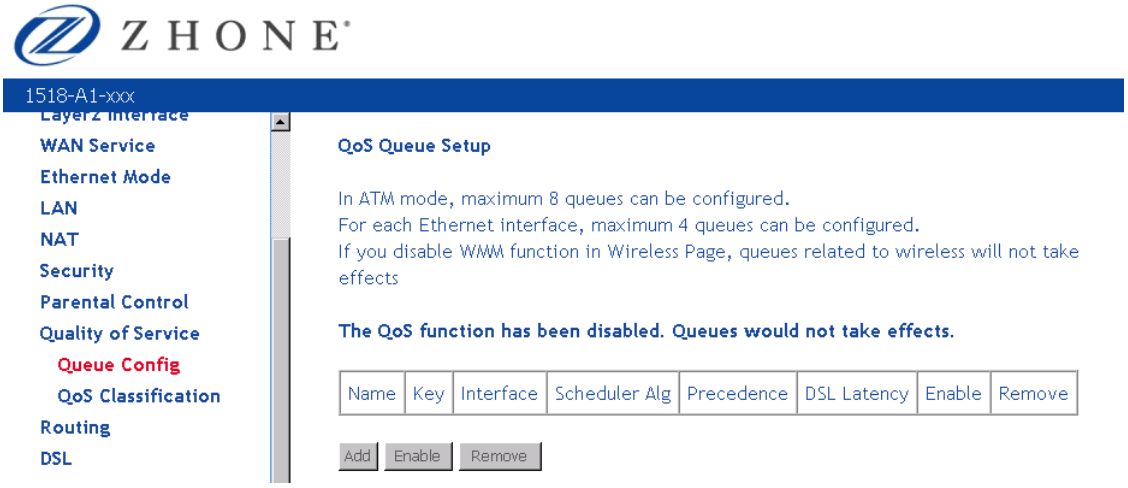
1. *From the **Quality of Services** page, check **Enable QoS**.*

2. *From the **Select Default DSCP Mark** drop down select the option as directed by your ISP.*

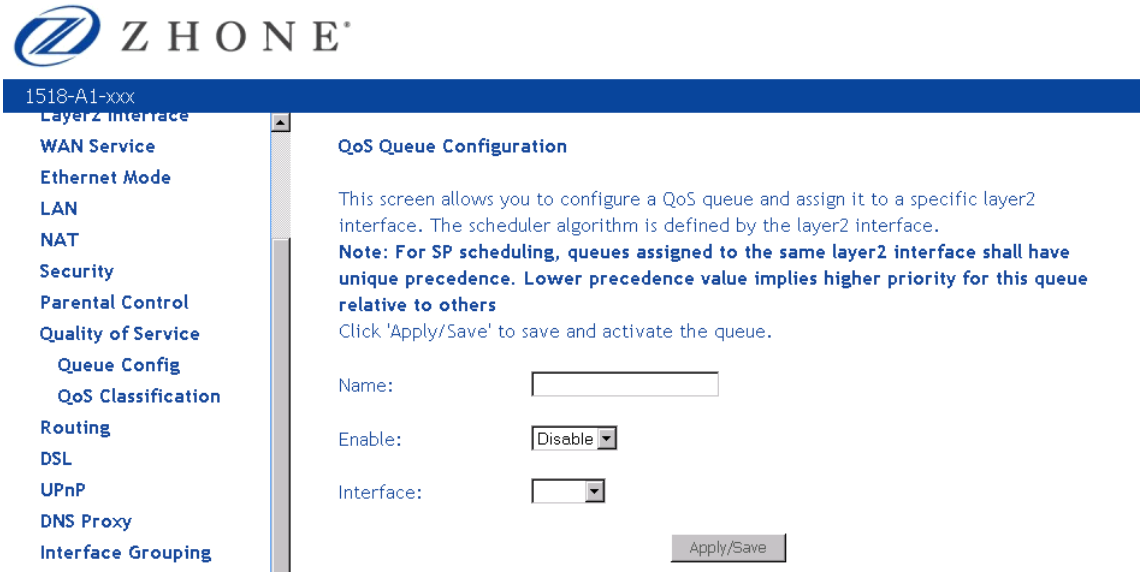
   Differentiated Services Code Point (DSCP) is a means to classify packets in the IP header of the packet.

To associate an interface with QoS:

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



4. *In the **QoS Queue Configuration** page enter the name of the queue and enable the queue by selecting **Enable** from the **Queue Configuration Status** drop down.*



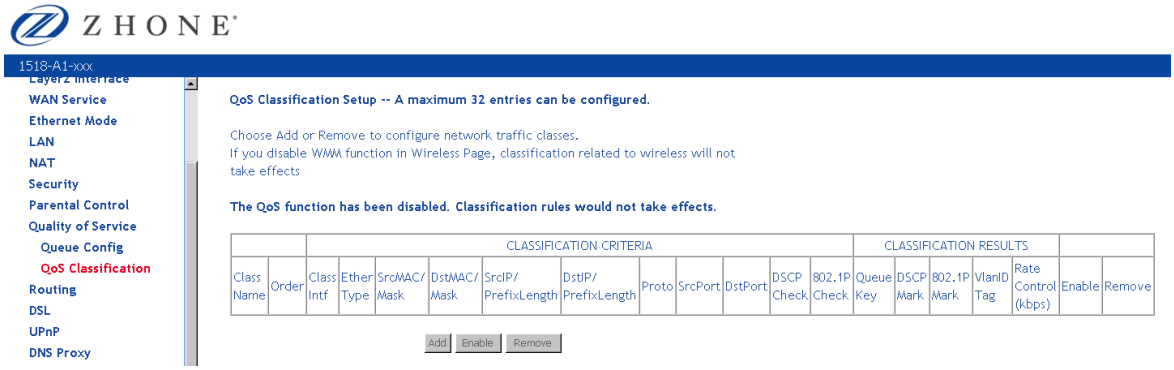
5. *Select the interface from the **Interface** drop down.*

6. *Set the priority for the queue from the **Precedence** drop down*

7. *Click **Save/Apply**.*

QoS Classification

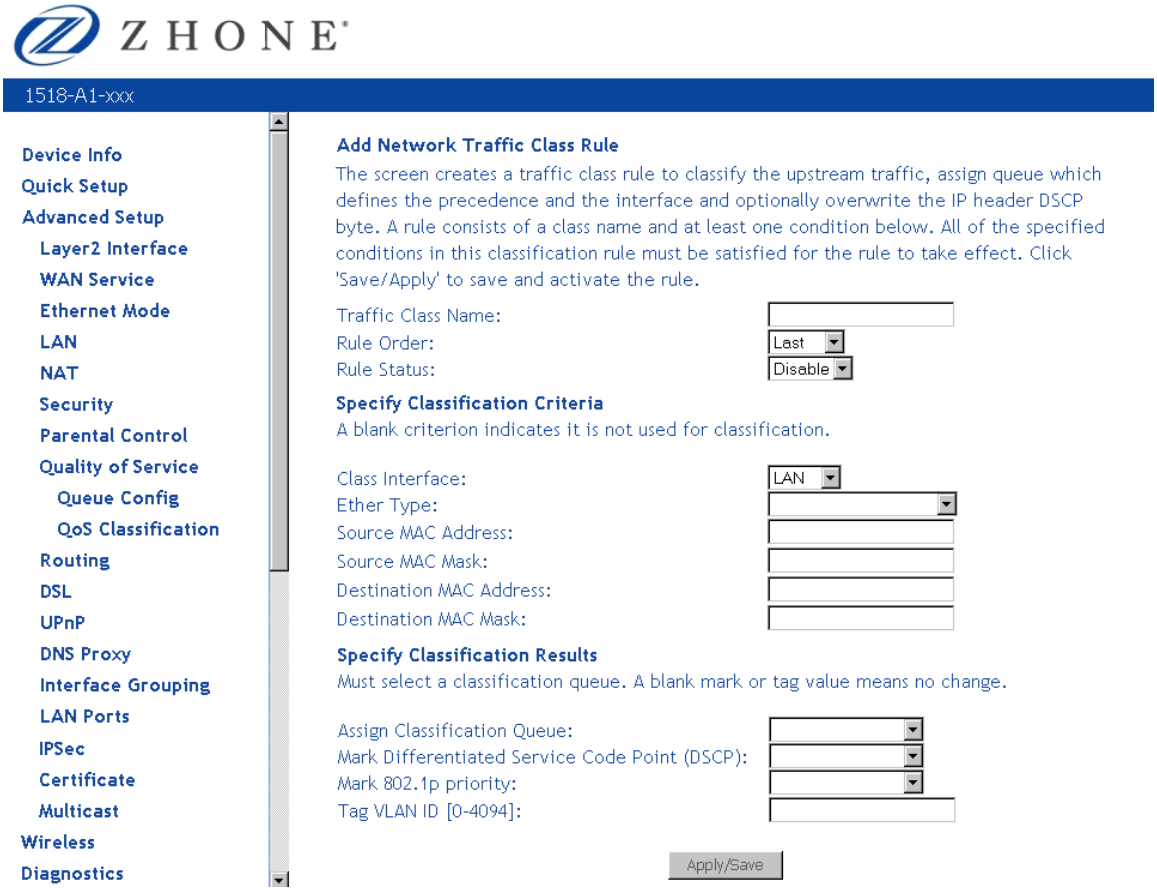
You can configure the Quality of Service to apply different priorities to traffic on the router.



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**.*



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.*

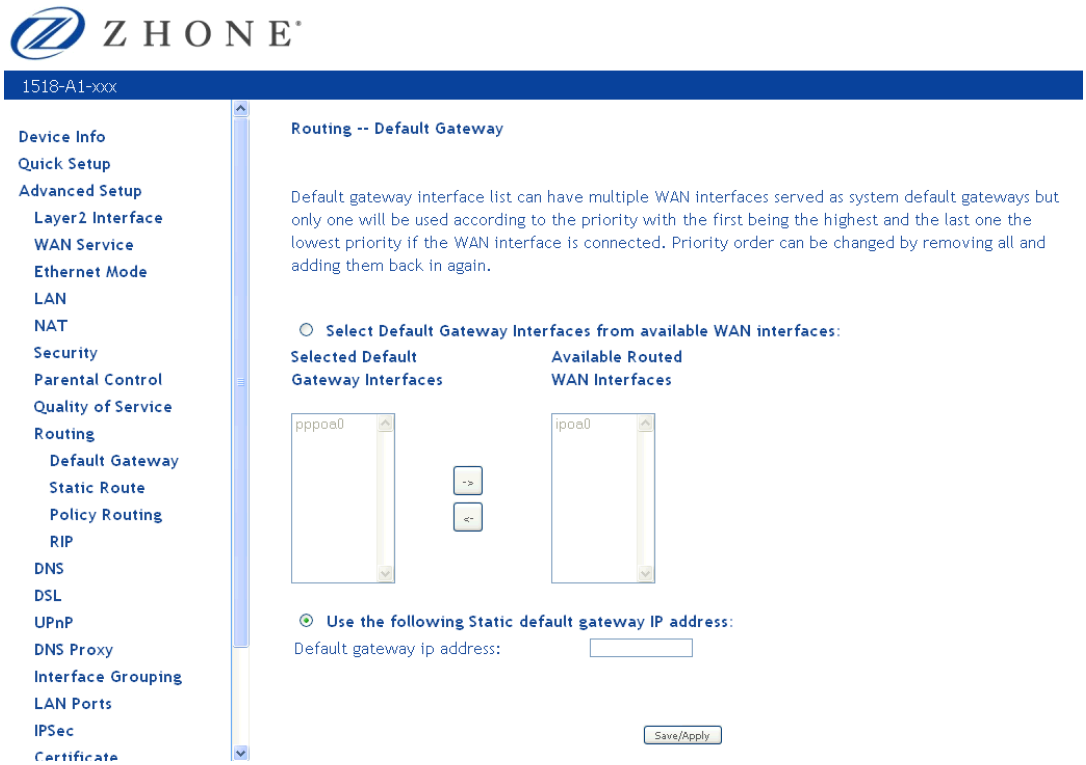
7. *Click **Save / Apply** to save the settings.*

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.

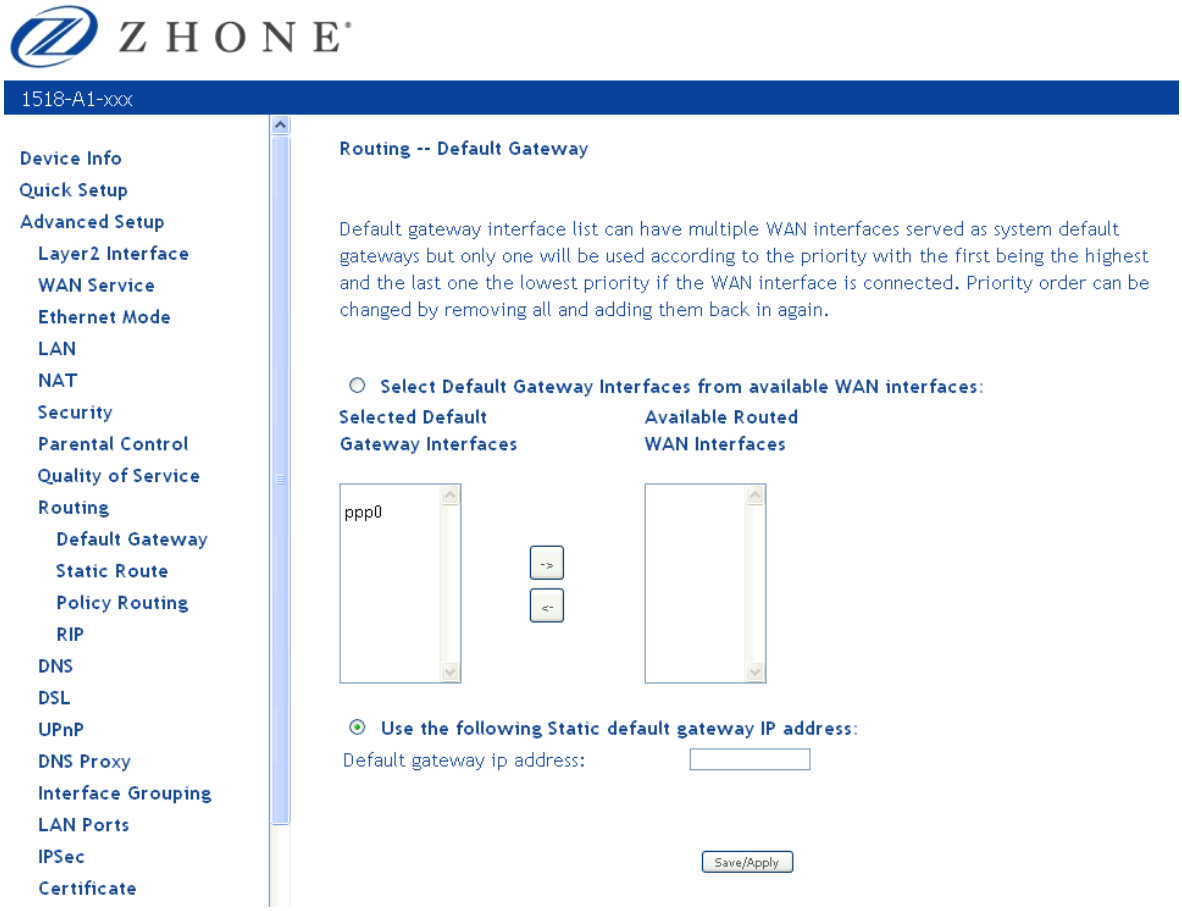
Default Gateway

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



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.

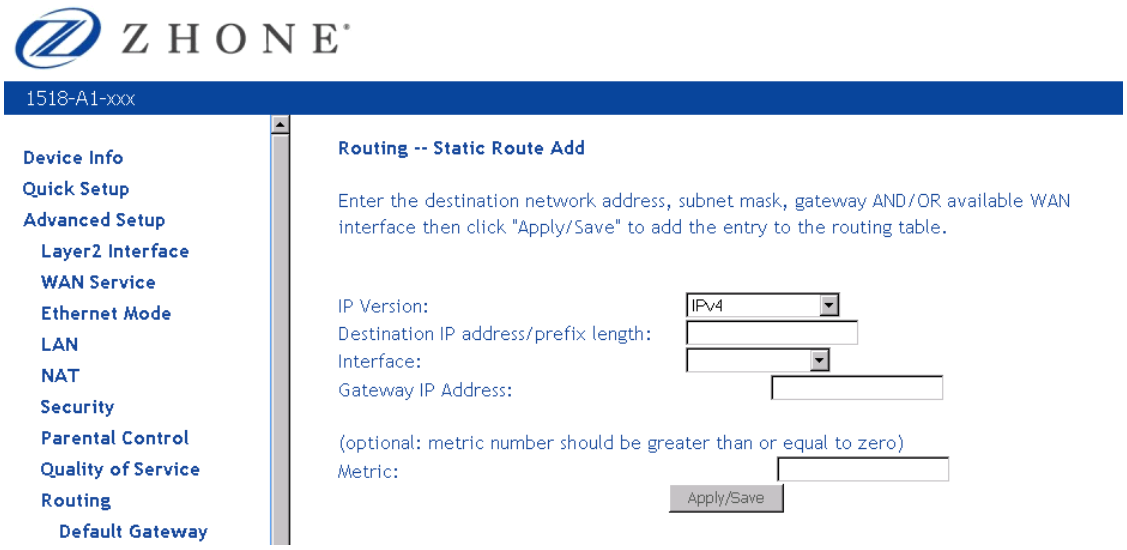


Static Route

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

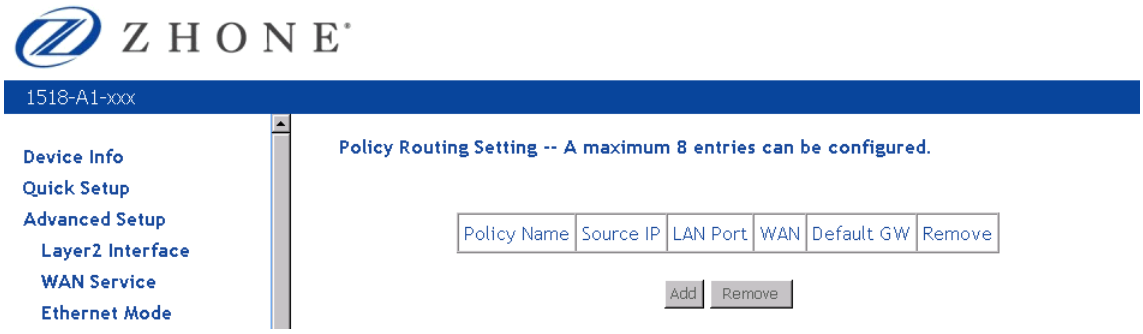
1. *Click **Add**.*

2. *Enter the route information and then click **Apply/Save**.*



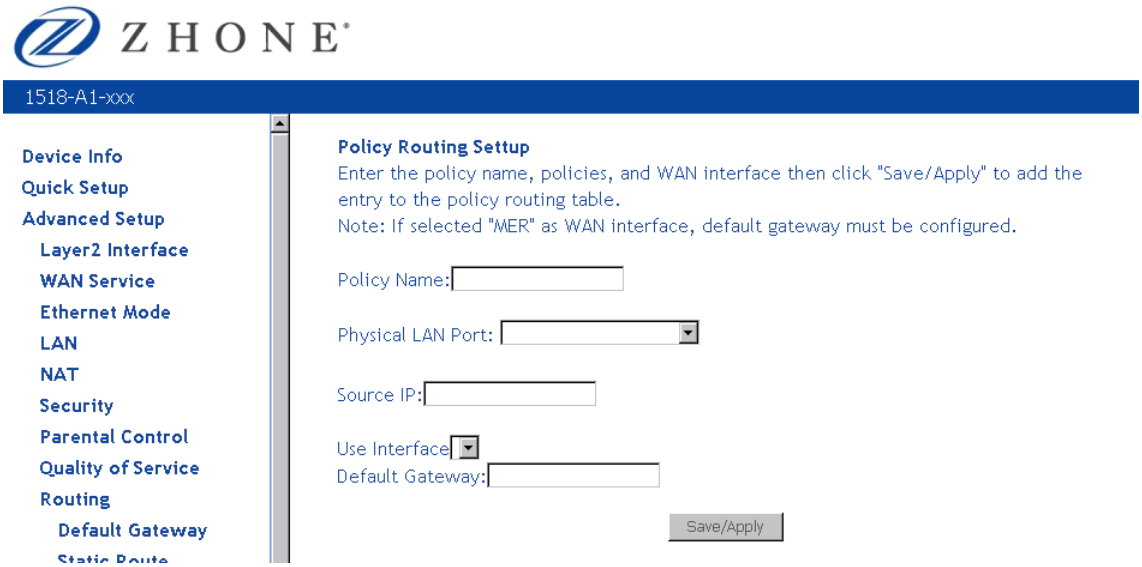
Policy Route

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.



To add a policy routing rule:

1. *Click **Add**.*



2. *Enter a unique name for the rule in the **Policy Name** text box.*

3. *Select the interface to associate with the rule from the **Use Interface** drop down*

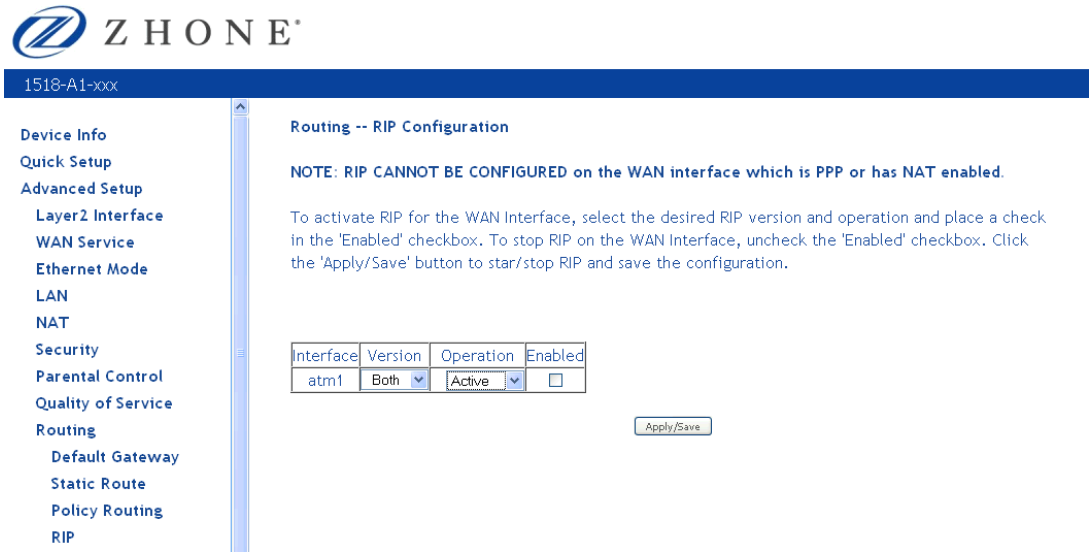
4. *Select the appropriate protocol and define other parameters for the routing rule:*

   - 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**.*

RIP

To enable RIP on an interface, open the **Routing – RIP Configuration** page.



Enter the RIP configuration and then click **Apply/Save**.

DNS

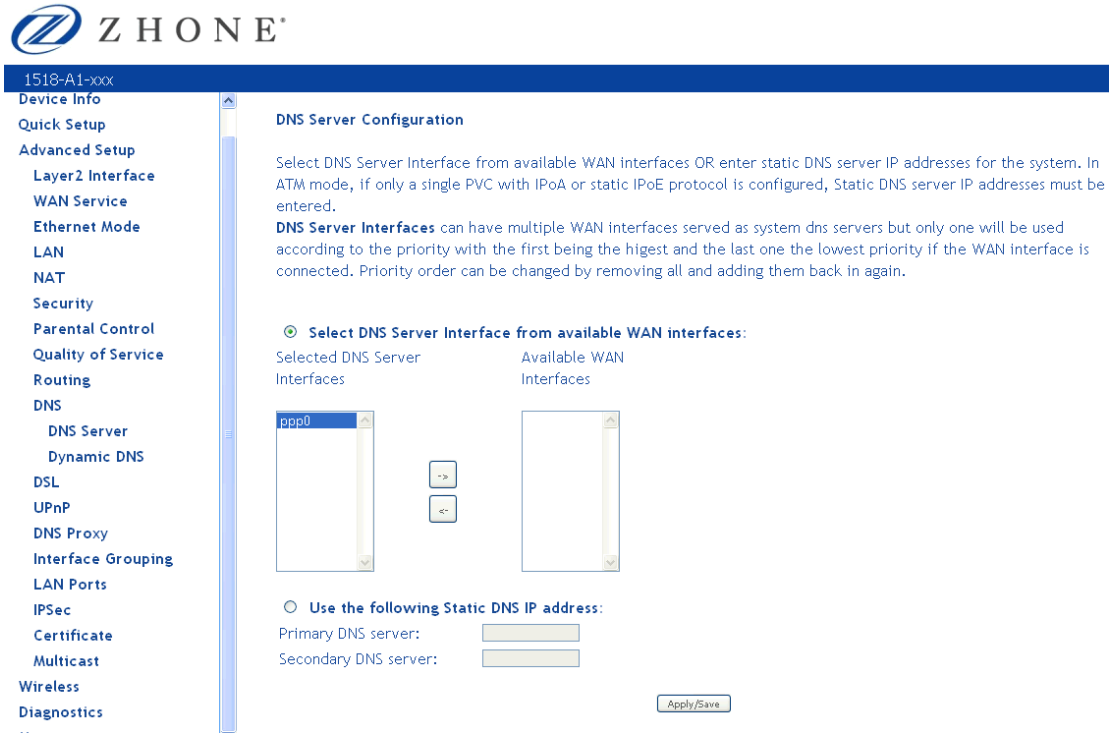
The **DNS Server Configuration** configures the DNS server settings for your router.

*If multiple WAN interfaces are configured, you can define the priority by their position in the **Selected DNS Server Interfaces** window. Top is the highest priority; bottom the lowest.*

Change the priority order by removing all items from the **Selected DNS Server Interfaces** window by selecting them, then clicking the right arrow button. Select the items in the priority order, then click the left arrow to move them into the **Selected DNS Server Interfaces** window.

For a **Static DNS IP Address**, enter a primary and secondary DNS server for your router.

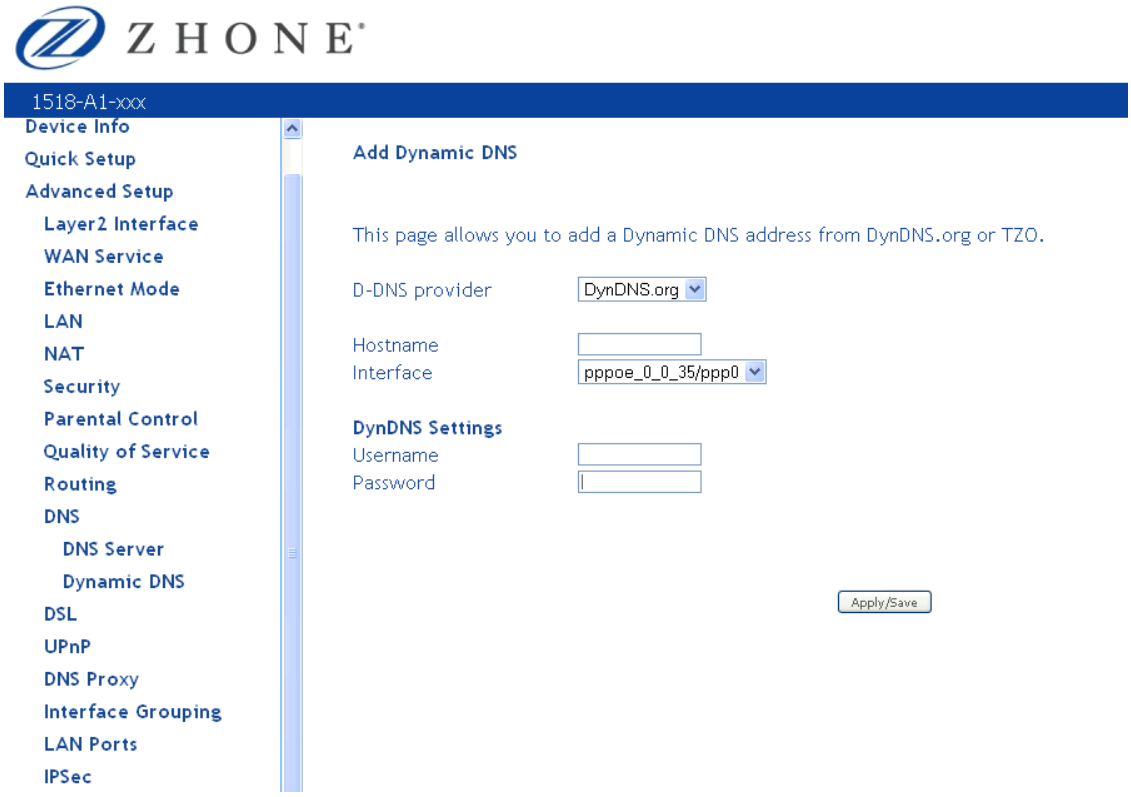
After you have configured the DNS settings, click **Apply / Save.**



Dynamic DNS

This screen allows you to enable dynamic DNS service.

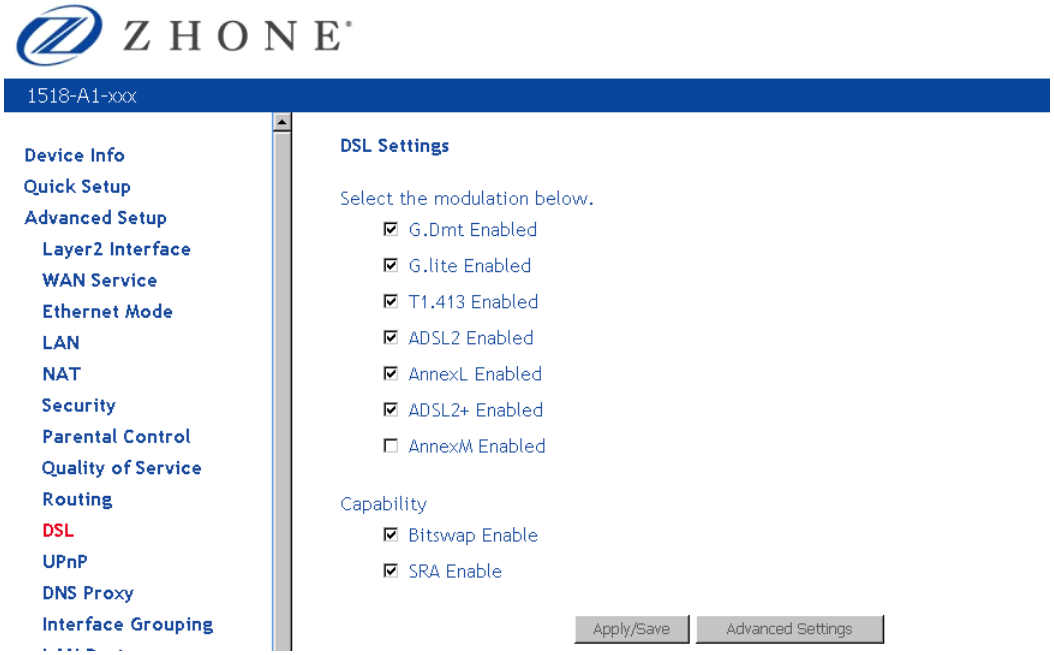
To configure the DDNS, select the DDNS provider from the drop down list and enter the information provided by the DDNS .



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 on **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 3218 ADSL router:

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

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

Capability

The following are included under Capability:

- Bitswap Enable
- SRA (Seamless Rate Adaptation) Enable

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.

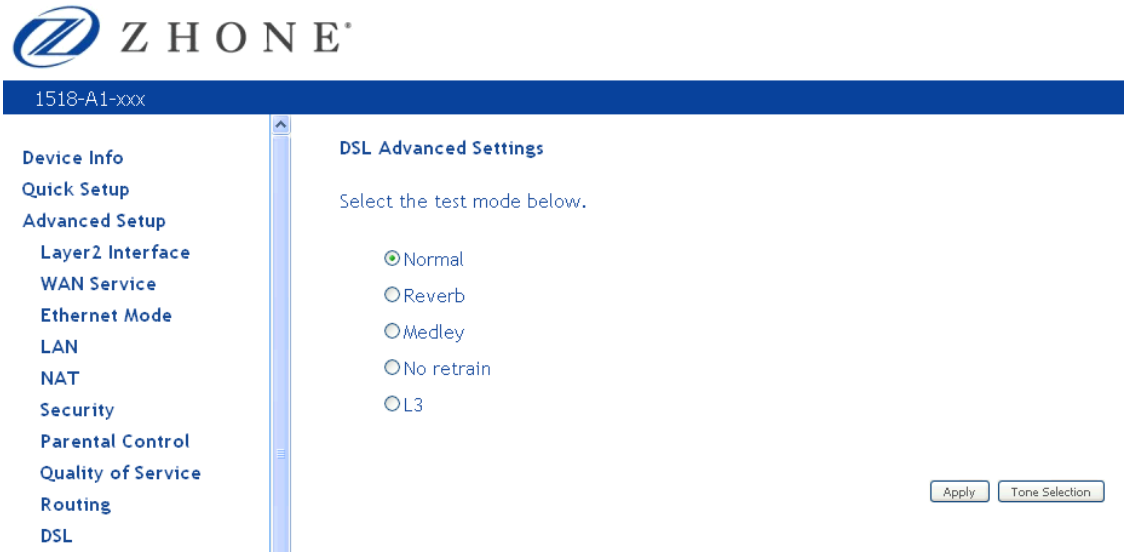
To view the DSL Advanced Settings screen, click **Advanced Settings** button on the **DSL Settings** screen.

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.

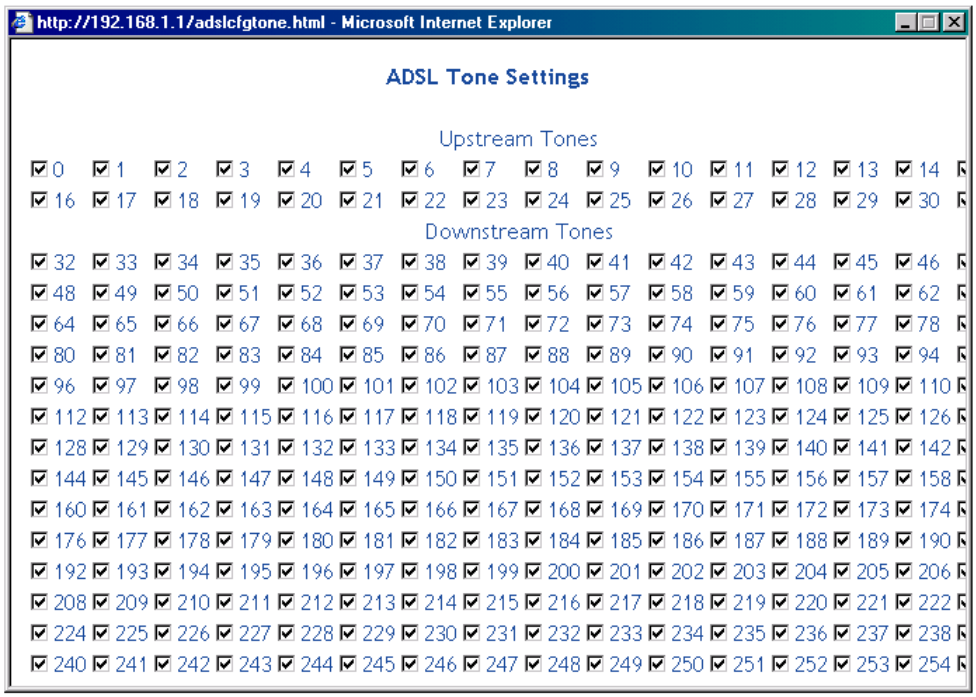
To run a test:

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.

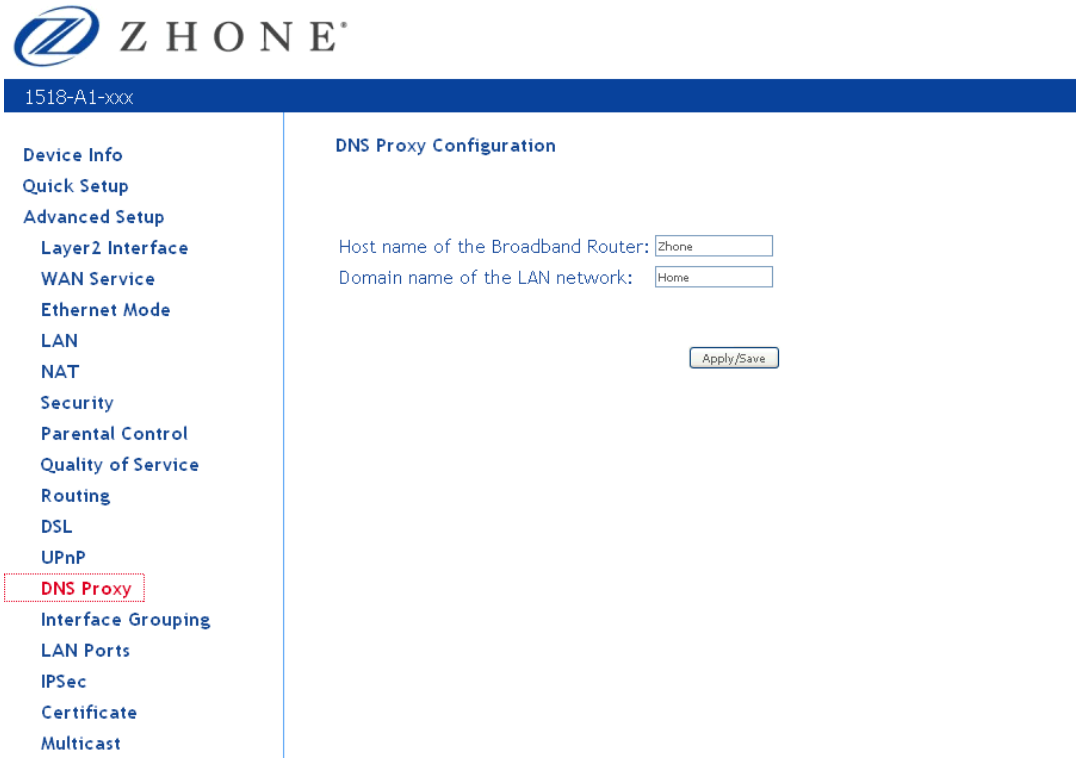


UPnP

Universal Plug and Play (UPnP) is used to connect devices such as game consoles or printers that are on the same subnet. Game consoles such as xBox or PS3 which requires network connections can use UPnP to be connected to the Internet.

DNS Proxy

By default the router has a Domain Name Service (DNS) running. All DNS resolution is performed by the router.



1. *In the **Host name of the Broadband Router** text box enter the Host Name for the DNS Server to be used.*

2. *In the **Domain name of the LAN network** text box enter the domain name of the local network.*

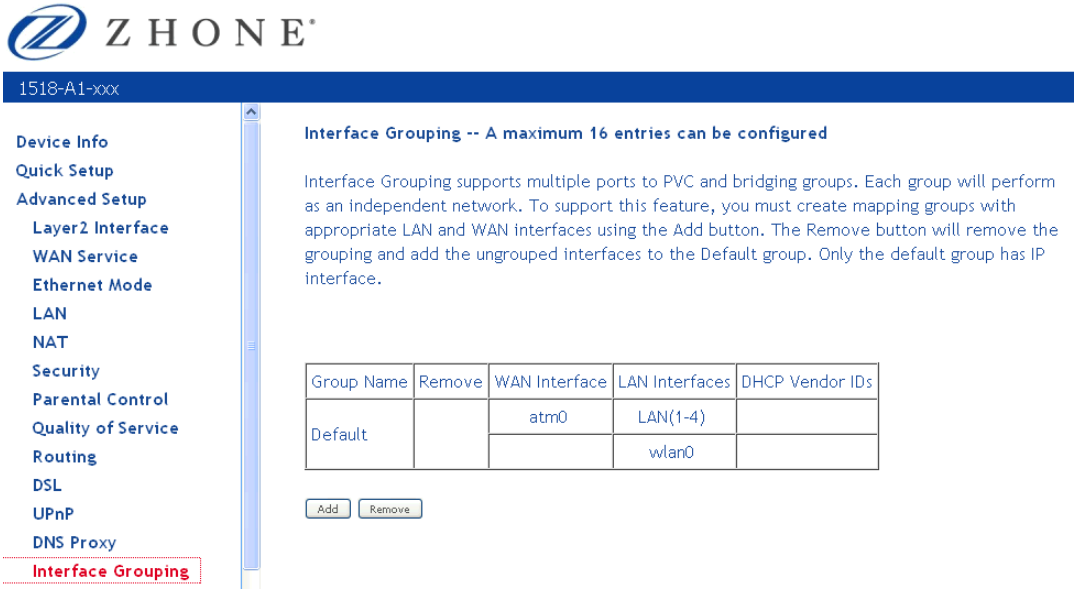
3. *Click **Save / Apply**.*

Interface Grouping

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:

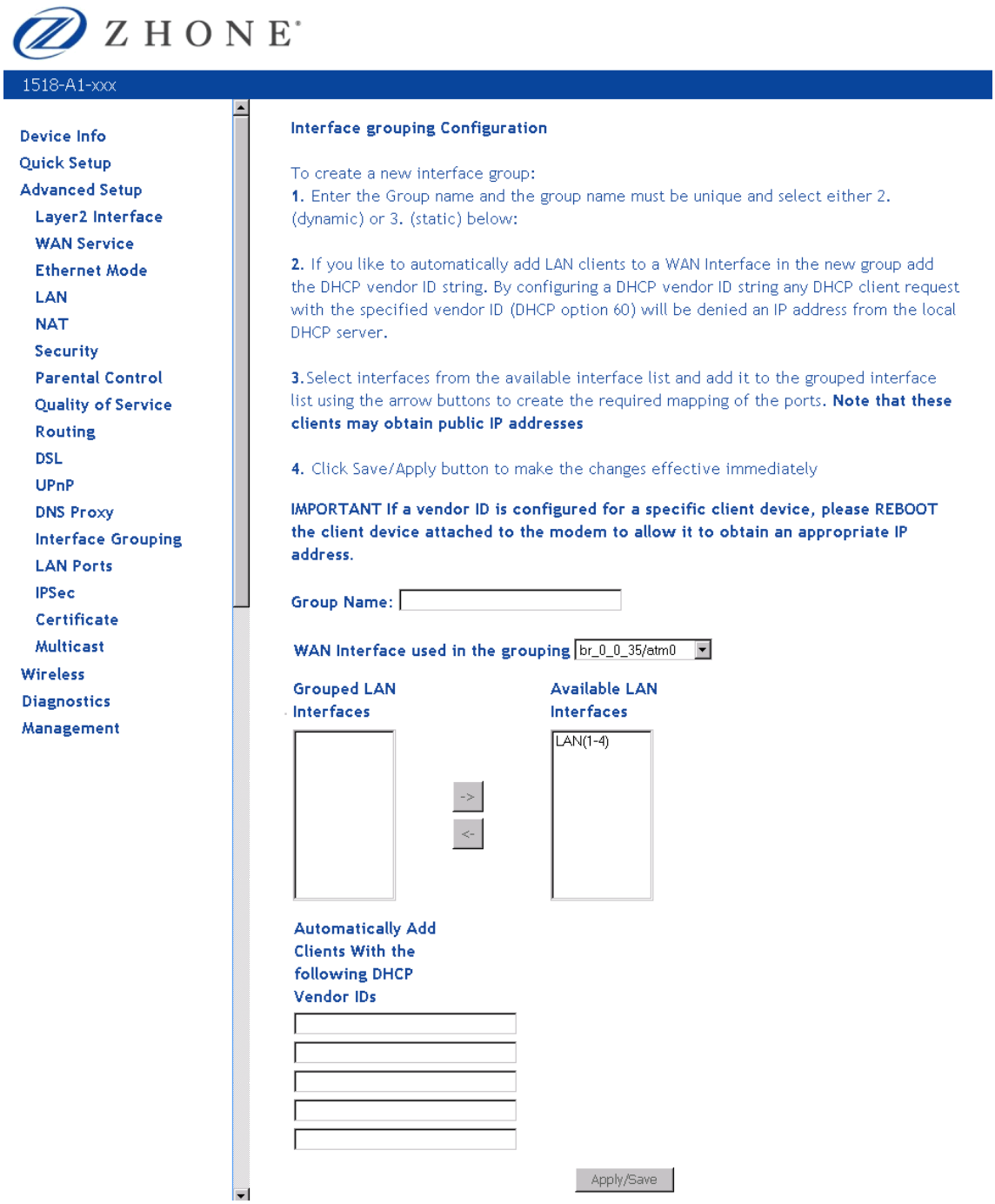
1. *Click **Add** button*



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.*

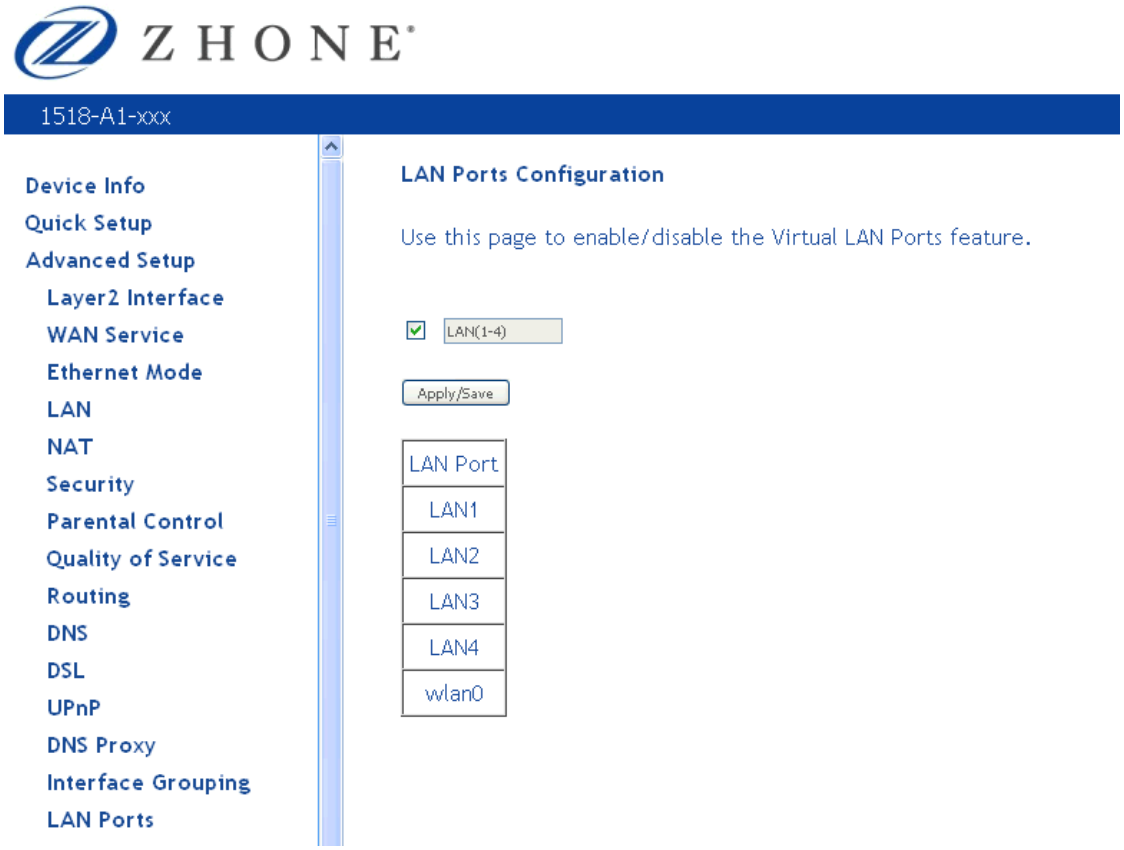


3. *Select interfaces from the available interface list and add them to the grouped interface list using the arrow buttons to create the required mapping of the ports.*

4. *Click **Save/Apply**.*

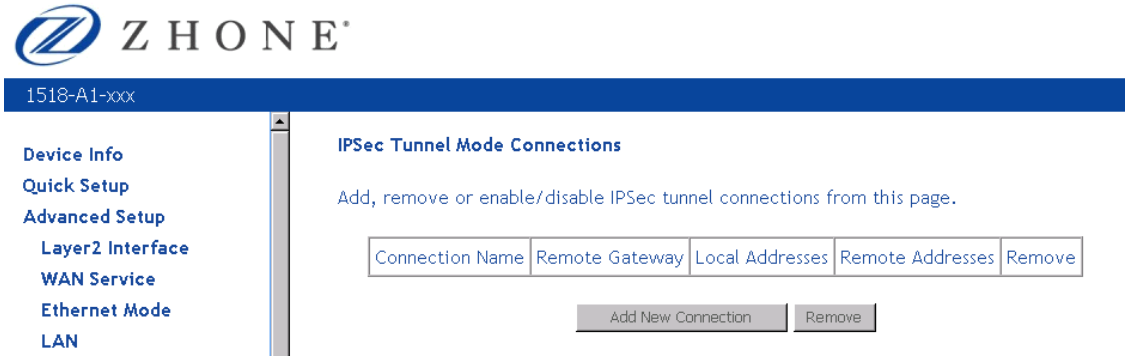
LAN Ports

Enable/disable virtual LANs. Virtual LANs are used to enhance security and manage traffic going to different networks.

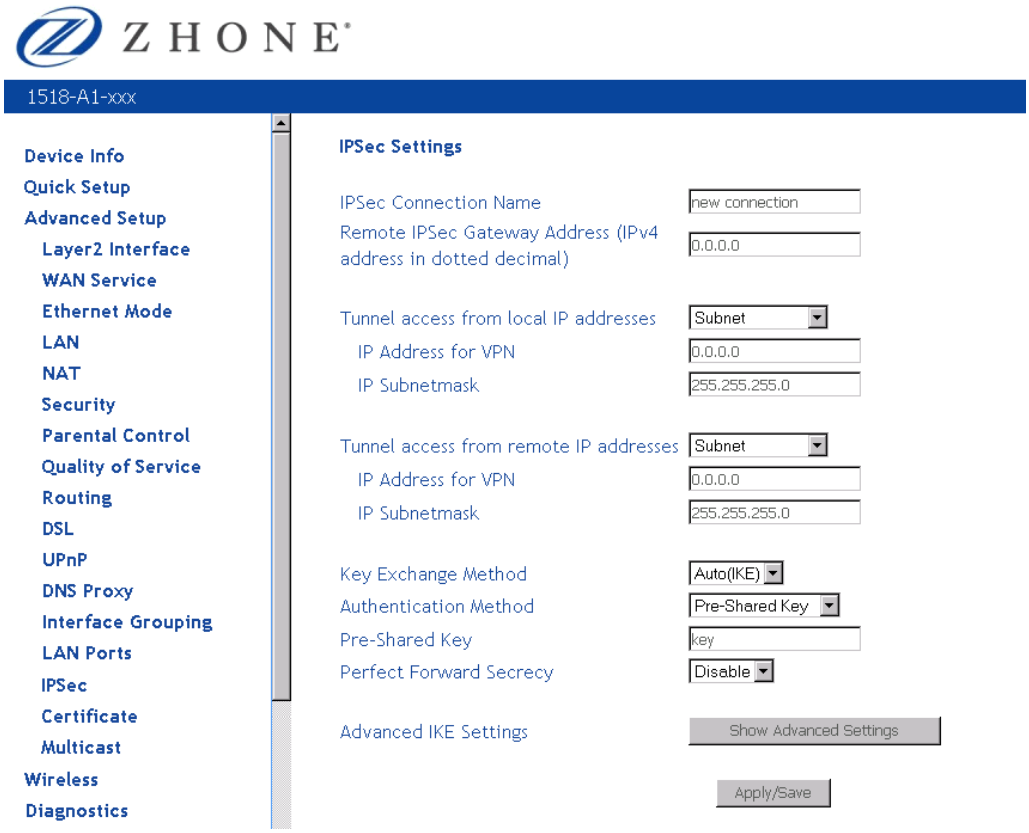


IPSec

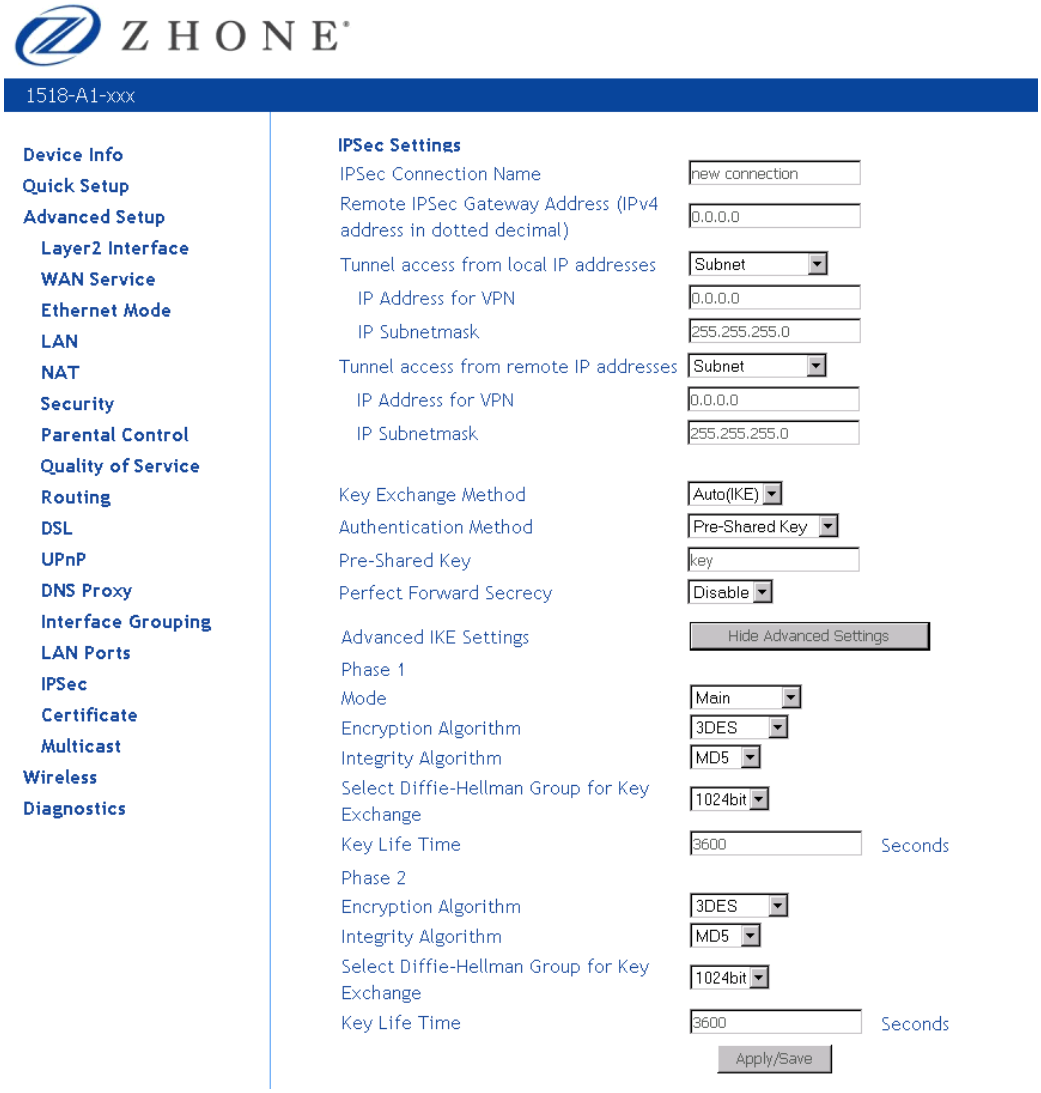
Internet Protocol Security (IPSec) allows you to set up secure tunnel access between two IP addresses. Encryption and key exchange make this a secure way to access remote networks. Contact your ISP for the necessary information to correctly configure this connection.



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


ZHONE
1518-A1-xxx
Device Info
Quick Setup
Advanced Setup
Layer2 Interface
WAN Service
Ethernet Mode
LAN
NAT
Security
Parental Control
Quality of Service
Routing
DSL
UPnP
DNS Proxy
Interface Grouping
LAN Ports
IPSec
Certificate
Multicast
Wireless
Diagnostics
IPSec Settings
IPSec Connection Name
new connection
Remote IPSec Gateway Address (IPv4 address in dotted decimal)
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
Show Advanced Settings
Apply/Save

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



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.

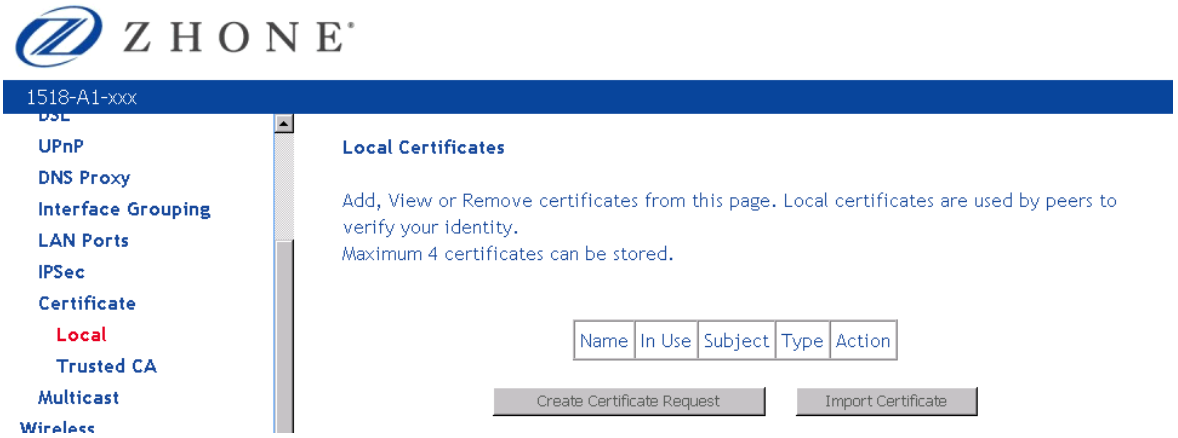
Note: Certificates are used with TR-069. Firmware that does not support TR-069 will not support certificates.

Local

A local certificate identifies your device over the network.

To apply for a certificate:

1. *Click **Create Certificate Request***



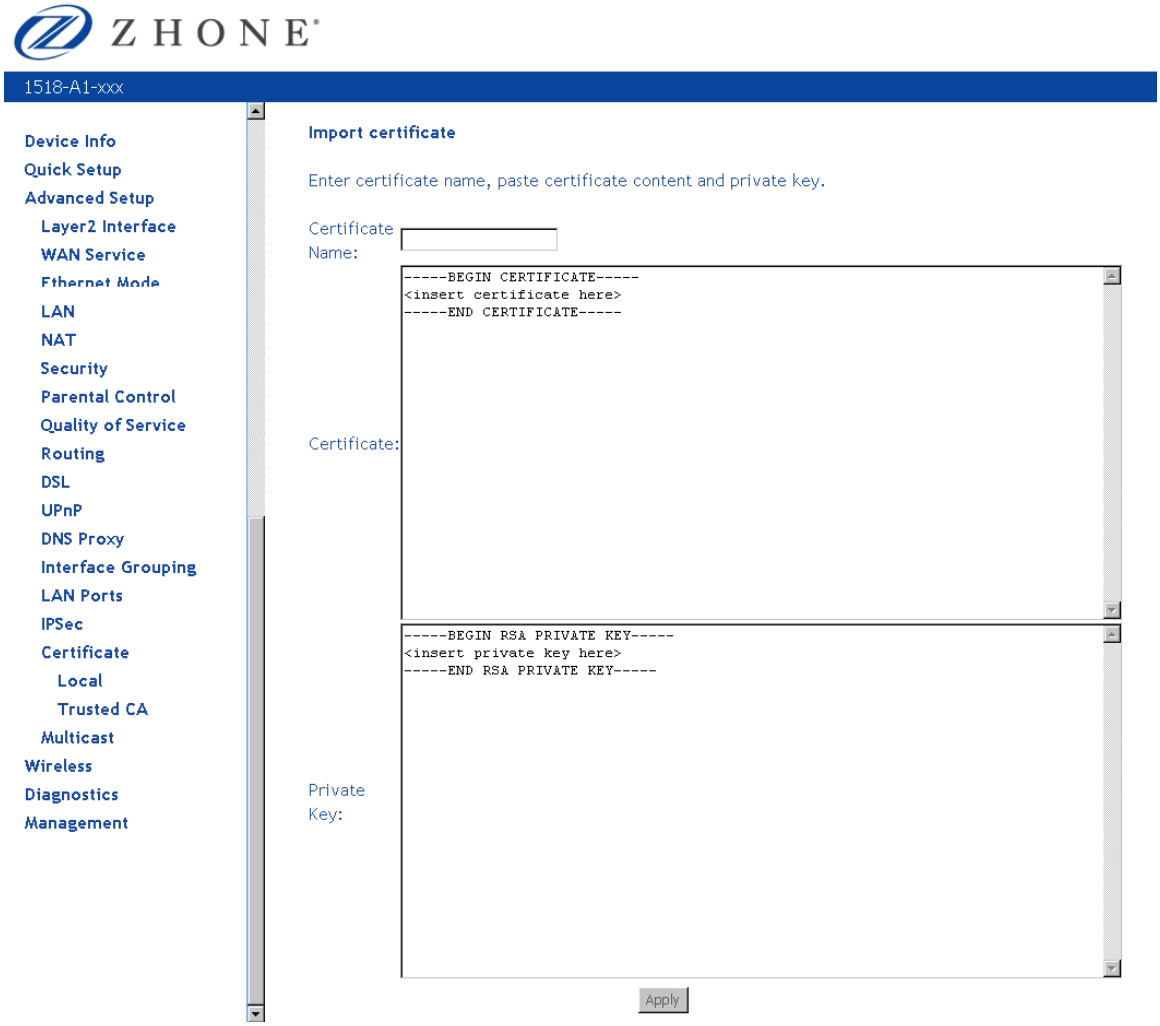
If you have an existing certificate, click on **Import Certificate** to retrieve it.

The **Create new certificate request** screen allows you to create 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.



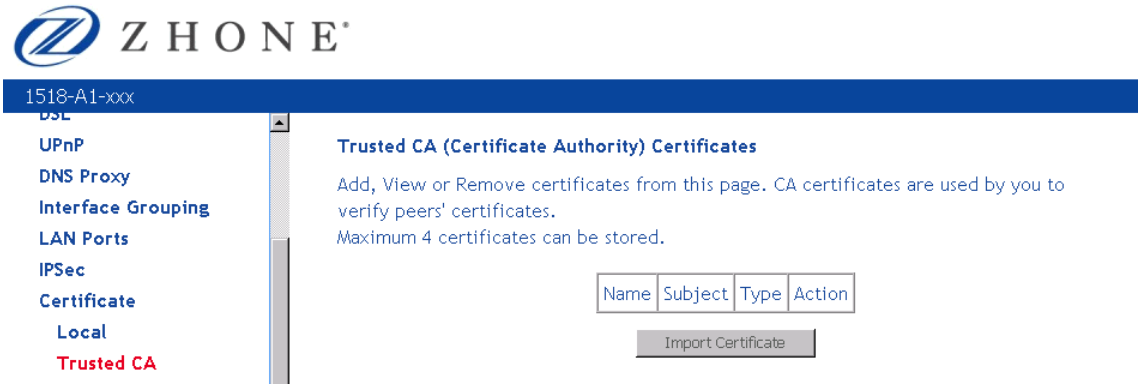
Trusted CA

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

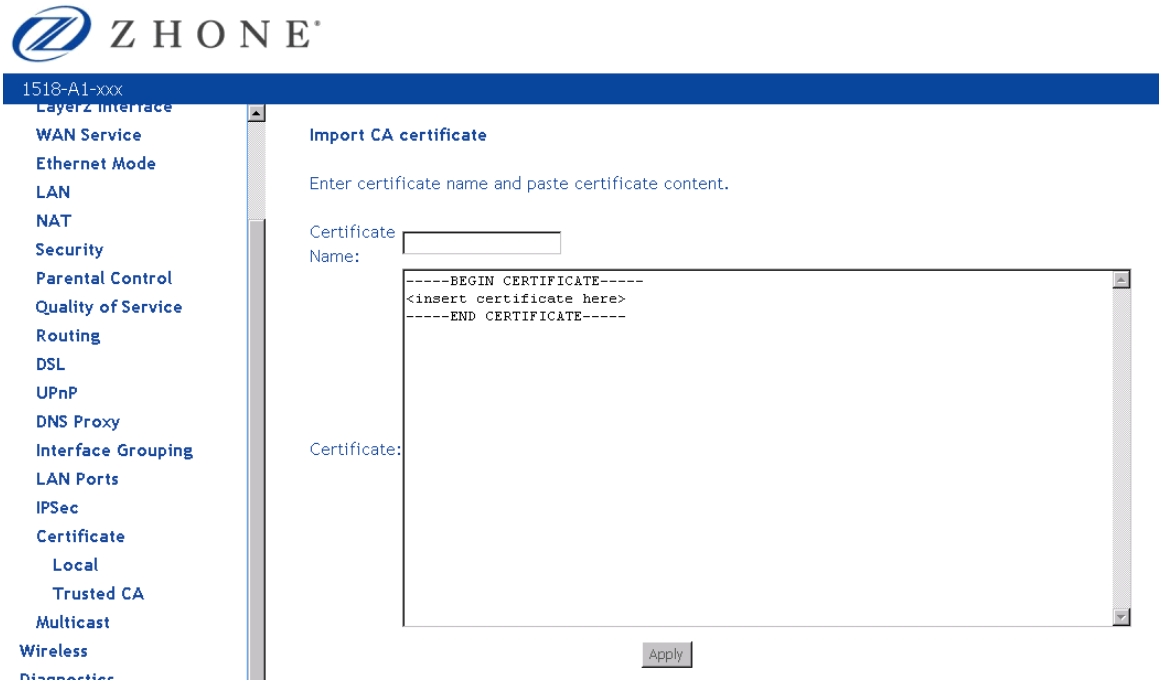
The **Trusted CA (Certificate Authority) Certificates** screen also allows you to view certificates. You can store up to 4 certificates.

To Import a certificate:

1. *Click on **Import Certificate***



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

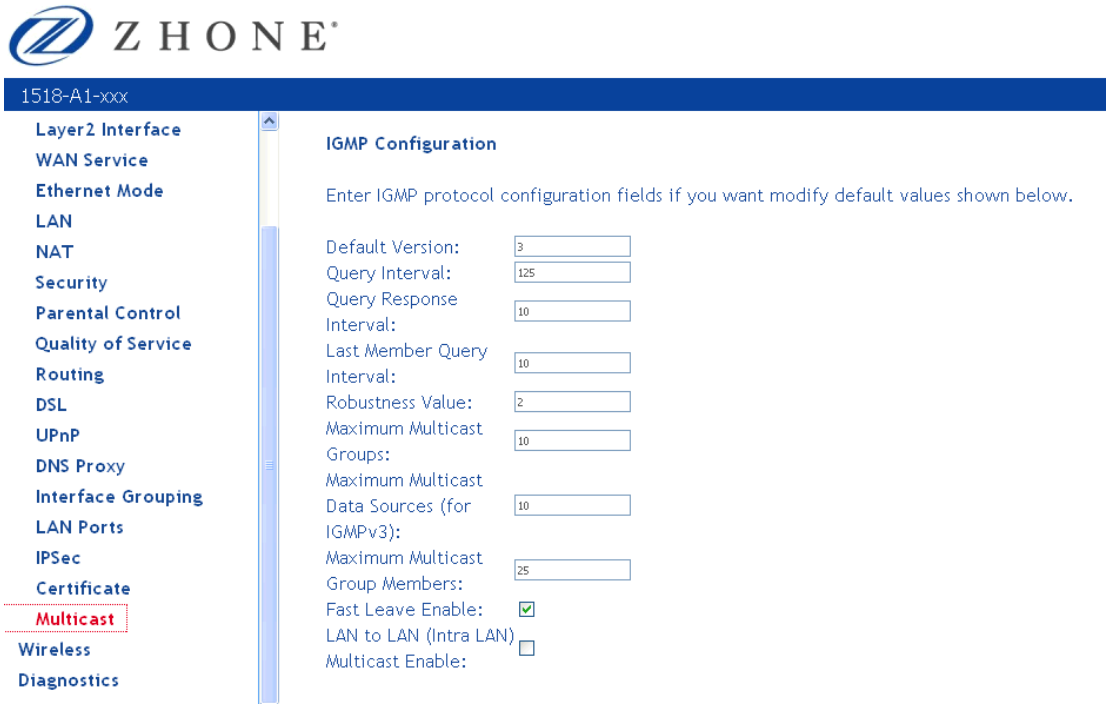


3. *In the Certificate text window paste the content of the certificate.*

4. *Click **Apply**.*

Multicast

The **Multicast** screen allows you to configure IGMP settings for multicast.



Wireless

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

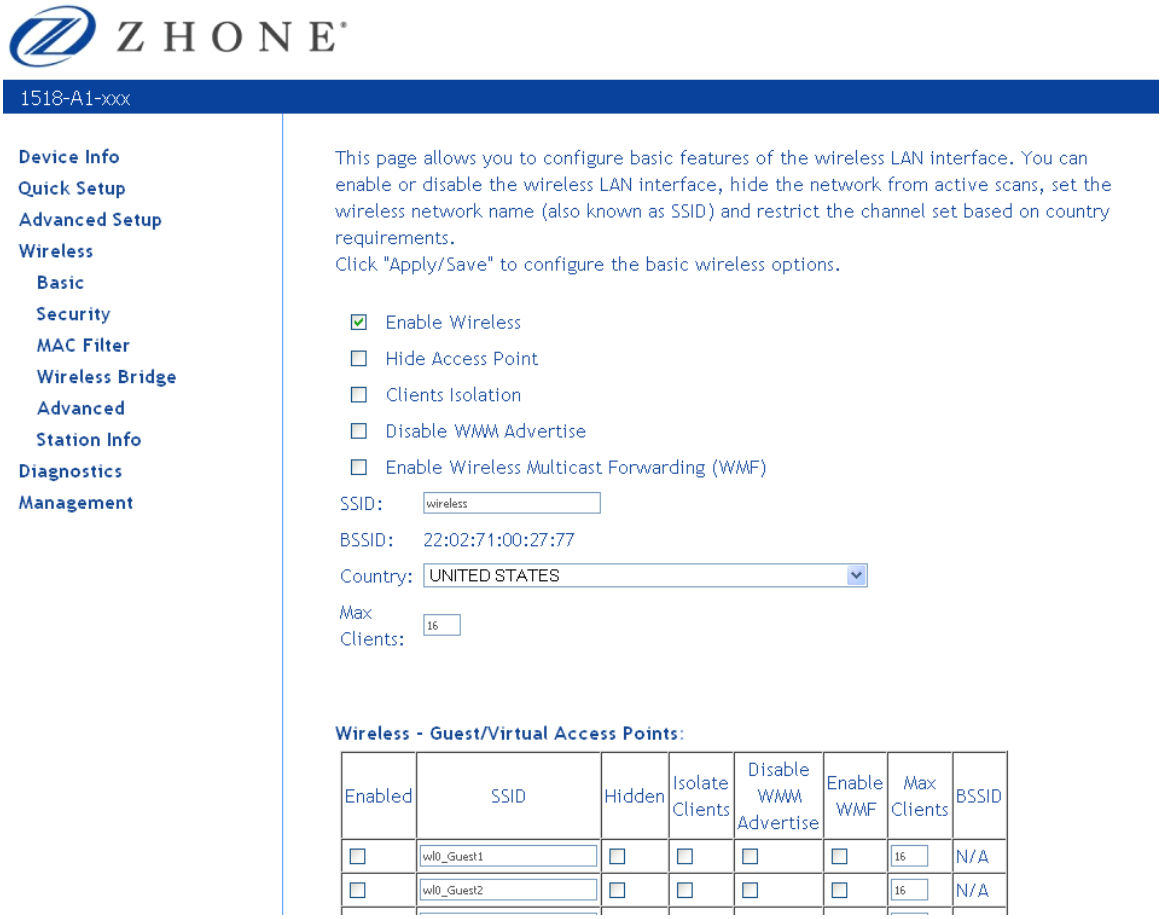
- Basic
- Security
- MAC filter
- Wireless bridge
- Advanced
- Quality of service and station info.

NOTE: The 1512 and 1511 do not provide wireless LAN.

Basic

The **Wireless – Basic** screen allows you to enable or disable the wireless function. 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.

ZHONE
1518-A1-xxx
Device Info
Quick Setup
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
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/Save" to configure the basic wireless options.
Enable Wireless
Apply/Save


ZHONE
1518-A1-xxx
Device Info
Quick Setup
Advanced Setup
Wireless
Basic
Security
MAC Filter
Wireless Bridge
Advanced
Station Info
Diagnostics
Management
This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless LAN interface, 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/Save" to configure the basic wireless options.
Enable Wireless
Hide Access Point
Clients Isolation
Disable WMM Advertise
Enable Wireless Multicast Forwarding (WMF)
SSID: wireless
BSSID: 22:02:71:00:27:77
Country: UNITED STATES
Max Clients: 16
Wireless - Guest/Virtual Access Points:
Enabled
SSID
Hidden
Isolate Clients
Disable WMM Advertise
Enable WMF
Max Clients
BSSID
wl0_Guest1
16
N/A
wl0_Guest2
16
N/A

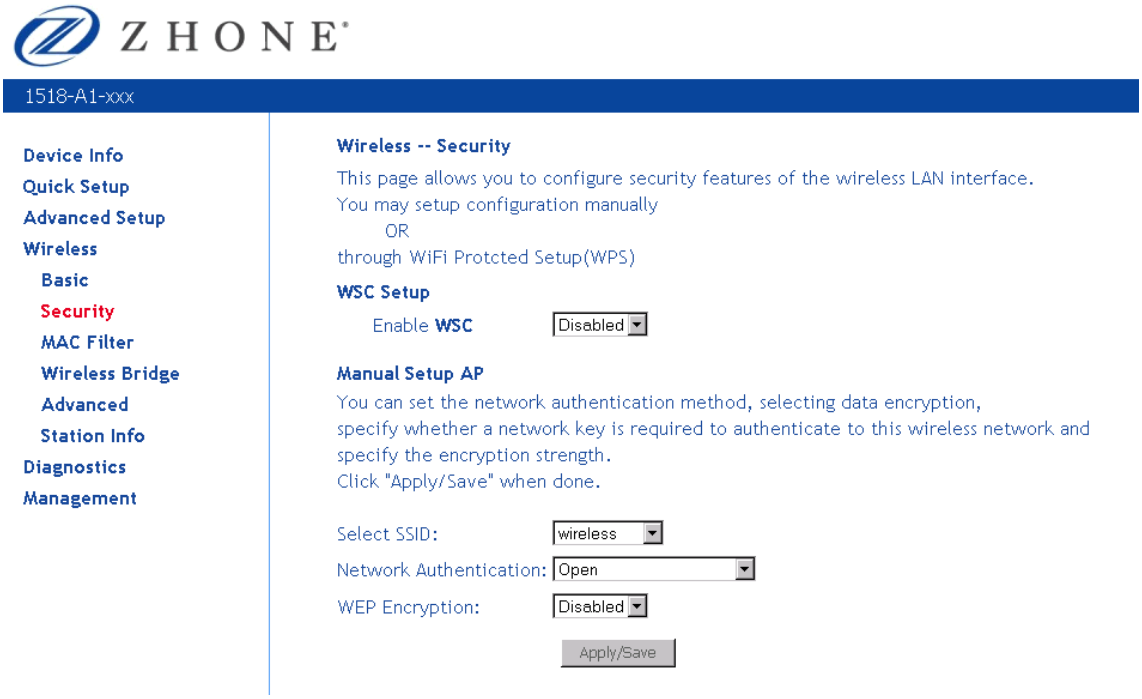
Security

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

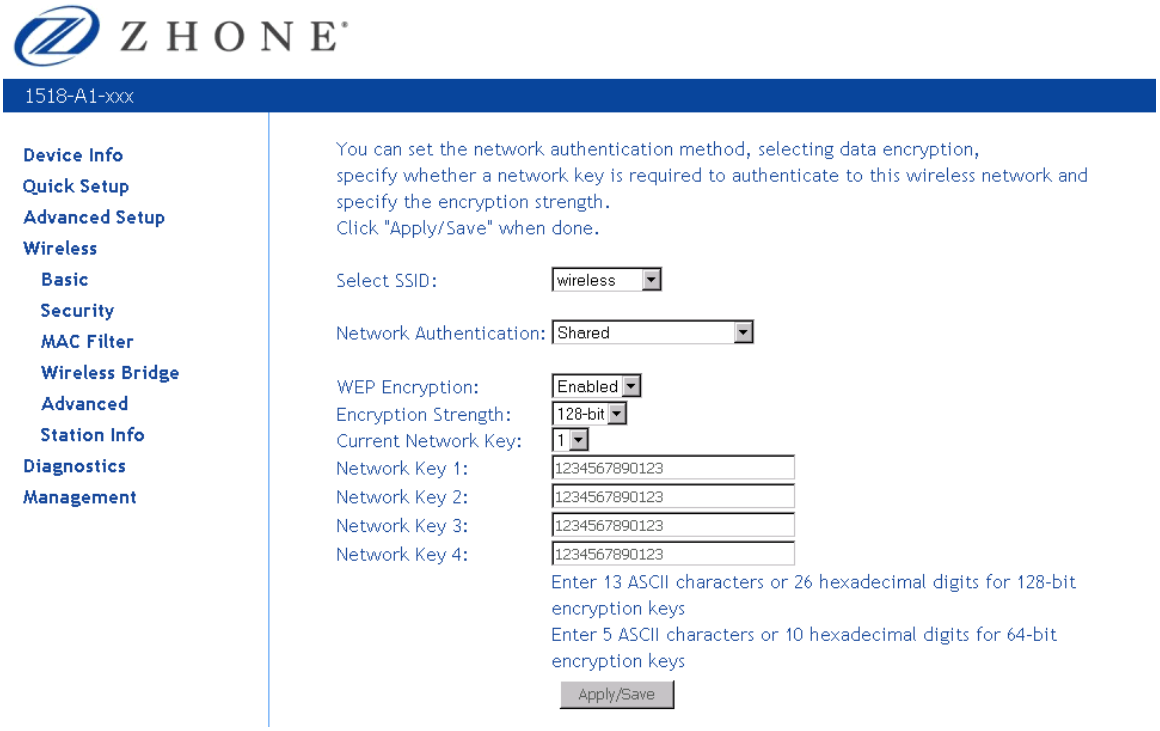
Note that depending on the network authentication that is selected, the screen will change accordingly so additional fields can be configured for the specific authentication method.

Network authentication methods include the following—

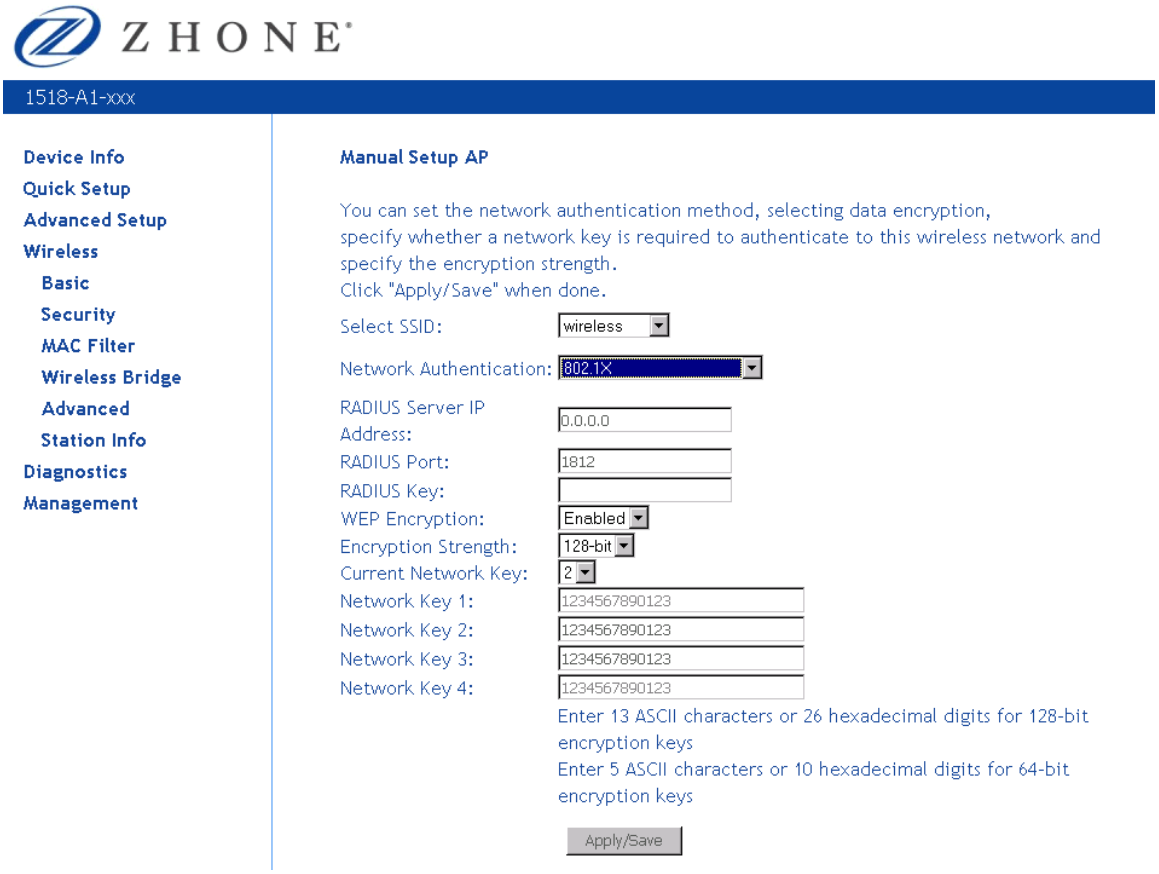
- **Open** — anyone can access the network. The default is a disabled WEP encryption setting



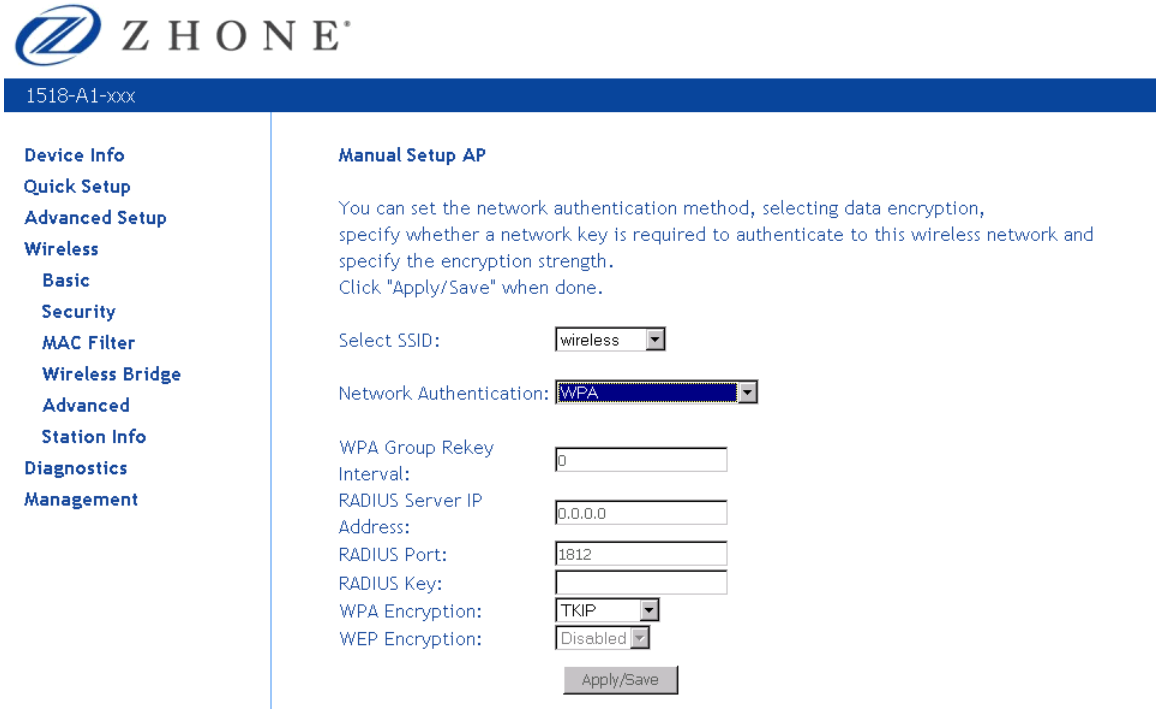
- **Shared** — WEP encryption is enabled and encryption key strength of 64-bit or 128-bit needs to be selected. Click on Set Encryption Keys to manually set the network encryption keys. Up to 4 different keys can be set and you can come back to select which one to use at anytime.



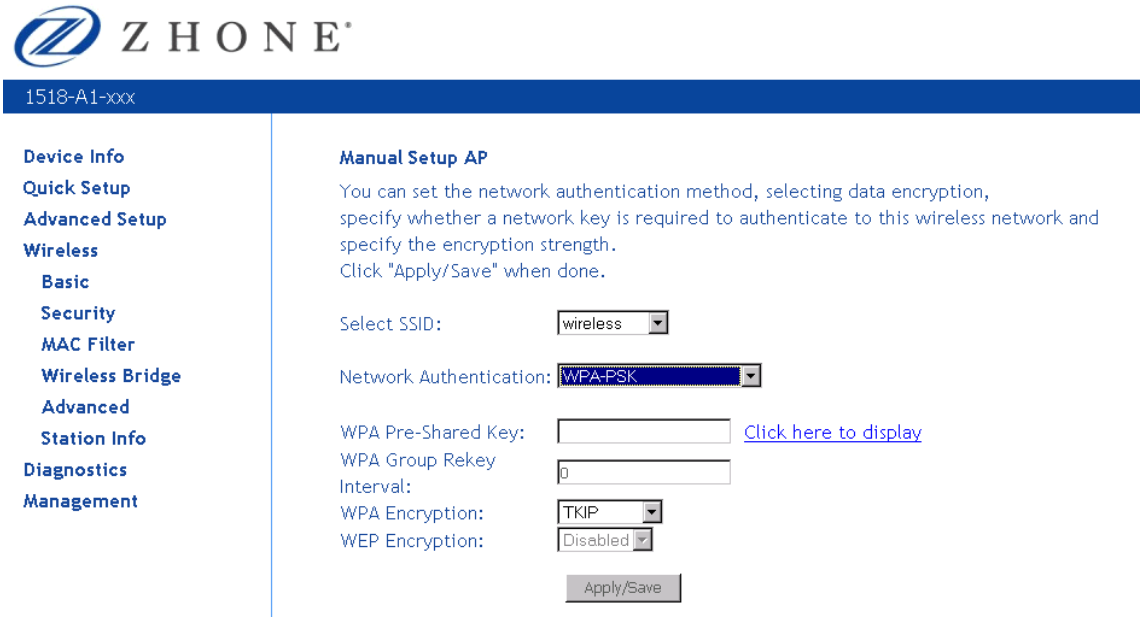
- **802.1X** — requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is also enabled and the encryption strength must also be selected.



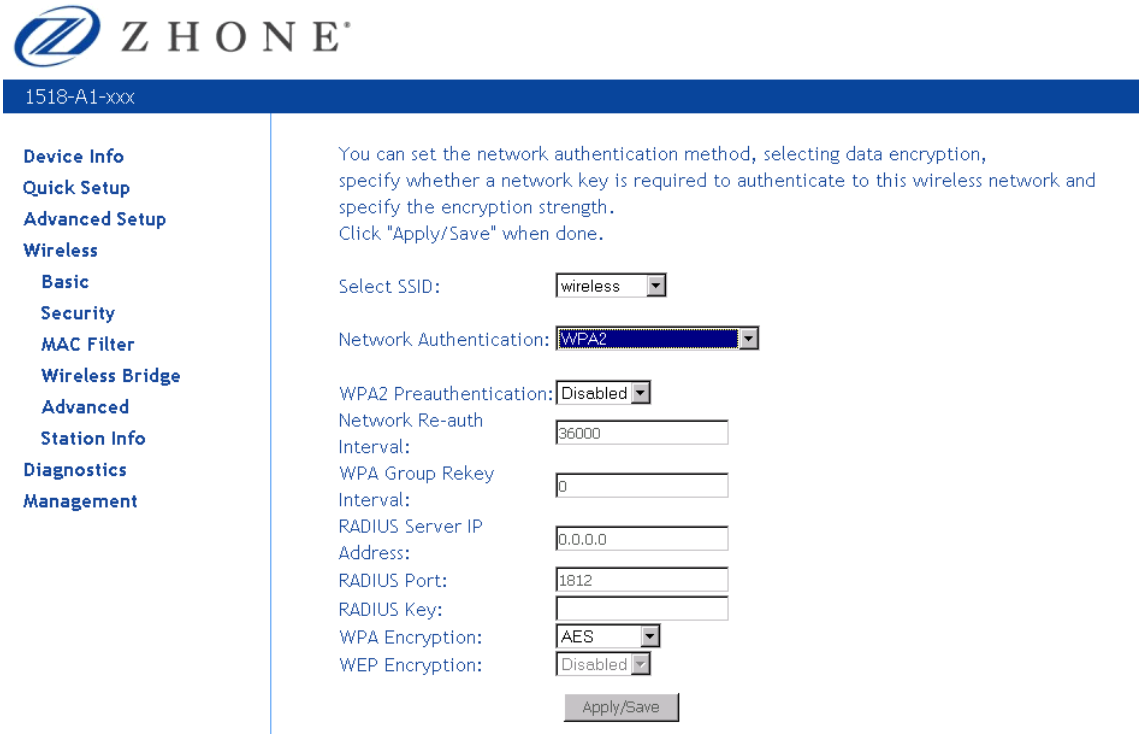
- **WPA** (Wi-Fi Protected Access) — usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses128-bit dynamic session keys (per user, per session, and per packet keys).



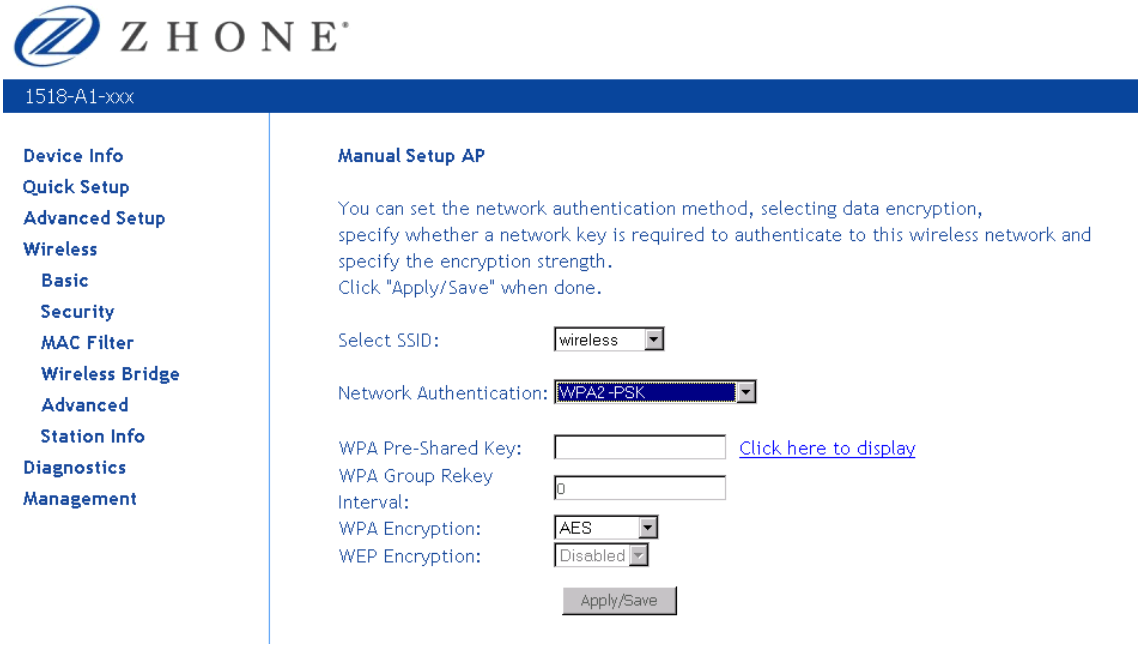
- **WPA-PSK** (Wi-Fi Protected Access – Pre-Shared Key) — WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise environment. The main difference is that the password is entered manually. A group re-key interval time is also required.



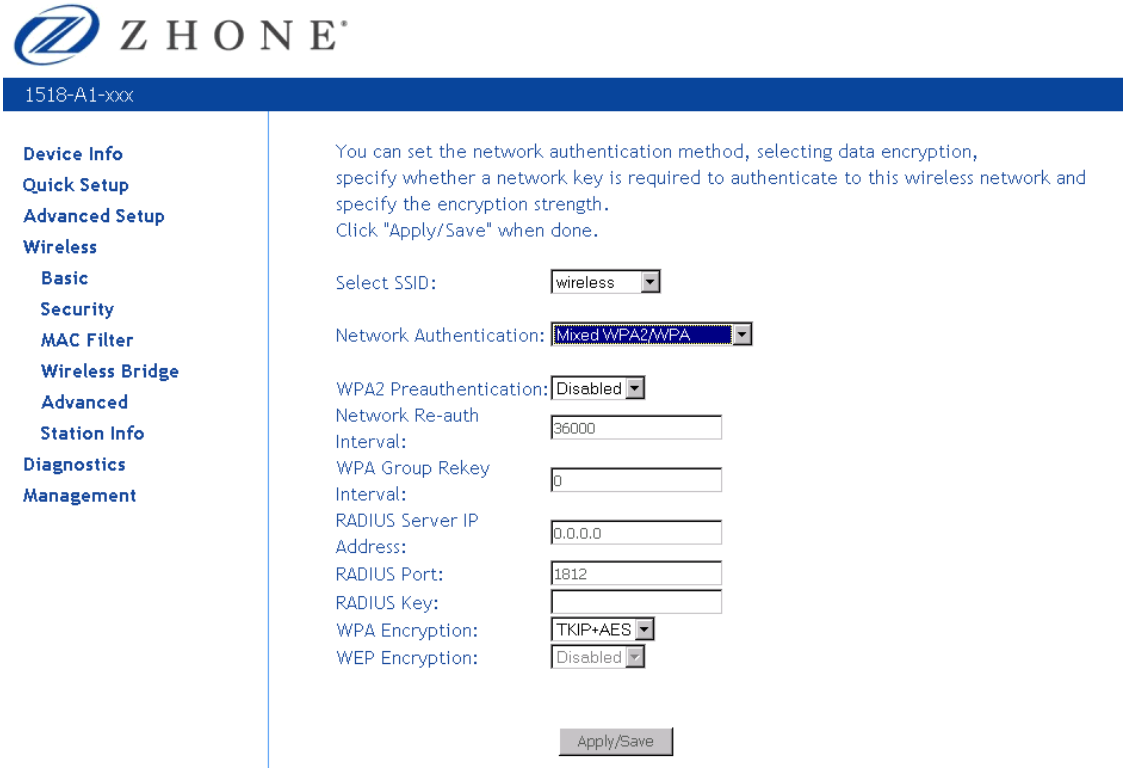
- **WPA2** (Wi-Fi Protected Access 2) — second generation WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method. Network re-authorization interval is the time in which another key needs to be dynamically issued.



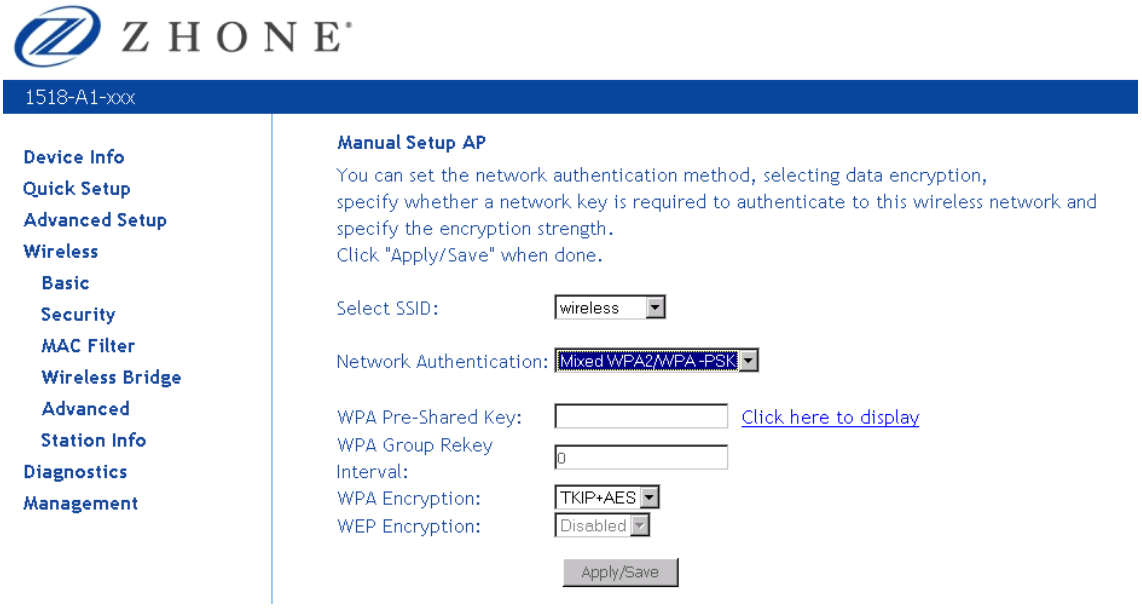
- **WPA2-PSK** (Wi-Fi Protected Access 2 – Pre-Shared Key) — suitable for home and SOHO environments, it also uses AES encryption and requires you to enter a password and a re-key interval time.



- **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 a as well as a group re-key interval time. Both TKIP and AES are used.



- **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

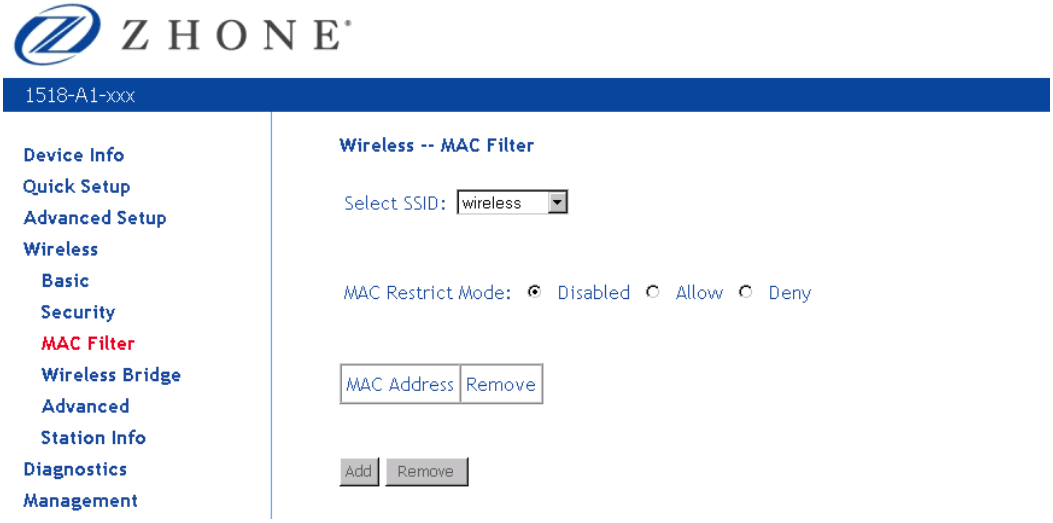
By default, MAC filter is disabled meaning any WiFi clients with the correct access will be allowed to access the Access Point. The MAC filter screen allows you to control what WiFi clients are allowed or deny to access the WiFi Access Point using the MAC address of the devices.

1. *Selected the SSID you want to WiFi client access.*

2. *To allow access only a selected WiFi client, select **Allow**, then click on **Add** to add the MAC addresses you want to be able to access the WiFi network.*

3. *To block certain WiFi Clients from accessing the WiFI network, select **Deny**, then click **Add** to add the MAC address of the WiFi client you want to block from Accessing the WiFi network.*

1.



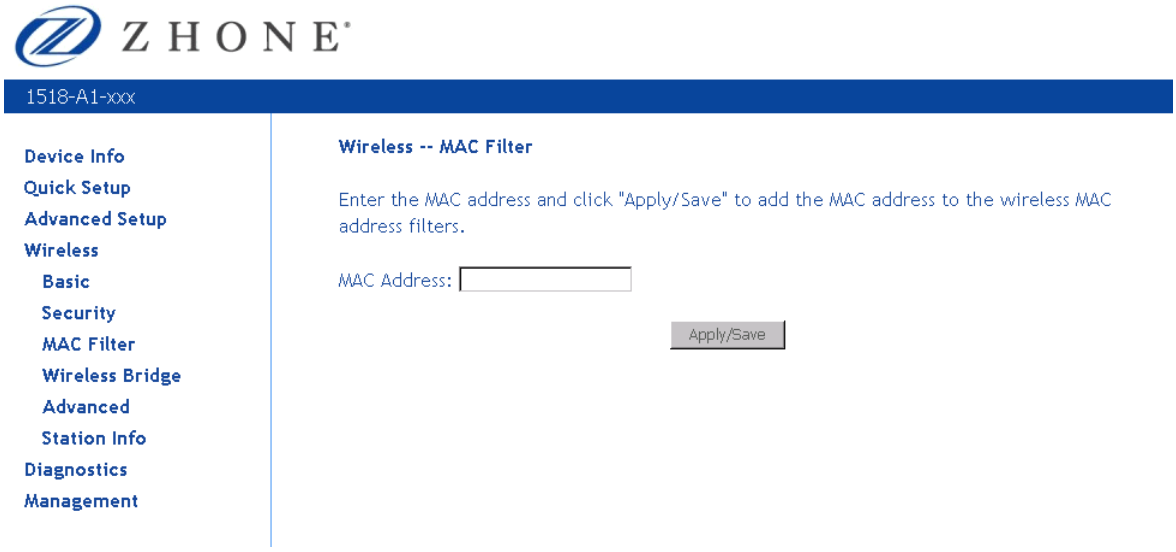
To add a MAC Filter:

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

2. *From one of the **MAC Restrict Mode** radio buttons, select **Disabled**, **Allow** or **Deny**.*

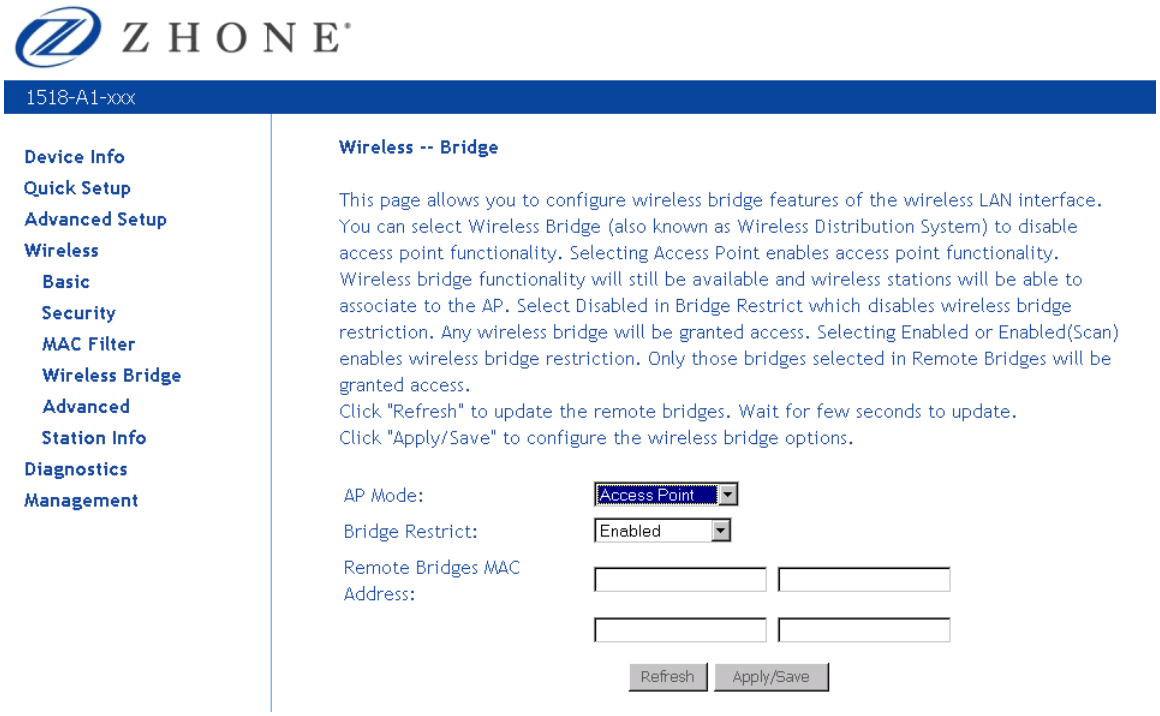
3. *Click **Add.***

4. *In the **Wireless - MAC Filter screen** 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:

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

   AP Mode options are

   - Access Point

- Wireless Bridge

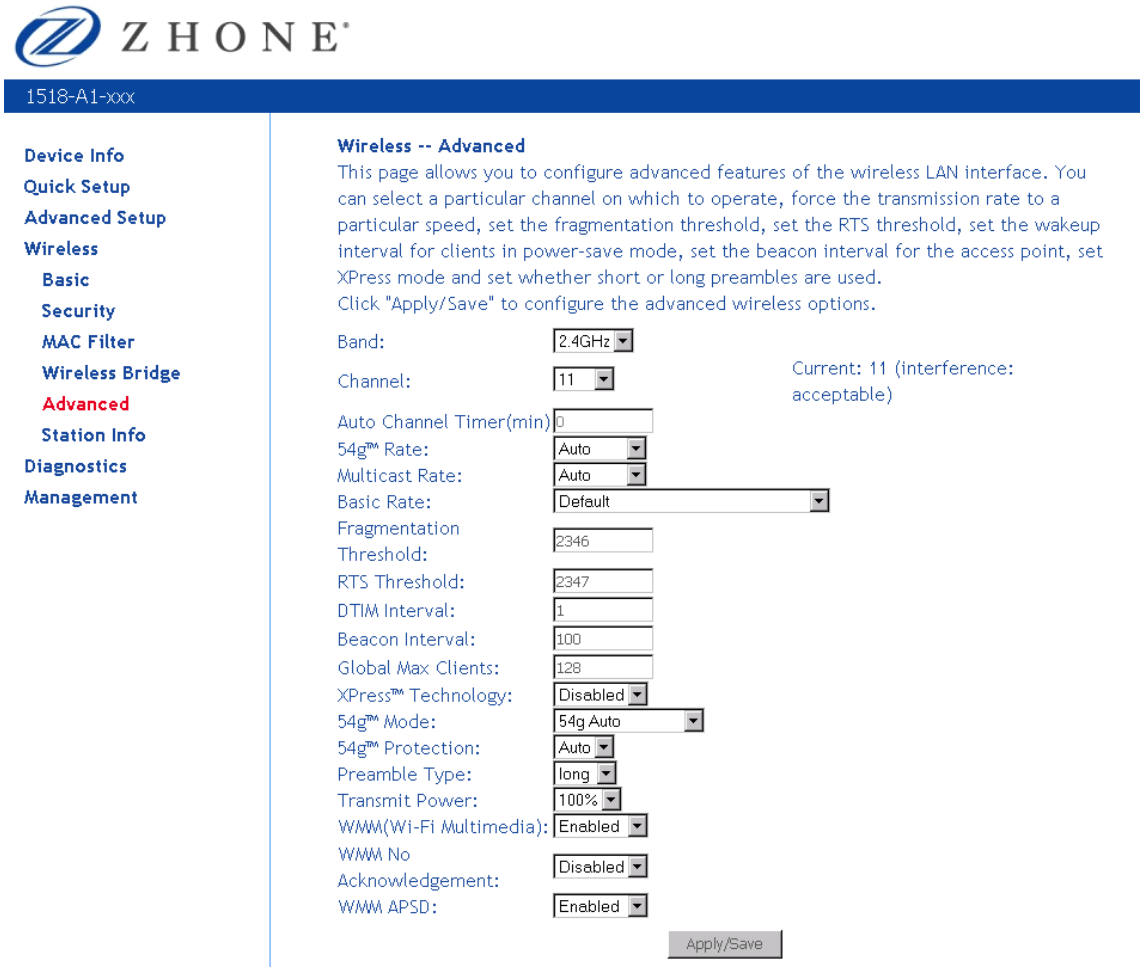
2. *From the **Bridge Restrict** dropdown select to **Enable**, **Disable** or **Refresh (Enabled Scan)**. If you have chosen to enable access point, in the **Remote Bridges MAC Address** text box(es) MAC address(es) for the bridge(s).*

3. *If you have chosen access point **Enabled (Scan)**, select the MAC addresses to restrict and clock **Apply / Save**.*

Advanced

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

Note: Do not change the settings on this screen if you are not familiar with WiFi settings.



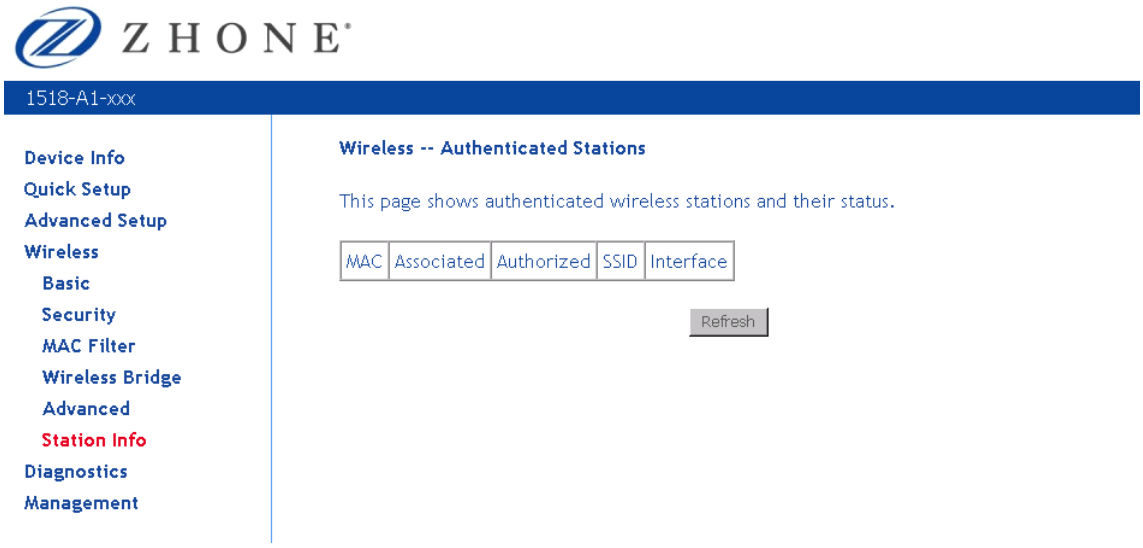
Advanced features include:

- **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 an 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.



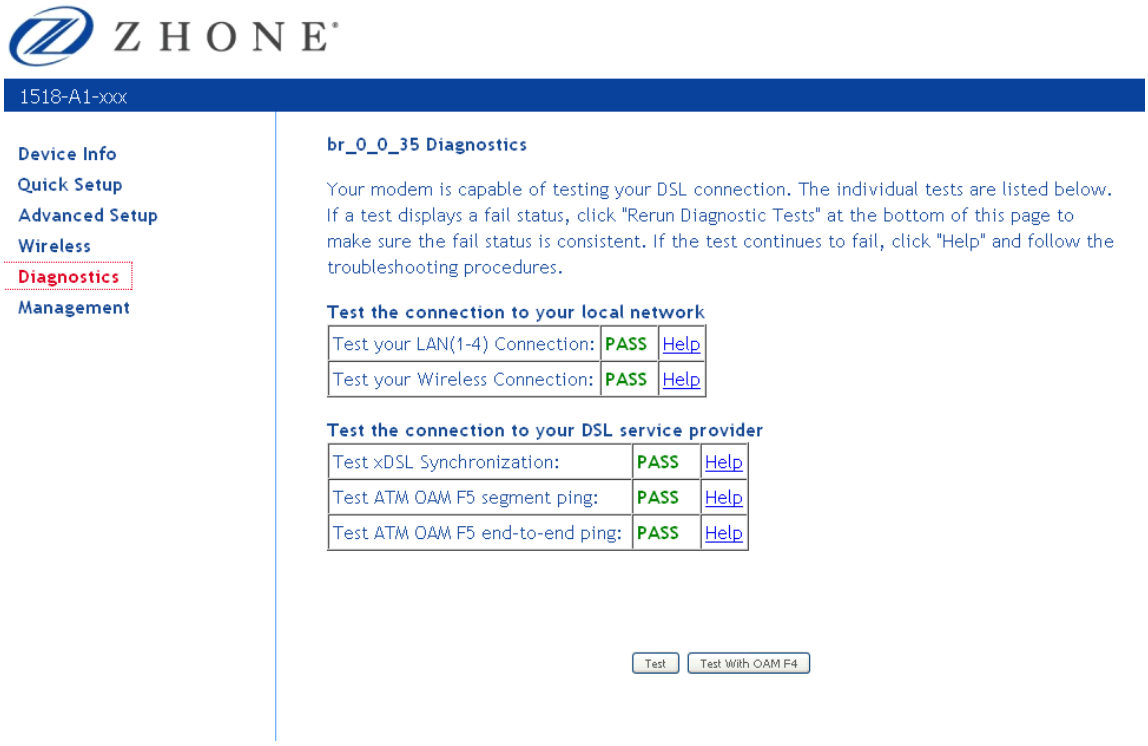
Diagnostics

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

The **Test** and **Test with OAM F4** buttons allow you to retest if necessary.

Click the **Next Connection** button to test your router's next connection.



Management

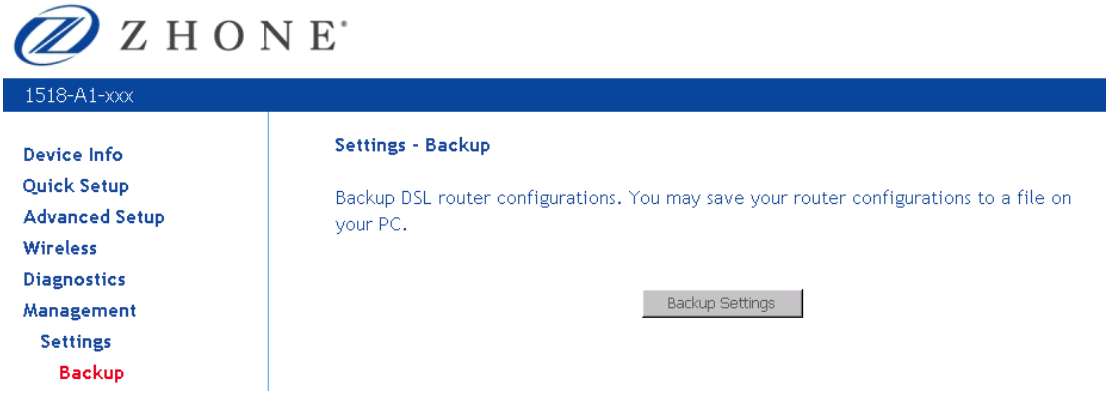
The Management section gives you access to certain setups for the purpose of maintaining the system, including backing up the configurations, viewing system log, maintaining access control, updating software, etc.

Settings

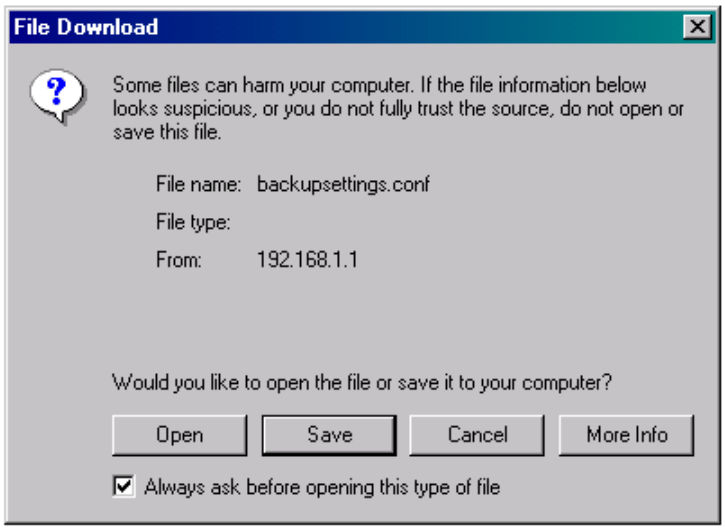
Backup Settings

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.



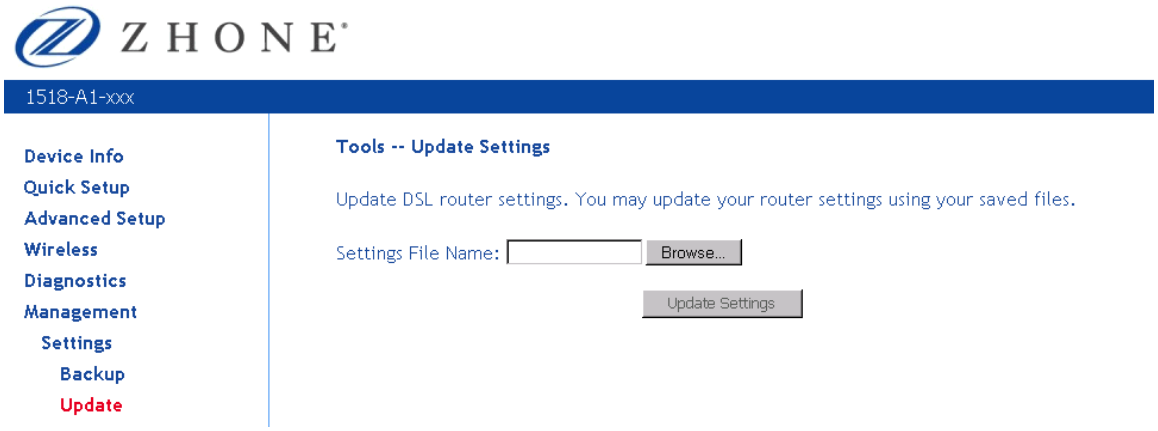
2. *Click* ***Save****.*

Update 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**.*



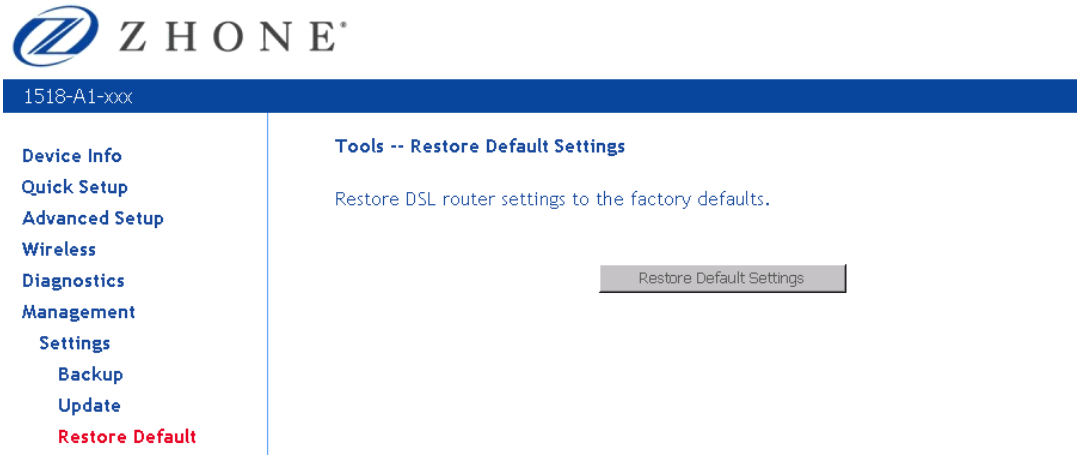
The router will restore settings and reboot to activate the restored settings.

Restore Default

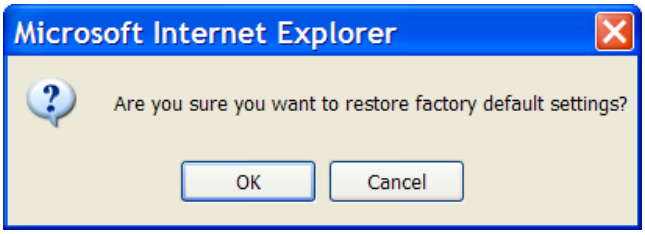
Restore Default will delete all configuration changes you have made and restore the router to factory default settings.

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.*

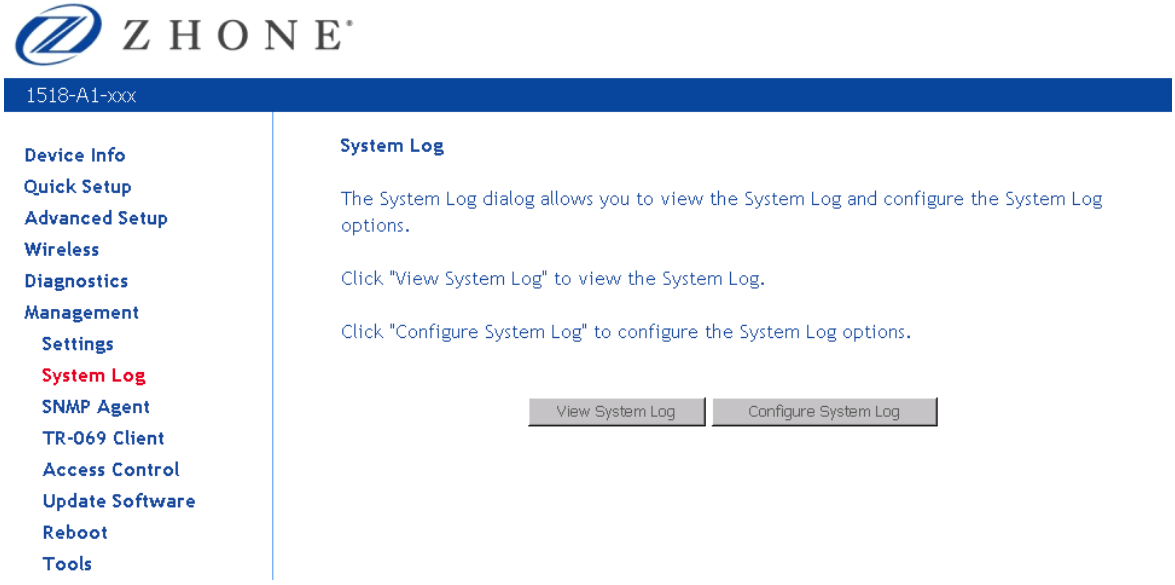


The router will restore the default settings and reboot.

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.

Note: Only configure this if you are instructed by your ISP technician during troubleshooting sessions.



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.

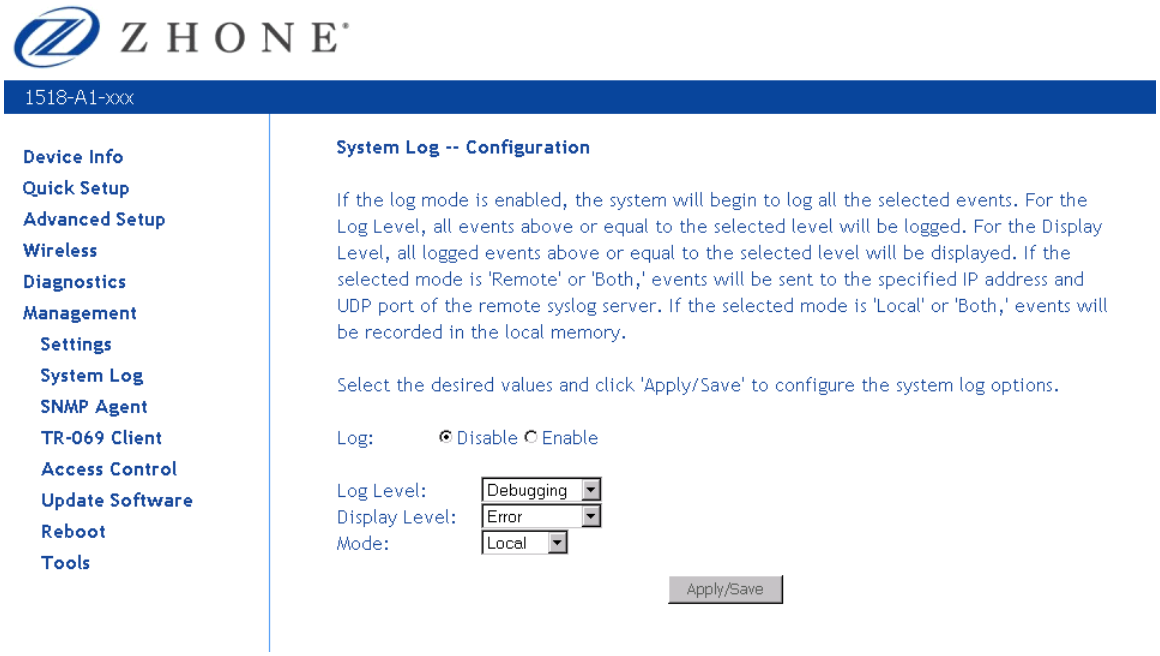
Refresh Close

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.



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.

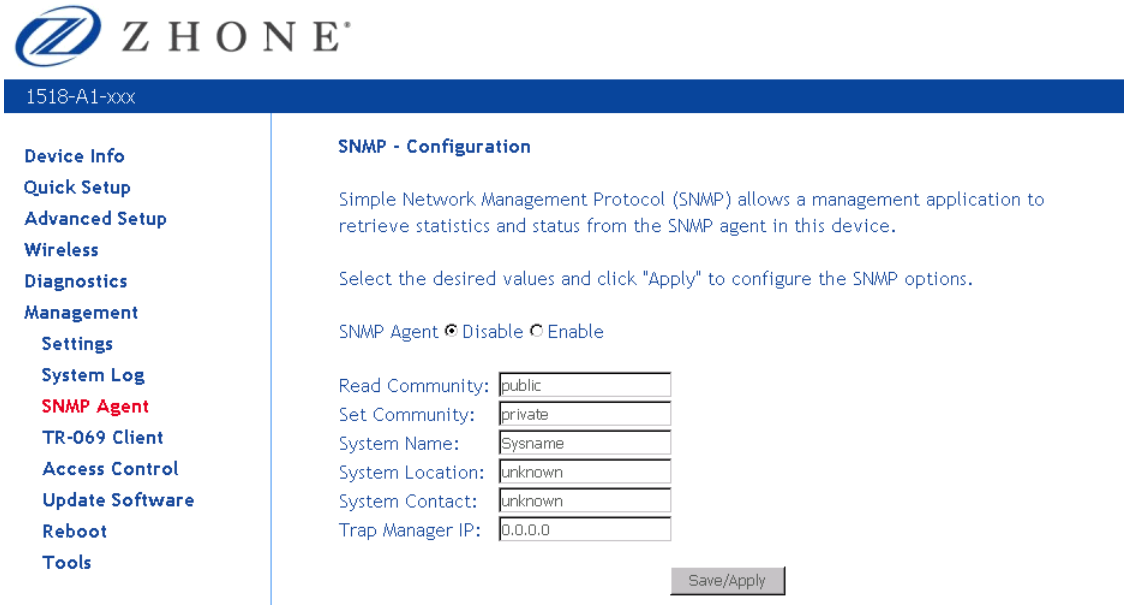
If the selected mode is **Local** or **Both**, events will be recorded in the local memory.

Select the desired values and click **Save/Apply** button to configure the system log.

SNMP Agent

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.

Note: Do not change this information unless you are instructed to by your ISP technician.



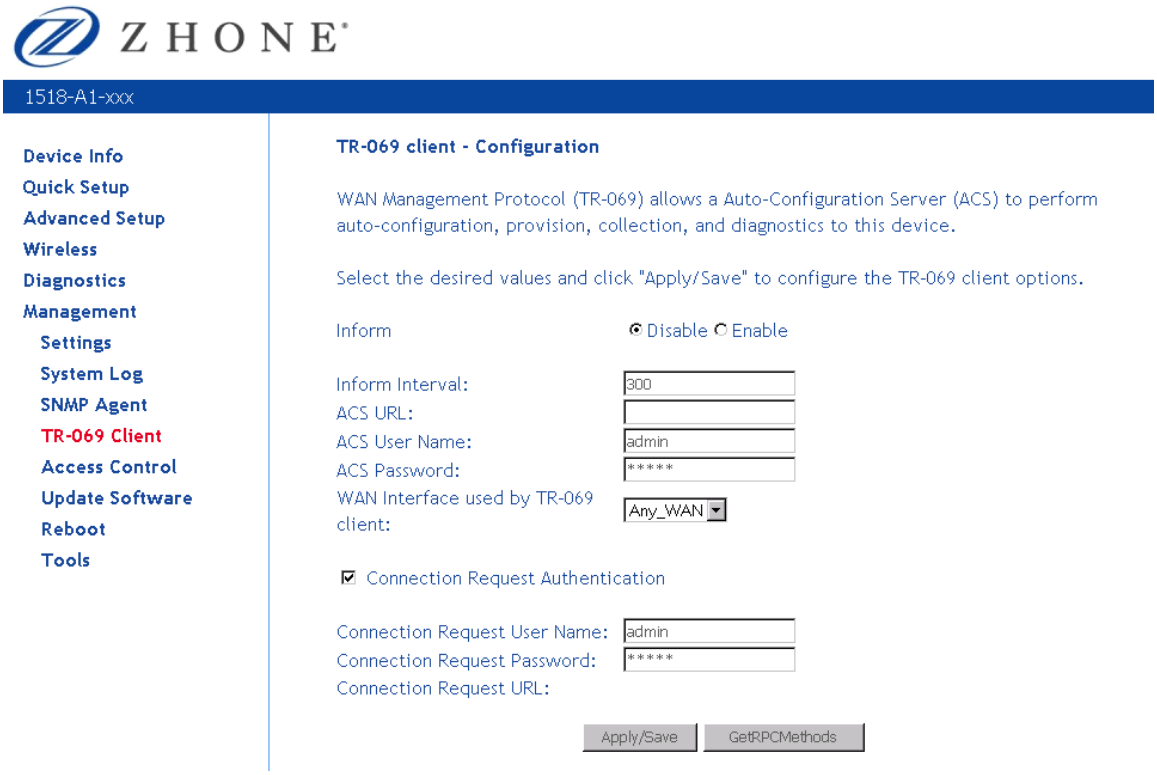
TR-069 Client

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

Note: Do not change this information unless you are instructed to by your ISP technician.

To enable the TR-069 client protocol:

1. *Select **Enable**.*



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

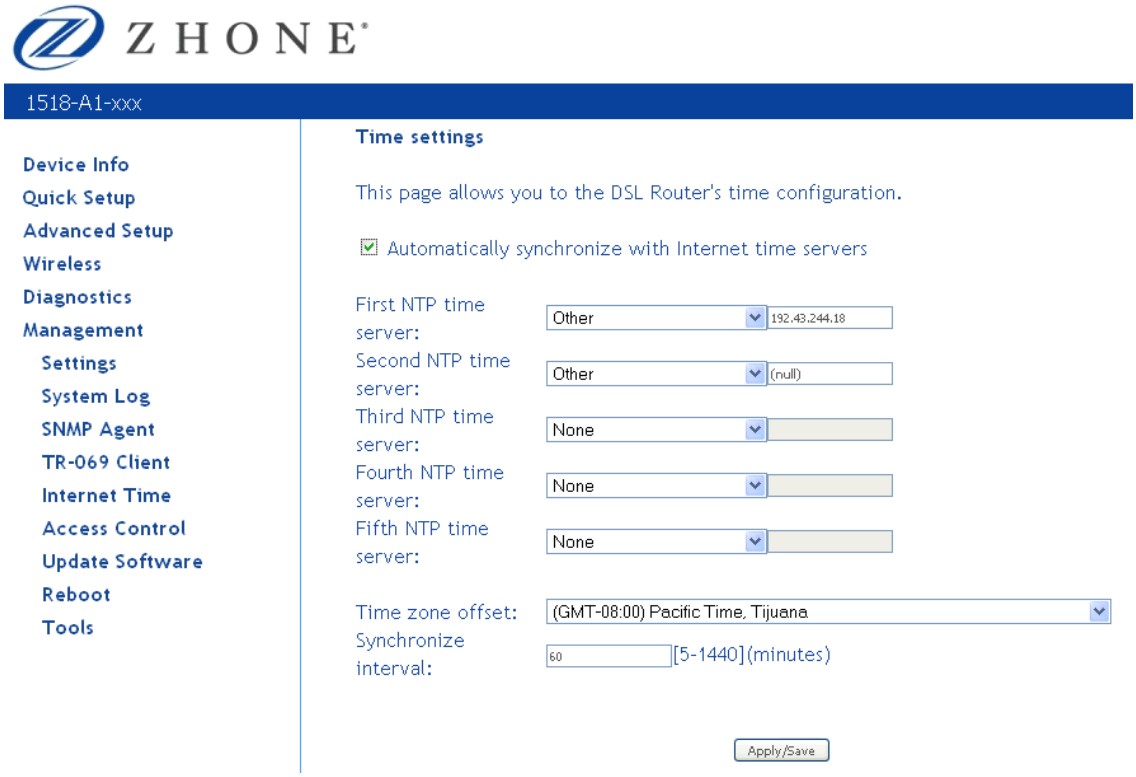
Internet Time

Your router can synchronize its internal clock servers with servers running Network Time Protocol (NTP).

1. *To enable NTP, click **Automatically synchronize with Internet time servers** and enter the NTP settings.*

2. *You may want to select a different NTP server or time zone.*

3. *Click **Apply / Save**.*



Access Control

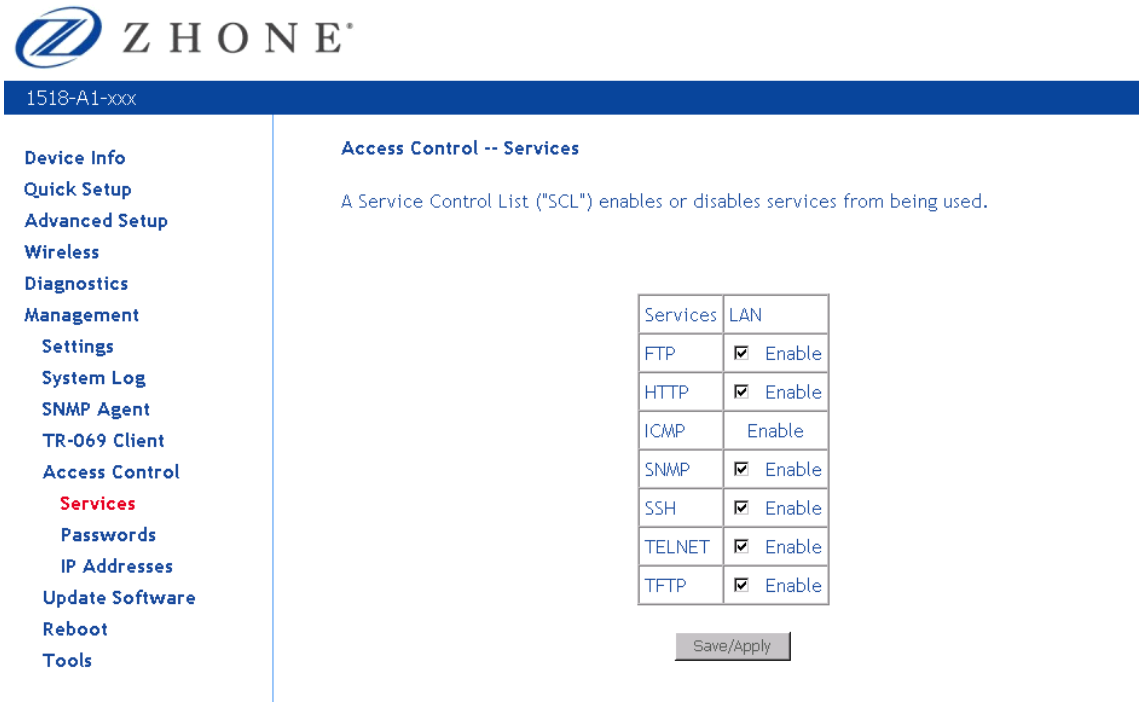
You can enable or disable some services of your router by LAN or WAN. If no WAN connection is defined, only the LAN side can be configured.

Note: Do not change this information unless you are instructed to by your ISP technician.

Services

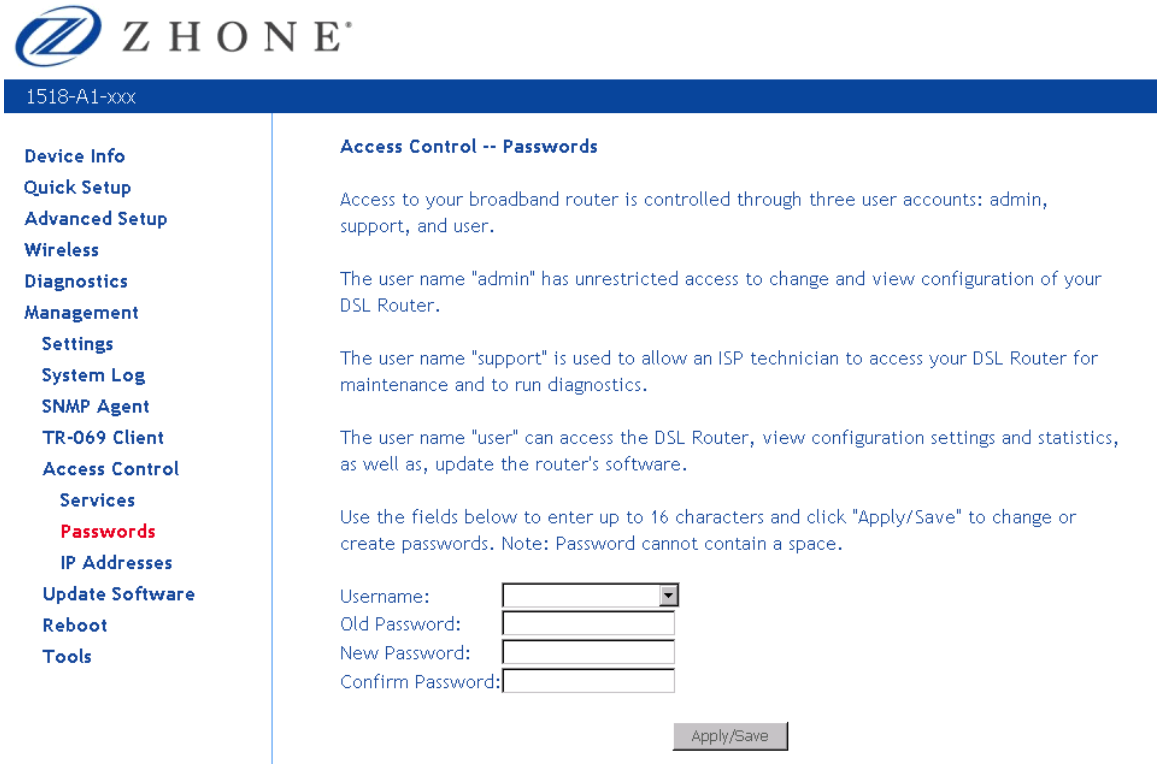
Services that can be enabled or disabled on the LAN/WAN are

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



Passwords

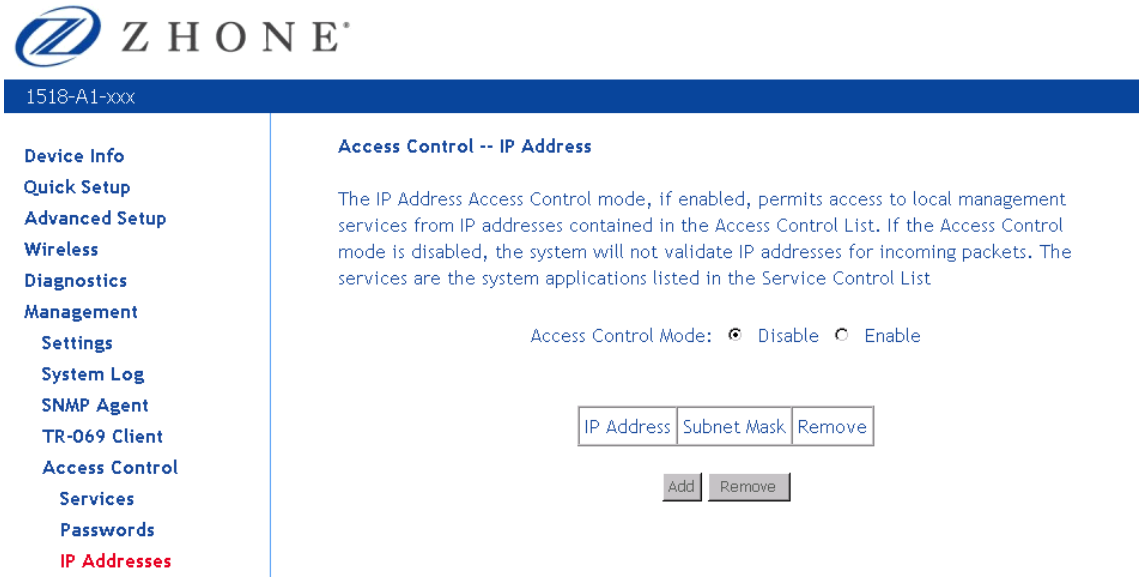
Access the **Passwords** screen under the **Access Control** section to change a password. Select an account and enter the current password and the new password and then click on the **Save / Apply** button.



IP Addresses

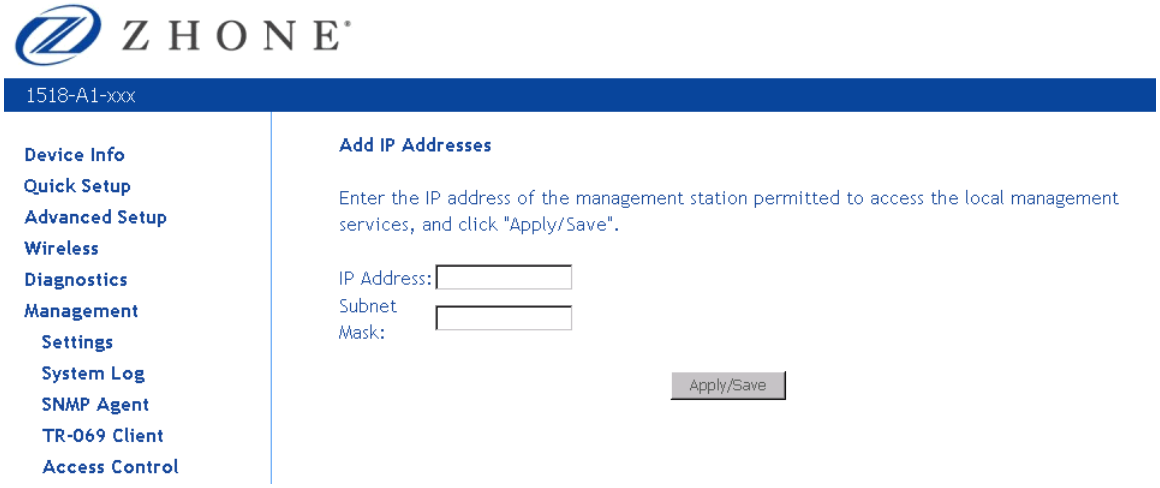
Web access to the router may be limited when Access Control Mode is enabled.

Note: Do not change this information unless you are instructed to by your ISP technician. Adding or changing the settings on this page may cause you to lose management access to the router.



To add the IP address to the IP address list:

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

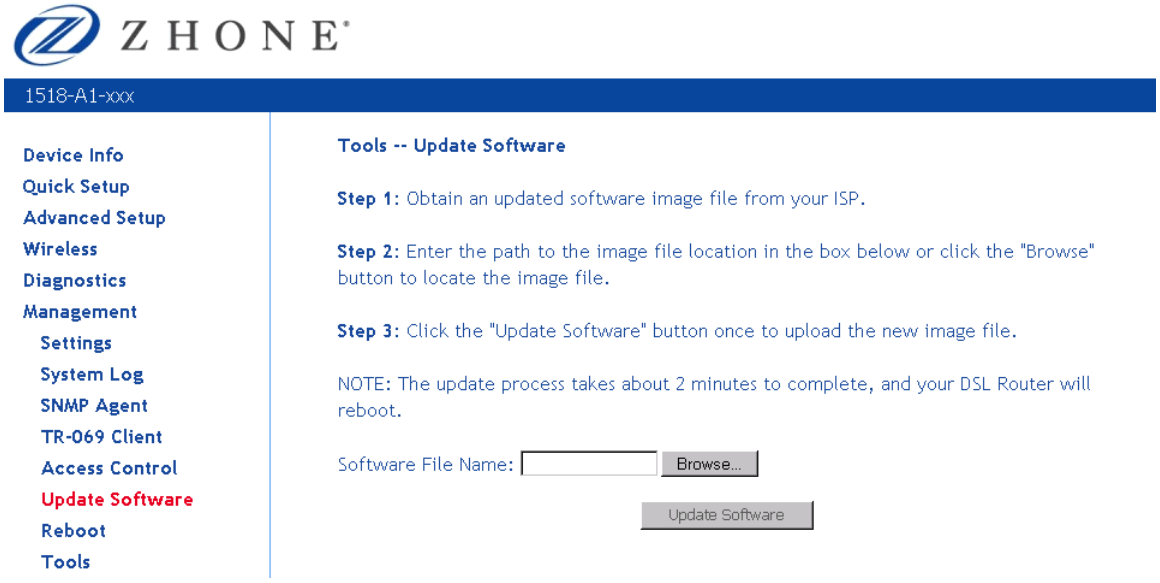


Update Software

Note: Do not perform this operation unless you are instructed to by your ISP technician.

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.*

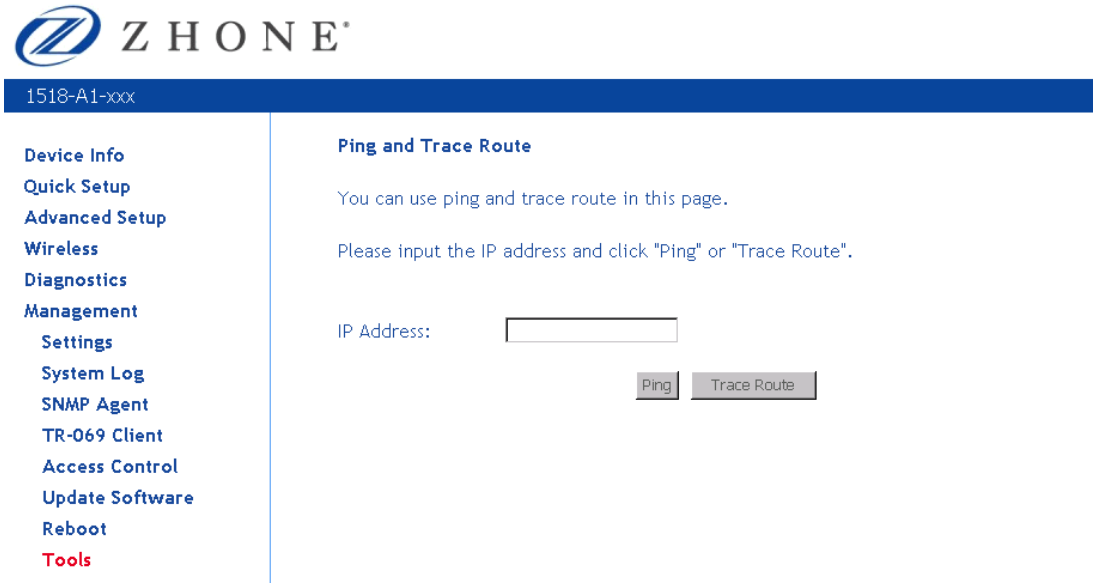


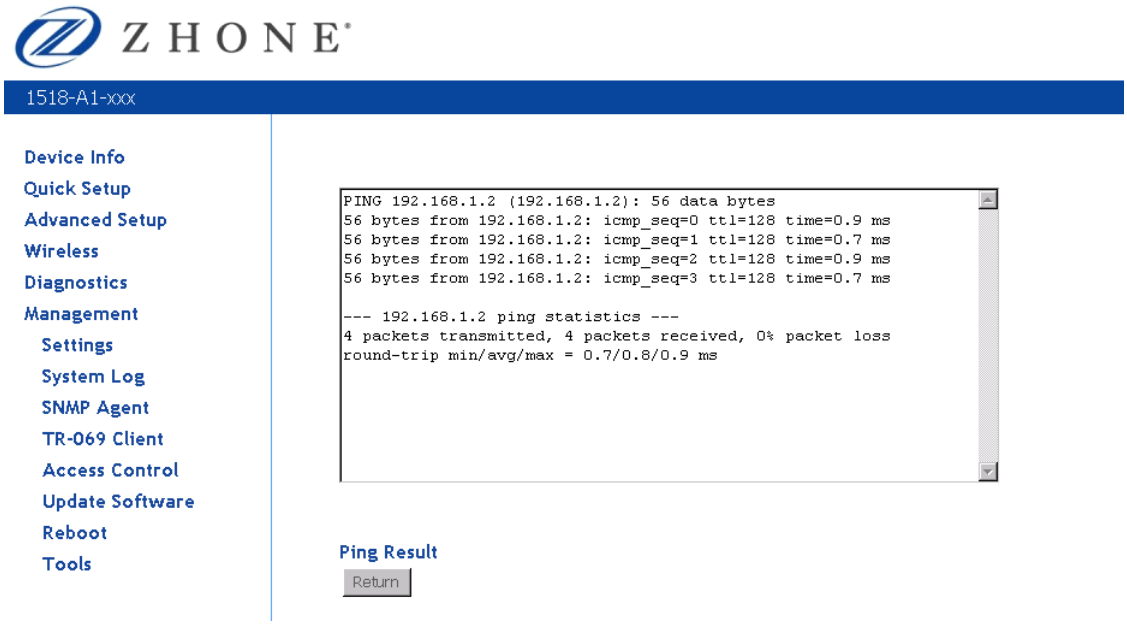
Reboot

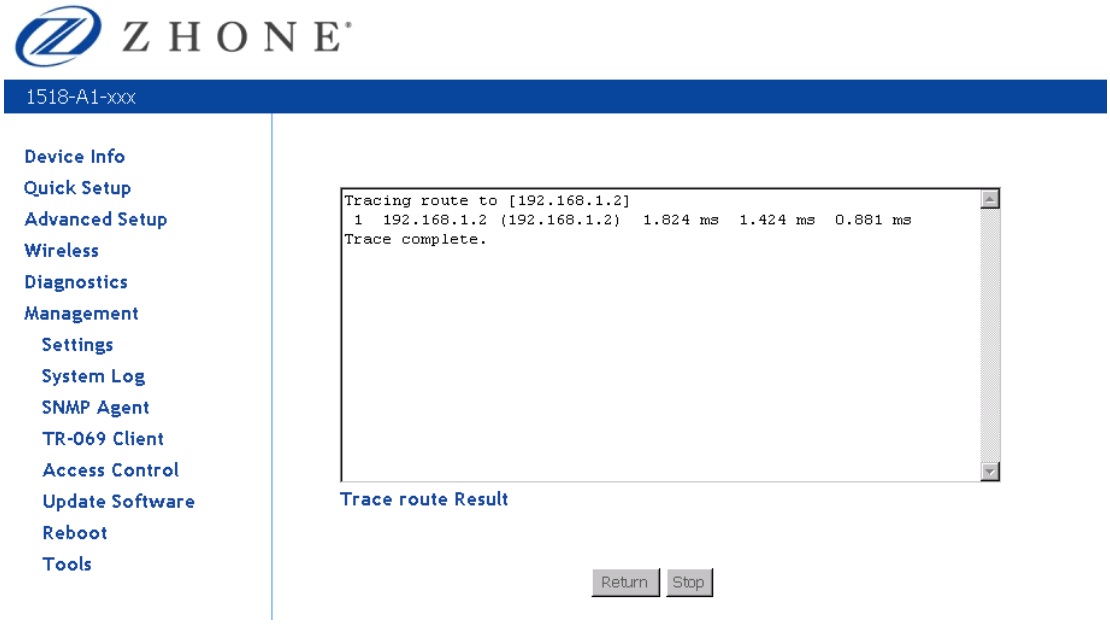
Clicking **Save/Reboot** saves all the configurations you have made, then reboots the router using the new configuration information.

Tools

The Ping and Trace Route tools may be used to verify accessibility and routes.






ZHONE
1518-A1-xxx
Device Info
Quick Setup
Advanced Setup
Wireless
Diagnostics
Management
Settings
System Log
SNMP Agent
TR-069 Client
Access Control
Update Software
Reboot
Tools
Tracing route to [192.168.1.2]
1 192.168.1.2 (192.168.1.2) 1.824 ms 1.424 ms 0.881 ms
Trace complete.
Trace route Result
Return
Stop

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. If the LED is off, make sure the router is turned on. If the LED is red, please contact your ISP.*

2. *Check the Ethernet network cable is plugged in correctly. If the LAN LED does not turn green when the Ethernet cable is connected to the router, check the cable.*

3. *Make sure you have connected the Ethernet port to the PC.*

4. *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 winipcfg /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.*

5. *If the router is in Bridge mode, you may need to set your PC to a fixed IP address within the same subnet as the modem (i.e. 192.168.1.2)*

The DSL 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 DSL LED is Always Off

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.

The Internet LED is Always Off

If the router is set to router mode (i.e. IPoE or IPoE or PPPoA), and the Internet LED is off, check the modem configuration.

View the **Router Summary** page and see if the router is configured properly. Check the WAN Status to make sure the link is up and the router is able to get a WAN IP address from the network.

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.

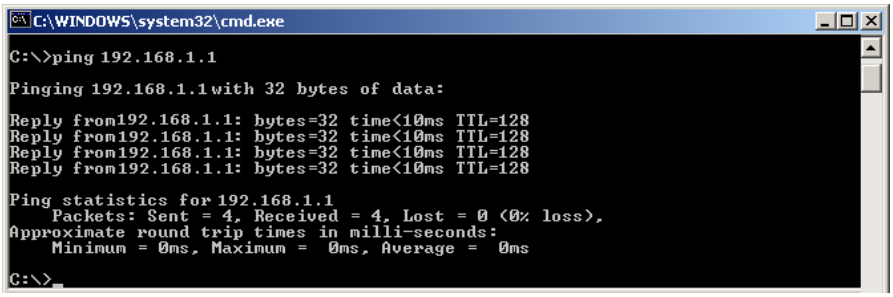
On Windows-based computers, you can execute a ping command from the Start menu.

1. *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

2. *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:



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.

Tracert

You can use the tracert command to determine the route to an external web site.

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

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

```
tracert www.zhone.com
```

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.

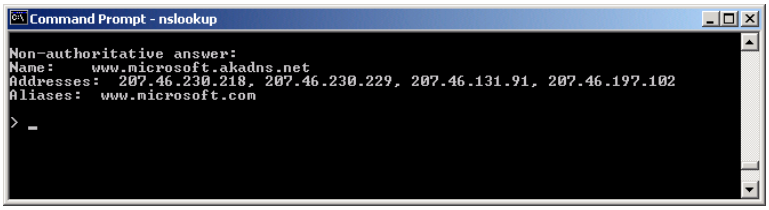
On Windows-based computers, you can execute the nslookup command from the Start menu.

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

   Nslookup

2. *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:



   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.

3. *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	File Transfer Protocol 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.
Gbps	Abbreviation of Gigabits per second, or one billion bits per second. Internet data rates are often expressed in Gbps.
Host	A device (usually a computer) connected to a network.
HTTP	Hyper-Text Transfer Protocol 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.
Hub	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.
ICMP	Internet Control Message Protocol An Internet protocol used to report errors and other network-related information. The ping command makes use of ICMP.
IEEE	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.
Internet	The global collection of interconnected networks used for both private and business communications.
Intranet	A private, company-internal network that looks like part of the Internet (users access information using web browsers), but is accessible only by employees.
IP	See TCP/IP.
IP address	Internet Protocol address 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.
ISP	Internet Service Provider A company that provides Internet access to its customers, usually for a fee.

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	Point-to-Point Protocol 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.
PPPoA	Point-to-Point Protocol over ATM 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.
PPPoE	Point-to-Point Protocol over Ethernet 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.
Protocol	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.
Remote	In a physically separate location. For example, an employee away on travel who logs in to the company's intranet is a remote user.
RIP	Routing Information Protocol The original TCP/IP routing protocol. There are two versions of RIP: version I and version II.
RJ-11	Registered Jack Standard-11 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.
RJ-45	Registered Jack Standard-45 The 8-pin plug used in transmitting data over phone lines. Ethernet cabling usually uses this type of connector.
Routing	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.
SDNS	Secondary Domain Name System (server) A DNS server that can be used if the primary DSN server is not available. See DNS.
Subnet	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.
Subnet mask	A mask that defines a subnet. See network mask.
TCP	See TCP/IP.
TCP/IP	Transmission Control Protocol/Internet Protocol 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

	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	Virtual Path Identifier 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.
WAN	Wide Area Network Any network spread over a large geographical area, such as a country or continent. With respect to the device, WAN refers to the Internet.
Web browser	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.
Web page	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.
Web site	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.
WEP	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.
Wireless	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.
Wireless LAN	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.
WPA	Wi-Fi Protected Access 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.
WWW	World Wide Web Also called (the) Web. Collective term for all web sites anywhere in the world that can be accessed via the Internet.