6381-A4 Combination Modem with in-line Filter Users Guide

Document Part Number: 830-01935-01
November, 2008

ZHONE

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

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.

⚠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.

Japan Notices

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

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

Table of Contents

About This Guide

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

Style and notation conventions

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

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

Note: A note provides important supplemental or amplified information.

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

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

Typographical conventions

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

Bold	Used for names of buttons, dialog boxes, icons, menus, profiles when placed in body text, and property pages (or sheets). Also used for commands, options, parameters in body text, and user input in body text.
`Fixed`	Used in code examples for computer output, file names, path names, and the contents of online files or directories.
`Fixed Bold`	Used in code examples for text typed by users.
`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
VoWi-Fi	Voice-over-Wifi
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity (IEEE 802.11 wireless networking)
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
ZMS	Zhone Management System

Contacting Global Service and Support

Contact Global Service and Support (GSS) if you have any questions about this or other Zhone products. Before contacting GSS, make sure you have the following information:

- Zhone product you are using
- System configuration
- Software version running on the system
- Description of the issue

Technical Support

If you require assistance with the installation or operation of your product, or if you want to return a product for repair under warranty, contact GSS. The contact information is as follows:

E-mail	support@zhone.com
Telephone (North America)	877-ZHONE20 (877-946-6320)
Telephone (International)	510-777-7133
Internet	www.zhone.com/support

If you purchased the product from an authorized dealer, distributor, Value Added Reseller (VAR), or third party, contact that supplier for technical assistance and warranty support.

Service Requirements

If the product malfunctions, all repairs must be performed by the manufacturer or a Zhone-authorized agent. It is the responsibility of users requiring service to report the need for service to Zhone Global Services and Support (GSS).

Chapter 1 Introduction

The 6381-A4 Combo Router/Modem is a USB/Ethernet Modem that gives you the flexibility of using either a USB or Ethernet connection.

The 6381-A4 provides the following features:

- Support for ADSL2+ and ReachDSL (ADSL/R)
- 10/100BaseT Ethernet port
- USB port
- The ability to connect multiple PCs to the Internet with just one WAN IP Address (when configured in router mode with NAT enabled)
- A user-friendly web interface for configuration and monitoring
- Single-session IPSec and PPTP passthrough for Virtual Private Network (VPN)
- Preconfigured port settings for many popular games
- Ability to act as a DHCP Server on your network
- Compatibility with virtually all standard Internet applications
- Address filtering and DMZ hosting
- Downloadable flash software upgrades
- Support for up to eight Permanent Virtual Circuits (PVCs)
- Support for up to two PPPoE sessions
- TR-069 support

This User Guide will show you how to connect your 6381-A4 and how to customize its configuration to get the most out of your new product.

System Requirements

In order to use your modem for Internet access, you must have the following:

- ADSL service subscription from your ISP.
- One computer with an Ethernet 10/100BaseT network interface card (NIC) or a free USB port.
- (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 5.5 or later.

Package Contents

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

- 6381-A4 device
- USB Cable
- RJ–45 Cable
- RJ-11 Cable
- Power adapter

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

LED	Mode	INDICATION
Power	Solid	Power is supplied to the modem.
	No light	The modem may not be turned on. Check if the power adapter is connected to the modem and plugged in.
Status	Solid	The DSL interface is successfully connected to a device through the LINE port.
	No Light	No carrier signal.
	Flashing	Carrier has been detected and modem is trying to train.
Activity	Flashing	Flickers according to the amount of transmitted or received DSL traffic present.
LAN	Solid	Ethernet interface is successfully connected to a device through the LAN port.
	No Light	Connection not established or cable is not connected
	Flashing	An indication of any network activity.
USB	Solid	USB interface is successfully connected to a device through the LAN port.
	No Light	Connection not established or cable is not connected
	Flashing	An indication of any network activity.

Back Panel

Port	Description
Line	RJ-11 cable connects to the phone jack in the wall.
Phone	RJ-11 cable connects to telephone (no external splitter necessary; unit has internal splitter).
USB	USB cable connects to the PC.
LAN	RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
Reset / Default	***No reset function on this model.*** ***Default settings***—press the button for 7 seconds or longer to revert to factory default settings.
Power	Connects to the power adapter.

Chapter 2 Hardware Installation and PC Setup

Overview

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

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

Connecting your hardware

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

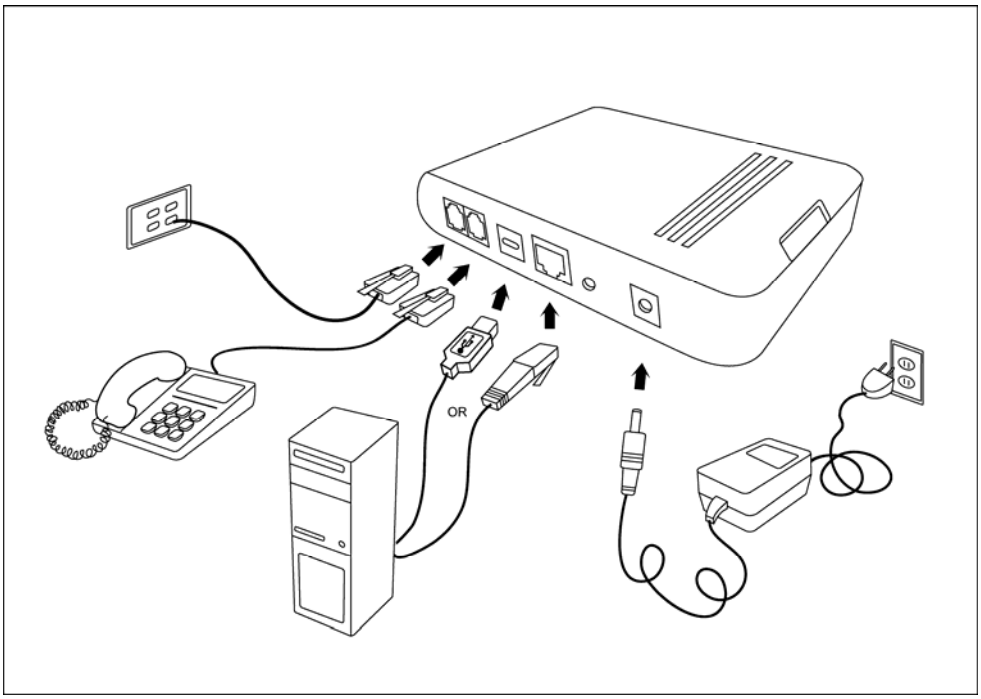
1. *Connect the ADSL Line and Telephone*

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

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

2. *Connect the PC to the Modem*

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



You can also use the supplied USB cable to connect your computer directly to the modem. Connect one end of the USB cable to the USB port on the back of the modem and connect the other end to a free USB port on your PC. The Found New Hardware Wizard will open on your PC. See USB Driver Installation instructions below.

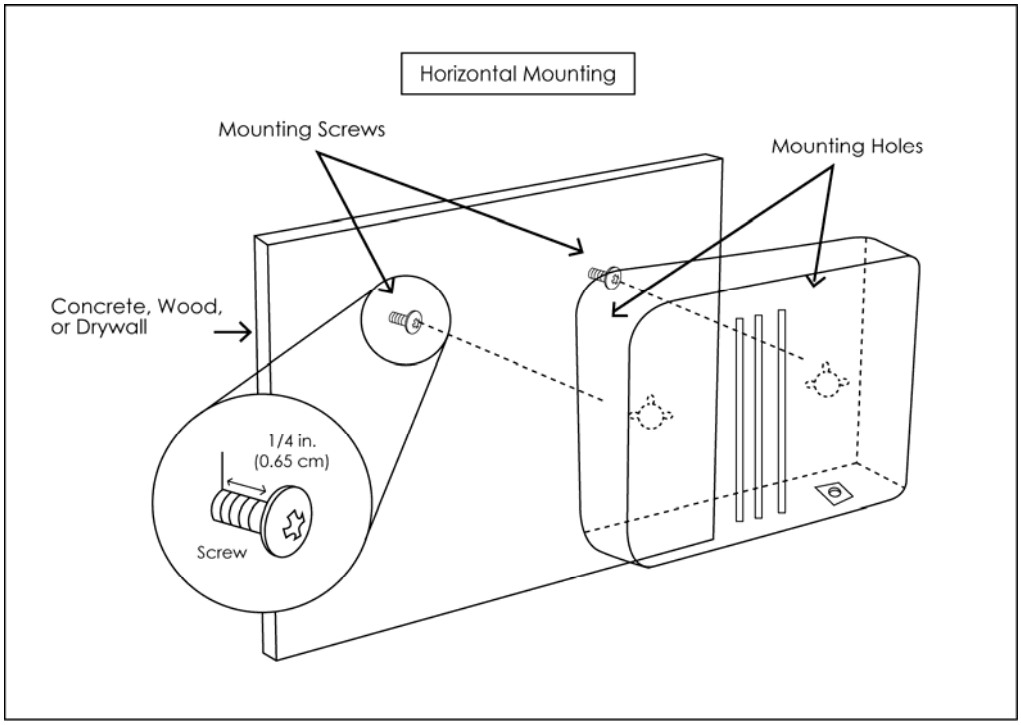
If your LAN has more than one computer, you can attach one end of an Ethernet cable to a hub or a switch and the other to the Ethernet port (labelled LAN) on the modem. Note that either a crossover or straight-through Ethernet cable can be used. The modem automatically recognizes the type of connection that is required.

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 Modem

The modem 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 modem without strain. The illustration below shows how to mount the modem horizontally on a wall.



Configuring Your Computer

Prior to accessing the modem 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 modem'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 and you can skip Windows USB Driver Installation, below. If you used the USB cable on a PC running a Windows operation system, install the provided USB driver. Windows 95 and Windows NT 4.0 do not support USB without additional software (not included with your router). If USB driver installation fails under those operating systems, contact your service provider.

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**.*

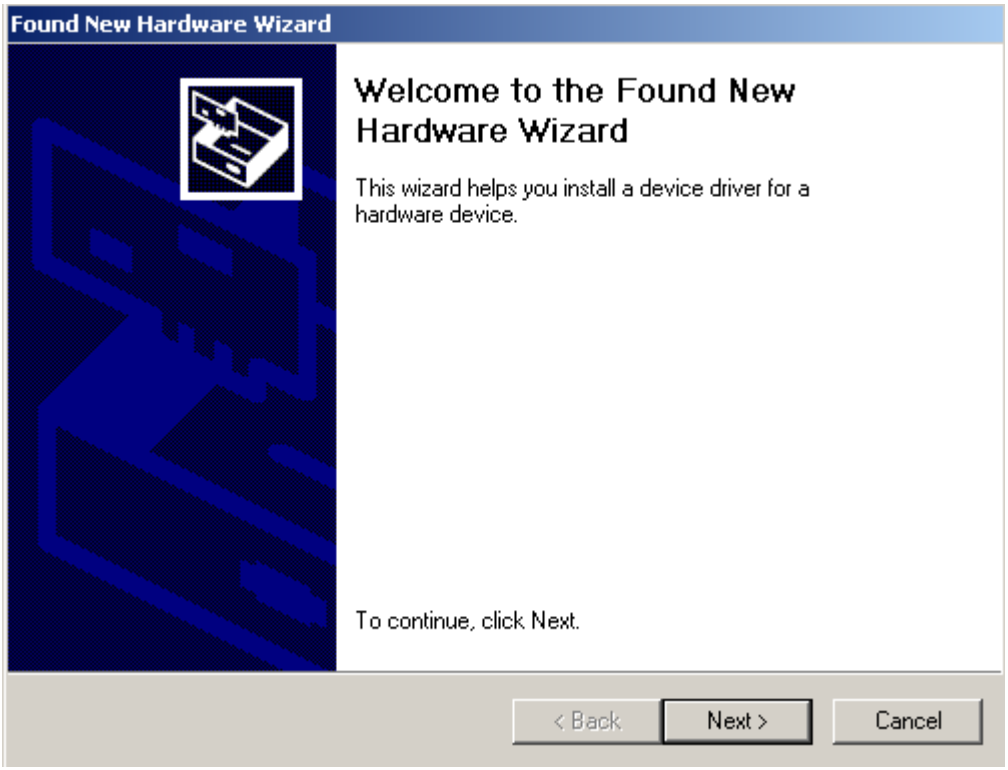
Installing USB Drivers

The following instructions will guide you through the installation of the USB driver.

Windows 2000

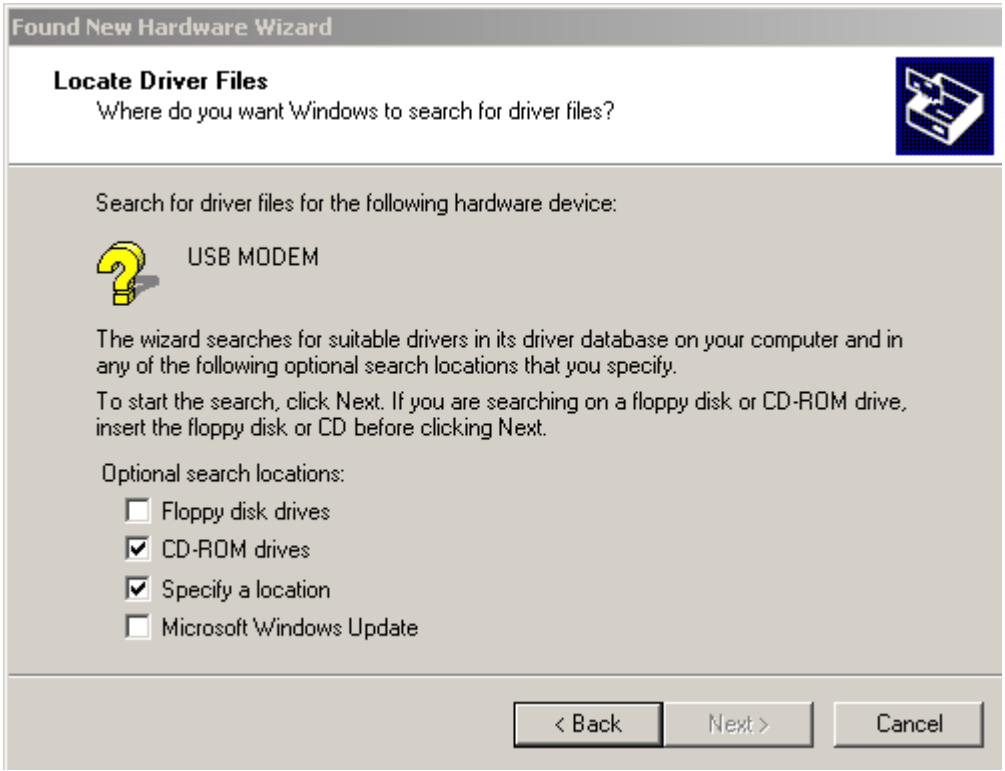
1. *When you attach the USB cable into the modem for the first time and turn on the device, the* ***Found New Hardware*** *window will pop up.*

2. *The* ***Found New Hardware Wizard*** *will appear shortly after informing you that a USB driver is needed. Click* ***Next*** *to continue with the installation.*

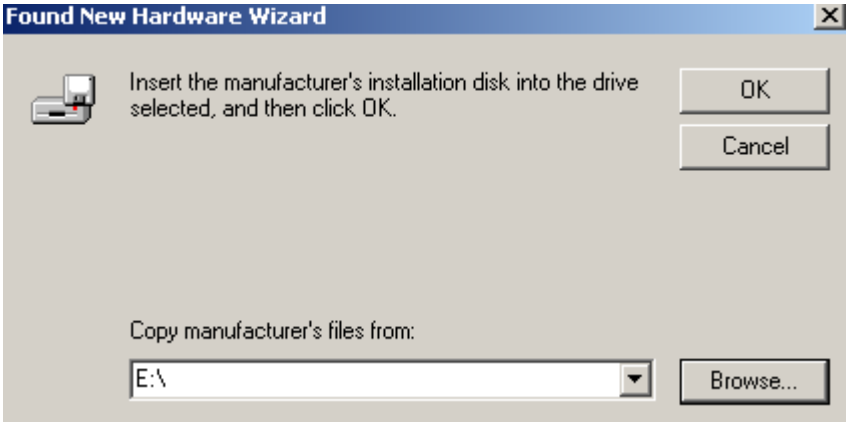


3. *The **Install Hardware Device Drivers** screen explains what a driver is and why you need it in order to run your modem using the USB plug. Typically, you will need to select the first option, the recommended option of searching for a suitable driver for your device. Click **Next.***

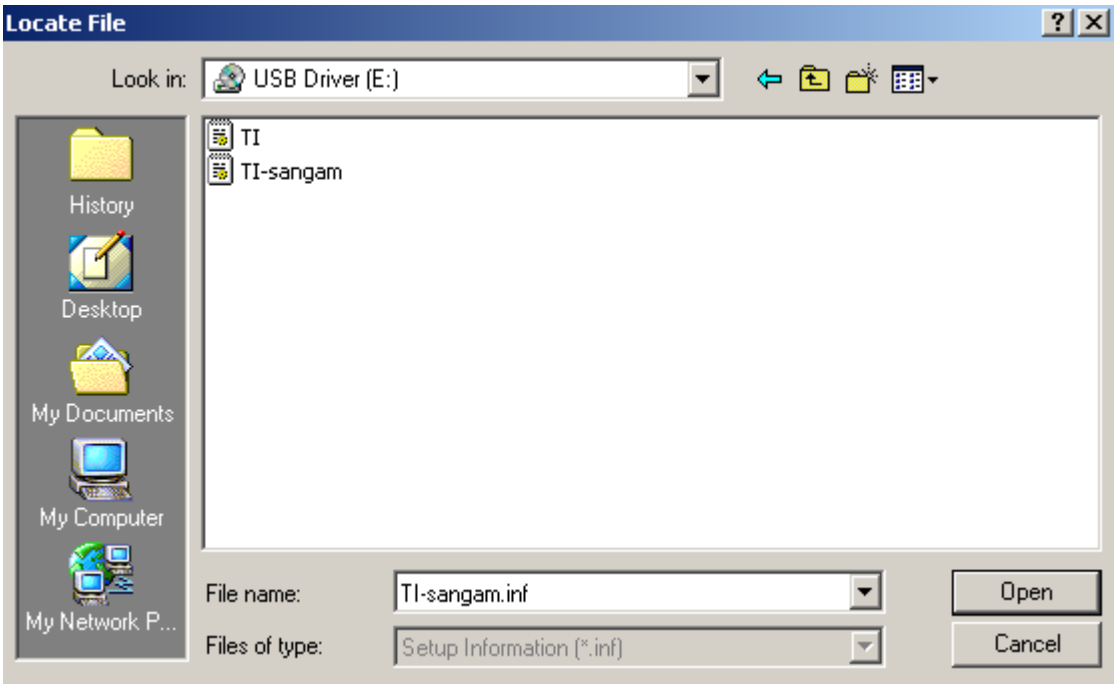
4. *Insert the USB driver installation CD if you have not already done so. Click **CD-ROM drives** and **Specify a location** and click **Next**.*



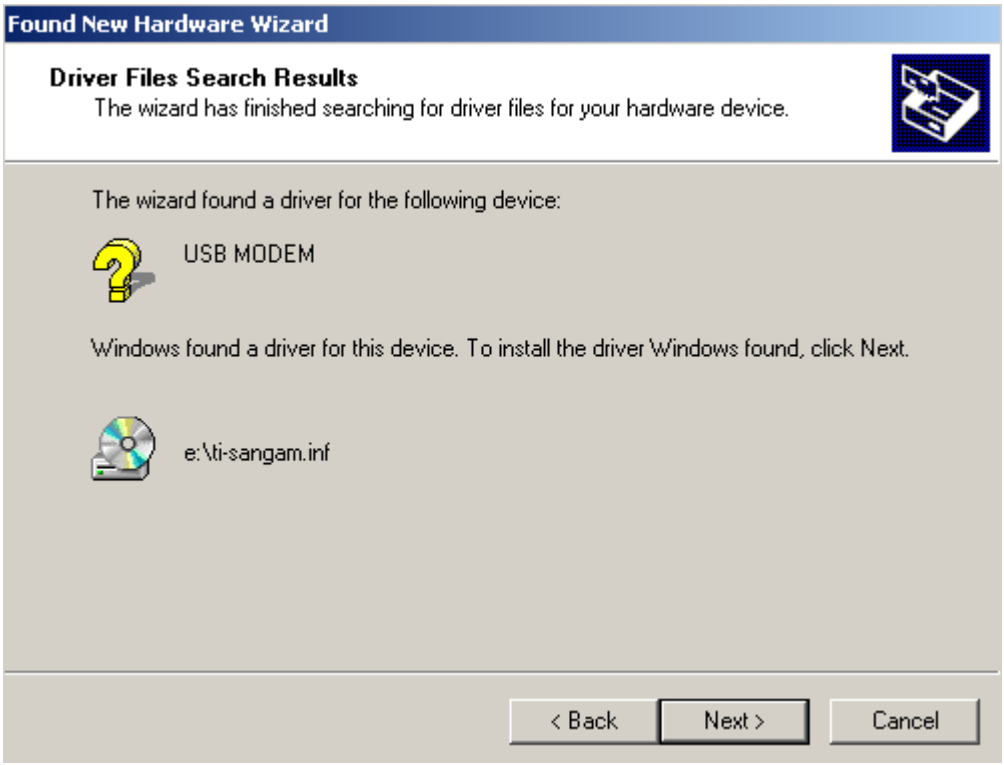
5. *Click **Browse** and select the E: drive where the CD-ROM is located. Then click **OK**.*



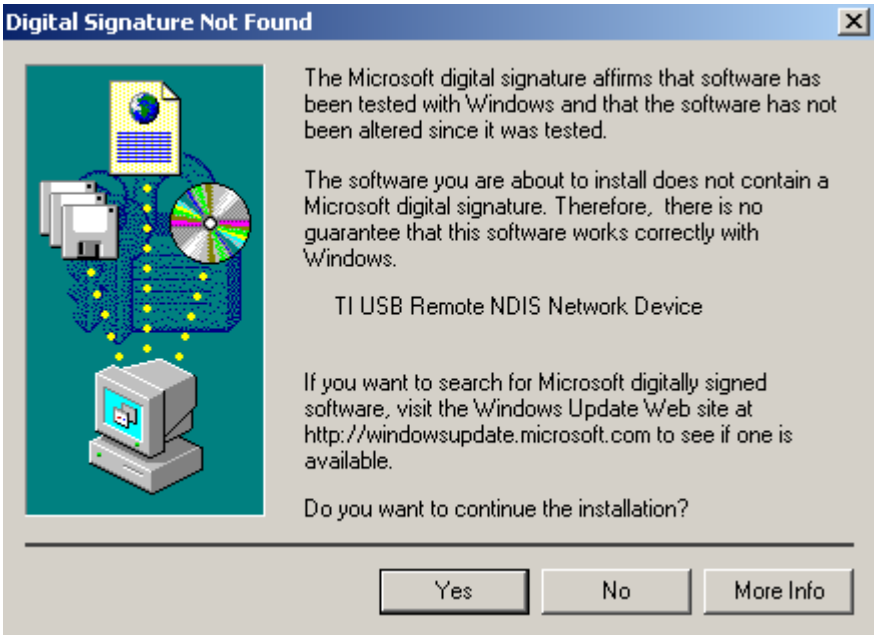
6. *Select the drive and the .inf files on the installation CD will appear, with the **TI-sangam.inf** file automatically appearing in the File name: drop-down window. Click **Open** to continue.*



7. *The **Driver Files Search Results** step allows you to confirm the .inf file that will be installed, thus allowing you to confirm that **ti-sangam.inf** is the USB driver that will be installed. Click **Next**.*



8. *Click **Yes** to continue the installation.*



9. *Once the driver has been installed, the Found New Hardware Wizard confirms installation. Click **Finish**.*

Chapter 3 The Web User Interface

The 6381 A4 combination modem/router has a Wide Area Network (WAN) connection which connects to your phone line. This connects to your Internet Service Provider (ISP) via the phone line. The Local Area Network (LAN) connection is where you plug in your local computers to the router. The router is normally configured to automatically provide all the PCs on your network with Internet addresses.

To set up your modem with a basic configuration, from the top navigation bar, select **Setup**. Setup is divided into two subsections—LAN Setup and WAN 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 modem you will first need to log in to the modem.

Notes:

- Before configuring your router, make sure you have followed the instructions in *Chapter 2 Hardware Installation and PC Setup*.
- 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.

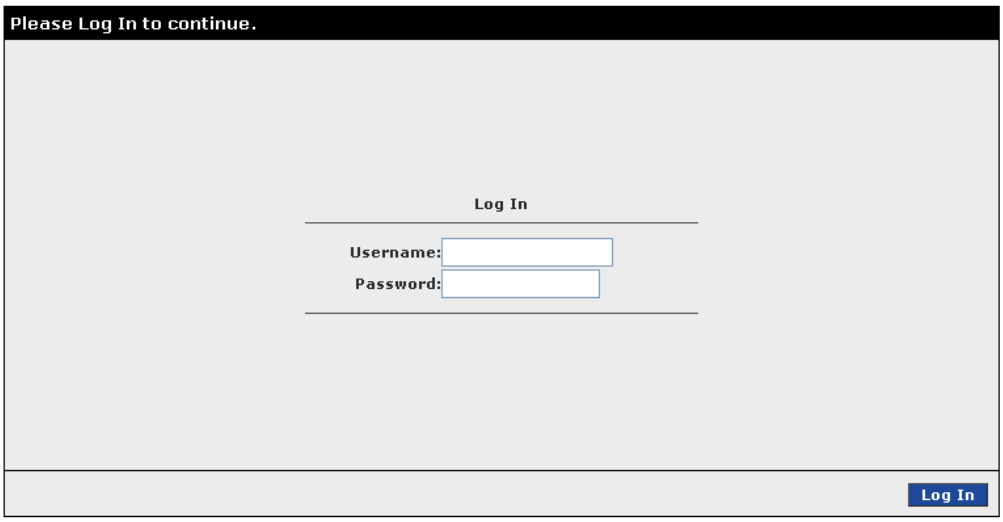
Log in to the Modem

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

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.

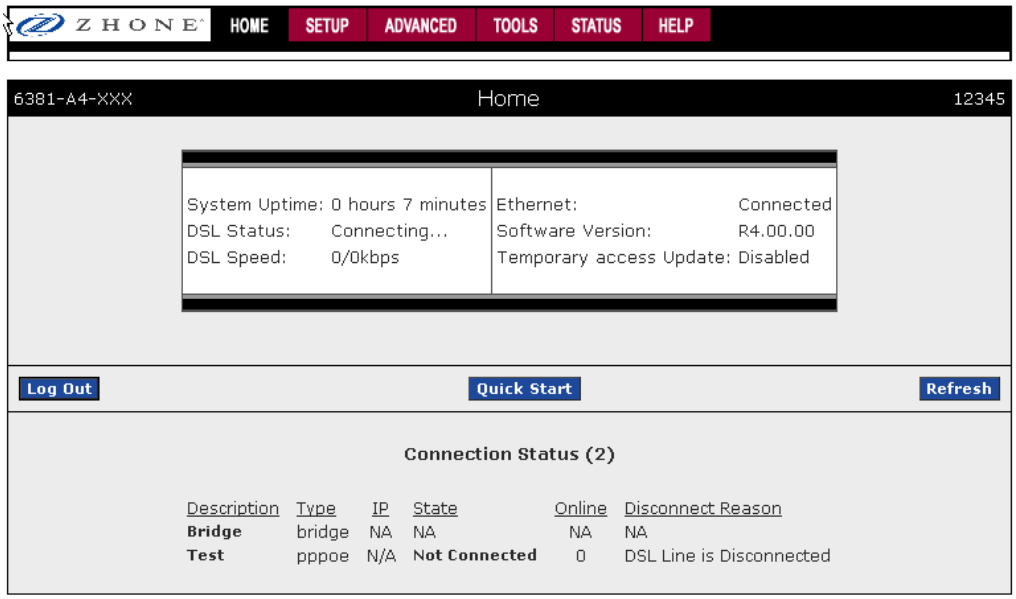


3. *Enter the default user name and password, and then click on **OK** to display the user interface.*

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

Home

The first screen that appears after the log in screen is the Home page. From this screen you can configure the LAN and WAN connections, configure the router's security, routing, and filtering, access debugging tools, obtain the status of the router, and view the online help.



The footer displays router status, connection information, and other useful information.

Click **Log Out** to close the session, **Refresh** to update the status display, or **Quick Start** to configure basic options.

Quick Start

The **Quick Start** screen gives you immediate access to the options you are most likely to need to specify or change. To access the **Quick Start** page, click the **Quick Start** button on the **Home** page.

The Quick Start page gives you quick access to setting up three types of connections. See New Connection on page 33 for more connection options.

- **DHCP** – The address of the router is automatically assigned
- **PPPoE** – Your service provider has restricted access by name and password
- **Static** – Your service provider has supplied a specific network address for your router

WAN Setup

Before the modem will pass any data between the LAN interface(s) and the WAN interface, the WAN side of the modem must be configured. Depending upon your DSL service provider or your ISP, you will need some (or all) of the following information before you can properly configure the WAN—

- Your DSL line VPI and VCI
- Your DSL encapsulation type and multiplexing
- Your DSL training mode

For **PPPoA** or **PPPoE** users, you also need these values from your ISP—

- Your username and password

For **RFC 1483 (Bridged** or **Routed IP Over ATM)** users, you may need these values from your ISP—

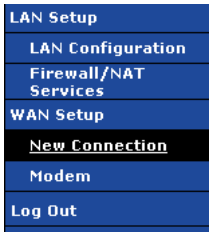
- Your DSL fixed Internet IP address
- Your Subnet Mask
- Your Default modem
- Your primary DNS IP address

Since multiple users can use the modem, the modem can simultaneously support multiple connection types. Hence, the user must set up different profiles for each connection. The modem supports the following protocols:

- DHCP
- PPPoA
- PPPoE
- Static
- Bridge
- CLIP

New Connection

A new connection is basically a virtual connection. Your router can support up to 8 different virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the router to pass data correctly.



To create a new connection:

1. *From the **Home** page, click **Setup** and then click **New Connection**.*

   The default PPPoE connection setup is displayed.

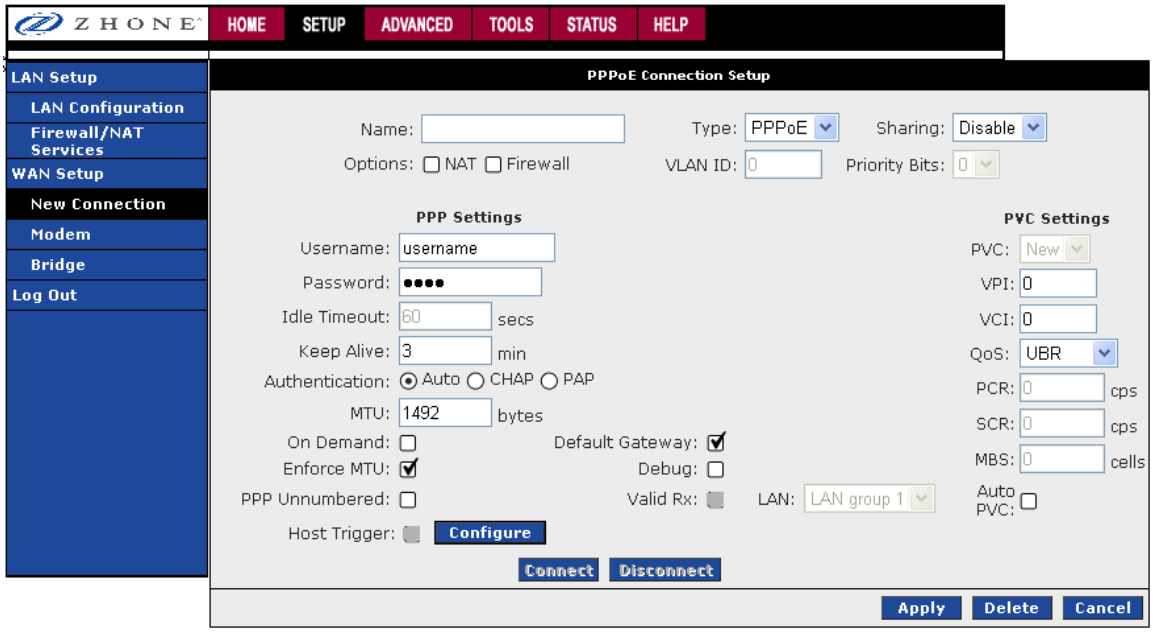
2. *In the **Type** dropdown select the protocol.*

3. *Define the protocol specific options as described in the following connection procedures.*

PPPoE Connection Setup

PPPoE is defined in the Internet standard RFC 2516. It is a method of encapsulating PPP packets over Ethernet. PPP (Point-to-Point Protocol) is a method of establishing a network session between network hosts. It usually provides a mechanism of authenticating users.

PPPoE provides the ability to connect to a network of hosts over a simple bridging access device to a remote access concentrator. With this model, each 6381 remote gateway uses its own PPP stack. Access control, billing, and type of service control can all be done on a per-user rather than per-site basis.



To configure the modem/router for PPPoE:

1. *From the **Home** page, click **Setup** and then click **New Connection**.*

   The default PPPoE connection setup is displayed.

2. *In the **Name** text box enter a unique name for the connection*

   The name must not have spaces and cannot begin with numbers.

3. *In the **Type** dropdown select **PPPoE***

   The PPPoE connection setup page is displayed.

4. *The **NAT** (Network Address Translation) and **Firewall** check boxes should be checked by default.*

   NAT enables the IP address on the LAN side to be translated to IP address on the WAN side. If NAT is disabled, you cannot access the Internet.

   The firewall is designed to provide protection from unauthorized Internet users accessing your network.

5. *To configure the connection sharing type, select **Disable**, **Enable** or **VLAN** from the **Sharing** drop down.*

Configure connection sharing as directed by your ISP.

DSL creates a permanent virtual connection (PVC) between network endpoints. This connection may be shared where each device may have access to the packets, or the connection may be segregated. In other words multiple connections over the same PVC are supported. VLAN support requires that the ISP have VLANs supported and identified

Disable	Disables connection sharing
Enable	Enables connection sharing
VLAN	Sets up a virtual LAN. To configure the VLAN you will need to provide a VLAN ID and Priority Bits. Priority is given to a VLAN connection from 0-7. All packets sent over the VLAN connection have the Priority bits set to the configured value.

6. *In the **PPP Settings** section, enter values as supplied by your ISP.*

PPP Settings:

Username	The username for the PPPoE access. This is provided by your DSL service provider or your ISP.
Password	The password for the PPPoE access. This is provided by your DSL service provider or your ISP.
Idle Timeout	Specifies that PPPoE connection should disconnect if the link has no activity detected for the specified number of seconds. This field is used in conjunction with the On Demand feature and is enabled only when the **On Demand** field is checked. To disable the timeout feature, enter a zero in this field.
Authentication	Specifies the authentication protocol: • Auto (the protocol is selected by the Central Office modem) • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol). Microsoft CHAP v2 is also supported with the Auto and CHAP options. However, MS CHAP v1 is not supported.
Keep Alive	When the **On Demand** option is not enabled, this value specifies the length of time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field. You can also enter any positive integer value in this field.
MTU	The Maximum Transmission Unit the DSL connection can send. It is a negotiated value. The PPPoE interface default MTU is 1492 (max) and PPPoA default MTU is 1500 (max). The minimum MTU value is 64.
On Demand	Enables On Demand mode. The connection disconnects if no activity is detected after the specified idle timeout value. When checked, this field enables the following fields: • Idle Timeout • Host Trigger • Valid Rx
Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.
Enforce MTU	Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MTU by changing TCP Maximum Segment Size to the PPP MTU. The **Enforce MTU** feature is enabled by default. It forces all TCP traffic to conform with PPP MTU by changing TCP maximum segment size to PPP MTU. If it is disabled, you may have issues accessing some Internet sites.

Debug Enables PPPoE connection debugging facilities. The **Debug** option is used by ISP technical support and ODM/OEM testers to simulate packets going through the network from the WAN side.

PPP Unnumbered Specifies that the calling and answering routers will not request IP addresses.

PPP Unnumbered is a special feature. It enables the ISP to designate a block of public IP addresses to the customer where it is statically assigned on the LAN side. PPP Unnumbered is, in essence, like a bridged connection.

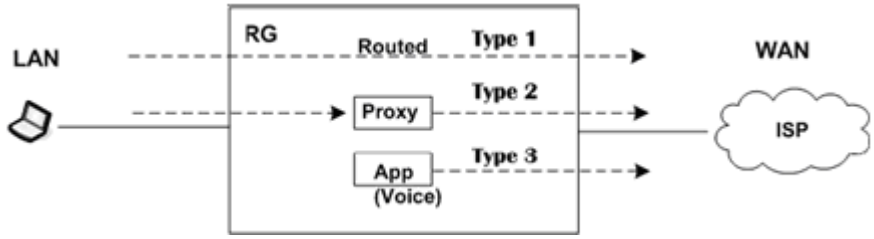
LAN The LAN field is associated with the PPP Unnumbered field and is enabled when the PPP Unnumbered field is checked. You can specify the LAN group the packets need to go to when the PPP Unnumbered feature is activated.

Valid Rx This field is used in conjunction with the On-Demand feature and is enabled only when the On Demand field is checked.

When the On-Demand feature is enabled and Valid Rx is unchecked, only packets going from the LAN side to the WAN side keep the link active. After the RG times out, no packets can be received from the WAN side to the LAN side.

When Valid Rx is checked, the incoming packets can keep the PPPoE WAN connection active. There is one condition; this incoming packet should belong to a connection initiated from a LAN-side device.

Host Trigger This field is used in conjunction with the On-Demand feature and is enabled only when the On Demand field is checked.



There are three types of packets:

- LAN packets (type 1): packets routed through the RG from LAN to WAN.
- Proxied packets (type 2): packets generated by the RG after receiving packets from the LAN side, such as DNS proxy.
- Locally generated packets (type 3): Packets generated by the RG, such as Voice, SNMP, etc.

When the On-Demand feature is enabled and Host Trigger is unchecked, only flow of type 1 packets keeps the link active, i.e., if the RG has not received type 1 packets for x mount of time (as specified in the Time Out field), the connection times out.

If Host Trigger is checked, type 2 and type 3 packets can keep the link active as well. You can configure the packets using the Trigger Traffic page, which is accessed by clicking the Configure button next to Host Trigger. The following fields can be used to identify the traffic of type 2 and/or type 3 that will keep the link alive:

- Source Port (the character * is used to denote any port)
- Destination Port (the character * is used to denote any port)
- Protocol (TCP, UDP, ICMP, or Specify the protocol number)

7. *In the **PVC Settings** section, enter values as supplied by your ISPI.*

PVC Settings:

PVC Permanent virtual circuit. This is a fixed virtual circuit between two users. It is the public data network equivalent of a leased line. No call setup or clearing procedures are needed.

VPI Virtual path identifier, equivalent to the virtual path connection (VPC).

VCI Virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch.

QoS Quality of service, a characteristic of data transmission that measures how accurately and how quickly a message or data is transferred from a source host to a destination host over a network. The three QoS options are:

- Undefined Bit Rate (**UBR**): When UBR is selected, the PCR, SCR, and MBS fields are disabled.
- Constant Bit Rate (**CBR**): When CBR is selected, the PCR field is enabled.
- Variable Bit Rate (**VBR**): When VBR is selected, the PCR, SCR, and MBS fields are enabled.

More on QoS is covered in Quality of Service (QoS) on page 92.

PCR Peak cell rate, measured in cells/sec, is the cell rate which the source may never exceed.

SCR Sustained cell rate, measured in cells/sec, is the average cell rate over the duration of the connection.

MBS Maximum burst size, a traffic parameter that specifies the maximum number of cells that can be transmitted at the Peak Cell Rate.

Auto PVC Auto-Sensing permanent virtual circuit. The overall operation of the auto-sensing PVC feature relies on end-to-end OAM pings to defined PVCs. There are two groups of PVCs: customer default PVCs which are defined by the OEM/ISP and the backup PVCs. The customer default must have 0/35 as the first default PVC. The backup list of PVCs must be of the following VPI/VCI: 0/35, 8/35, 0/43, 0/51, 0/59, 8/43, 8/51, and 8/59. The lists of PVCs are defined in XML and are configurable. The Auto-Sensing PVC feature itself is also configurable in that the auto-search mechanism can be disabled.

Upon DSL synchronization, end-to-end OAM pings will be conducted for each defined PVC. The result of the pings will be recorded in an array for later use to determine the usability of the particular PVC for connectivity. This list helps the PVC manage the available PVC for use, and needs to be synchronized with connections made without Auto-Sensing PVC. Update to this list is performed for any change in DSL synchronization.

During connection establishment, the PVC module will first search through the list of defined default PVCs. If a PVC is found from the default list that is ping-able and not in use, the PVC module will update for that particular PVC as in-use from the list and continues processing. If a PVC is not found in the default, the backup PVC list is used. If no PVC is found again, the module will let the end-user know that no available VCC was found.

With the connection established, the PVC is stored in flash as the connection default PVC. Therefore upon reboot, this PVC is automatically chosen as the PVC for that connection. This saved PVC in environment space of flash overrides the PVC connection saved in XML configuration space of flash for that connection. During the connection establishment processing, the saved PVC will be checked to see whether a connection can be made with the PVC. If the PVC is OAM ping-able, the connection process continues. If the PVC is not OAM ping-able, the search for available PVC starts. The process of PVC selection is the same as described above.

The list of default PVCs and backup PVCs need to be global for the management of all connections, non Auto-Sensing PVC connection, as well as, Auto-Sensing PVC connections. These lists allow the end-users to establish connectivity without keeping track of the PVC used.

8. *Select the Quality of Service (**QOS**).*

Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:

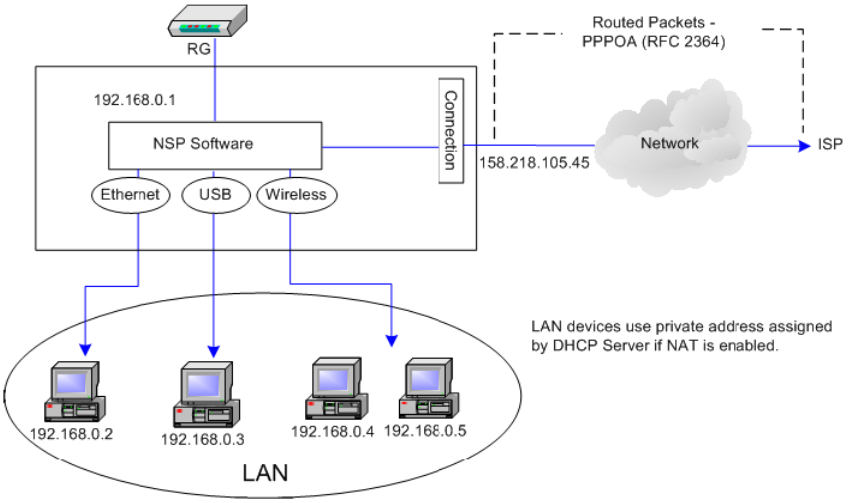
- PCR (Peak Cell Rate)
- SCR (Sustainable Cell Rate)
- MBS (Maximum Burst Size)
- CDVT (Cell Delay Variation Tolerance)

9. *To complete the connection you must now click the **Apply** button.*

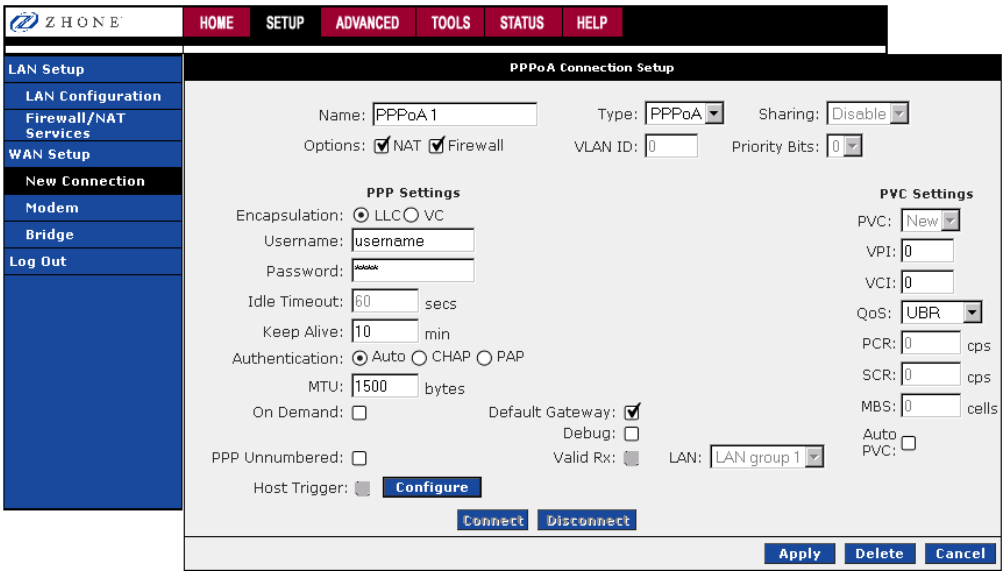
The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

PPPoA Connection Setup

PPPoA is defined in the Internet standard RFC 2364. It is a method of encapsulating PPP packets over ATM cells which are carried over the DSL line.



PPP (Point-to-Point Protocol) is a method of establishing a network session between network hosts. It usually provides a mechanism of authenticating users. LLC and VC are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.



By selecting PPPoA, you force your router to act as the termination point for the PPPoA connection. This frees up your PC resources and allows multiple users to utilize the PPPoA connection.

To configure the router for PPPoA:

1. *From the **Home** page, click **Setup** and then click **New Connection**.*

   The default PPPoA connection setup is displayed as the default setup.

2. *In the **Type** dropdown select **PPPoA***

The PPPoA connection setup page is displayed.

3. *In the **Name** text box enter a unique name for the connection*

   The name must not have spaces and cannot begin with numbers.

4. *The **NAT** (Network Address Translation) and **Firewall** check boxes should be checked by default.*

   NAT enables the IP address on the LAN side to be translated to IP address on the WAN side. If NAT is disabled, you cannot access the Internet.

   The firewall is designed to provide protection from unauthorized Internet users accessing your network.

5. *To configure the connection sharing type, select **Disable**, **Enable** or **VLAN** from the **Sharing** drop down.*

   Configure connection sharing as directed by your ISP.

   DSL creates a permanent virtual connection (PVC) between network endpoints. This connection may be shared where each device may have access to the packets, or the connection may be segregated. In other words multiple connections over the same PVC are supported. VLAN support requires that the ISP have VLANs supported and identified

Disable	Disables connection sharing
Enable	Enables connection sharing
VLAN	Sets up a virtual LAN. To configure the VLAN you will need to provide a VLAN ID and Priority Bits. Priority is given to a VLAN connection from 0-7. All packets sent over the VLAN connection have the Priority bits set to the configured value.

6. *In the **PPP Settings** section, enter values as supplied by your ISP.*

   PPP Settings:

Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the data link layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two options are provided: Logical Link Control (**LLC**) and Virtual Channel (**VC**).
Username	The username for the PPPoA access. This is provided by your DSL service provider or your ISP.
Password	The password for the PPPoA access. This is provided by your DSL service provider or your ISP.
Idle Timeout	Specifies that PPPoA connection should disconnect if the link has no activity detected for the specified number of seconds. This field is used in conjunction with the **On Demand** feature and is enabled only when the **On Demand** field is checked. To disable the timeout feature, enter a zero in this field.
Keep Alive	When the **On Demand** option is not enabled, this value specifies the length of time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter a 0 in this field. You can also enter any positive integer value in this field.
Authentication	Specifies the authentication protocol: • Auto (the protocol is selected by the Central Office modem) • PAP (Password Authentication Protocol) • CHAP (Challenge Handshake Authentication Protocol).

	Microsoft CHAP v2 is also supported with the Auto and CHAP options. However, MS CHAP v1 is not supported.
MTU	The Maximum Transmission Unit the DSL connection can send. It is a negotiated value. The PPPoA interface default MTU is 1492 (max) and PPPoA default MTU is 1500 (max). The minimum MTU value is 64.
On Demand	Enables On Demand mode. The connection disconnects if no activity is detected after the specified idle timeout value. When checked, this field enables the following fields: • Idle Timeout • Host Trigger • Valid Rx
Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.
Enforce MTU	Check this box if you experience problems accessing the Internet over a PPPoE connection. This feature will force all TCP traffic to conform with PPP MTU by changing TCP Maximum Segment Size to the PPP MTU. The **Enforce MTU** feature is enabled by default. It forces all TCP traffic to conform with PPP MTU by changing TCP maximum segment size to PPP MTU. If it is disabled, you may have issues accessing some Internet sites.
Debug	Enables PPPoA connection debugging facilities. The **Debug** option is used by ISP technical support and ODM/OEM testers to simulate packets going through the network from the WAN side.
PPP Unnumbered	Specifies that the calling and answering routers will not request IP addresses. PPP Unnumbered is a special feature. It enables the ISP to designate a block of public IP addresses to the customer where it is statically assigned on the LAN side. PPP Unnumbered is, in essence, like a bridged connection.
LAN	The LAN field is associated with the PPP Unnumbered field and is enabled when the PPP Unnumbered field is checked. You can specify the LAN group the packets need to go to when the PPP Unnumbered feature is activated.

7. *In the **PVC Settings** section, enter values as supplied by your ISP.*

Please see PVC Settings from the PPPoE Setup procedure.

8. *Select the Quality of Service (**QOS**).*

Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:

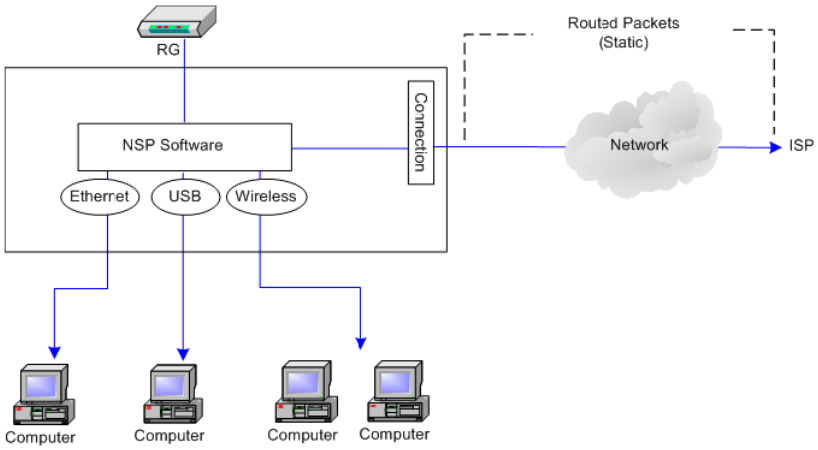
- PCR (Peak Cell Rate)
- SCR (Sustainable Cell Rate)
- MBS (Maximum Burst Size)
- CDVT (Cell Delay Variation Tolerance)

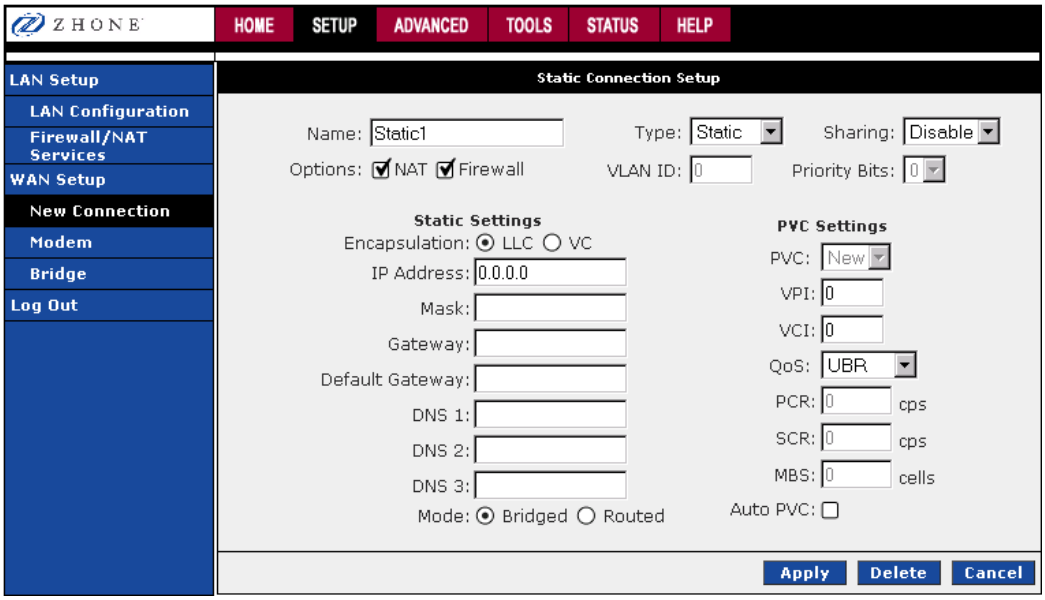
9. *To complete the connection you must now click the **Apply** button.*

The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Static Connection Setup

A static connection is used whenever a known static IP is assigned. The accompanying information such as the subnet mask and the default gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers give you access to other web servers. The valid IP addresses range is from 1.0.0.0 to 223.255.255.254.





To configure the router for a Static connection:

1. *From the **Home** page, click **Setup** and then click **New Connection**.*

   The default PPPoE connection setup is displayed as the default setup.

2. *In the **Type** dropdown select **Static***

   The Static connection setup page is displayed.

3. *In the **Name** text box enter a unique name for the connection*

   The name must not have spaces and cannot begin with numbers.

4. *Network Address Translation (**NAT**) and the **Firewall** options are enabled by default. Leave these options enabled.*

5. *In the **Static Settings** section, select the **Encapsulation** Type (**LLC** or **VC**) as supplied by your ISP.*

   If you are not sure, just leave the default.

6. *Enter your enter your assigned **IP Address**, Subnet **Mask**, **Gateway**, **Default Gateway**, and Domain Name Services (**DNS**) values as provided by your ISP.*

7. *For the static configuration, you can also select a **Bridged** connection or a **Routed** connection as provided by your ISP.*

8. *In the **PVC Settings** section, enter values for **VPI** and **VCI** as supplied by your ISP.*

   For more information, please see PVC Settings from the PPPoE Setup procedure.

9. *Select the quality of service (**QOS**). Leave the default value if your ISP did not provide this information.*

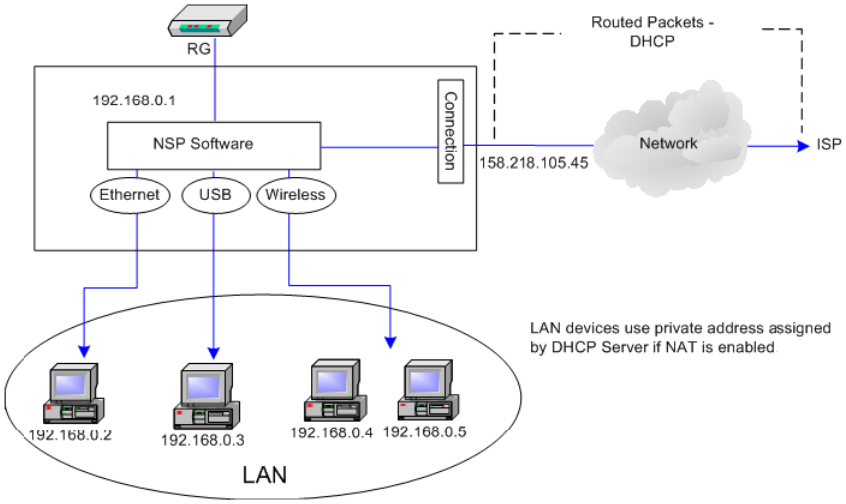
   The **PCR**, **SCR**, and **MBS** fields are enabled/disabled depending on the QoS selection. Enter the values provided by the ISP or leave the defaults.

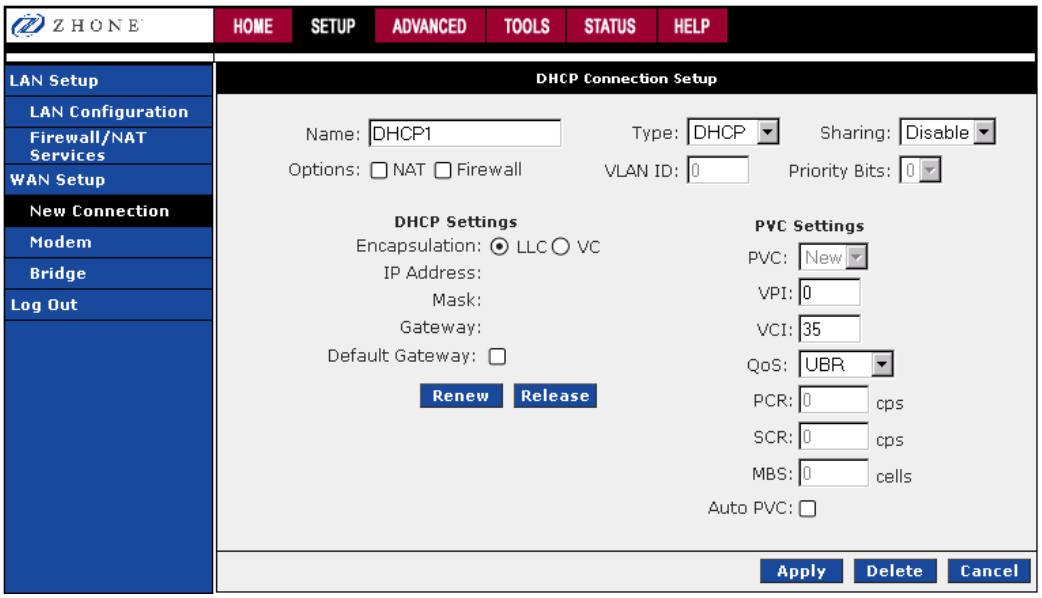
10. *To complete the connection click **Apply**.*

    The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

DHCP Connection Setup

Dynamic Host Configuration Protocol (DHCP) allows the router to automatically obtain the IP address from the server. This option is commonly used in situations where IP is dynamically assigned and is not known prior to assignment.





To configure the router for a DHCP connection:

1. *From the **Home** page, click **Setup** and then click **New Connection**.*

   The default PPPoE connection setup is displayed as the default setup.

2. *In the **Type** dropdown select **DHCP.***

   The DHCP connection setup page is displayed.

3. *In the **Name** text box enter a unique name for the DHCP connection*

   The name must not have spaces and cannot begin with numbers.

4. *Network Address Translation (**NAT**) and the **Firewall** options are enabled by default. Leave these options enabled.*

5. *If your DSL line is connected and your DSL provider is supporting DHCP, you can click the **Renew** button and the router will retrieve an IP Address, Subnet Mask, and Default Gateway address.*

   At any time you can renew the DHCP address by clicking on the Renew button.

6. *In the **PVC Settings** section, enter values for **VPI** and **VCI** as supplied by your ISP.*

   For more information, please see PVC Settings from the PPPoE Setup procedure.

7. *Select the quality of service (**QOS**).*

   Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:

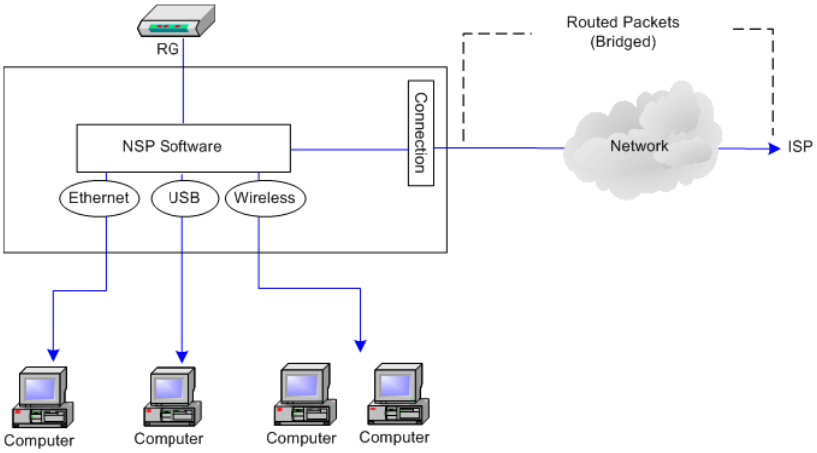
   - **PCR** (Peak Cell Rate)
   - **SCR** (Sustainable Cell Rate)
   - **MBS** (Maximum Burst Size)
   - **CDVT** (Cell Delay Variation Tolerance)

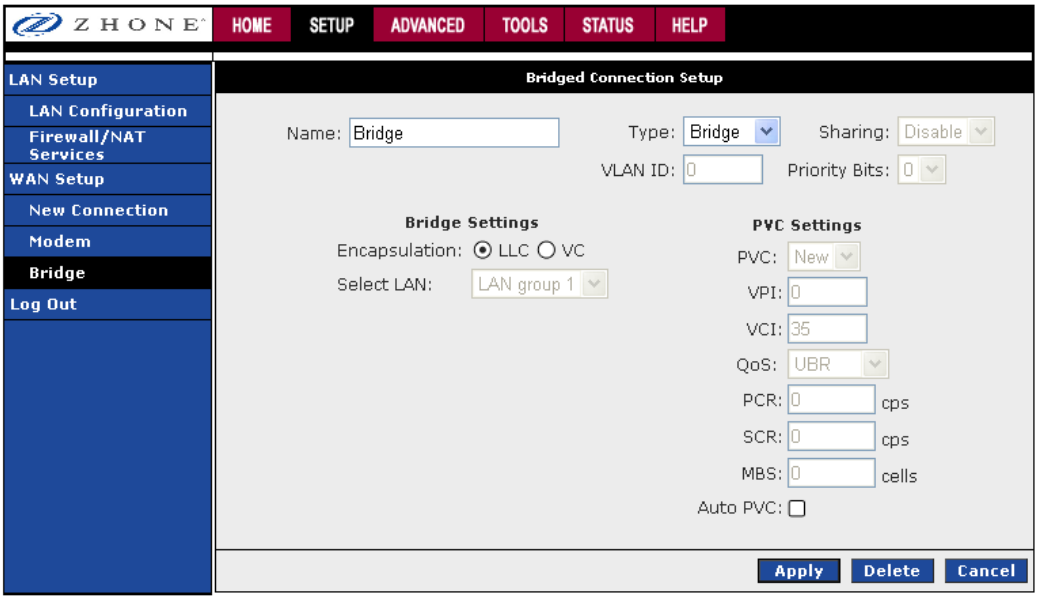
8. *To complete the connection click **Apply**.*

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Bridge Connection Setup

A pure bridged connection does not assign and IP address to the WAN interface. NAT and firewall rules are not enabled. This connection method makes the RG act as a bridge for passing packets between the WAN interface and the LAN interface.





To configure the 6381 as a bridge:

1. *From the **Home** page, click **Setup** and then click **New Connection**.*

   The default PPPoE connection setup is displayed.

2. *In the **Type** dropdown select **Bridge***

   The Bridge connection setup page is displayed.

3. *In the **Name** text box enter a unique name for the bridge*

   The name must not have spaces and cannot begin with numbers.

4. *Network Address Translation (**NAT**) and the **Firewall** options are enabled by default. Leave these options enabled.*

5. *In the **Bridge Settings** section, select the **Encapsulation** Type (**LLC** or **VC**) as supplied by your ISP.*

   If you are unsure, just leave the default settings.

Encapsulation	The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. As an example, in Internet terminology, a packet would contain a header from the data link layer, followed by a header from the network layer (IP), followed by a header from the transport layer (TCP), followed by the application protocol data. Two encapsulation options are provided: • Logical Link Control (**LLC**) • Virtual Channel (**VC**).
Select LAN	Select the LAN group for the bridged connection. The following options are available: • **LAN Group 1** • **LAN Group 2** • **LAN Group 3** • **None** This bridged connection will be added to the selected LAN group. If you select None, the connection is not added to any LAN group but to the Interfaces box on the LAN Configuration page which can be configured to a LAN group on the same page.

6. *In the **PVC Settings** section, enter values for **VPI** and **VCI** as supplied by your ISP*

   For more information, please see PVC Settings from the PPPoE Setup procedure.

7. *Select the quality of service (**QOS**).*

   Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:

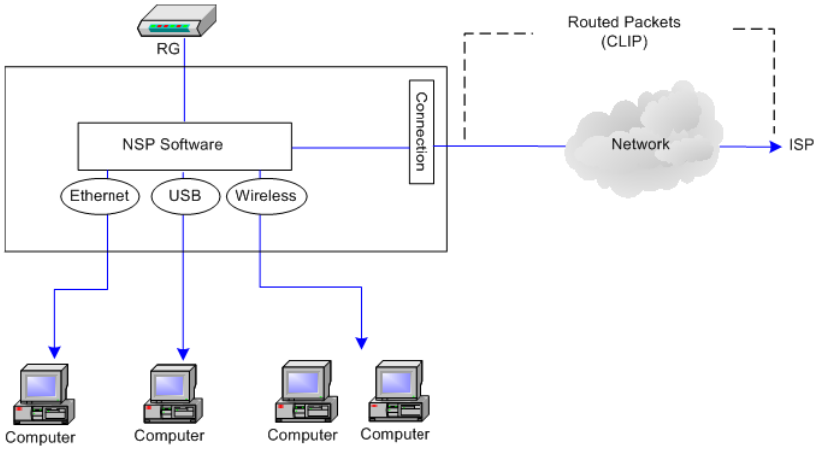
   - **PCR** (Peak Cell Rate)
   - **SCR** (Sustainable Cell Rate)
   - **MBS** (Maximum Burst Size)
   - **CDVT** (Cell Delay Variation Tolerance)

8. *To complete the connection click **Apply**.*

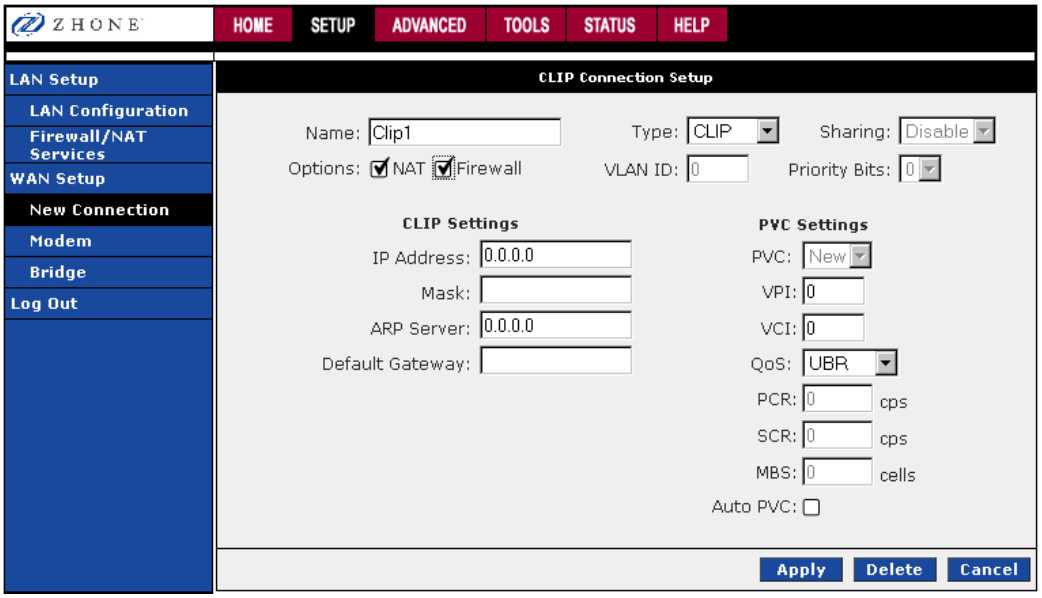
   The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

CLIP Connection

Classical IP and ARP over ATM (CLIP) allow IP datagrams and ARP (Address Resolution Protocol) requests and replies to be transmitted over ATM using ATM Adaptation Layer 5 (AAL5).



CLIP, defined in RFC 2225, provides the ability to transmit IP packets over an ATM network. The 6381's CLIP support encapsulates an IP datagram in an AAL5 PDU frame using RFC 2225 and it uses an ATM-aware version of the address resolution protocol (ATMARP). The 6381's CLIP support only allows support for PVCs; SVCs are not supported by the 6381 RG.



To configure a CLIP connection:

1. *From the **Home** page, click **Setup** and then click **New Connection**.*

   The default PPPoE connection setup is displayed.

2. *In the **Type** dropdown select **CLIP***

   The CLIP connection setup page is displayed.

3. *In the **Name** text box enter a unique name for the connection*

The name must not have spaces and cannot begin with numbers.

4. *Select **NAT** and **Firewall** if you want them active for this connection.*

Firewall and NAT services must be enabled.

5. *In the **PVC section**, select the **VPI** and **VCI** settings as provided by your ISP.*

For more information, please see PVC Settings from the PPPoE Setup procedure.

6. *Enter the **IP address** and subnet **mask**, the address of the **ARP Server** and the address of the **Default Gateway** as provided by your ISP.*

IP Address	IP address of the CLIP connection provided by your ISP.
Mask	Subnet mask provided by your ISP.
ARP Server	IP address of the Address Resolution Protocol (ARP) server provided by your ISP.
Default Gateway	If checked, this WAN connection acts as the default gateway to the Internet.

7. *Select the quality of service (**QOS**).*

Leave the default value if your ISP did not provide this information. Depending on the QoS you select, you may also enter:

- **PCR** (Peak Cell Rate)
- **SCR** (Sustainable Cell Rate)
- **MBS** (Maximum Burst Size)
- **CDVT** (Cell Delay Variation Tolerance)

8. *To complete the connection click **Apply**.*

The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Modify a Connection

When you create a connection, the connection will be displayed in the WAN Setup section of the left navigation pane.

To modify a connection:

1. *From the top navigation bar, click **Setup**.*

2. *In the left hand navigation pane, select the connection you want to modify. The connections are listed by unique names given upon creation of the connection.*

3. *Make changes as appropriate*

4. *Click **Apply***

   The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Delete a Connection

To delete a connection:

1. *From the top navigation bar, click **Setup**.*

2. *In the left hand navigation pane, select the connection you want to modify. The connections are listed by name.*

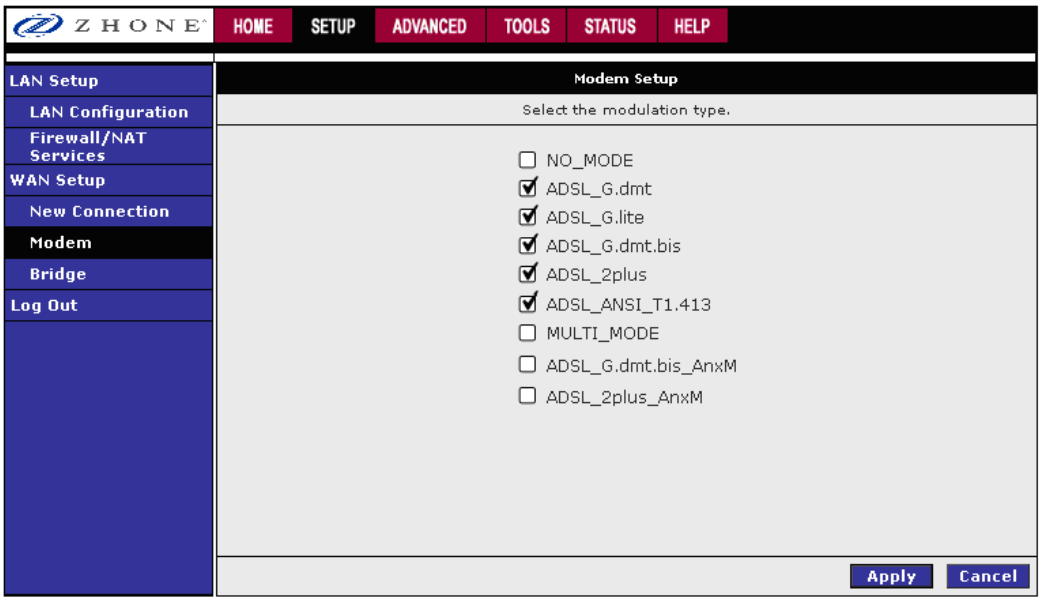
3. *Click **Delete**.*

If you delete a connection, to make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Modem

The Modem Setup page allows you to select any combination of DSL training modes including:

- NO_MODE
- ADSL_G.dmt (G Discrete Multi-Tone): G.dmt (G.992.1)
- ADSL_G.lite: G.lite (G.992.2)
- ADSL_G.dmt.bis
- ADSL_2plus
- ADSL_ANSI_T1.413
- Multi_MODE
- ADSL_G.dmt.bis_AnxM
- ADSL_2plus_AnxM



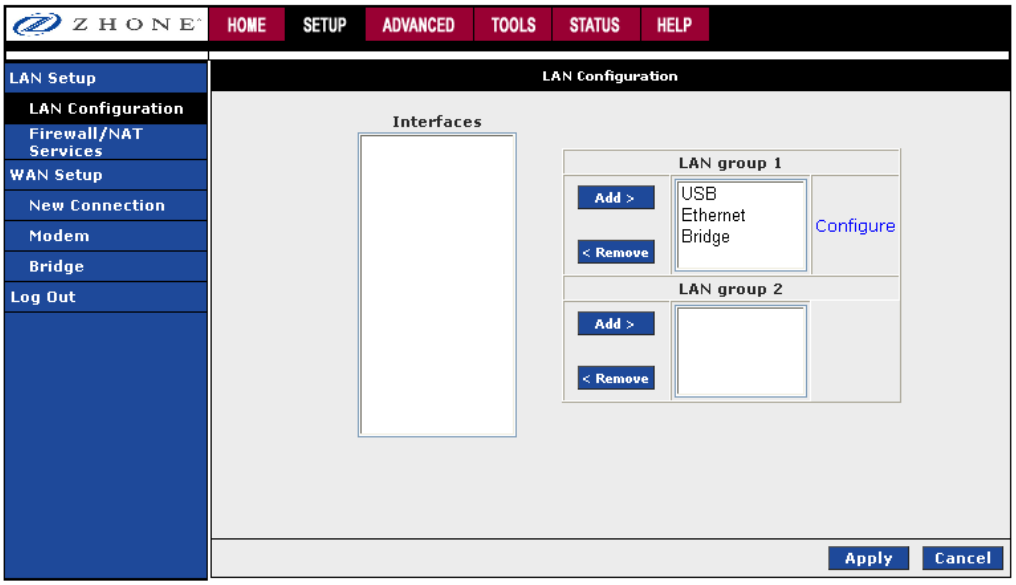
LAN Setup

On one side of your modem, you have your own Local Area network (LAN) connections. This is where you plug in your local computers to the modem. The modem is normally configured to automatically provide all PCs on your network with Internet addresses.

The RG provides LAN configuration for multiple LAN bridge groups. Up to five LAN bridge groups are supported. The LAN interfaces could include: Ethernet, USB, and Bridge. It is possible to assign any LAN interface to any bridge group but only one group, except that the Ethernet interface needs to stay in LAN group 1. Each LAN group can then be configured with static IP address, dynamic IP address, or be unmanaged (no IP).

LAN Configuration

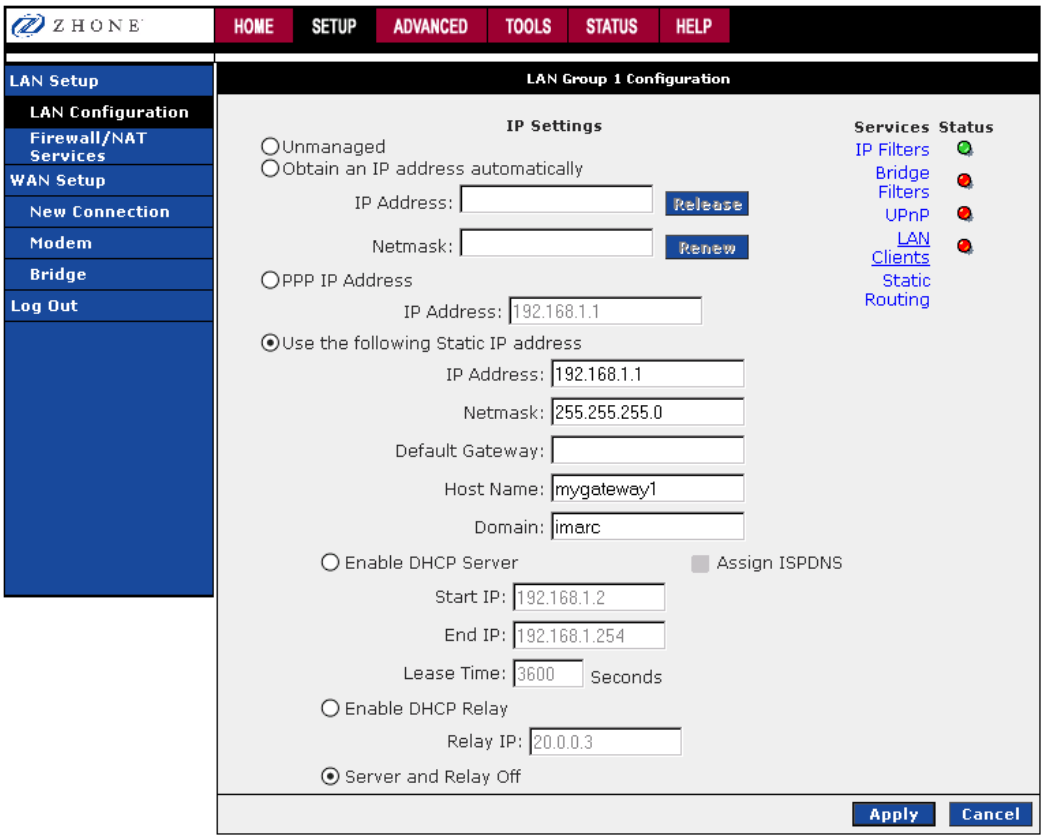
By default, both the Ethernet port and USB port are in LAN Group 1. The USB port may be removed from LAN Group 1 and added to LAN Group 2 for configuring separately.



You can configure the USB interface and WLAN interfaces to a different LAN group; however, the Ethernet interface is default in LAN group 1 and cannot be moved.

The LAN Group Configuration page allows you to configure settings for each defined LAN group.

You can also view the status of advanced services that can be applied to this LAN group. A green status indicates that the services have been enabled, while a red status indicates that the service is currently disabled.



To configure the LAN:

1. *From the **Home** page, click **Setup** and then click **LAN Configuration**.*

   The LAN Configuration page is displayed.

2. *To the right of the **LAN group 1** field click **Configure***

   The LAN Group 1 Configuration page is displayed.

3. *Set the LAN features:*

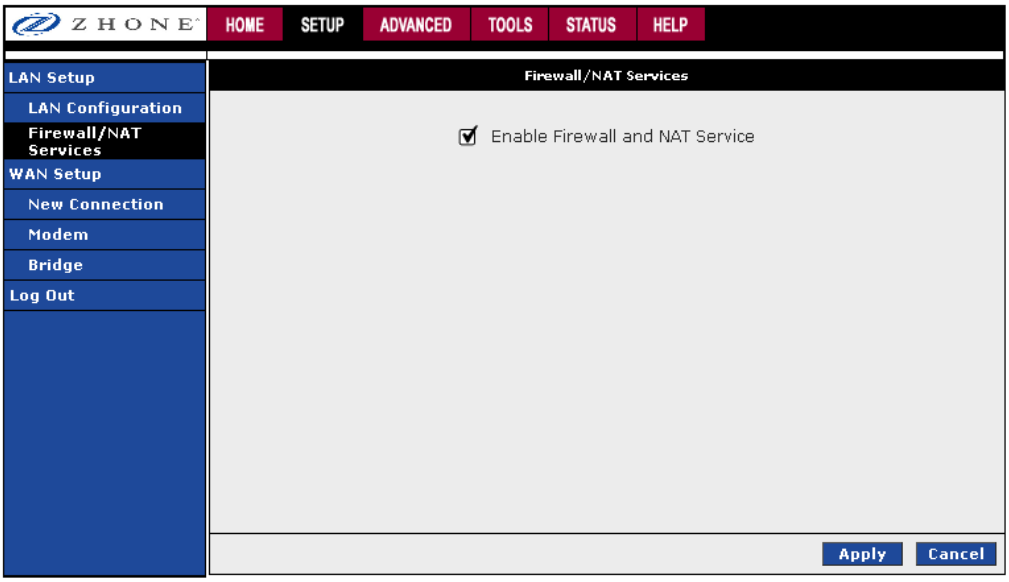
   LAN configuration features:

Unmanaged	Unmanaged is a state when the LAN group is not configured and no IP address has been assigned to the bridge.
Obtain an IP address automatically	When this function is enabled, your RG acts like a client and requests an IP address from the DHCP server on the LAN side.
IP Address	You can retrieve/renew an IP address from the DHCP server using the **Release** and **Renew** buttons.
Netmask	The subnet mask of your 6381 RG.
PPP IP Address	Enables/disables PPP unnumbered feature.
IP Address	The IP address should be different from, but in the same subnet as the WAN-side IP address.
Use the following Static IP address	This field enables you to change the IP address of the 6381 RG.
IP Address	The default IP address of the RG (as shown) is 192.168.1.1.

Netmask	The default subnet mask of your RG is 255.255.255.0. This subnet allows the 6381 RG to support 254 users. If you want to support a larger number of users you can change the subnet mask.
Default Gateway	The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP provides you with the IP address of the default gateway.
Host Name	The host name is used in conjunction with the domain name to uniquely identify the RG. It can be any alphanumeric word that does not contain spaces.
Domain	The domain name is used in conjunction with the host name to uniquely identify the RG. To access the web pages of the RG you can type 192.168.1.1 (the IP address) or mygateway1.ar7 (Host Name.Domain).
Enable DHCP Server	Enables/disables DHCP. By default, your RG has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of the two DHCP servers. See the DHCP server configuration section for more information.
Assign ISP DNS	Enable/disables the Assign ISP DNS feature when the DHCP server of your 6381 RG has been enabled.
Start IP	The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the IP address value of the RG. For example, if the IP address of the RG is *192.168.1.1* (default), then the starting IP address must be *192.168.1.2* (or higher). Note: If you change the start or end values, make sure the values are still within the same subnet as the RG. In other words, if the IP address of the RG is *192.168.1.1* (default) and you change the DHCP start/end IP addresses to be *192.168.1.2*/*192.168.1.100*, you cannot communicate with the RG if your host has DHCP enabled.
End IP	The End IP Address is where the DHCP server stops issuing IP addresses. The ending address cannot exceed a subnet limit of 254, hence the max value for the default gateway is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users do not get access to network resources. If this happens, you can increase the Ending IP address (to the limit of 254) or reduce the lease time. Note: If you change the start or end values, make sure the values are still within the same subnet as the IP address of the RG. In other words, if the IP address of the RG is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.168.1.2/192.168.1.100, you cannot communicate with the RG if your host has DHCP enabled.
Lease Time	The Lease Time is the amount of time that a network user is allowed to maintain a network connection to the RG using the current dynamic IP address. At the end of the Lease Time, the lease is either renewed or a new IP is issued by the DHCP server. The amount of time is in units of seconds. The default value is 3600 seconds (1 hour). The maximum value is 999999 seconds (about 278 hours).
Enable DHCP Relay	In addition to the DHCP server feature, the 6381 RG supports DHCP relay which means the 6381 RG is then a DHCP relay agent. When the RG is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay agent, it is responsible for forwarding the requests and responses negotiated between the DHCP clients and the server.
Relay IP	The IP address of the DHCP relay server.
Server and Relay Off	When the DHCP server and relay functions are turned off, the network administrator must carefully configure the IP address, Subnet Mask, and DNS settings of every host on your network. Do not assign the same IP address to more than one host. Also, your RG must reside on the same subnet as all the other hosts.

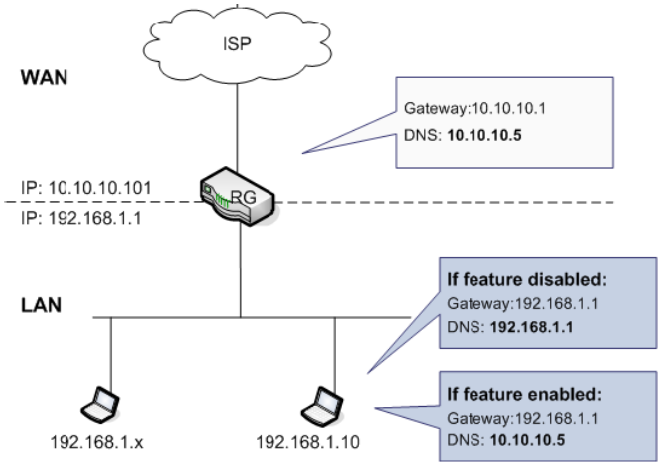
Firewall / NAT Services

The default setting for firewall and NAT services is enabled.



Enable/Disable DHCP

By default, the router has DHCP server (LAN side) disabled. If you already have a DHCP server running on your network, do not enable the router's DHCP server.



To enable DHCP:

1. *From the navigation bar at the top, click* ***Setup****.*

2. *Under* ***LAN Setup****, select* ***LAN Configuration****.*

   This will bring up the LAN Configuration Screen.

3. *In the* ***LAN Group 1*** *window, click the* ***Configure*** *link to the right of the LAN group 1 window.*

   The LAN Group 1 Configuration screen appears.

4. *Select the “Enable DHCP Server” radio button.*

5. *In the **Start IP** text box enter a Start IP address.*

   The Start IP Address is where the DHCP server starts issuing IP addresses. This value must be greater than the router's IP address value. For example, if the router's IP address is 192.168.1.1 (the default) than the Start IP address must be 192.168.1. 2 or higher.

6. *In the **End IP** text box enter the end IP address.*

   The End IP Address is the last address the DHCP server can issue. The ending address cannot exceed a subnet limit of 254. The maximum IP address for a router using the default address is 192.168.1.254. If the DHCP server runs out of DHCP addresses, users will not get access to network resources. If this situation occurs, you can increase the Ending IP address (to the limit of 254) or reduce the lease time.

   Note: If you change the start or end values, make sure the values are still within the same subnet as the router's IP address. For example, if the router's IP address is 192.168.1.1 (the default), and you change the DHCP Start and End IP addresses to be 192.128.1.2 and 192.128.1.100, you will not be able to communicate with the router if your PC has DHCP enabled.

7. *In the **Lease Time** text box enter the number of seconds a user will be allowed to be connected to the router with their dynamic IP address.*

   The Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. The amount of time is in units of seconds; the default value is 3600 seconds (1 hour).

8. *Click **Apply***

   The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

In addition to the DHCP server feature, the router supports the DHCP relay function. When the router is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the router is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server.

If the DHCP server and relay are turned off, you must configure the IP address, subnet mask and DNS settings of every computer on your network. Do not assign the same IP address to more than one computer. Your router must be on the same subnet as the computers.

Changing the Router's IP address

Your router's default IP address and subnet mask are 192.168.1.1 and 255.255.255.0, respectively. This subnet mask allows the router to support 254 users. Since the DHCP server issues a maximum of 255 addresses, there is not much advantage to changing the subnet mask to increase the number of addresses. Further, remember that if you change your router’s IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet.

The default gateway is the routing device used to forward all traffic that is not addressed to a station within the local subnet. Your ISP will provide you with the default gateway address.

The Hostname can be any alphanumeric word beginning with a letter and containing no spaces. The domain name is used to in conjunction with the host name to uniquely identify the router.

To change the router's IP address:

1. *In the navigation bar at the top of the screen, click **Setup**.*

2. *Under **LAN Setup**, select LAN Configuration.*

This will bring up the **LAN Configuration Screen**.

3. *In the LAN Group 1 window click the **Configuration** link.*

The LAN Group 1 Configuration screen appears.

4. *Select the “Use the following Static IP Address” radio button.*

5. *In the **IP Address** text box enter a new IP Address.*

6. *In the **Netmask** text box enter a new Netmask.*

7. *Click **Apply***

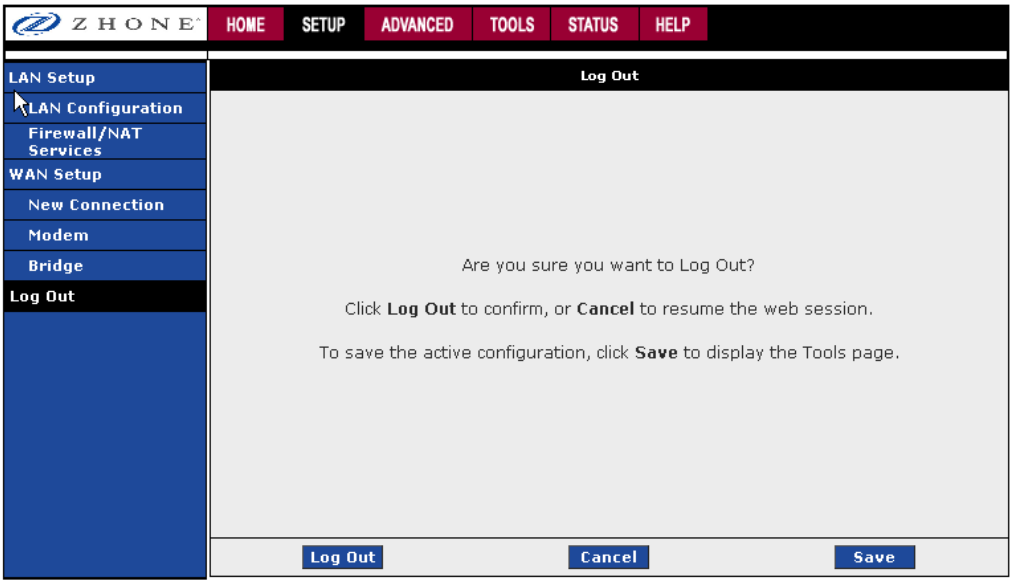
The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Log Out

To log out of configuration screen at any time

1. *When the **Setup**, **Advanced**, **Tools**, **Status**, or **Help** screens are selected, click **Log Out**. From the **Home** page click the **Log Out** button.*

2. *Click the **Save** button to save your configurations and then click on **Log Out** to exit.*



Advanced

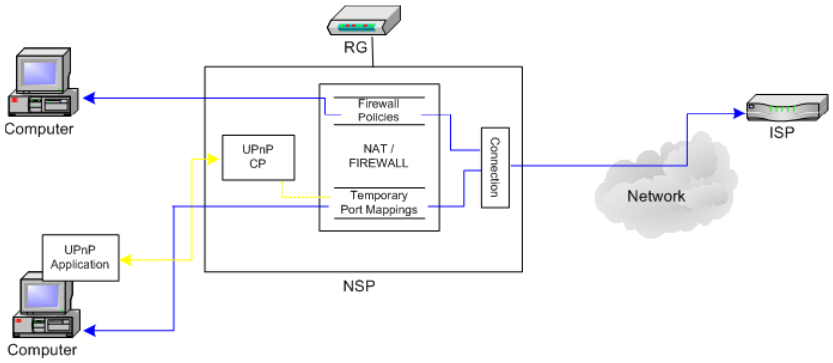
The modem supports a multitude of advanced features. For basic modem functionality you do not need to utilize these advanced features. The features help with routing, security, port configuration, and plug-and-play capability.

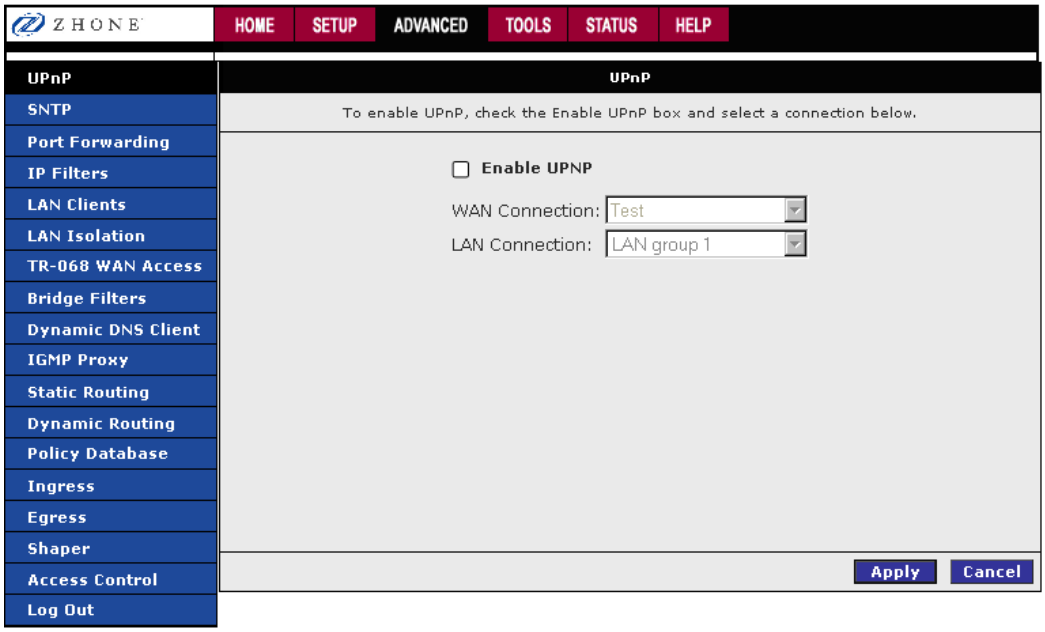
UPnP

The 6381 supports a control point for Universal plug and play (UPnP), version 1.0 and supports two key features: NAT traversal and Device Identification. This feature requires an active WAN connection. In addition, the PC should support this feature.

The UPnP application sits on top of a HTTP based socket listening for UPnP requests. With NAT Traversal, when an UPnP command is received to open ports in NAT, the application translates the request into IP table commands to open the ports in NAT and the firewall, mapping them back to the IP address of the PC on the LAN making the request. The connection to open the ports on is given to UPnP when it starts up and is part of the configuration of the application.

For Device Identification, the application will send a description of the 6381 RG as a control point back to the device making the request. An example of how this works is with Windows XP. You can go into the network for Windows XP and you will see the RG represented. You can then click on the RG and get access to its web pages.





To enable UPnP, you must first have a WAN connection configured. Once a WAN connection is configured:

1. *From the navigation bar at the top of the screen click **Advanced***

2. *From the left hand navigation pane select **UPnP**.*

   This will bring up the screen shown below.

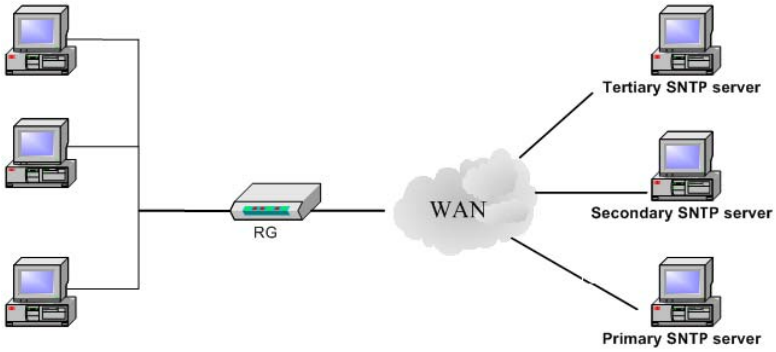
3. *Check **Enable UPnP** and then select which connection (**WAN** or **LAN**) will utilize UPnP.*

4. *Click **Apply***

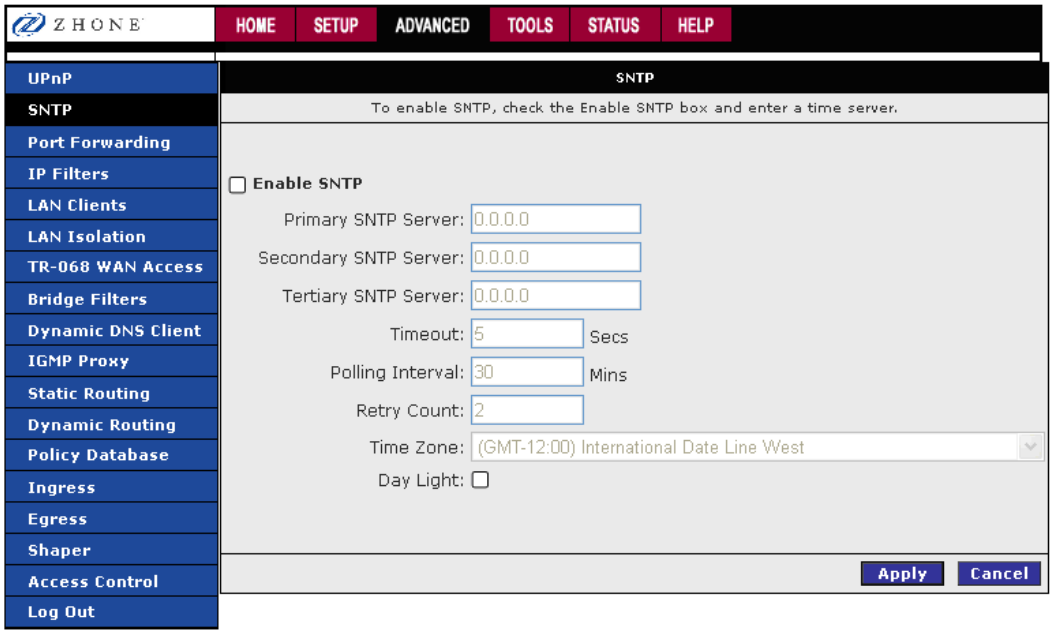
   The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

SNTP

Simple network timing protocol (SNTP) is a protocol used to synchronize the system time to public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers. The 6381 supports SNTP client functionality in compliance with IETF RFC 2030. The system clock time in the 6381 can be configured to send client requests to the configured SNTP server addresses periodically.



The main function of the Simple Network Time Protocol (SNTP) is to provide the network with a precise time based on Internet standards. Enter the information of the SNTP server to which you will be connecting.

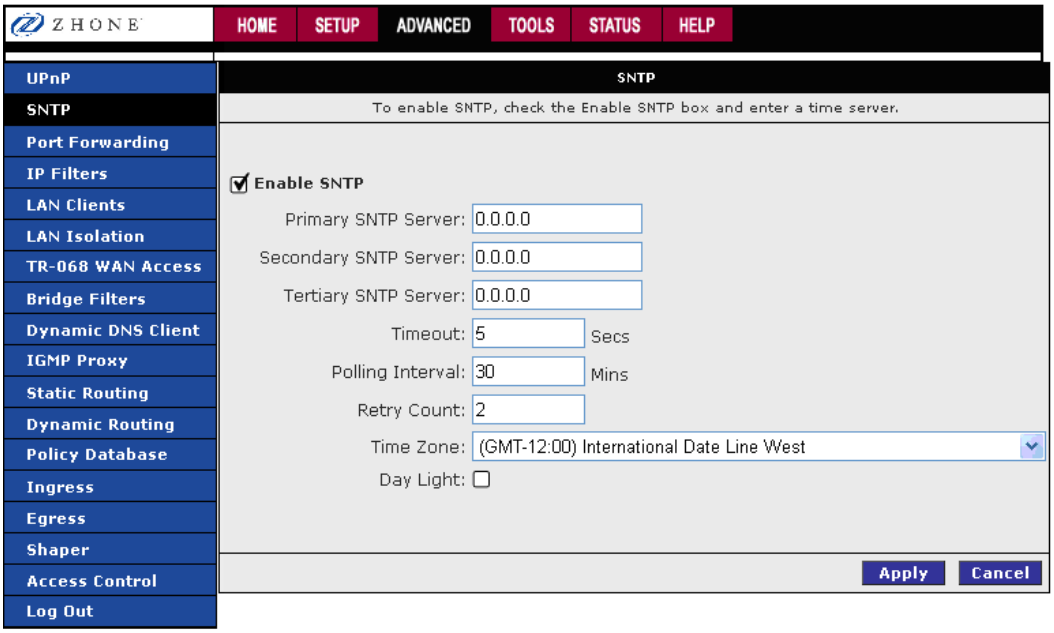


To configure SNTP:

1. *From the navigation bar at the top of the screen click* ***Advanced***

2. *From the left hand navigation pane select* ***SNTP****.*

3. *Check **Enable SNTP.***



4. *Specify one or more SNTP servers in the **Primary SNTP Server**, **Secondary SNTP Server**, and **Tertiary SNTP Server** fields and the SNTP options.*

Primary SNTP Server	The IP address or the host name of the primary SNTP server. This IP address can be provided by ISP or user-defined.
Secondary SNTP Server	The IP address or the host name of the secondary SNTP server. This IP address can be provided by ISP or user-defined.
Tertiary SNTP Server	The IP address or the host name of the tertiary SNTP server. This IP address can be provided by ISP or user-defined.
Timeout	If the RG failed to connect to a SNTP server within the Timeout period, it retries the connection.
Polling Interval	The amount of time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.
Retry Count	The number of times the RG tries to connect to an SNTP server before it tries to connect to the next server in line.
Time Zone	The time zone in which the RG resides.
Day Light	Check/uncheck this option to enable/disable daylight saving time (DST). Note: DST is not automatically enabled or disabled. You need to manually enable and disable it.

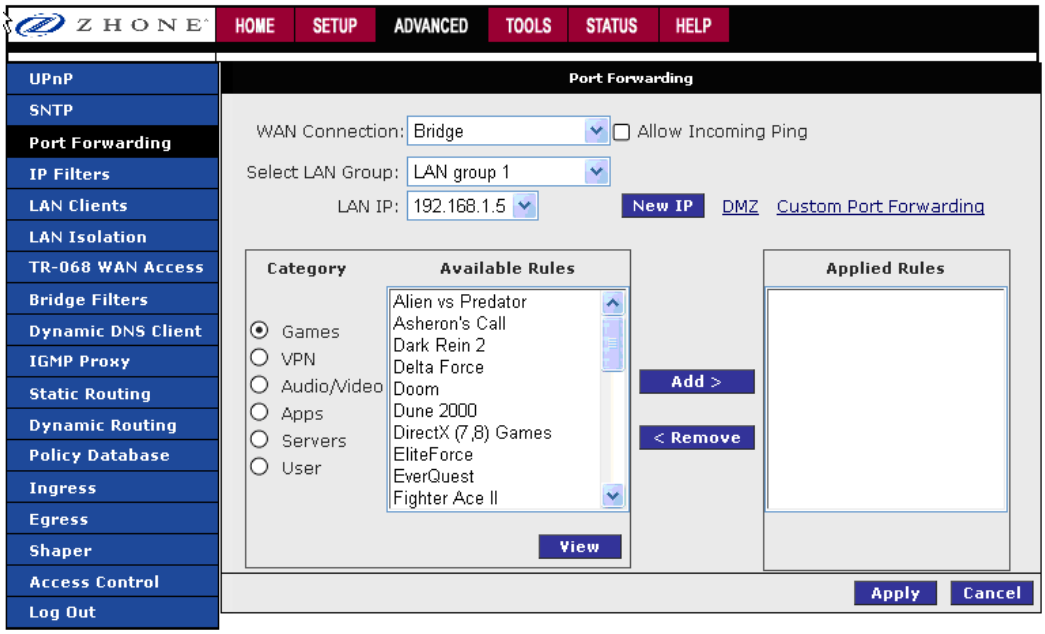
5. *Click **Apply***

The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Port Forwarding

The port forwarding (or virtual server) feature allows you to direct incoming traffic to specific LAN hosts based on a protocol port number and protocol. Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet or play Internet games. When users send this type of request to your network via the Internet, the modem will forward those requests to the appropriate PC. Port forwarding can be used with DHCP assigned addresses but remember that a DHCP address is dynamic (not static). For example, if you were configuring a NetMeeting server, you would want to assign this server a static IP address so that the IP address is not reassigned. Also remember that if an Internet user is trying to access an Internet application, they must use the WAN IP address. The port forwarding will translate the WAN IP address into a LAN IP address.

NOTE: To configure a port you must have an existing LAN client with an IP address. You can add a LAN client on the **LAN Clients** page.



A database of predefined port forwarding rules allows you to apply one or more rules to one or more members of a defined LAN group. You can view the rules associated with a predefined category and add the available rules for a given category. You can also create, edit, or delete your own port forwarding rules.

To configure a service, game, or other application:

1. *From the navigation bar at the top of the screen click **Advanced***

2. *From the left hand navigation pane select **Port Forwarding**.*

3. *From the **WAN Connection** dropdown select the external connection.*

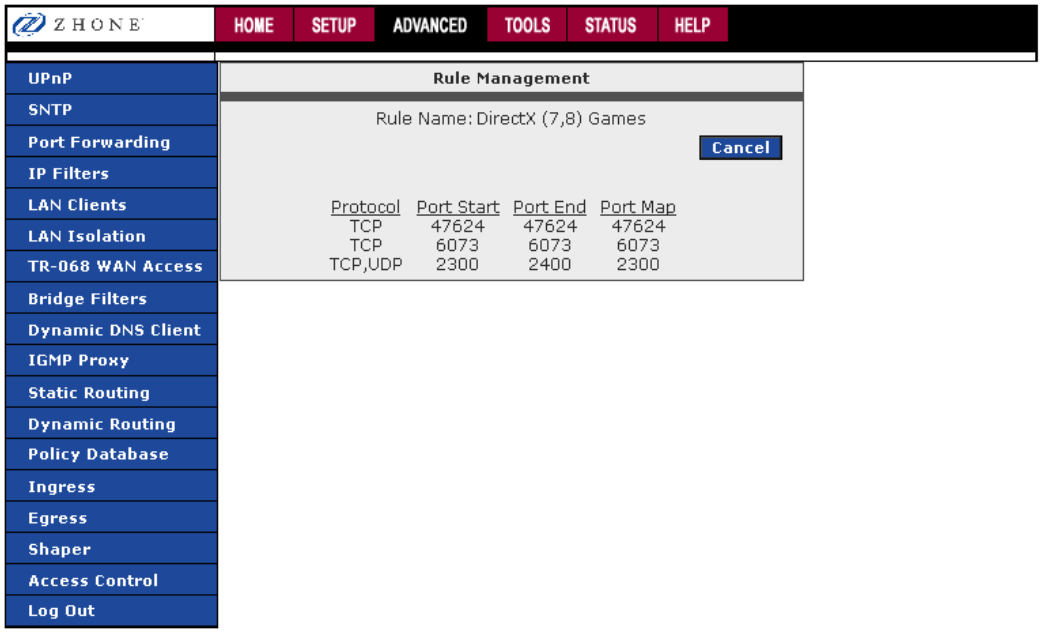
   If the desired LAN IP is not available in the LAN IP drop-down menu, you can add it using the LAN Client page, which is accessed by clicking **New IP**. See LAN Clients on page 72.

Port Forwarding Fields:

WAN Connection	Select the WAN connection to which port forwarding is applied.
Select LAN Group	Select the LAN Group to which port forwarding is applied.
LAN IP	Select the IP address to host the service.
Allow Incoming Ping	Enabling incoming ping (ICMP) requests on the Port Forwarding page allows the RG to respond to a ping from the Internet.
DMZ	Demilitarized zone. By setting a PC on your local network as demilitarized zone (DMZ), you can choose to forward all incoming packets that cannot be routed to a specific IP address to the PC with the DMZ IP address. This opens the access to the DMZ host from the Internet. This function is disabled by default. By enabling DMZ, you add an extra layer of security protection for hosts behind the firewall.
Custom Port Forwarding	This link takes you to the **Custom Port Forwarding** page.
Category	Custom and user-defined categories.
Available Rules	Predefined and user-defined IP filtering rules for each category.
Applied Rules	Lists the IP filtering rules you elect to apply for each given category.

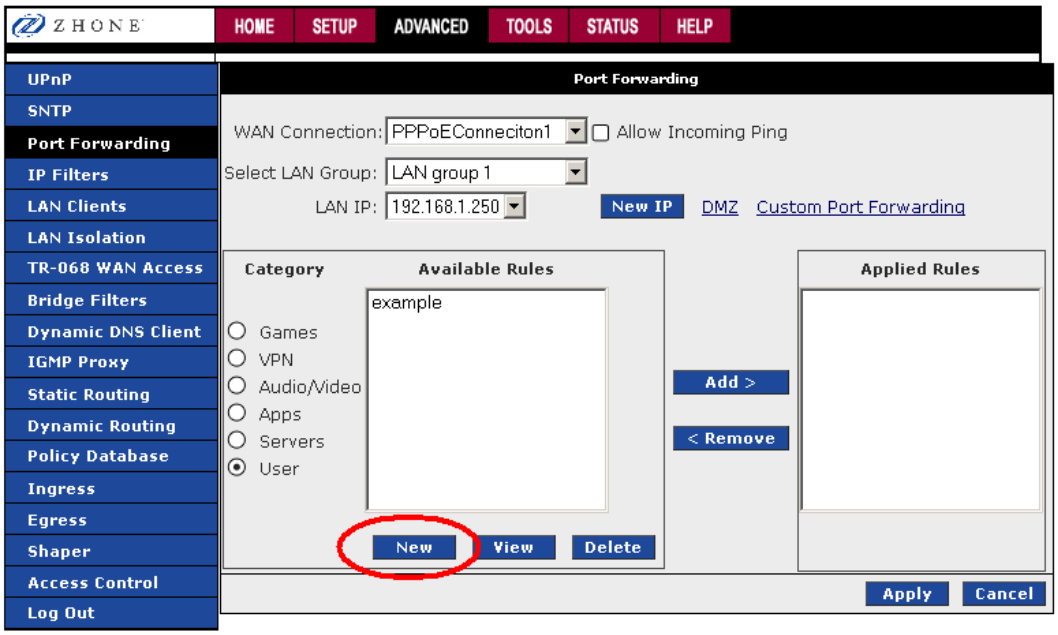
4. *Select the available rules for a given category and click **Add** to apply the rule for the category.*

You can view a rule associated with a predefined filter on the **Rule Management** page. You get to the rule management page by selecting a rule from the list in the **Available Rules** pane, then clicking **View**.

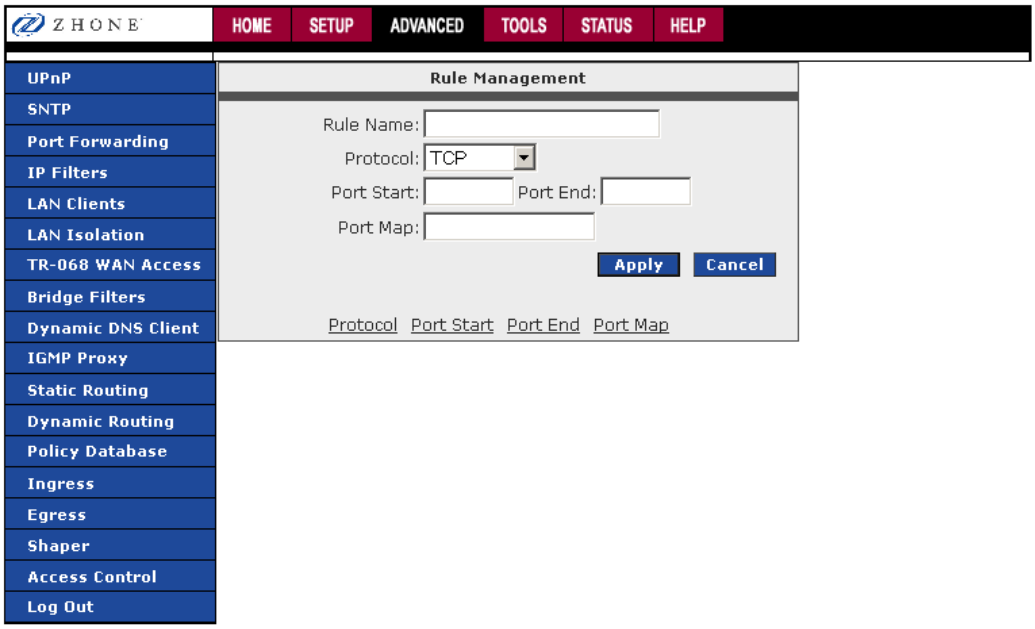


5. *To add a custom application, select the User category, click **New** and fill in the port, protocols and description for your application.*

The **New**, **View**, and **Delete** buttons become available only when the **User** category is selected. All the custom rules you create fall under the **User** Category.



The Rule Management page populates for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map** fields, and then click **Apply**.



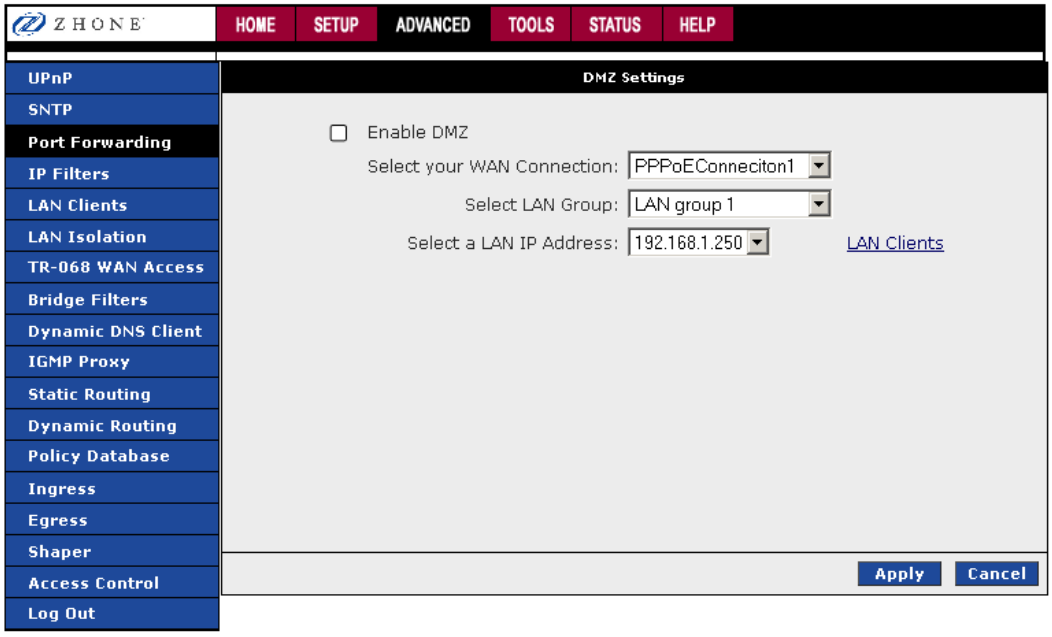
6. *Continue to add rules as they apply from each category.*

7. *Click **Apply***

The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

DMZ Settings

1. *On the **Port Forwarding** page, click the DMZ link.*



2. *Check the **Enable DMZ** box.*

DMZ Fields:

Enable DMZ	Enables/disables the Demilitarized Zone feature. This field is unchecked (disabled) by default.
Select your WAN Connection	Select the WAN connection on which the DMZ feature will be applied.
Select LAN Group	Select the LAN Group on which the DMZ feature is applied.
Select a LAN IP Address	Select the LAN IP address you are going to use as the DMZ host. This host is exposed to the Internet. Be aware that this feature may expose your local network to security risks.
LAN Clients	This link takes you to the LAN Clients page. More information on LAN Clients can be found See LAN Clients on page 72.

3. *Select the **WAN Connection**, **LAN Group**, and **LAN IP Address.***

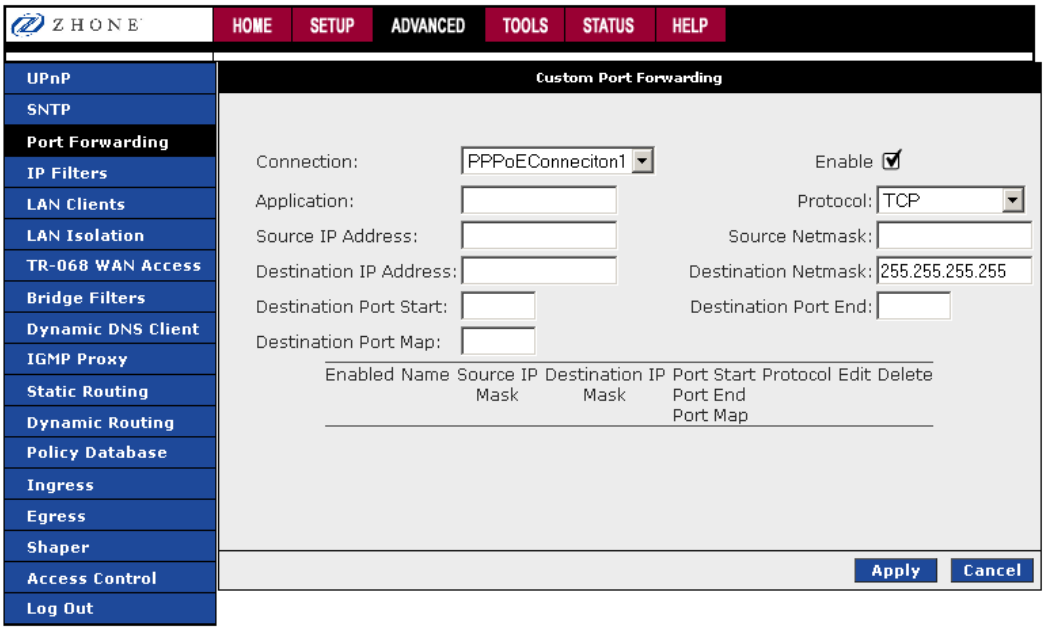
   DMZ is configurable per LAN segment.

4. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Custom Port Forwarding

The Custom Port Forwarding page allows you to create up to 15 custom port forwarding entries to support specific services or applications, such as concurrent NAT/NAPT operations.



1. *On the **Port Forwarding** page, click the **Custom Port Forwarding** link.*

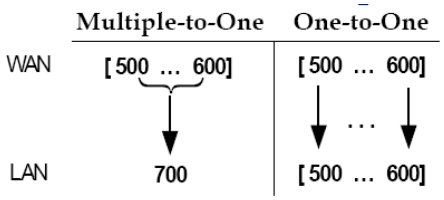
2. *Select the connection to which the **Custom Port Forwarding** rule will be applied.*

3. *Set the appropriate **Protocol**, **Source IP Address**, **Source Netmask**, **Destination IP Address**, **Destination Netmask**, **Destination Port Start**, **Destination Port End** and **Destination Port Map** as described below/*

Custom Port Forwarding Fields:

Connection	Select the WAN connection on which the Custom Port Forwarding rule is to be applied.
Enable	The **Enable** button is checked by default, meaning this rule is automatically applied when you click the **Apply** button.
Application	Name of the application for which your ports will be opened.
Protocol	There are three options available: TCP, UDP, and TCP and UDP.
Source IP Address	You can define the source IP address from which the incoming traffic is allowed. Enter 0.0.0.0 for all.
Source Netmask	Netmask of the source IP address. Enter *255.255.255.255* for all.
Destination IP Address	The LAN-side destination IP address for incoming traffic.
Destination Netmask	The LAN-side destination netmask for incoming traffic. The default value of this field is 255.255.255.255.
Destination Port Start	The starting port number that is to be opened for this application.
Destination Port End	The ending port number that is to be opened for this application.
Destination Port Map	Destination port mapped on the LAN (destination) side to which packets are forwarded. There are two types of port mapping: • One-to-one (one port mapped to one)

- Multiple-to-one (multiple ports mapped to one port)



NOTE: Wildcard (*) entries are allowed for IP Address/Netmask and Port range fields.

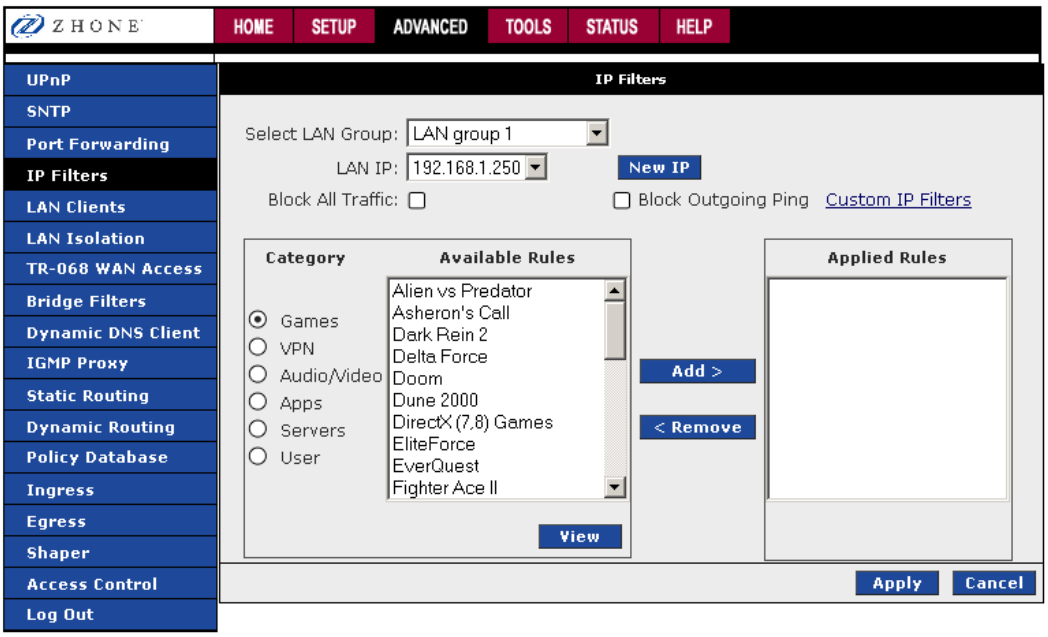
4. *Click **Apply***

The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

IP Filters

The IP filtering feature allows you to block specific applications/services based on the IP address of a LAN device. You can use the **IP Filters** page to block specific traffic (for example block web access) or any traffic from a computer on your local network.

A database of predefined IP filters allows you to apply one or more filtering rules to one or more members of a defined LAN group. You can view the rules associated with a predefined filter and add the available rules for a given category. You can also create, edit, or delete your own IP filter rules.



IP Filters fields:

Select LAN Group	Select the LAN group to which the IP filters feature will be applied.
LAN IP	Select the IP address in the given LAN group to which the IP Filters feature will be applied.
Block All Traffic	When checked, complete network access is blocked for the specific IP address.
Block Outgoing Ping	Blocking outgoing ping (ICMP) generated from a particular LAN IP can be used if your host has a virus that attempts a Ping-of-Death Denial of Service attack.
Custom IP Filters	This link takes you to the **Custom IP Filters** page. See Custom IP Filters on 71.
Available Rules	Predefined and user-defined IP filtering rules for each category.
Applied Rules	Lists the IP filtering rules you elect to apply for each given category.

To configure an IP Filter rule:

1. *From the navigation bar at the top of the screen click **Advanced***
2. *From the left hand navigation pane select **IP Filters**.*
3. *From the **Select LAN Group** drop down, select the LAN group to which the changes will be applied.*

4. *From the **LAN IP** drop down select the IP address.*

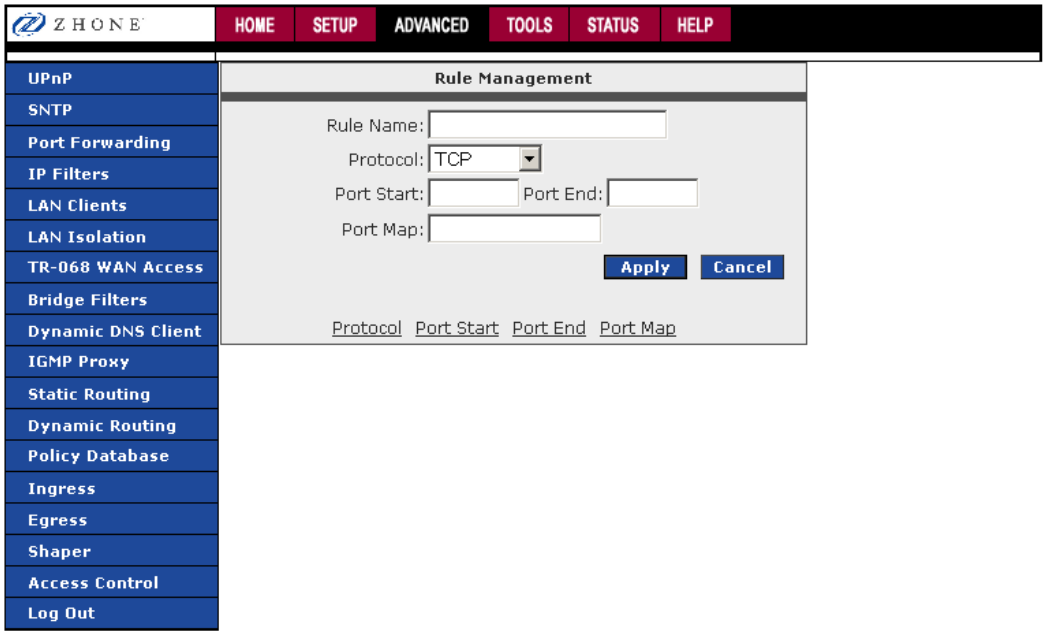
   If the desired LAN IP is not available in the LAN IP drop-down menu, you can add it using the LAN Client page, which is accessed by clicking **New IP**. See IP Filters on page 69.

5. *From the **Available Rules** pane select the appropriate rules, and then click **Add** to move the rule to the **Applied Rules** pane. To create a custom IP filter rule, click **Custom IP Filters**.*

6. *If a rule is not in the list, you can create your own rule in the **User** category. Select **User**, and then click **New**.*

   The **New**, **View**, and **Delete** buttons become available only when the **User** category is selected. All the custom rules you create fall under the **User Category**.

   The Rule Management page populates for you to create new rules. Enter **Rule Name**, **Protocol**, **Port Start**, **Port End**, and **Port Map** fields, and then click **Apply**.



   The rules you create will appear in the **Available Rules** box in the User category. You can view or delete the rules you create.

7. *Continue to add rules as they apply from each category using the **Add** button.*

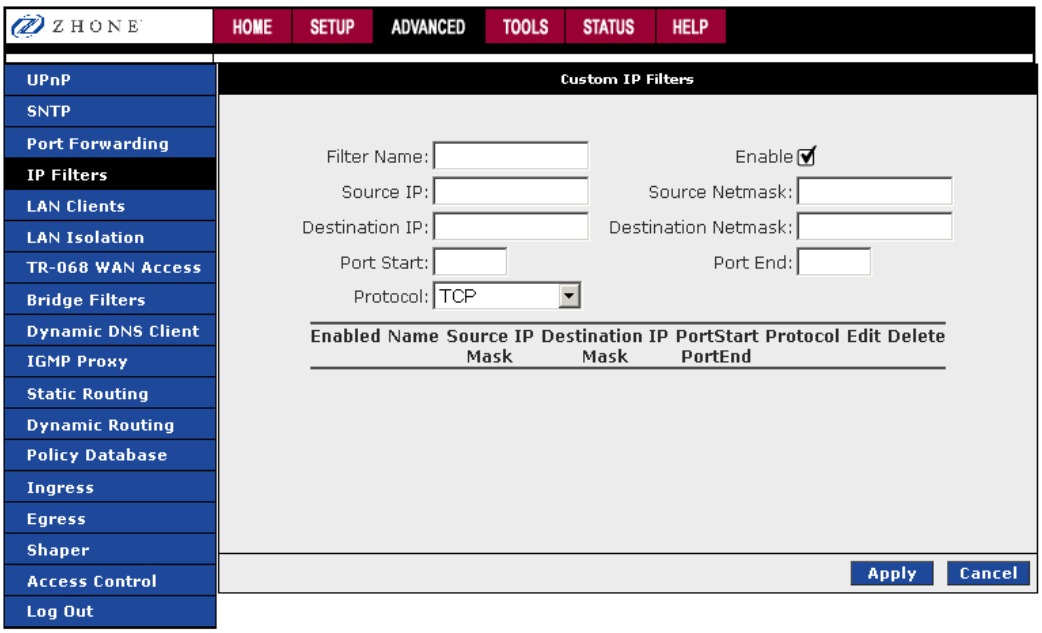
8. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Custom IP Filters

The Custom IP Filters page allows you to define up to 20 custom IP filtering entries to block specific services or applications based on:

- Source/destination IP address and netmask
- TCP port (ranges supported)
- Protocol



Custom IP Filter fields:

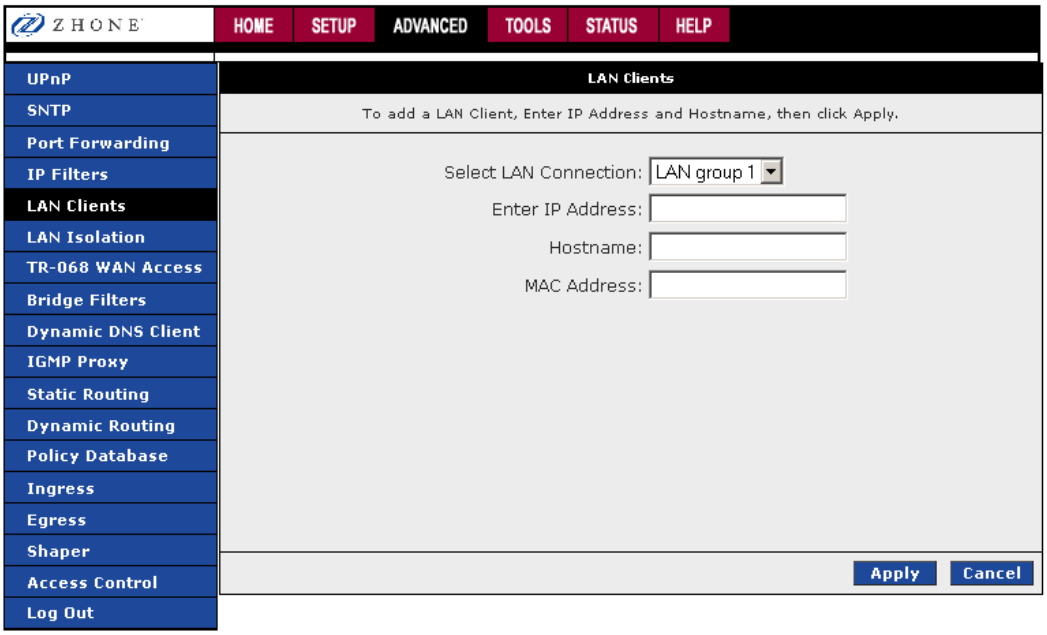
Filter Name	Name of the IP filter rule you are creating.
Enable	The **Enable** button is checked by default, meaning this rule is automatically applied when you click **Apply**.
Source IP	The LAN-side source IP address assigned to outgoing traffic on which filtering is applied.
Source Netmask	Netmask of the source IP on your LAN side.
Destination IP	You can define the destination IP address to which your source IP will be banned access. Enter 0.0.0.0 for all.
Destination Netmask	Netmask of the destination IP. Enter 255.255.255.255 for all.
Port Stat	The starting port number that will be blocked for this application.
Port End	The ending port number that will be blocked for this application.
Protocol	There are five options available: TCP, UDP, TCP and UDP, ICMP, and Any.

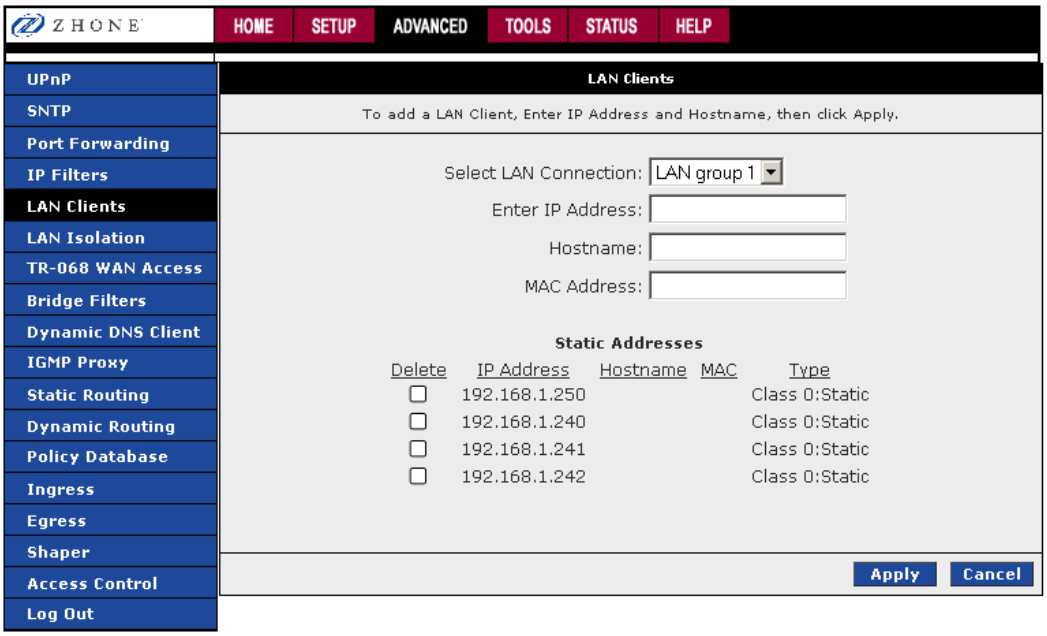
LAN Clients

The LAN clients feature allows you to see all the hosts on the LAN segment. Each host is qualified to be either dynamic (host obtained a lease from this 6381 RG) or static (host has a manually-configured IP address).

You can add a static IP address (belonging to the 6381 RG's LAN subnet) using the **LAN Clients** page. Any existing static entry falling within the DHCP server's range can be deleted and the IP address is made available for future allocation.

Dynamic clients will only be displayed in the list only when the DHCP server is running.





Select LAN Connection	Select the LAN connection to which the client is to be added.
Enter IP Address	Assign the dynamic IP address to the host here. This is a mandatory field.
Hostname	Hostname of the client. This is an optional field.
MAC Address	MAC address of the host. This is an optional field.

To configure a LAN client:

1. *From the navigation bar at the top of the screen click **Advanced***

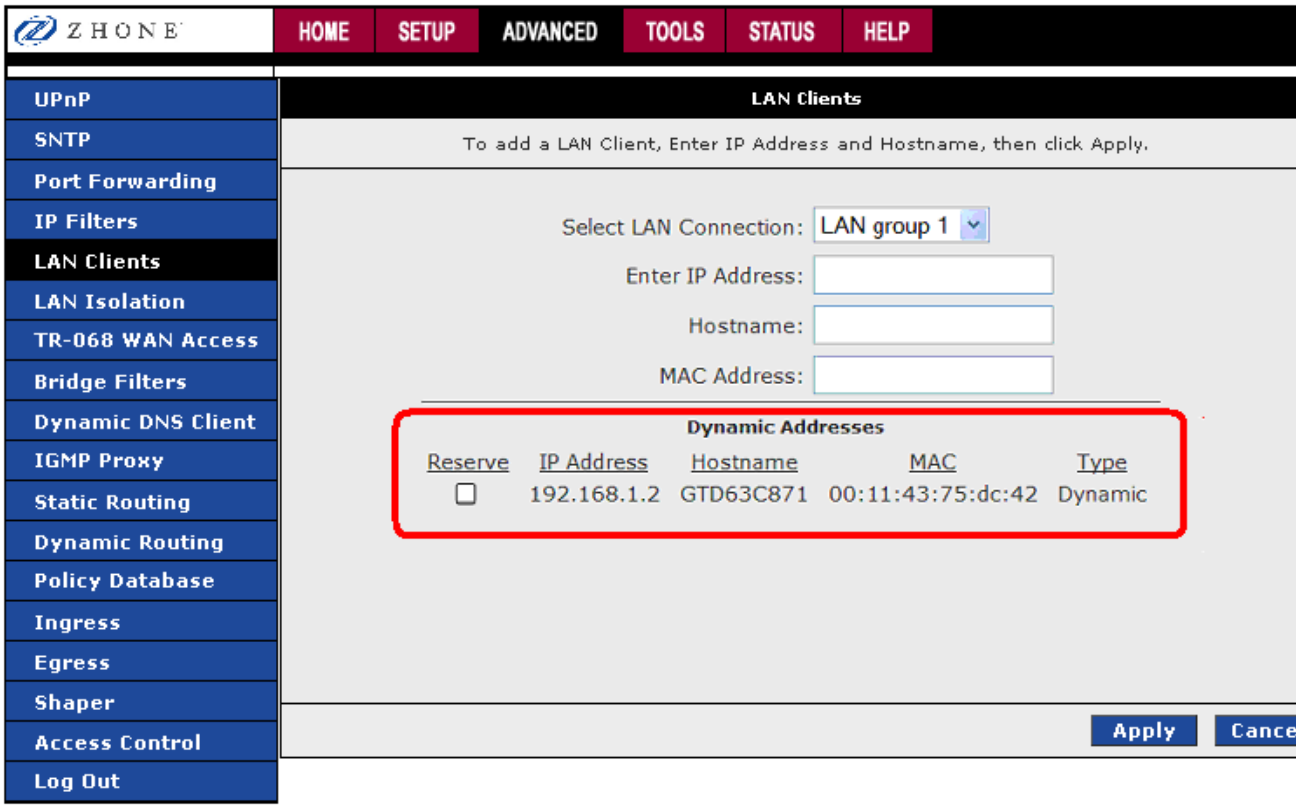
2. *From the left hand navigation pane select **LAN Clients**.*

   If DHCP is used, all DHCP clients are automatically assigned.

   If a fixed IP address server is on the LAN and you want this server to be visible via the WAN, you must add its IP address. Once the IP address has been added, you can apply Port Forwarding and Access Control rules to this IP address.

3. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

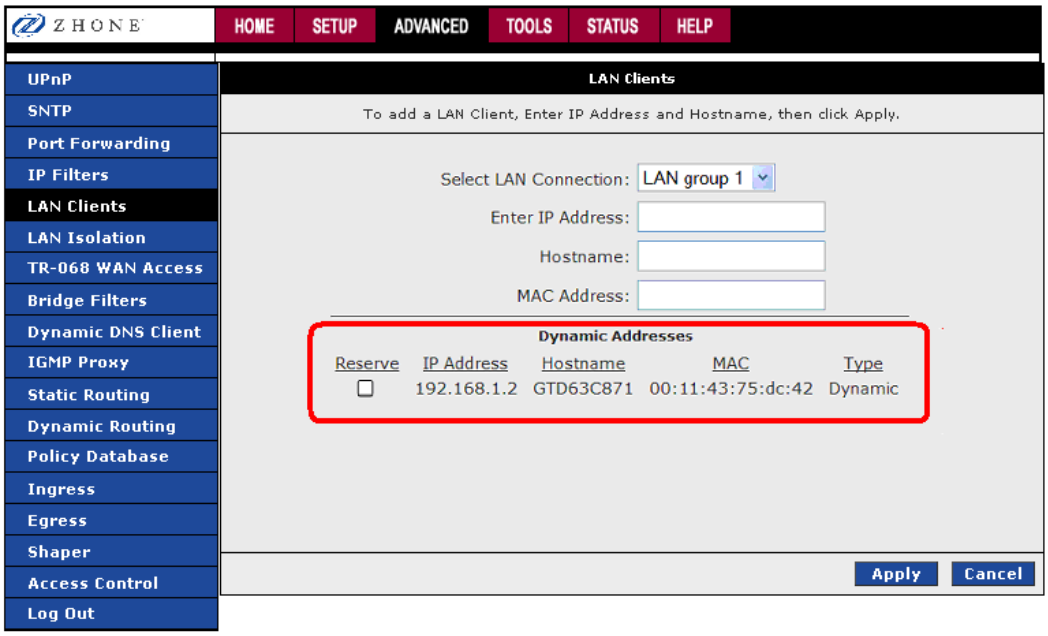


To convert a dynamic entry into a static entry:

1. *From the navigation bar at the top of the screen click **Advanced***

2. *From the left hand navigation pane select **LAN Clients**.*

3. *For a Dynamic Address, click **Reserve**, then **Apply***

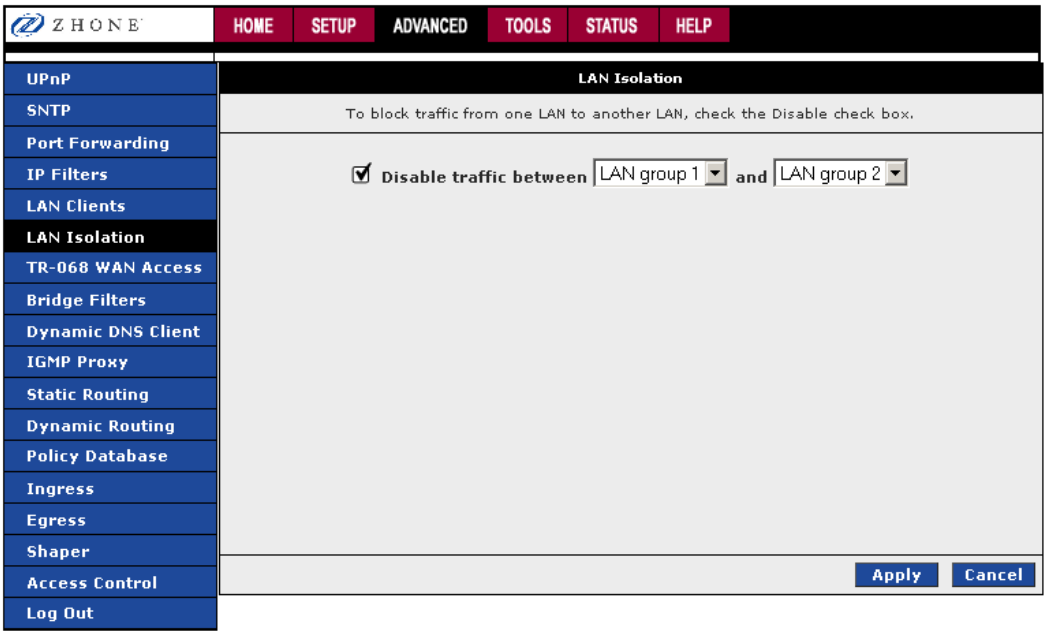


4. *Click **Apply***

The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

LAN Isolation

The LAN Isolation page allows you to disable the flow of packets between LAN groups. This ability to isolate LAN groups allows you to secure information in private portions of the LAN (such as a hot spot deployment) from other publicly accessible LAN segments.



To block traffic between LAN groups:

1. *From the navigation bar at the top of the screen click **Advanced***

2. *From the left hand navigation pane select **LAN Isolation**.*

3. *Enter a check in the **Disable traffic between** check box*

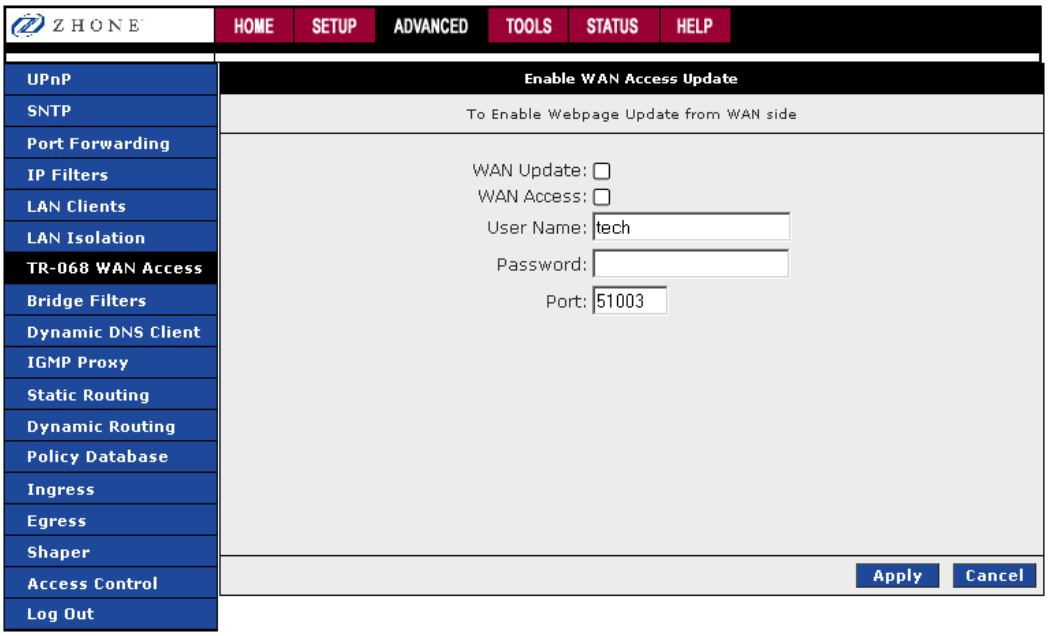
4. *From the **Disable traffic between** dropdowns select the LAN groups to isolate from each other.*

5. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

TR–068 WAN Access

The **TR-068 WAN Access** page enables you to give temporary permission to someone (such as technical support staff) to be able to access your 6381 RG through the Internet (from the WAN side).



WAN Update	Check this field to give the account read and write access.
WAN Access	Check this field to give the account read-only access.
User Name	User name of the WAN access account.
Password	Password of the WAN access account.
Port	Enter the port number to be opened for the temporary WAN access.

To create a temporary user account for a remote access to your 6381 RG:

1. *Check **WAN Update** to enable write privilege of the 6381 RG.*
2. *Check **WAN Access** to enable read privilege of the 6381 RG.*
3. *Enter a user name and password in the **User Name** and **Password** fields (and communicate it to the service technician to whom you are giving this privilege).*
4. *Enter a port number In the **Port** field (for example, 51003).*
5. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

To access your RG remotely, from the remote PC, enter the following in the URL:

http(s)://10.10.10.5:51003

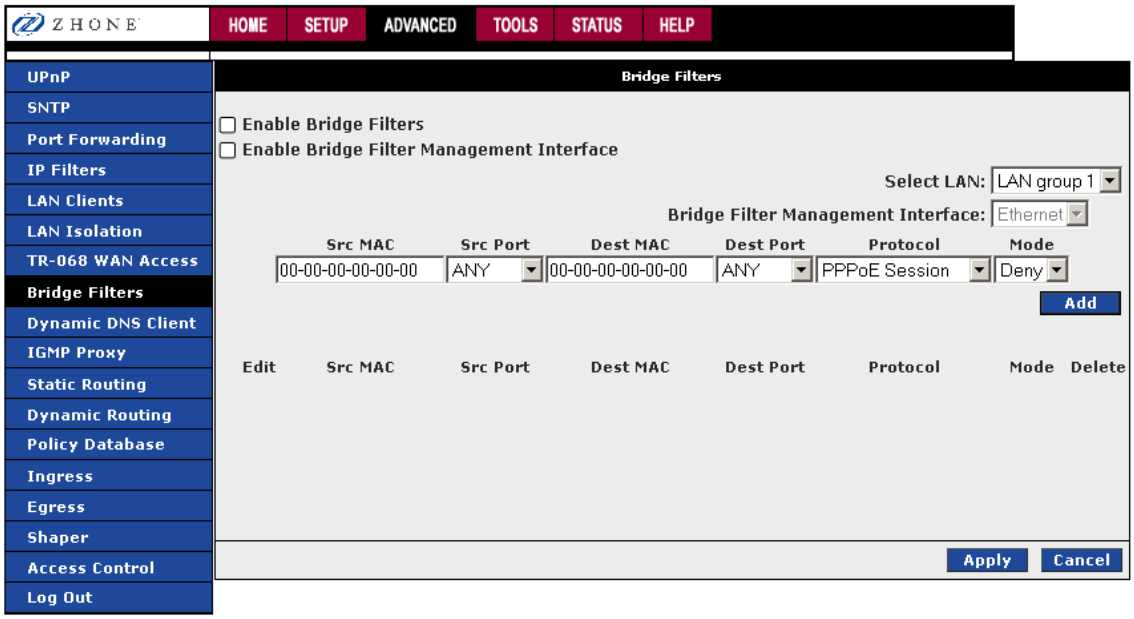
Syntax: http(s)://***WAN IP of RG***:***Port Number***

From the moment the account is enabled, the user is expected to log in within 20 active minutes, otherwise the account expires. Once the user has logged in, if the session remains inactive for more than 20 minutes, the user will be logged out and the account expires.

Bridge Filters

The bridge filtering mechanism provides a way for the users to define rules to allow/deny frames through the bridge based on source MAC address, destination MAC address and/or frame type. When bridge filtering is enabled, each frame is examined against the defined filter rules sequentially, and when a match is determined, the appropriate filtering action (determined by the access type selected, i.e. allow or deny) is performed. The user should note that the bridge filter only examines frames from interfaces that are part of the bridge itself. Twenty filter rules are supported with bridge filtering.

The **Enable Bridge Filter Management** interface allows you to select a **Bridge Filter Management Interface** and keeps you from getting locked out of the 6381 on the interface of the LAN group specified in the **Select LAN** dropdown.



Enable Bridge Filters	Enables/disables bridge filtering. It can be set/unset during any add, edit, or delete operation. It can also be set/unset independently by clicking **Apply**.
Enable Bridge Filter Management Interface	When checked, it enables the Bridge Filter Management Interface field. This ensures that you do not get locked out of the RG on the interface of the LAN group specified in the next two fields.
Select LAN	Select your LAN group to enable the Bridge Filter Management Interface feature.
Bridge Filter Management Interface	Select the interface of the LAN group to have the Bridge Filter Management Interface feature enabled. Depending on the LAN group that is selected, the interface selections are Ethernet, USB, and/or WLAN.
SRC MAC	The source MAC address. It must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as don't care. Blanks can be used in the MAC address space and are also considered as don't care.
SRC Port	Source port. You can choose from Any, Ethernet, USB, WLAN, or WAN Bridge Connection Port for the particular bridge. If any of the selections are not available, please check your DSL connection.
Dest MAC	The destination MAC address.
Dest Port	Destination port. You can choose from Any, Ethernet, USB, and WLAN.

Protocol	You can choose from the following options: PPPoE Session, PPPoE Discovery, IPX - Ethernet II, RARP, IPv6, IPv4, and Any.
Mode	There are two filtering modes: Deny and Allow.

1. *From the navigation bar at the top of the screen click **Advanced***

2. *From the left hand navigation pane select **Bridge Filters**.*

   The User Interface for Bridge Filter allows the user to add/edit/delete, as well as, enables the filter rules.

3. *Check **Enable Bridge Filters**.*

4. *To add rules, simply define the source MAC address, destination MAC address and frame type with desired filtering type (i.e. allow/deny), and click **Add**.*

   The MAC address must be in a xx-xx-xx-xx-xx-xx format, with 00-00-00-00-00-00 as “automatically allow”. Blanks can be used in the MAC address space, and would be considered also as “automatically allow”.

   Note: On a windows based machine, you can find a MAC address with the ipconfig program. At a command prompt, type: ipconfig /all

5. *To edit/modify an existing filter rule, select the desired rule created previously from **Add** in the **Edit** select box.*

   The selected filter rule will appear on top section, as with the **Add** filter rule. Make the desired change to the MAC address, frame type and/or access type, and click **Apply**.

   The **Enable Bridge Filters** check box allows the user to enable or disable bridge filtering. It can be set/unset during any add/edit/delete operation. It can also be set/unset independently by just pressing the “Apply” button.

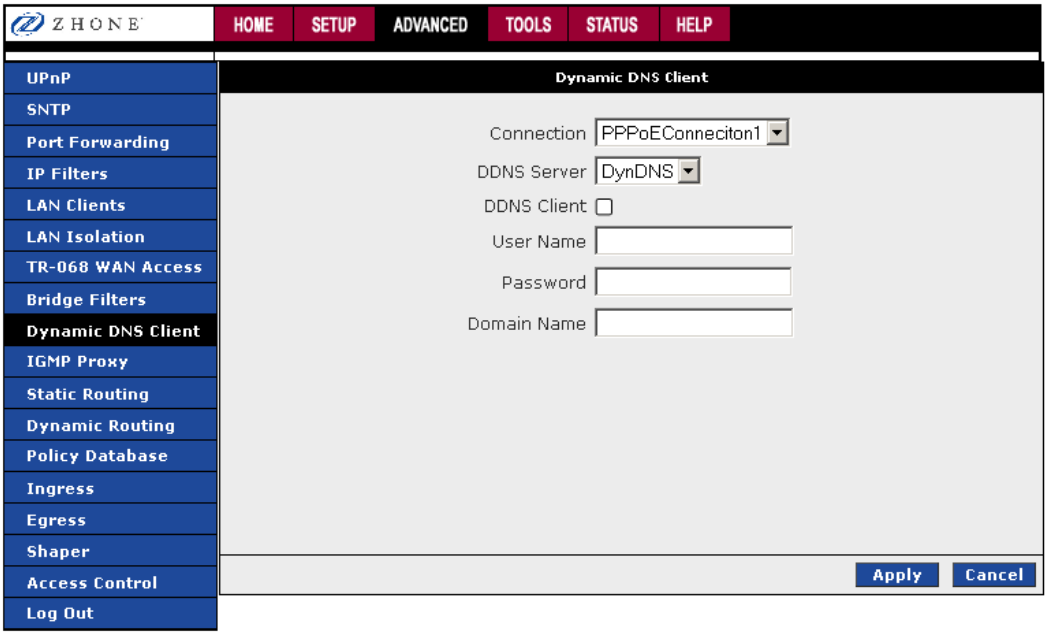
6. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Dynamic DNS Client

Each time the 6381 connects to the Internet; your ISP assigns a different IP address to the 6381. In order for you or other users to access your 6381 from the WAN-side, you need to manually track the IP that is currently used. The Dynamic DNS feature allows you to register your 6381 with a DNS server and access your 6381 each time using the same host name.

The Dynamic DNS Client page allows you to enable/disable the Dynamic DNS feature.



Connection	This field defaults to your 6381 RG's WAN connection over which the RG will be accessed.
DDNS Server	This is where you select the server from different DDNS service providers. A charge may occur depends on the service you select.
DDNS Client	Enables/disables the DDNS client feature for the WAN connection. This field is disabled by default.
User Name	User name assigned by the DDNS service provider.
Password	Password assigned by the DDNS service provider.
Domain Name	Domain name to be registered with the DDNS server.

To connect to a DDNS Server:

1. *From the navigation bar at the top of the screen click **Advanced***

2. *From the left hand navigation pane select **Dynamic DNS Client**.*

3. *From the **Connection** drop down select the WAN connection over which your 6381 will be accessed.*

4. *From the **DDNS Server** drop down select the DDNS server from DDNS Service Providers.*

   DDNS Service Providers may charge for this service.

5. *Enter the **User Name** and Password as assigned by the DDNS Service Provider.*

6. *Enter the **Domain Name** to be registered with the DDNS server.*

7. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

IGMP Proxy

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a Host Group. A host group is a set of one or more hosts identified by a single IP destination address.

Internet Group Management Protocol (IGMP) Proxy allows for forwarding of multicast traffic between networks. Unlike broadcast which sends traffic to all possible addresses (and because it requires duplication and transmission broadcasts may require a great deal of computation time from the sending device), multicast provides a mechanism so data can be sent to a limited number of devices. Unlike sending multiple normal unicast transmissions, which send transmissions a single specific device (then many times over), multicast provides an option which does not require many transmissions to be sent. Multicast has a group membership mechanism where one data stream can be received by more than one device, so multicast does not require the network bandwidth of multiple unicast transmissions.

Multicasting is useful when the same data needs to be sent to more than one device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth. The multicast feature also enables you to receive multicast video streams from multicast servers.

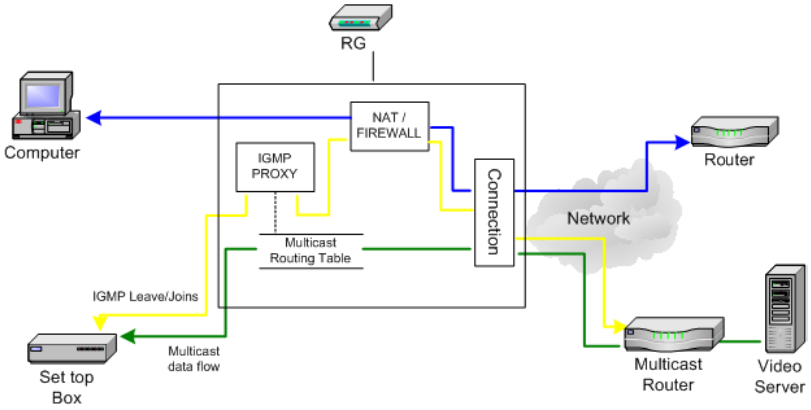
With multicast, datagrams are sent to all hosts in a Host Group. A host group is a set of one or more hosts identified by a single IP destination address. Host groups follow these standards:

- Anyone can join or leave a host group at will.
- There are no restrictions on a host's location.
- There are no restrictions on the number of members that may belong to a host group.
- A host may belong to multiple host groups.
- Non-group members may send UDP datagrams to the host group.

Multicast provides a means for devices in host groups to get the datagrams from the host group IP address. Multicast also enables you to receive multicast video streams from multicast servers.

IP hosts use IGMP to report their multicast group memberships to neighboring routers. Similarly, multicast routers use IGMP to discover which of their hosts belong to multicast groups. Your 6381 supports IGMP proxy that handles IGMP messages. When enabled, your 6381 acts as a proxy for a LAN host making requests to join and leave multicast groups, or a multicast router sending multicast packets to multicast groups on the WAN side.

On a Join, the proxy sets up a multicast route for the interface and PC requesting the video content. It then forwards the Join to the upstream multicast router. The Multicast IP traffic will then be forwarded to the requesting device. Multicast traffic does not pass trough the Firewall or NAT. On a leave, the Proxy removes the route and then forwards the leave to the upstream Multicast router.



The IGMP Proxy page allows you to enable multicast on available WAN or LAN interfaces.

Upstream	The interface from which IGMP requests from hosts are sent to the multicast router.
Downstream	The interface on the router which sends to hosts in the multicast group database.
Ignore	No IGMP requests nor multicast data is forwarded.

Here are a few examples to demonstrate how to configure interfaces

- WAN Interface as Upstream IGMP Proxy

  The multicast server is in the WAN network. Hosts on the LAN side can send IGMP requests through the WAN interface. The WAN will pass multicast packets from the multicast server to hosts on the LAN side.

  WAN interface on which the multicast router exists: Upstream

  Interface(s) of any LAN groups receiving multicast: Downstream

  Interface(s) of any WAN groups receiving multicast: Downstream

  Interface(s) of any LAN or WAN groups not receiving or providing multicast: ignore

- LAN Interfaces as the Upstream IGMP Proxy

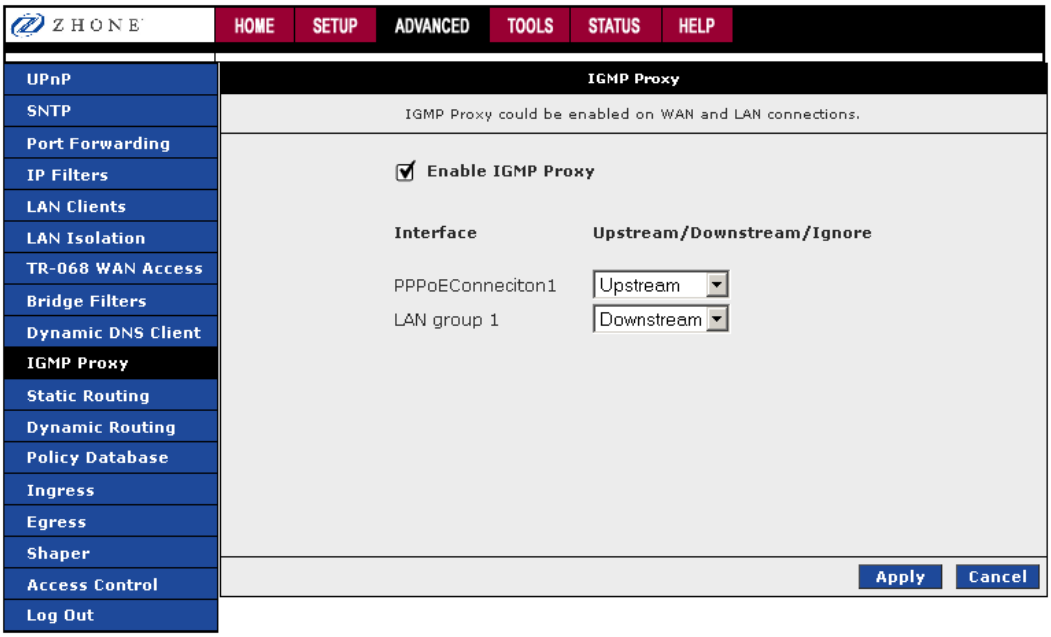
  The multicast is on the LAN side. Hosts on the Hosts on the WAN network can send IGMP requests through the LAN interface. The LAN interface, acting as the upstream interface, forwards data multicast from the LAN-side multicast server to hosts on the network.

  LAN group interface on which the router exists: Upstream

  Interface(s) of WAN group(s) receiving multicast: Downstream

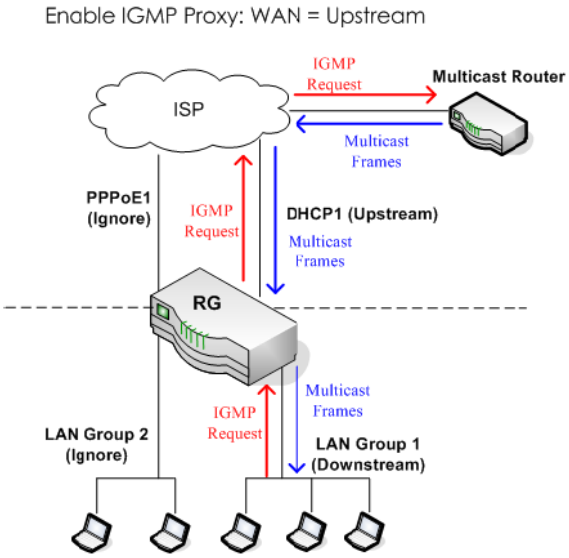
  Interface(s) of any LAN group(s) receiving multicast: Downstream

  Interface(s) of any LAN or WAN group(s) not receiving or providing multicast: ignore



Configure a WAN Interface as the Upstream IGMP Proxy

The following procedure applies when the multicast server in on the network. Hosts on your LAN side can send IGMP requests through the WAN interface. And the WAN will pass multicast packets from the multicast server to the hosts on the LAN side.



As shown above the WAN interface DHCP1 is enabled as the upstream IGMP interface, which forwards IGMP requests from LAN group 1 to the multicast router on the network and forwards multicast frames from the multicast router to hosts on the downstream interface (LAN group 1). No IGMP request nor data multicast are forwarded to PPPoE1 or LAN Group 2.

To configure a WAN interface as the Upstream IGMP Proxy:

1. *From the navigation bar at the top of the screen click* ***Advanced***

2. *From the left hand navigation pane select* ***IGMP Proxy****.*

3. *Enter a check in the **Enable IGMP Proxy** check box*

4. *From the **Interface** **Upstream/Downstream/Ignore** dropdowns select the LAN groups to and whether they should allow IGMP proxies from upstream or downstream.*

   To match the example above:

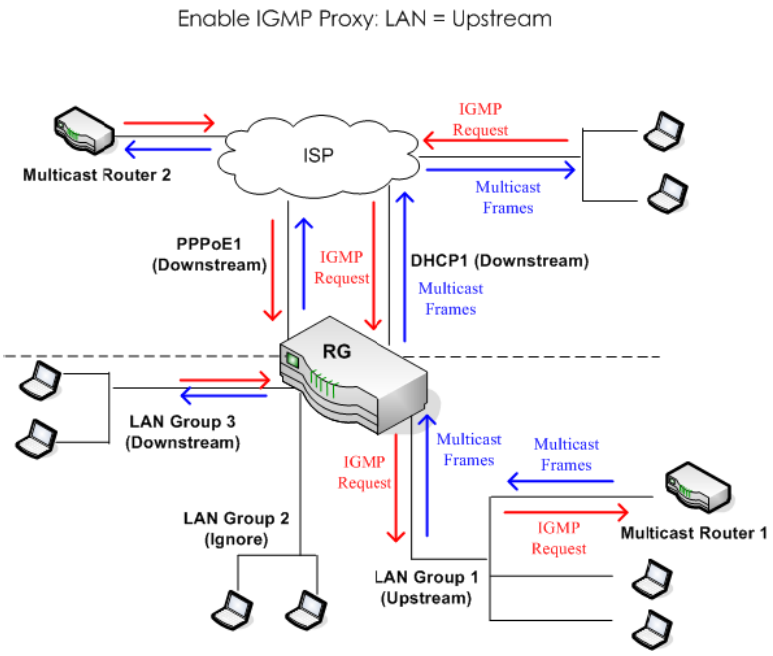
   - DHCP1: Upstream
   - PPPoE1: Ignore
   - LAN group 1: Downstream
   - LAN group 2: Ignore

5. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Configure a LAN interface as the Upstream Interface

The following procedure applies when the multicast server in on the LAN side. Hosts on the network can sent IGMP request from the WAN side through the LAN interface. And the LAN interface, acting as the upstream interface, forwards data multicast from the LAN-side multicast server to hosts on the network.



In the example shown above, there is a multicast router on the LAN side and LAN Group 1 interface is enabled as the upstream IGMP proxy. IGMP requests from the network are forwarded to LAN group 1 and multicast frames from multicast router 1 are forwarded to hosts on the LAN side (LAN group 3) and on the WAN side (DHCP1 and PPPoE1). No IGMP request nor data multicast are forwarded to LAN Group 2.

To configure your LAN group 1 as the upstream interface:

1. *From the navigation bar at the top of the screen click **Advanced***

2. *From the left hand navigation pane select **IGMP Proxy**.*

3. *Enter a check in the **Enable IGMP Proxy** check box*

4. *From the **Interface** **Upstream/Downstream/Ignore** dropdowns select the LAN groups to and whether they should allow IGMP proxies from upstream or downstream.*

   To match the example above:

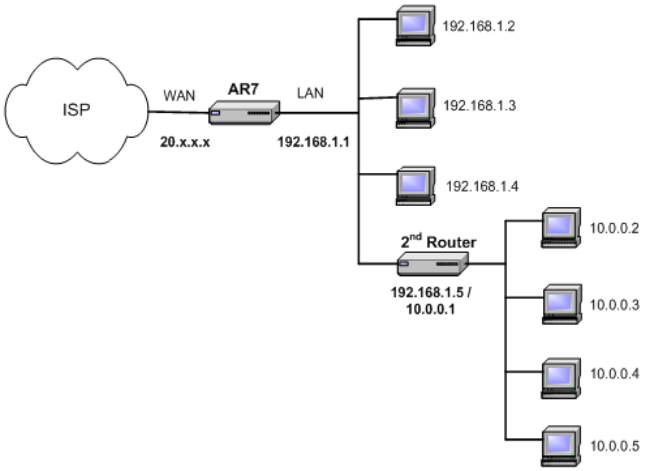
   - DHCP1: Downstream
   - PPPoE1: Downstream
   - LAN group 1: Upstream
   - LAN group 2: Ignore
   - LAN group 3: Downstream

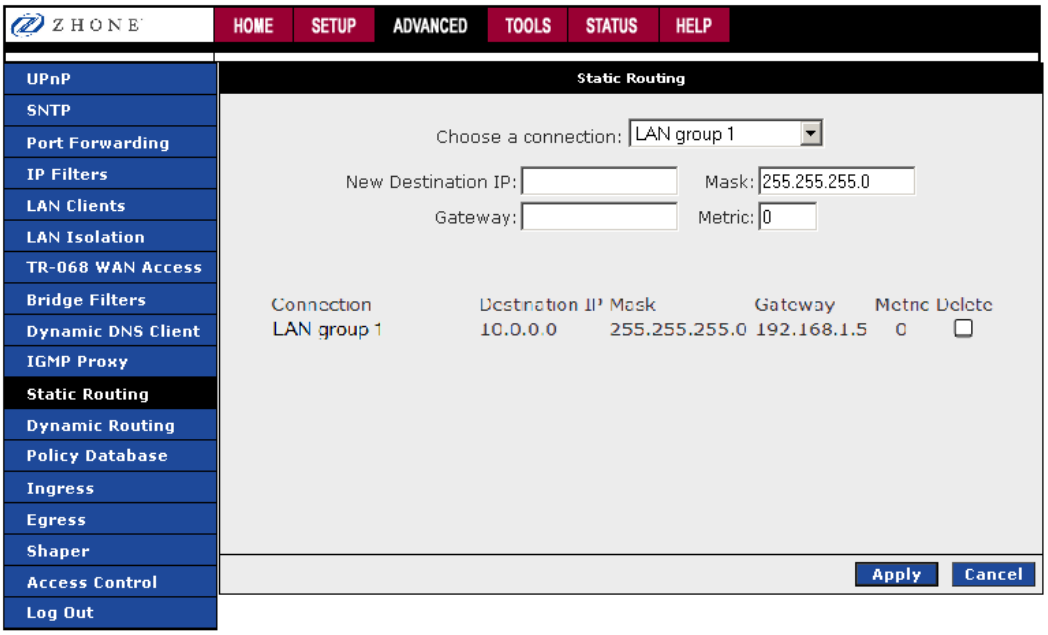
5. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Static Routing

The **Static Routing** page enables you to define routes for specific subnets on the WAN/LAN side. The 6381 RG allows you to manually program the RG's routing table. Up to 16 static routes can be added.





New Destination IP	The address of the remote LAN network or host to which you want to assign a static route. For a standard Class C IP domain, the network address is the first three fields of the New Destination IP, while the last field should be 0.
Subnet Mask	Identifies which portion of an IP address is the network portion, and which portion is the host portion. For a full Class C Subnet, the Subnet Mask is 255.255.255.0.
Gateway	Gateway is the IP address of the device that allows contact between the modem and the remote network or host.
Metric	Metric determines the maximum number of steps (hops) between network nodes that data packets will travel. A node is any device on the network (such as a router or switch).

To define a static route between networks:

6. *From the navigation bar at the top of the screen click **Advanced***

7. *From the left hand navigation pane select **Static Routing**.*

8. *From the **Choose a connection** dropdown select the connection which to add the static route.*

9. *In the **New Destination IP**, **Gateway**, **Mask**, and **Metric** text boxes, enter the appropriate information.*

   To match the example above:

   - **New Destination IP**: *10.0.0.0* (the network IP address of the subnet)
   - **Mask**: *255.255.255.0* (the subnet mask)
   - **Gateway**: *192.168.1.5* (the LAN-side IP address of the second router, through which the stations in the subnet access the network)
   - **Metric**: *0*

   You are telling the RG that a new subnet with an IP of *10.0.0.0* and a netmask of *255.255.255.0* has been added and can access the RG via station *192.168.1.5*. The metric is *0* since the subnet is one level down on the LAN.

10. *You can add up to 16 entries.*

11. *Click **Apply***

    The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Dynamic Routing

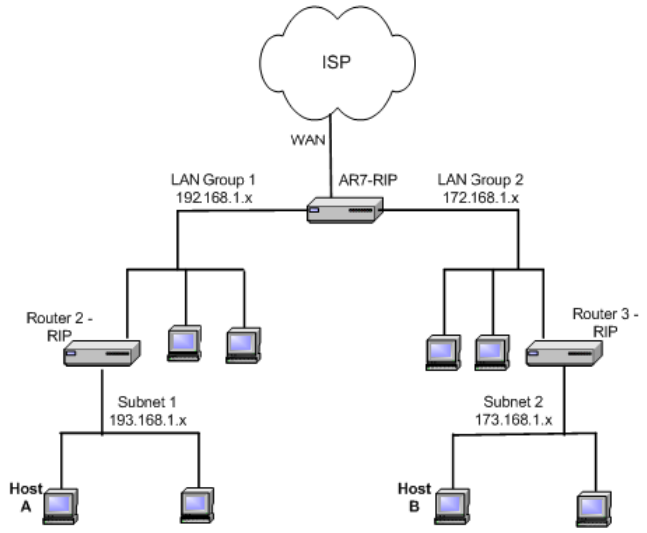
Dynamic Routing enables the 6381 RG to dynamically define routes for WAN and LAN subnets. Dynamic routing uses routing information protocol (RIP) for exchanging routing information with other routers in the network. It is supported across both WAN and LAN interfaces. Any RIP-enabled router sends out automatic update packets containing its own routing table on a periodic basis (every 30 secs). Similarly, it accepts such periodic updates from other routers and adds, deletes, or modifies routes in its own routing table accordingly. The router is also expected to receive requests for its routing table and respond accordingly. Use the Dynamic Routing page to define dynamic routing routes for the available interfaces.

Dynamic Routing allows the modem to automatically adjust to physical changes in the network. The modem, using the routing information protocol (RIP), determines the network packets' route based on the fewest number of hops between the source and the destination. The RIP protocol regularly broadcasts routing information to other modems on the network. The 6381 support RIP across both WAN and LAN interfaces.

RIP enabled routers send out updates of its routing table periodically and accepts updates from other routers to add, delete or modify routes in its routing table. The router will also send updates to its routing table upon request.

You can enable dynamic routing on all routers, so you do not have to manually enter the individual routes. To enable dynamic routing you need to enable all routers on this network and they should use the same protocol so they are able to communicate with each other.

To demonstrate the use of the dynamic routing feature, consider an expanded version of the network used in the static routing example (see **Static Routing**).

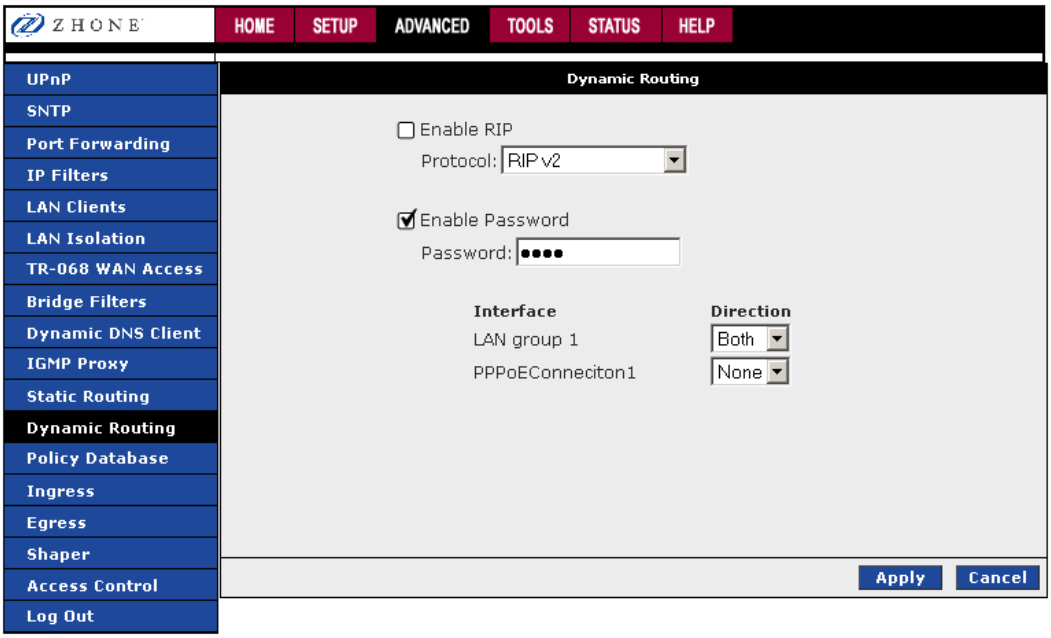


As shown above, you have a network with two LAN connections (192.168.1.x and 172.168.1.x), and each has a router and a subnet. How can host A in subnet 1 (193.168.1.x) talk to host B in subnet 2 (173.168.1.x)? You have two options:

• As shown using the static routing feature (see Static Routing), you can add both subnets to the routing table using the Static Routing page (two separate entries).

• You can enable dynamic routing on all routers without having to manually enter the individual routes. Keep in mind that you need to enable all routers on this network and they should use the

same protocol to be able to communicate with each other. The following procedure shows you how to enable and configure the dynamic routing feature on your RG.



Enable RIP	Enables/disables RIP.
Protocol	The following three RIP versions are available: • RIP v1 (UDP protocol) • RIP v2 (multicast protocol) • RIP v1 compatible (UDP protocol with multicast format) Note: Routers using RIP v1 or RIP v1-compatible protocol can talk to each other, but not to routers using RIP v2 protocol.
Enable Password	This is an optional field. RIP version v2 compatibility allows you to provide simple plain-text password-based authentication to RIP packets. This field is disabled if RIP v1 protocol is selected.
Password	The password can be up to 16 characters long.
Direction	Normally when RIP is enabled on a router, it dynamically learns/provides routes on all its configured interfaces. This parameter allows you to select the interfaces on which RIP is expected to learn and distribute routing information. This feature allows you to control how and which routes get distributed through the network. For example, by selecting In only mode, routes to private LAN networks are prevented from being sent over to the WAN-side router.

To enable dynamic routing:

1. *From the navigation bar at the top of the screen click* ***Advanced***

2. *From the left hand navigation pane select* ***Dynamic Routing****.*

3. *If appropriate, select* ***Enable RIP*** *and from the* ***Protocol*** *dropdown select the appropriate version of RIP.*

   The protocol is dependent upon the entire network. Most networks support RIP v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If Rip V2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If RIP V1 Compatible is selected, routing data will be sent in RIP v2 format using multicasting.

4. *For additional security with RIPv2 check **Enable Password** and enter a password.*

   Dynamic routing does not required the additional security. RIP v2 provides simple plain-text password-based authentication to RIP packets. The **Enable Password** field is disabled if RIP v1 protocol is selected.

5. *From the **Interface** **Direction** drop down select the appropriate direction for each interface.*

   Direction determines the direction that RIP routes will be updated.

In	The router will only incorporate received RIP information.
Out	The router will only send out RIP information.
Both	The router will incorporate received RIP information and send out updated RIP information.
None	Dynamic routing is disabled for this interface. Use when dynamic routing is enabled for other interfaces.

   To match the example above:

   - **LAN group 1**: *Both*
   - **LAN group 2**: *Both*

   You also need to enable dynamic routing on the routers 2 and 3.

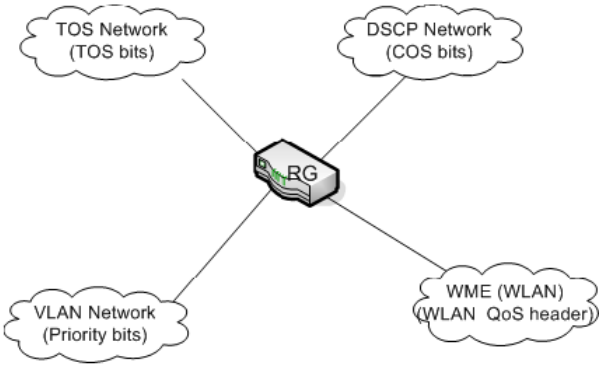
6. *Click **Apply***

   The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Quality of Service (QoS)

Quality of Service permits network administrators to prioritize how packets are handled, so that information with differing requirements, voice, video and data, will work properly. Network administrator configure routers to handle the different priority packets, however different networks use differing QoS marking.

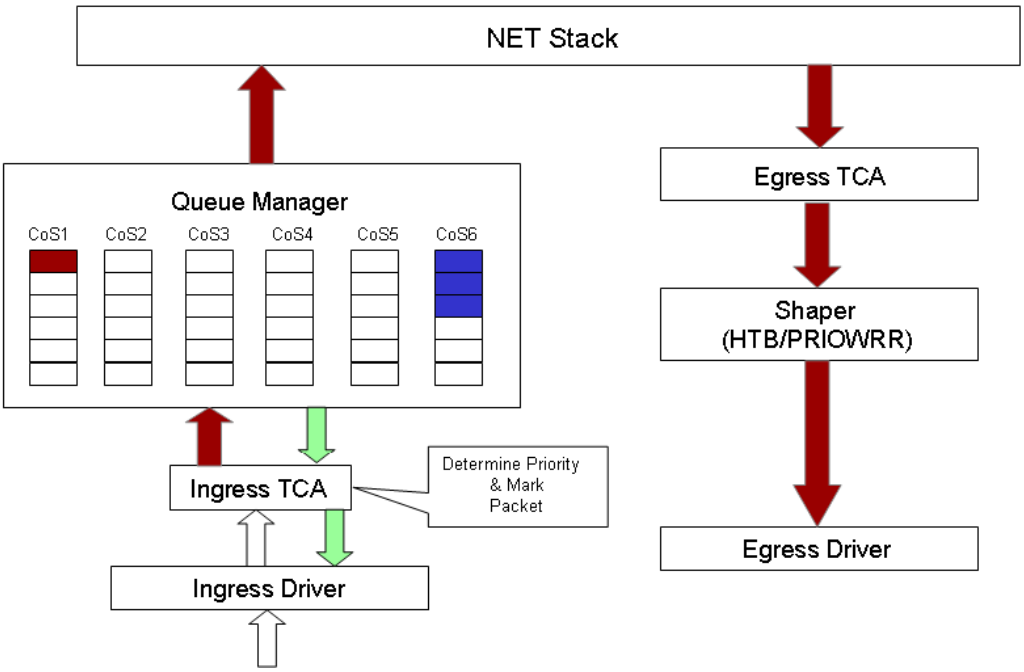
Note: QoS pages are for use by network administrators or Internet Service Providers (ISP). Users should not configure the Policy Database, Ingress, Egress or Shaper pages unless directed to do so by their ISP.



A ToS network (Type of Service) uses flags in the IP header to set priorities. A DSCP network (Differentiated Services Code Point) uses a field in an IP packet to describe different levels of service to assign to traffic. A VLAN (Virtual LAN as used with Level 2 bridges) uses priority bit in the VLAN header. WLAN use WLAN QoS header.

To work with the differing means of prioritizing packets and bandwidth, the 6381 maps the other priority schemes either to or from the CoS priority that it uses. Upon ingress (when the packet arrives on the WAN or LAN interface of the 6381) the priority is translated to CoS. Upon egress (when the packet leaves on the WAN or LAN interface of the 6381) the priority is translated from CoS. These mappings are set by a traffic conditioning agreement (TCA) for each interface: Ingress = domain mapping to CoS, Egress = CoS mapping to domain. There are also options for honoring (trusted mode) or not honoring (untrusted mode).

The 6381 uses a Class of Service (CoS) to define priorities. The 6381 uses six classes of CoS: CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. CoS1 is the highest priority and CoS6 the lowest.



Terms:

- Ingress: Packets arriving into the RG from a WAN/LAN interface.
- Egress: Packets sent from the RG to a WAN/LAN interface.
- Trusted mode: Honors the domain mapping (ToS byte, WME, WLAN user priority).
- Untrusted mode: Does not honor domain mapping. This is the default QoS setting.

Forwarding rules based on CoS are:

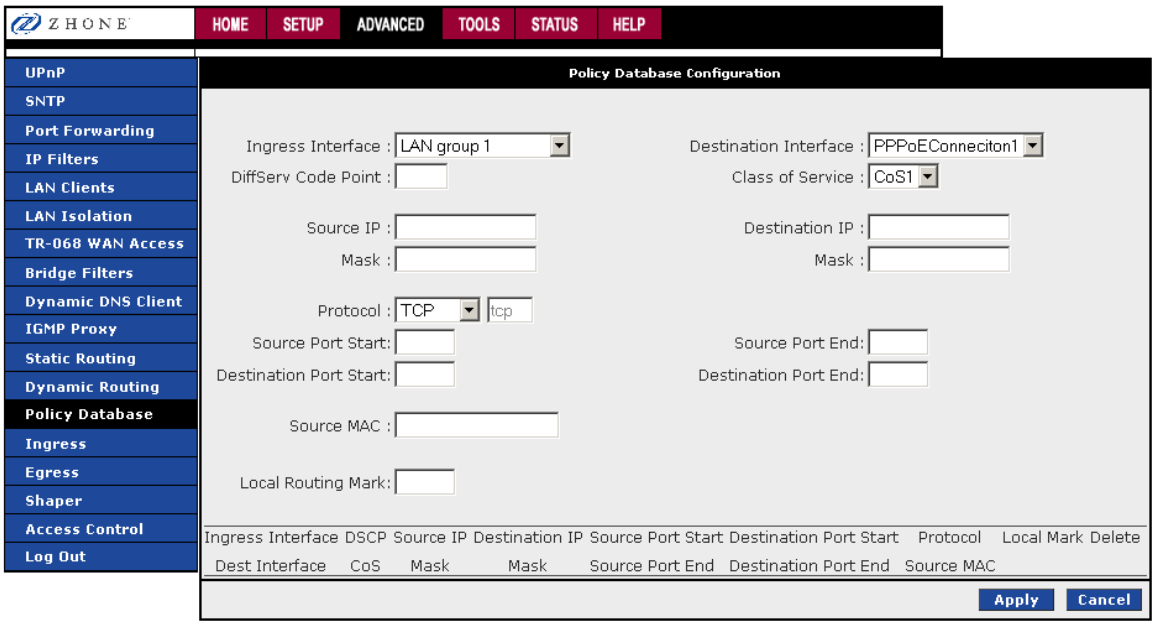
- CoS1 has absolute priority and is used for expedited forwarding (EF) traffic. This is always serviced till completion.
- CoS2-CoS5 are used for assured forwarding (AF) classes. They are serviced in a strict round robin manner using the following priority scheme: CoS2 > CoS3 > CoS4 > CoS5
- CoS6 is for best effort (BE) traffic. This is only serviced when there is no other class of service. If QoS is not enabled on your RG, all traffic will be treated as best effort.

QoS is defined in the following four GUI pages:

- **Policy Database** for configuring QoS for multiple connections
- **Ingress** for ingress mapping from an outside domain
- **Egress** for egress mapping to an outside domain
- **Shaping** for determining the servicing of the CoS queues including rate limiting.

Policy Database

The Policy Database page allows you to configure QoS for multiple WAN connections; you can classify packets based on fields in the packet. The **Ingress** and **Egress** pages allow you to configure QoS per interface.



Fields that can be configured for setting policies:

Field	Description
Ingress Interface	The incoming traffic interface for a Policy Routing rule. Selections include LAN interfaces, WAN interfaces, Locally generated (traffic), and not applicable. Examples of Locally generated traffic are: voice packets, packets generated by applications such as DNS, DHCP or other applications.
Destination Interface	The outgoing traffic interfaces for a Policy Routing rule. Selections include LAN Interfaces and WAN interfaces.
DiffServ Code Point	The diffServ code point (DSCP) field value ranges from 1 to 255. This field cannot be configured alone; additional fields like IP, Source MAC, and/or Ingress Interface should be configured.
Class of Service	The selections are (in the order of priority): CoS1, CoS2, CoS3, CoS4, CoS5, CoS6, and N/A.
Source IP	The IP address of the traffic source. (Wild cards are allowed.)
(Source) **Mask**	The source IP netmask. This field is required if the source IP has been entered. (Wild cards are allowed.)
Destination IP	The IP address of the traffic destination. (Wild cards are allowed.)
(Destination) **Mask**	The netmask of the destination. This field is required if the destination IP has been entered. (Wild cards are allowed.)
Protocol	The selections are TCP, UDP, ICMP, Specify, and none. If you choose Specify, you need to enter the protocol number in the box next to the Protocol field. This field cannot be configured alone; additional fields like IP, Source MAC, and/or Ingress Interface must also be configured. The **Protocol** field is also required if the source port or destination port has been entered.

Source Port	The source protocol port. You cannot configure this field without entering the protocol first.
Destination Port	The destination protocol port or port range. You cannot configure this field without entering the protocol first.
Source MAC	The MAC address of the traffic source.
Local Routing Mark	The **Local Routing Mark** field is enabled only when Locally Generated is selected in the **Ingress Interface** field. The mark for DNS traffic generated by different applications are described below: • Dynamic DNS: 0xE1 • Dynamic Proxy: 0xE2 • Web Server: 0xE3 • MSNTP: 0xE4 • DHCP Server: 0xE5 • IPtables Utility: 0xE6 • PPP Daemon: 0xE7 • IP Route: 0xE8 • ATM Library: 0xE9 • NET Tools: 0xEA • RIP: 0xEB • RIP v2: 0xEC • UPNP: 0xEE • Busybox Utility: 0xEF • Configuration Manager: 0xF0 • DropBear Utility: 0xF1 • Voice: 0

Policy routing if selected, uses the egress interface. The ingress interface is not applicable if policy routing is used.

Currently routing algorithms make decision based on destination address, i.e., only Destination IP address and subnet mask is supported. The Policy Routing page enables you to route packets on the basis of various fields in the packet. The following fields can be configured for Policy Routing:

- Destination IP address/mask
- Source IP address/mask
- Source MAC address
- Protocol (TCP, UDP, ICMP, etc)
- Source port
- Destination port
- Incoming interface
- DSCP

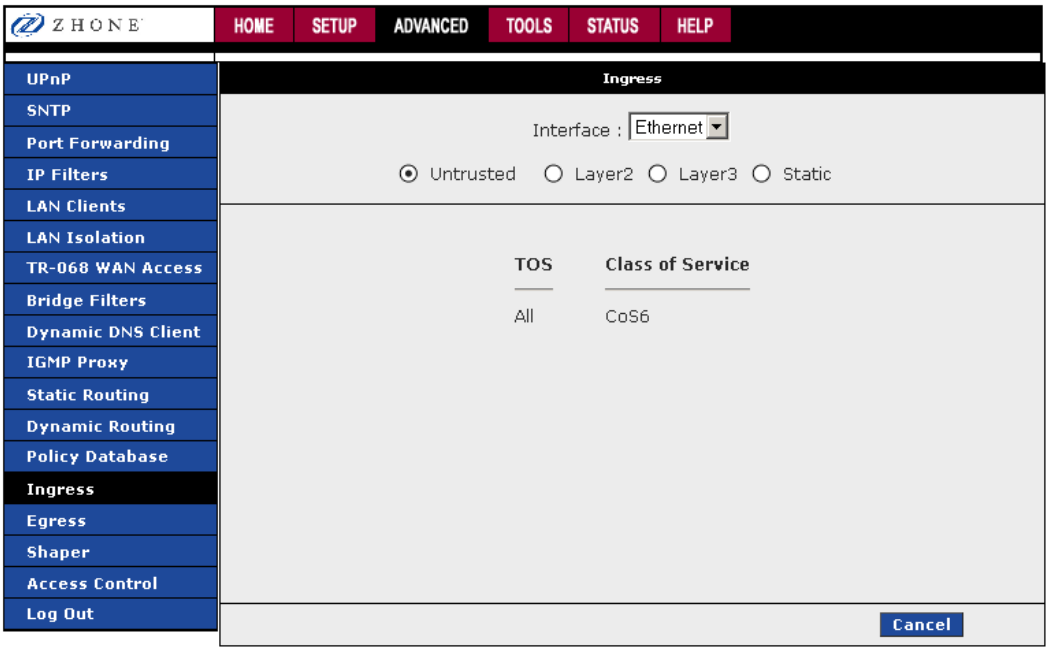
Ingress

Configure Quality of Service (QoS) for packets entering the device. Ingress denotes packets arriving into the 6381 from a WAN or LAN interface. The mappings are converted to CoS.

QoS can be configured on a per interface basis. Select the interface — USB, Ethernet, Bridge — which needs to be configured.

Ingress Untrusted Mode

Untrusted is the default Ingress page setting for all interfaces. In this mode, no domain mapping is honoured in the RG. All packets are treated as CoS6 (best effort)



Untrusted	The default Ingress page setting. No domain mapping is honoured. All packets are treated as CoS6, the best effort priority.
Layer2	Enables you to map an incoming packet with layer 2 (MAC addresses and bridging, rather than by IP address and routing) with VLAN segregation for priority. Only configurable on WAN interfaces.
Layer3	Enables you to map type of service (ToS) bits of incoming packets from the IP network to CoS for each WAN/LAN interface.
Static	Enables you to configure a static CoS for all packets received on a WAN or LAN interface.

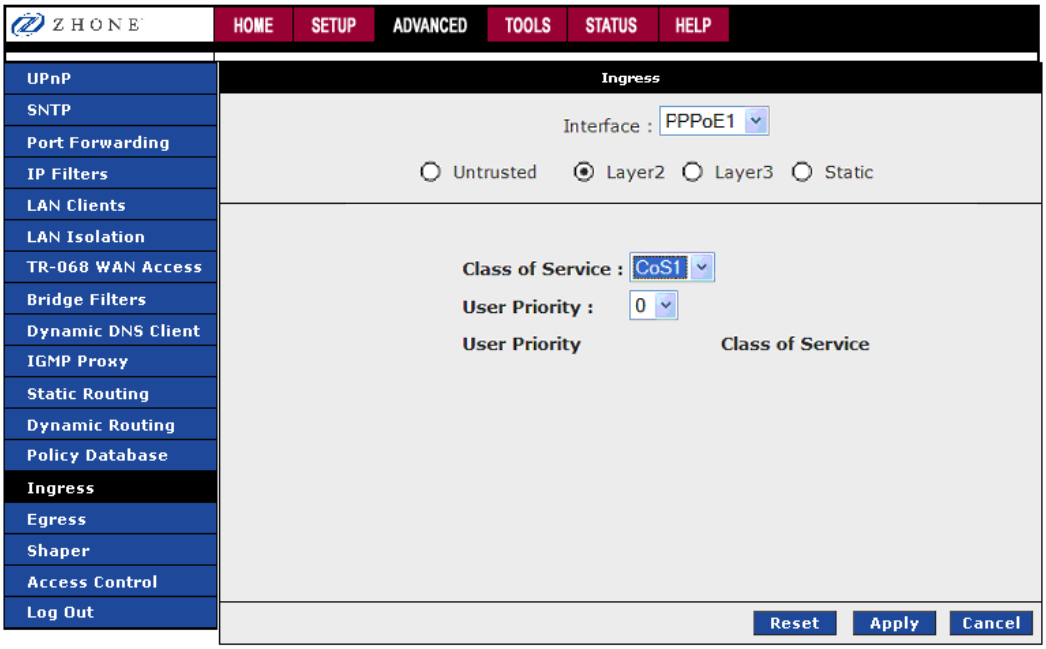
To configure QoS on ingress:

1. *From the navigation bar at the top of the screen click **Advanced***
2. *From the left hand navigation pane select **Ingress**.*
3. *On the **Ingress** page, select the interface from the **Interface** drop down.*
4. *Select the appropriate **Untrusted**, **Layer2**, **Layer3**, or **Static** radio button.*
5. *Click **Apply***

The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Ingress Layer 2 Configuration

Layer 2 page enables you to map an incoming packet with VLAN priority to CoS. This feature is only configurable on the WAN interfaces as VLAN is only supported on the WAN side in the current software release.



Interface	Select the WAN interface here to configure the CoS for incoming traffic. Only WAN interface can be selected as VLAN is currently supported only on the WAN side.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
User Priority	The selections are 0, 1, 2, 3, 4, 5, 6, 7.

To configure Ingress Layer 2 to CoS:

1. *From **Interface** drop-down box, select PPPoE to configure QoS on this WAN interface.*

2. *Select **CoS1** in **Class of Service** and **5** in **Priority Bits**.*

   Any packets with priority marking 5 is mapped to CoS1, the highest priority that is normally given to the voice packets.

3. *Click **Apply** to temporarily activate the settings.*

4. *Select **CoS2** in the **Class of Service** field and **1** in the **Priority Bits** field.*

   Any packets that have priority bits of 1 are mapped to CoS2, which is the second highest priority. This is given to the high priority packets such as video.

5. *Click **Apply** to temporarily activate the settings.*

The changes take effect when you click Apply; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

6. *Repeat step 2-5 to add more rules to PPPoE1.*

   Up to eight rules can be configured for each interface.

   Any priority bits that have not been mapped to a CoS default to CoS6, the lowest priority.

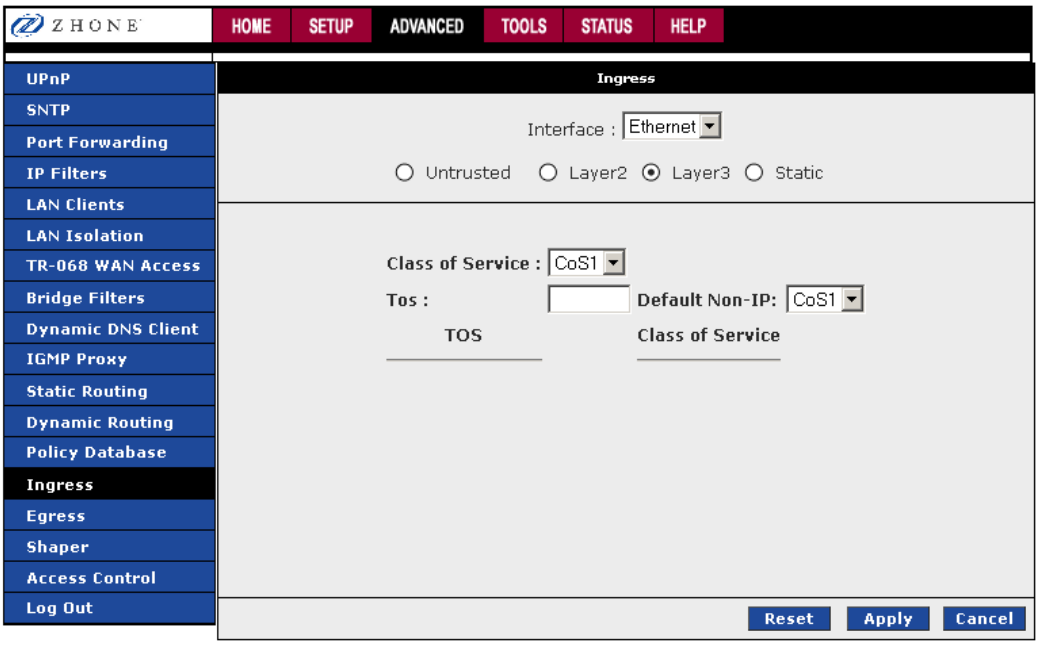
7. *Repeat step 1-6 to create rules to another WAN interface.*

   Any WAN interface that is not configured has the default Untrusted mode.

8. *To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page, click **Save All**.*

Ingress Layer 3 Configuration

The Layer 3 page allows you to map ToS bits of incoming packets from the IP network to CoS for each WAN/LAN interface.



Interface	For both WAN and LAN interfaces, you can configure QoS for layer 3 (IP) data traffic.
Class of Service	This CoS field allows you to map incoming layer 3 WAN/LAN packets to one of the following CoS (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.
ToS	The type of service field takes values from 0 to 255.
Default Non IP	A static CoS can be assigned to all layer 3 incoming packets (per interface) that do not have an IP header, such as PPP control packets and ARP packets. The default is CoS1 (recommended).

To configure Ingress Layer 3 to CoS:

1. *From **Interface** drop-down box, select **LAN Group 1** to configure QoS on this interface.*

2. *Select **CoS1** in **Class of Service** and enter **22** in Type of Service (**ToS**).*

Any incoming packet from LAN Group 1 (layer 3) with a ToS of 22 is mapped to CoS1, the highest priority, which is normally given to the voice packets.

3. *Leave the default value CoS1 in Default Non-IP.*

   Any incoming packet from LAN Group 1 without an IP is mapped to CoS1, the highest priority.

4. *Click **Apply** to temporarily activate the settings.*

   The changes take effect when you click **Apply**; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

5. *Repeat step 2-4 to add more rules to LAN Group 1.*

   Up to 255 rules can be configured for each interface.

   Any ToS that have not been mapped to a CoS is treated as CoS6, the lowest priority.

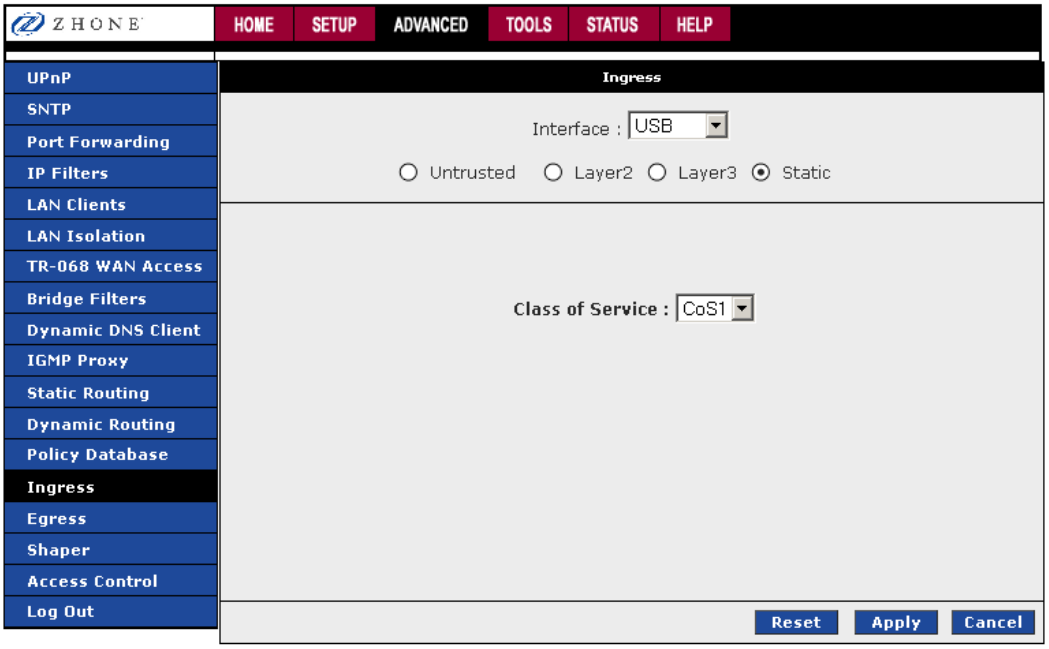
6. *Repeat step 1-5 to create rules to another WAN/LAN interface.*

   Any WAN/LAN interface that is not configured has the default Untrusted mode.

7. *To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page, click **Save All**.*

Ingress Static Configuration

The Ingress - Static page enables you to configure a static CoS for all packets received on a WAN or LAN interface.



To configure Ingress static QoS settings:

1. *At the **Interface** drop-down box, select **Ethernet**.*

You are configuring QoS on this interface only. Any WAN/LAN interface that is not configured has the default Untrusted mode.

2. *Select **CoS1** in **Class of Service**.*

   All incoming traffic from the Ethernet interface receives CoS1, the highest priority.

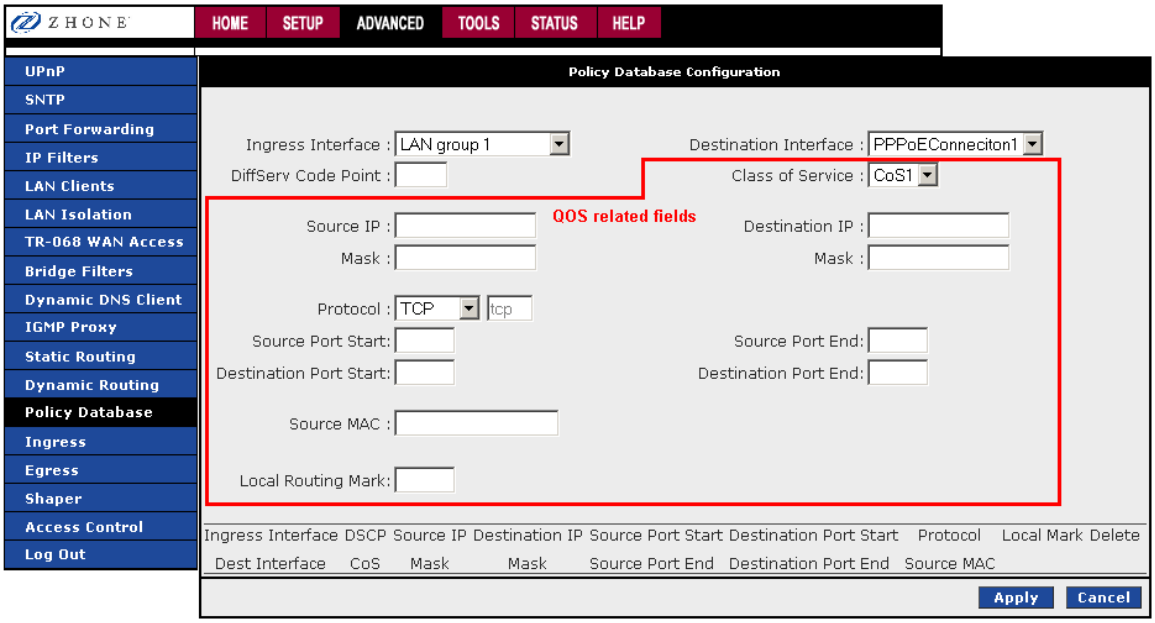
3. *Click **Apply** to temporarily activate the settings.*

   The changes take effect when you click Apply; however, if the RG configuration is not saved, these changes will be lost upon RG reboot.

4. *To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page, click **Save All**.*

Ingress Payload Database Configuration

The Policy Database Configuration page enables you to configure QoS payload database and policy routing.



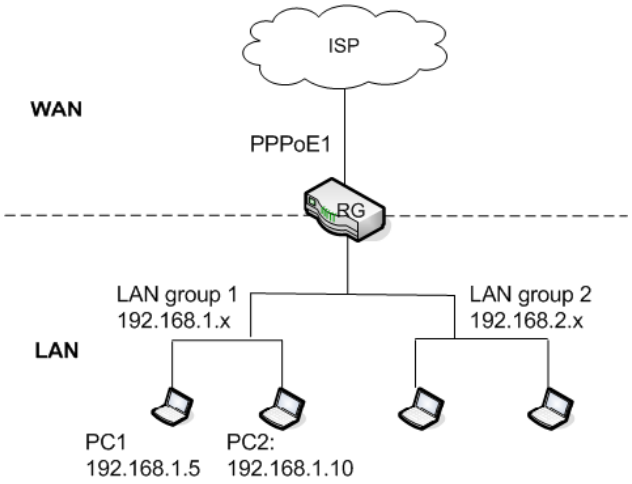
QoS can be configured in the Ingress and Egress pages on a per interface basis. The Policy Database page enables you to classify packets on the basis of various fields in the packet.

The following fields can be configured for QoS:

- CoS
- Source IP address/mask
- Destination IP address/mask
- Protocol
- Source port start
- Source port end
- Destination port start
- Destination port end
- Source Mac address

Ingress Interface	This field is applicable for policy routing configuration only (see Policy Database)
Destination Interface	This field is applicable for policy routing configuration only (see Policy Database)
DiffServ Code Point	This field is applicable for policy routing configuration only (see Policy Database)
Class of Service	The selections are (in the order of priority): CoS1, CoS2, CoS3, CoS4, CoS5, CoS6, and N/A.
Source IP	The IP address of the traffic source.
Mask	The source IP netmask. This field is required if the source IP has been entered.
Destination IP	The IP address of the traffic destination.
Mask	The netmask of the destination. This field is required if the destination IP has been entered.
Protocol	The selections are TCP, UDP, ICMP, Specify, and none. If you choose Specify, you need to enter the protocol number in the box next to the Protocol field. This field cannot be configured alone, additional fields like **IP** and/or **Source MAC** should be configured. This field is also required if the source port or destination port has been entered.
Source Port Start	The starting port of the source protocol. You cannot configure this field without entering the protocol first.
Source Port End	The ending port of the source protocol. You cannot configure this field without entering the protocol first.
Destination Port Start	The starting port of the destination protocol. You cannot configure this field without entering the protocol first.
Destination Port End	The ending port of the destination protocol. You cannot configure this field without entering the protocol first.
Source MAC	The MAC address of the traffic source.
Local Routing Mark	This field is applicable for policy routing configuration only (see Policy Database)

To configure QoS to give PC1 traffic over PC2 traffic



In our example there are two PCs in LAN group 1. You use PC 1 (192.168.1.5) to download movies and PC 2 (192.168.1.10) to surf the internet.

1. *In the **Ingress** field, select **N/A** (not applicable).*

   The field is applicable for policy routing only.

2. *In the **Destination Interface** field, select **N/A**.*

The field is applicable for policy routing only.

3. *In the **Class of Service** field, leave the default **CoS1**.*

4. *In the **Destination IP** field, enter **192.168.1.5**.*

5. *In the **Destination IP Mask** field, enter **255.255.255.255**.*

6. *In the **Protocol** field, leave the default selection, **TCP**.*

7. *Click **Apply** to temporarily activate the settings on the page.*

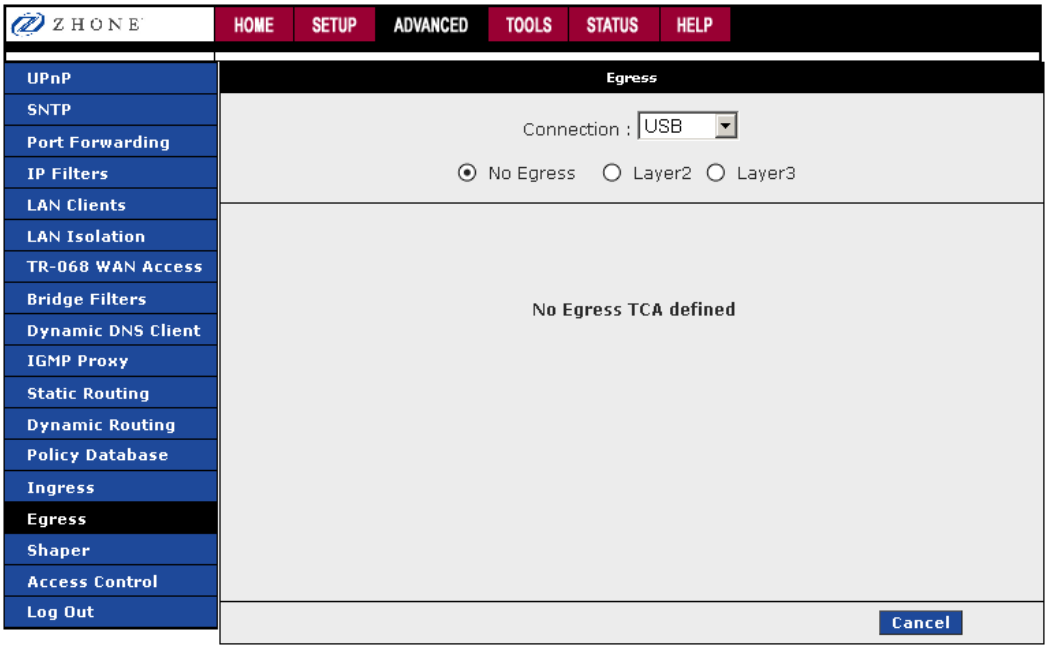
   The rule is generated at the bottom of the page.

8. *To make the change permanent, click **Tools** and select **System Commands**. On the **System Commands** page, click **Save All**.*

Egress

Egress denotes the direction of a frame exiting an interface. For outgoing packets the CoS marking needs to be translated to mapping understood by the network domains.

No Egress	The default **Egress** page setting. Domain mappings of the packets are not altered
Layer2	Enables you to map an outgoing packet to user priority bits which are honoured by the VLAN bridged network. Only supported on WAN interfaces.
Layer3	Enables you to map CoS to ToS bits so priority marking of outgoing packets work properly on IP networks.



To configure QoS on egress:

1. *From the navigation bar at the top of the screen click **Advanced***
2. *From the left hand navigation pane select **Egress**.*
3. *On the **Egress** page, select the interface from the **Interface** drop down.*
4. *Select the appropriate **No Egress**, **Layer2**, or **Layer3** radio button.*
5. *Click **Apply***

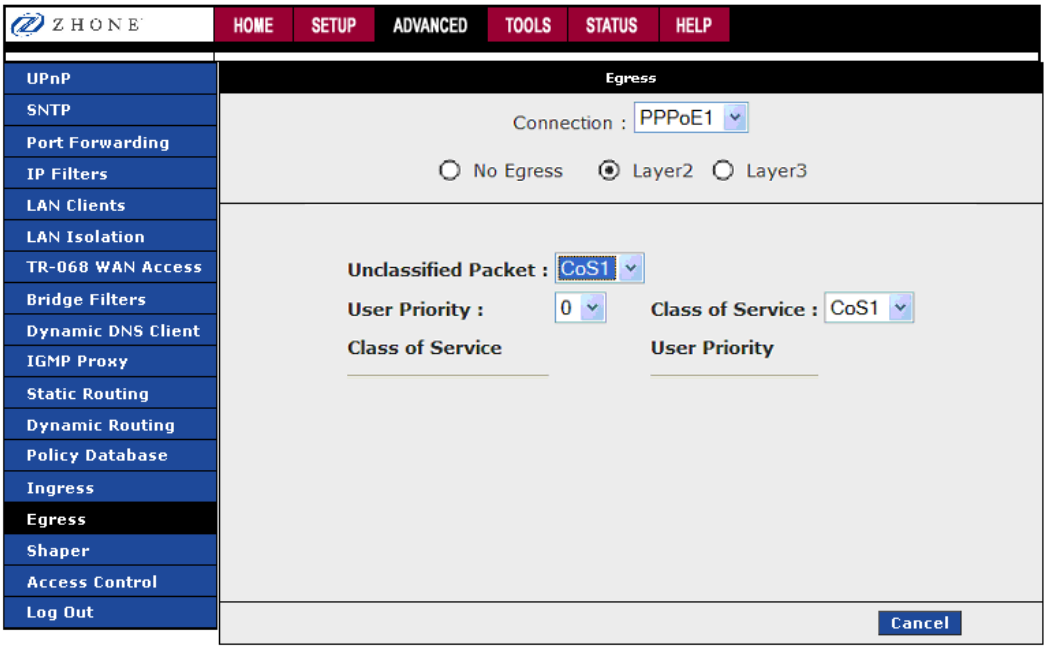
   The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

No Egress Mode

The default Egress page setting for all interfaces is **No Egress**. In this mode, the domain mappings of the packets are untouched.

Egress Layer 2 Configuration

The Egress Layer 2 feature enables you to map the CoS of an outgoing packet to user priority bits, which is honored by the VLAN network. This feature is available on the WAN interface only.



Interface	Select the WAN/LAN interface here to configure the QoS for outgoing traffic to the IP network.
Default Non-IP	Locally generated packets (such as ARP packets) do not have a CoS marking. You can define the CoS for all unclassified outgoing packets on layer 3 using this field. The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6. The default value is CoS1 (recommended).
Translated ToS	The Type of Service field takes values from 1 to 255. The selections are 0, 1, 2, 3, 4, 5, 6, 7.
Class of Service	The selections are (in the order of descending priority): CoS1, CoS2, CoS3, CoS4, CoS5, and CoS6.

WLAN QoS Support

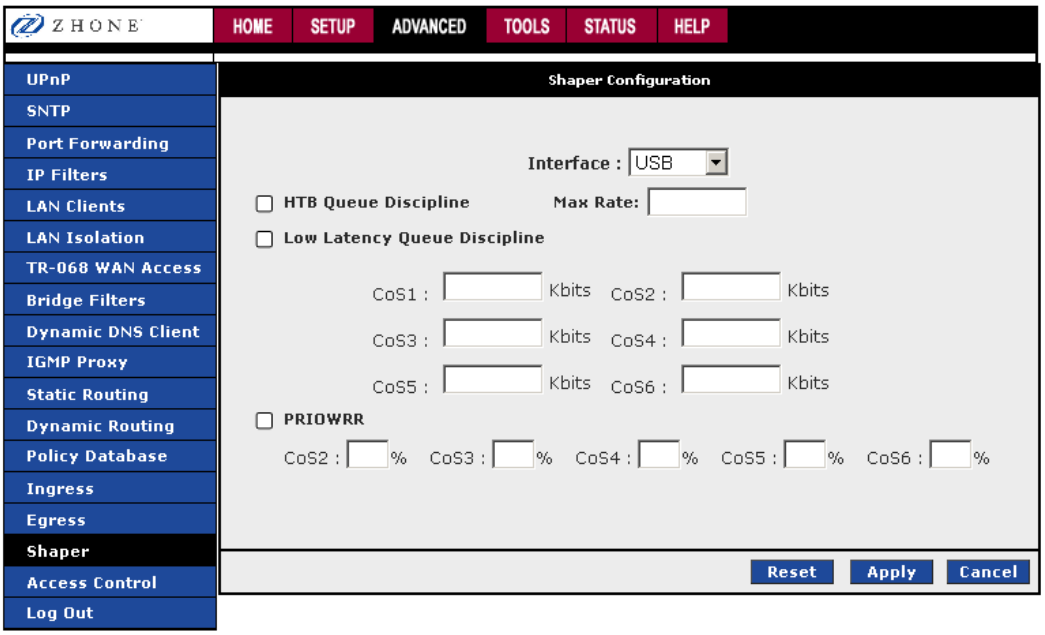
The WLAN QoS is supported; however, it is hard-coded and is not configurable on the Ingress and Egress pages.

User Priority	Class of Service	WME Priority	DSCP Map
0 (Best-Effort)	CoS5	0	0 (0x0)
1 (Background)	CoS6	1	8 (0x20)
2 (Background)	CoS6	2	16 (0x40)
3 (Best-Effort)	CoS5	3	24 (0x60)
4 (Video)	CoS2	4	32 (0x80)
5 (Video)	CoS2	5	40 (0xA0)
6 (Voice)	CoS1	6	48 (0xC0)
7 (Voice)	CoS1	7	56 (0xE0)

There is no shaper support on WLAN interface.

Shaper

The shaper provides a way of determining priorities of different traffic classes. Three shaper algorithms are supported: HTB (hierarchical token bucket), Low Latency Queue Discipline, and PRIOWRR (priority based round robin).



HTB Shapes the traffic of a class over the specific interface. All CoSx (where x= 1 to 6) is assigned a specific rate that data will be shaped to meet; for example, if CoS1 is 100Kbps even 300Kbps of data is received on the interface only 100Kbps will be sent. Of the **Max Rate** entered rates for each CoS channel may be configured. If Max Rate is 300Kbps, **Cos1** is configured for 100Kbps, **CoS2** and **CoS3** are configured for 150Kbps each and CoS6 for 300Kbps. CoS6 can use the whole 300Kbps of bandwidth only when there are no CoS1, CoS2, or CoS3 packets.

Low Latency CoS1 is not rate limited, so the **CoS1** field is disable when **Low Latency Queue Discipline** is checked. CoS1 takes priority (much as if CoS1 was set to **Max Rate**) If

CoS2 is configured for 100Kbs and CoS6 for 300Kbps, CoS2 takes 100Kbps when there are no CoS1 packets. CoS6 can take 300Kbps when there are no CoS1 or CoS2 packets.

PRIOWRR Queues CoS2 to CoS6 are serviced round robin. CoS1 has the highest priority and is not controlled by the WRR data shaping algorithm.

PRIOWRR does not use **Max Rate**. Percentages of packets received are sent out. CoS2 to CoS6 will not be serviced while there are CoS1 packets. CoS2 to CoS6 will share based on the percentages of the packets. PRIOWRR is similar to Low Latency except that Low Latency is rate based and PRIOWRR is packet based.

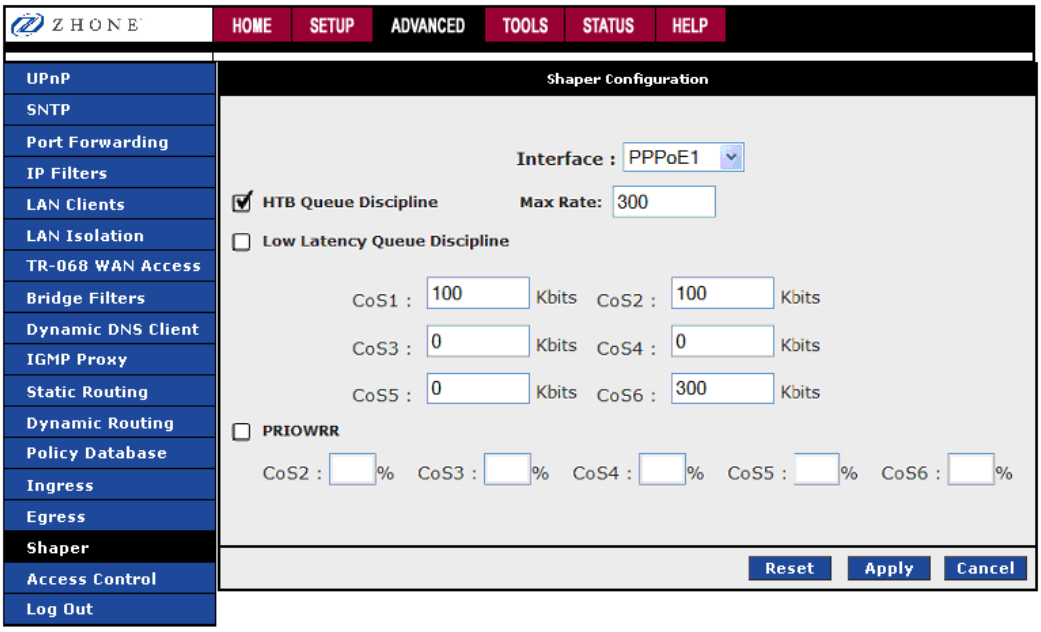
To configure Shaper:

1. *From the navigation bar at the top of the screen click **Advanced***
2. *From the left hand navigation pane select **Shaper**.*
3. *On the **Shaper** page, select the interface from the **Interface** drop down.*
4. *Select the appropriate shaper algorithm (**HTB**, **Low Latency** or **PRIOWRR**) and adjust rates as appropriate.*
5. *Click **Apply***

   The Apply button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

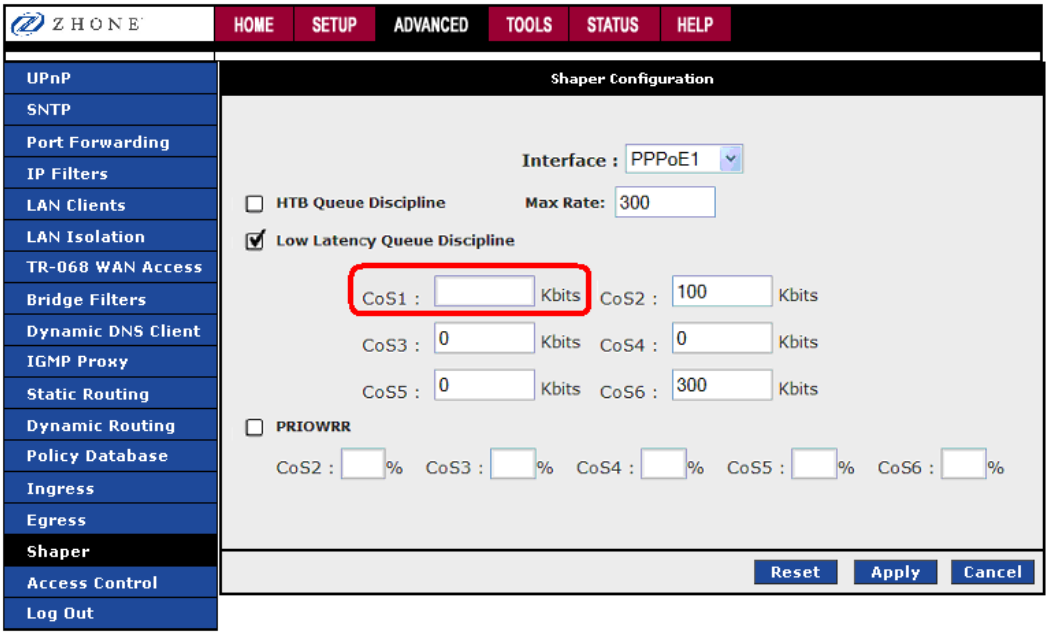
Example 1: HTB Queue Discipline Enabled

In the example below, HTB Queue Discipline is enabled. The PPPoE1 connection has a total of 300 kbits of bandwidth, of which 100 kbits is given to CoS1 and another 100 kbits is given to CoS2. When there is no CoS1 or CoS2 packets, CoS6 packets have the whole 300 kbits of bandwidth.



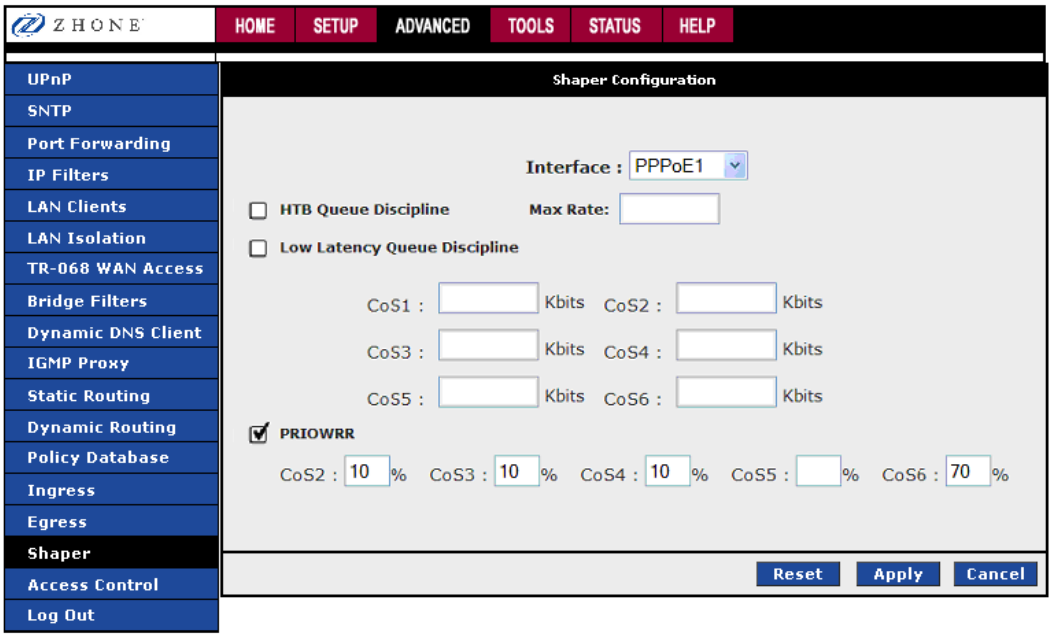
Example 2: Low Latency Queue Discipline Enabled

In this example Low Latency Queue Discipline is enabled. CoS1 is not rate controlled (hence the field is disabled). CoS2 takes 100 kbits when there are no CoS1 packets. CoS6 has 300 kbits when there are no CoS1 or CoS2 packets. This is similar to the HTB queue discipline as they are both rate-based algorithm, except that CoS1 is handled differently.



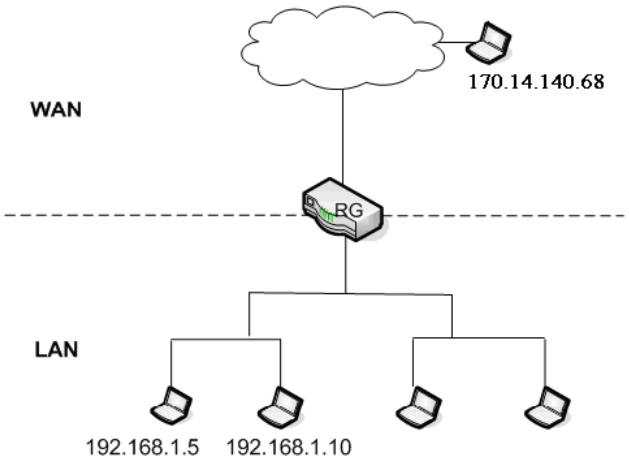
Example 3: PRIOWRR Enabled

In this third example, PRIOWRR is enabled. Since PRIOWRR operates only on the number of packets being transmitted, the max rate field has been disabled. Only percentage can be assigned to the CoS2 - CoS6. CoS1 is not rate controlled (hence the field is not displayed). When there are no CoS1 packets, CoS2, CoS3, CoS4 each has 10 percent, and CoS6 has 70 percent. This is similarly to the Low Latency Queue discipline, except that one is packet-based, and the other is rate-based.

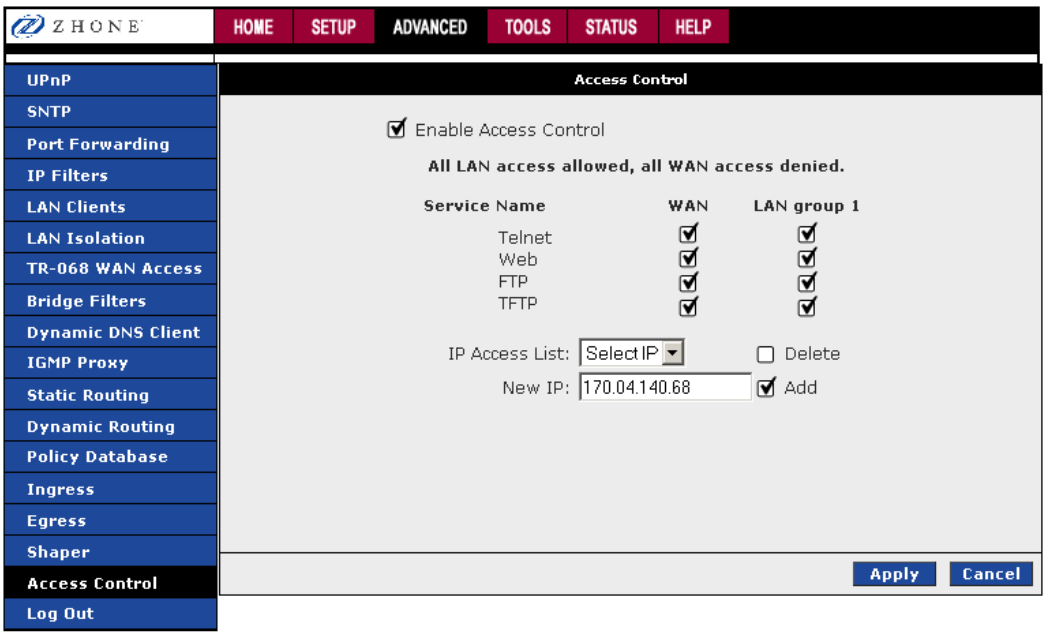


Access Control

The Access Control page provides a means to allow Telnet, Web, FTP (file transfer protocol) or TFTP (trivial FTP) access to the 6381 RG for devices which are either on the WAN or LAN sides of the 6381 RG.



When **Enable Access Control** is checked, the devices in the **IP Access List**, designated by their **IP Addresses** will have the access defined in the **WAN** or **LAN group 1** column.



To configure access to the 6381 RG:

1. *From the navigation bar at the top of the screen click **Advanced***
2. *From the left hand navigation pane select **Access Control**.*
3. *To enable access to the 6381 check **Enable Access Control**.*
4. *To enable access to a device within your network, select the **Telnet**, **Web**, **FTP** or **TFTP** options for **LAN group 1**, and add the IP for that address to the **IP Access List***

5. *Click **Apply***

6. *To enable access to a device outside your network (on the WAN side of the 6381 RG), select the **Telnet**, **Web**, **FTP** or **TFTP** options for **WAN**, and add the IP for that address to the **IP Access List***

7. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Chapter 4 Tools

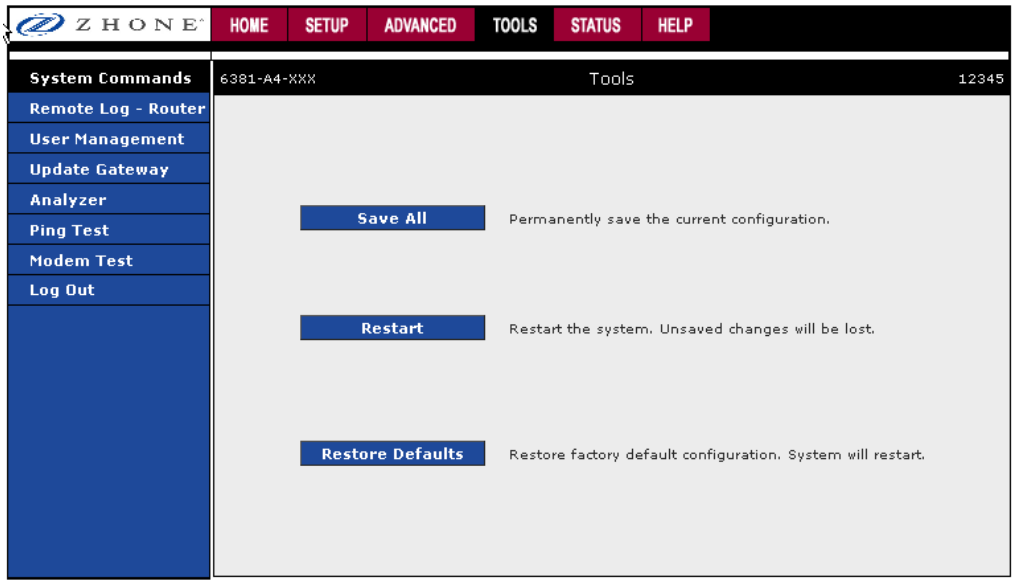
This section provides access to the following pages—

- System Commands
- Remote Log—Modem
- User Management
- Analyzer
- Ping Test
- Modem Test

System Commands

To make the changes permanent, click on **Tools** (at the top of the page) and select **System Commands**. The following commands are used to configure the modem:

- **Save all:** Press this button in order to permanently save the current configuration of the modem. If you do re-start the system without saving your configuration, the modem will revert back to the previously saved configuration.
- **Restart:** Use this button to re-start the system. If you have not saved your configurations, the modem will revert back to the previously saved configuration upon re-starting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
- **Restore Defaults:** Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

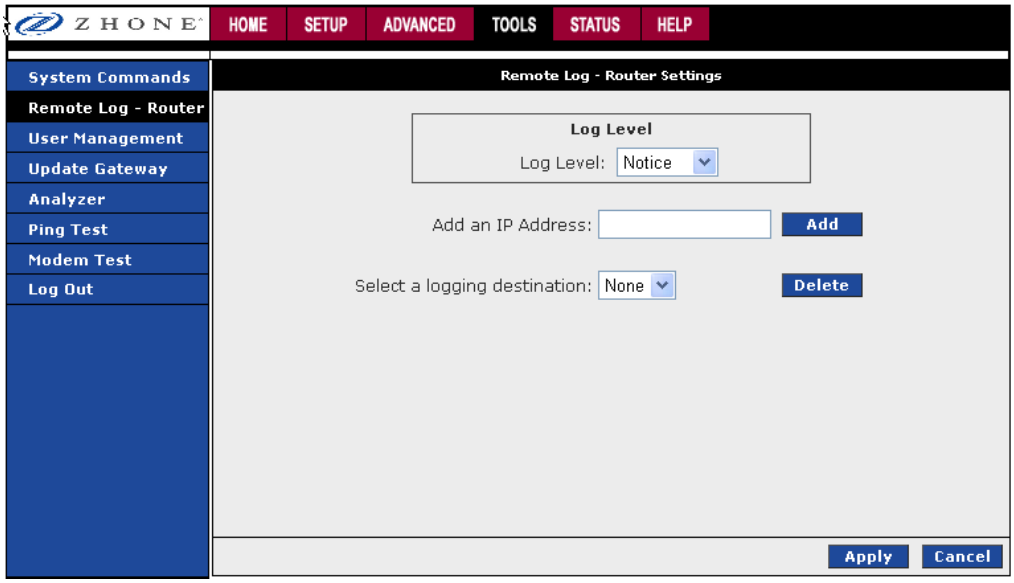


Remote Log - Router

The remote log feature forwards all logged information to a remote PC. The type of information forwarded to the remote PC depends upon the Log level. Each log message is assigned a severity level, which indicates how seriously the triggering event affects router functions. When you configure logging, you must specify a severity level for each facility. Messages that belong to the facility which are rated at that level or higher are logged to the destination.

For PPPoE and PPPoA connections, you can select Debug in the Log Level field if you want to log the connection information. This is helpful when trying to debug connection problems. The remote log feature allows you to forward all logged information to one (or more) remote syslog server. The type of information forwarded to the remote server depends upon the Log level. Each log message is assigned a severity level, which indicates how seriously the triggering event affects RG functions. When you configure logging, you must specify a severity level. Log messages that are rated at that level or higher are sent to the syslog server and can be viewed using the syslog server application, which can be downloaded from the web or comes with a linux machine.

You can display the system log for your RG by clicking the **System Log** link from the Status main page.



To forward logging information:

1. *From the navigation bar at the top of the screen click **Tools***
2. *From the left hand navigation pane select **Remote Log - Router**.*
3. *In the **Log Level** drop down select the severity level to notify the address*

Severity Level	Description
Panic	System panic or other condition that causes the router to stop functioning.
Alert	Conditions that require immediate correction, such as a corrupted system database.
Critical	Potentially critical conditions, such as hard drive errors.
Error	Error conditions that generally have less serious consequences than errors in

	the panic, alert, and critical levels.
Warning	Conditions that warrant monitoring.
Notice	Conditions that are not errors but might warrant special handling.
Info	Events or non-error conditions of interest.
Debug	Software debugging messages. Specify this level only if so directed by your technical support representative.

4. *In the **Add an IP Address** text box enter the destination IP address (if not already existing).*

5. *From the **Select a logging destination** drop down, select a destination for the severity level.*

6. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

For PPPoE and PPPoA connections, select **Debug** if you want to log the connection information. This is helpful when trying to debug connection problems. Verify that the Debug box is checked on the PPPoA or PPPoE Connection Setup screen.

User Management

You can change your modem's username, password and the idle timeout; you will need to log back onto the modem once the timeout expires.

If you forget your password, press and hold the reset to factory defaults button for 10 seconds. The modem will reset to its factory default configuration and all custom configurations will be lost.

To change user management settings:

1. *From the navigation bar at the top of the screen click **Tools***

2. *From the left hand navigation pane select **User Management**.*

3. *To change the user name (from the default "Admin"): in the **User Name** text box enter a new user name for the device.*

4. *To change the password (from the default "Admin"): In the **Password** text box enter the new password, then again in the **Confirm Password** text box.*

5. *To change the idle timeout settings: in the **Idle Timeout** text box enter the idle timeout duration in minutes.*

6. *Click **Apply***

   The **Apply** button will temporarily save this connection. To make the change permanent, click **Tools** (at the top of the page) and select **System Commands**. On the **System Commands** page, click **Save All**.

Update Gateway

You can remotely update the router's firmware from the web interface.

To upgrade the firmware

1. *From the navigation bar at the top of the screen click* ***Tools***

2. *From the left hand navigation pane select* ***Update Gateway****.*

3. *Click* ***Update Gateway****.*

4. *To upgrade the firmware, click* ***Browse****, find the firmware file to download.*

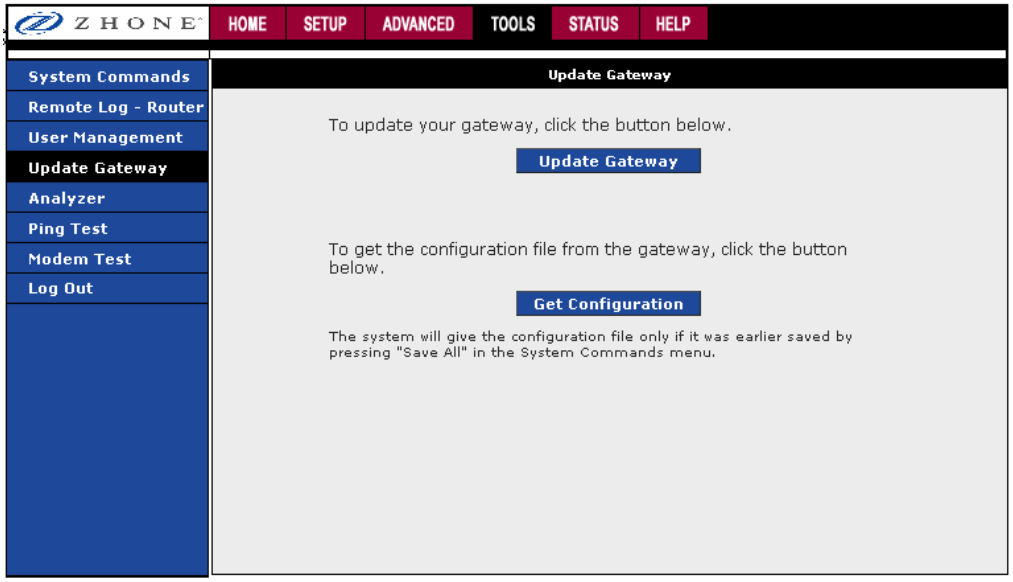
   Make sure this is the correct file.

5. *Click* ***Upgrade Firmware****.*

   Once the upgrade is complete the modem will reboot. You will need to log back onto the modem after the firmware upgrade is complete.

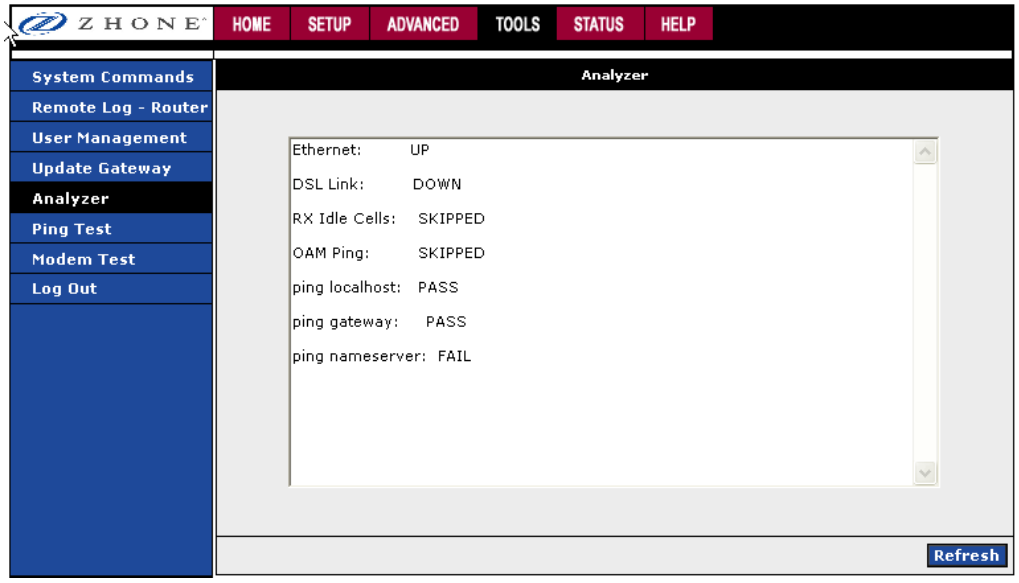
The firmware upgrade should take less than 5 minutes to complete. If it takes longer than 5 minutes, something has gone wrong.

Note: Do not remove power from the modem during the firmware upgrade procedure.



Analyzer

This section shows a diagnosis of the various statuses.

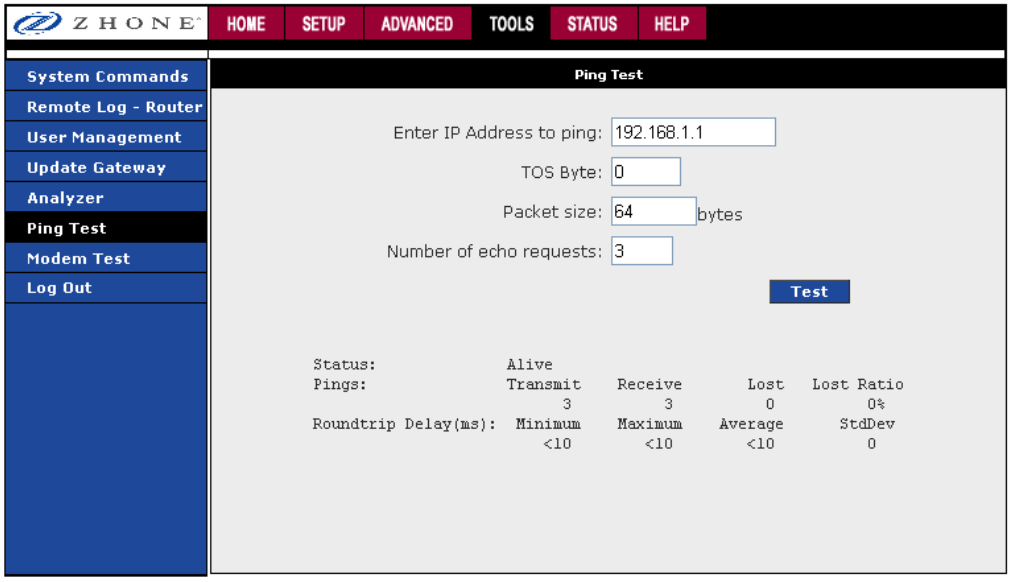


Ping Test

Once you have your modem configured, make sure you can ping the network. You can get to the Ping web page by going to the Home screen, under the Tools title, and clicking Ping Test. Type the target address that you want to ping. If you have your PC connected to the modem via the default DHCP configuration, you should be able to ping the network address 192.168.1.1.

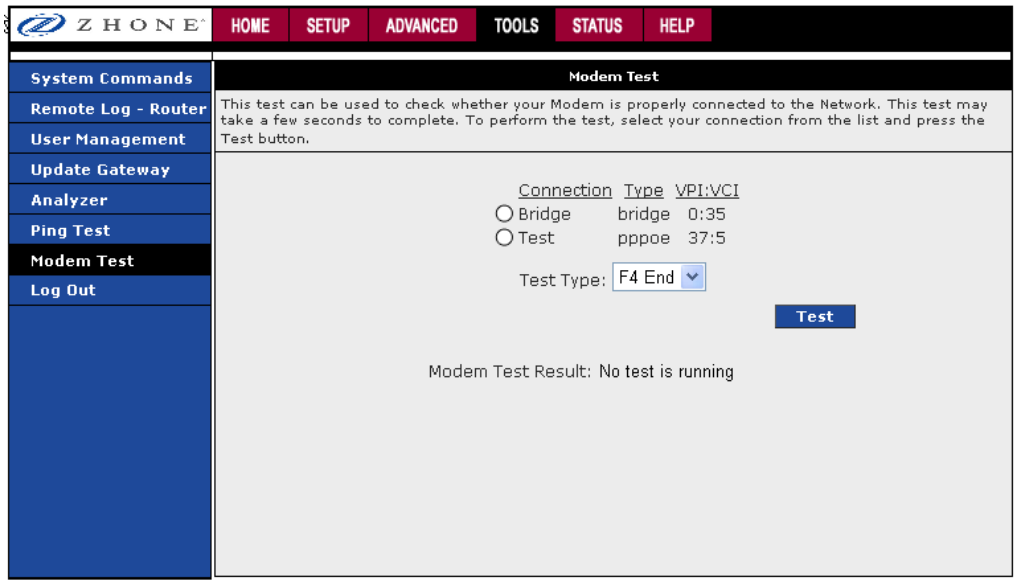
If your ISP has provided their server address you can try to ping the address. If the pings for both the WAN and the LAN side complete, and you have the proper protocols configured, you should be able to access the Internet.

By default when you select ping test, the modem will ping itself 3 times. If this first ping test does not pass, the TCP/IP protocol is not loaded for some reason, and then you should restart the modem.



Modem Test

The Modem Test is used to check whether your modem is properly connected to the WAN Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button. Before running this test, make sure you have a valid DSL link. If the DSL link is not connected, this test will always fail.



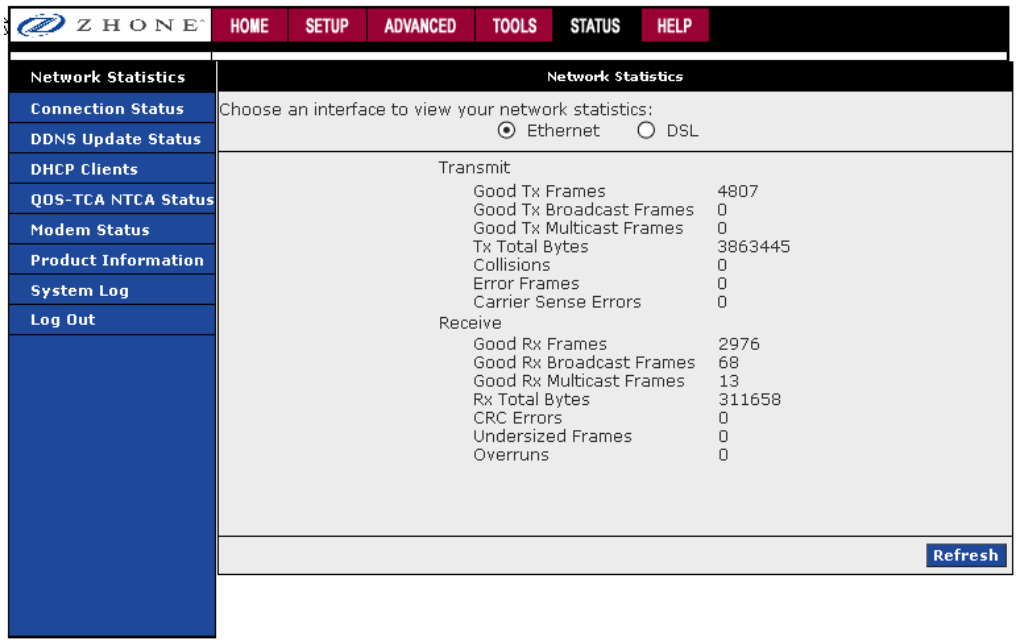
Chapter 5 Status

The Status section allows you to view the Status/Statistics of different connections and interfaces.

- Network Statistics – Select to view the Statistics of different interfaces: Ethernet, USB, and DSL.
- Connection Status – Select to view the Status of different connections.
- DHCP Clients – Select to view the list of DHCP clients.
- Modem Status – Select to view the Status and Statistics of your broadband (DSL) connection.
- Product Information – Select to view the router's driver and run-time information
- System Log

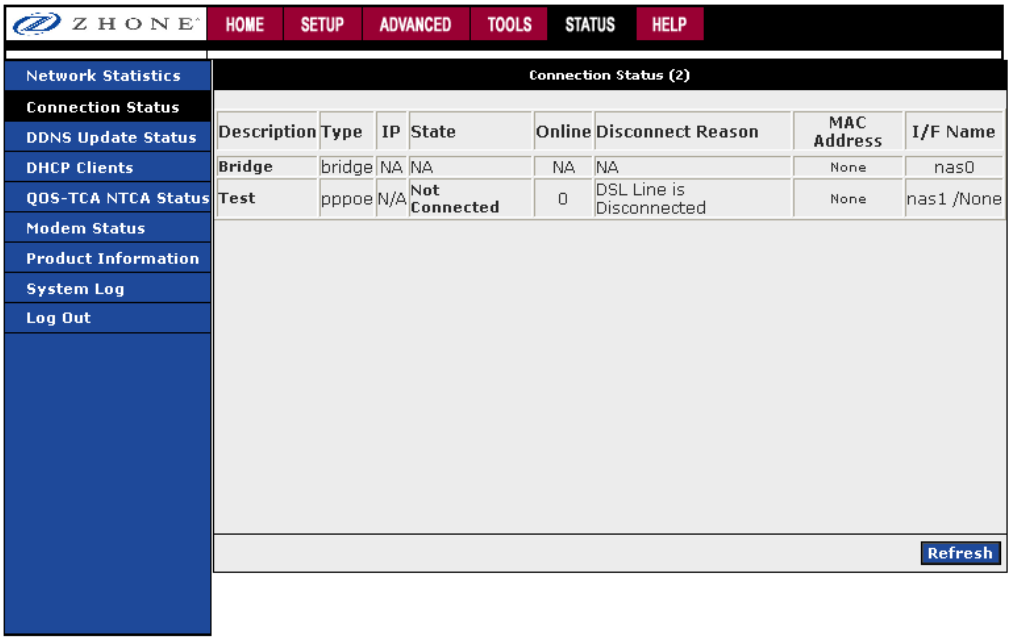
Network Statistics

Select to view the Statistics of different interfaces - Ethernet/USB/DSL.



Connection Status

Select to view the Status of different connections.

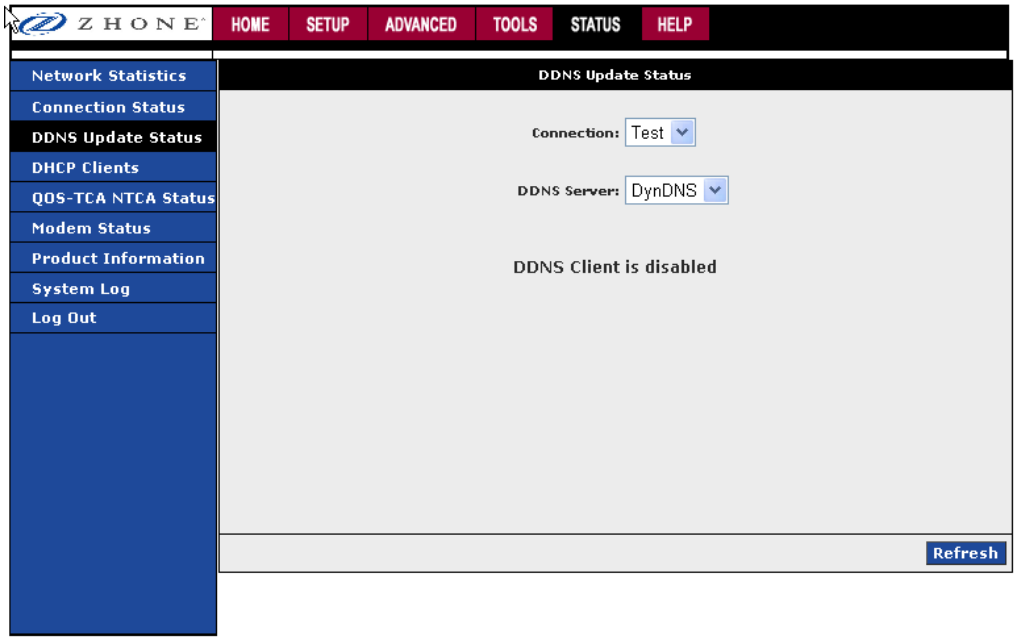


Description	Type	IP	State	Online	Disconnect Reason	MAC Address	I/F Name
Bridge	bridge	NA	NA	NA	NA	None	nas0
Test	pppoe	N/A	Not Connected	0	DSL Line is Disconnected	None	nas1 /None

DDNS Update Status

Select to view the DDNS status for the WAN connections.

You can view the DDNS update status of your WAN connection from the DDNS Status page.



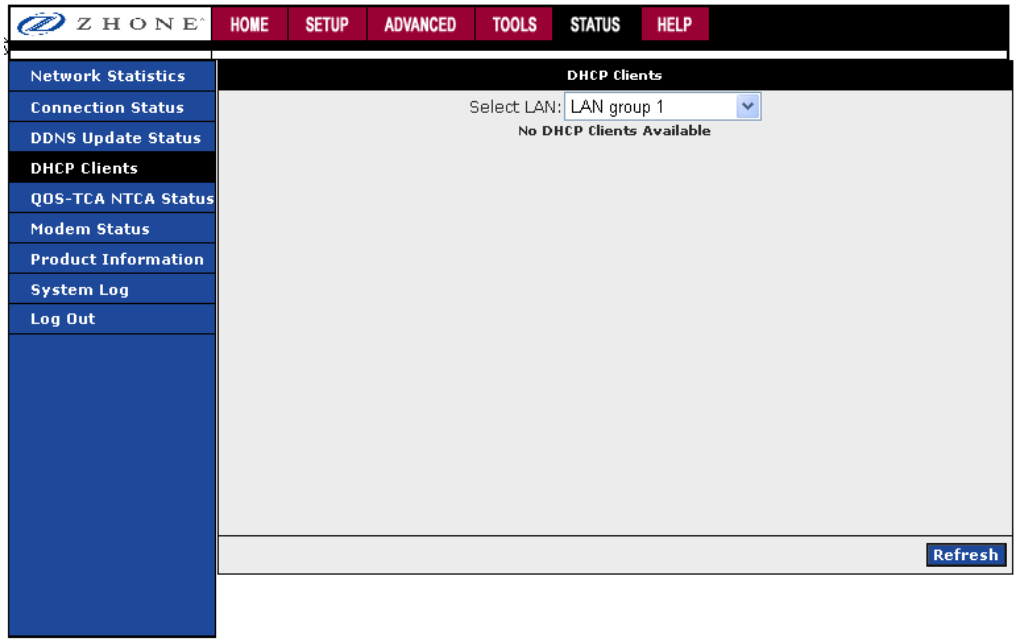
The DDNS client is disabled by default for your RG. When DDNS client is enabled, the DDNS client updates every time the RG gets a new IP address. The DDNS Status page provides you the DDNS update status of your RG.

DHCP Clients

Select to view the list of DHCP clients.

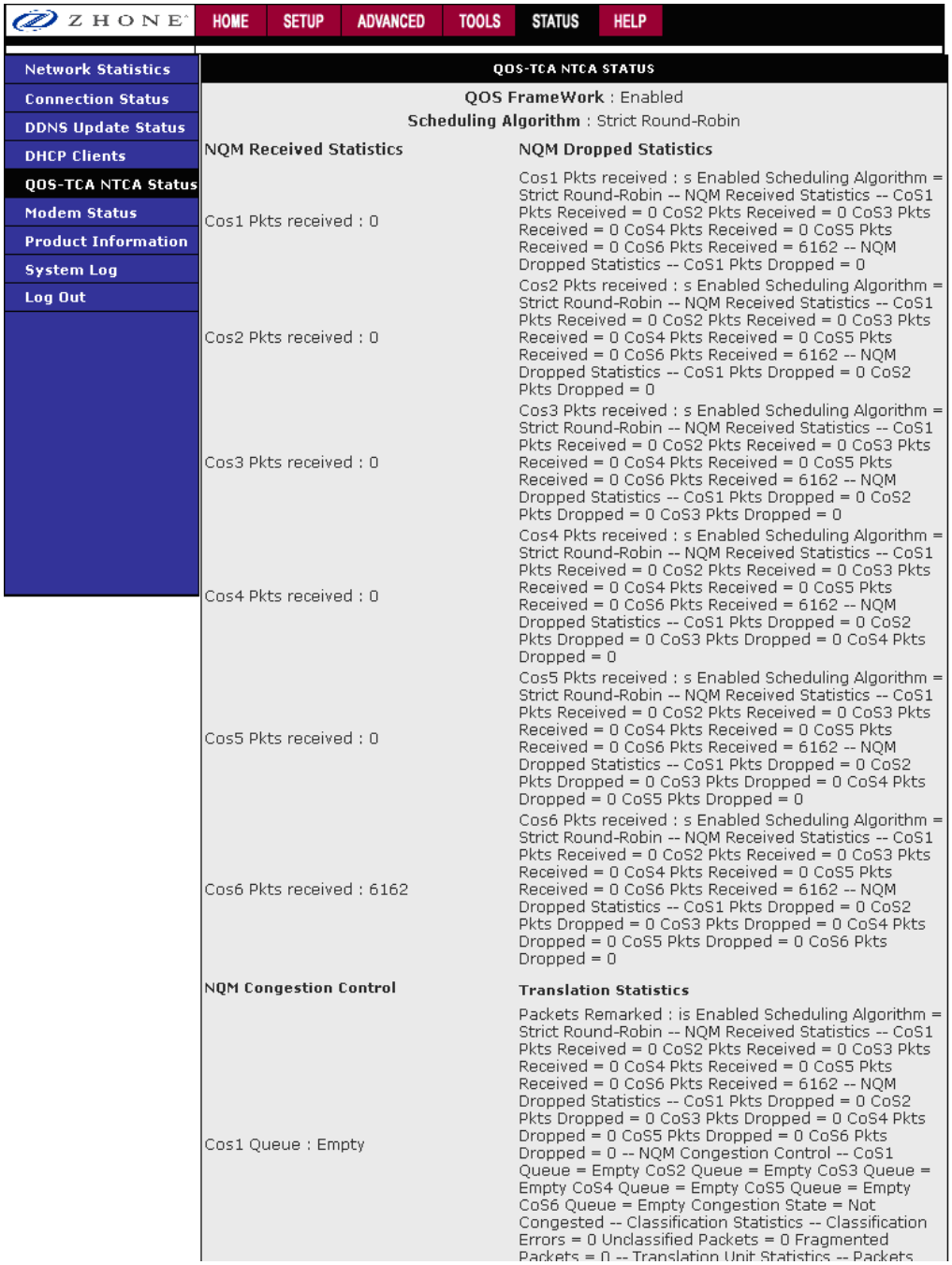
If you have enabled the DHCP server, you can view a list of the DHCP clients from the DHCP Clients page which will display:

- MAC Address
- IP Address
- Host Name
- Lease Time



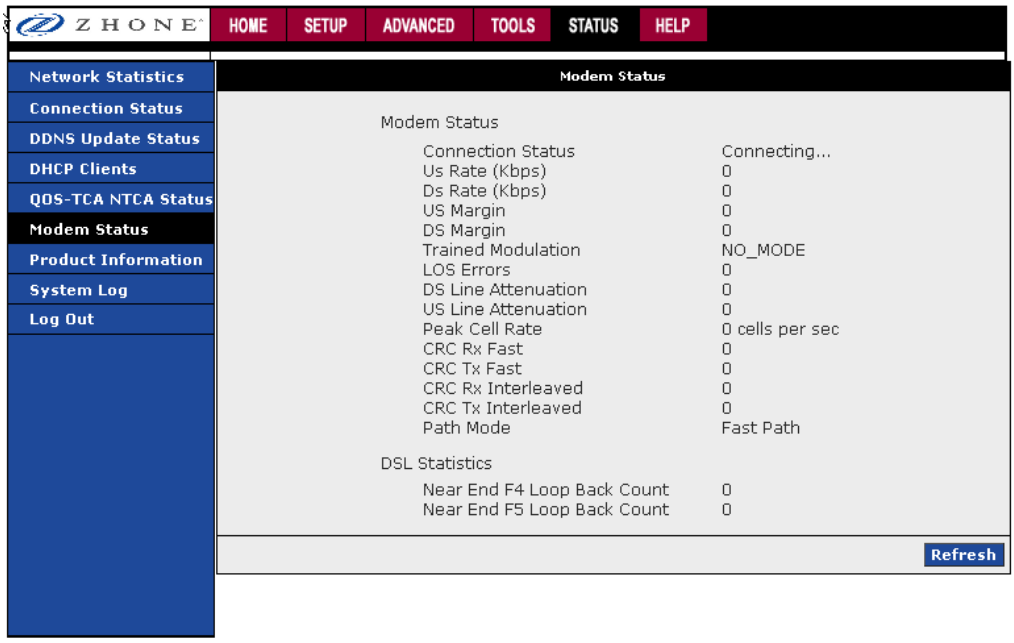
QOS-TCA NTCA Status

This page shows modem's packet transfer statistics.



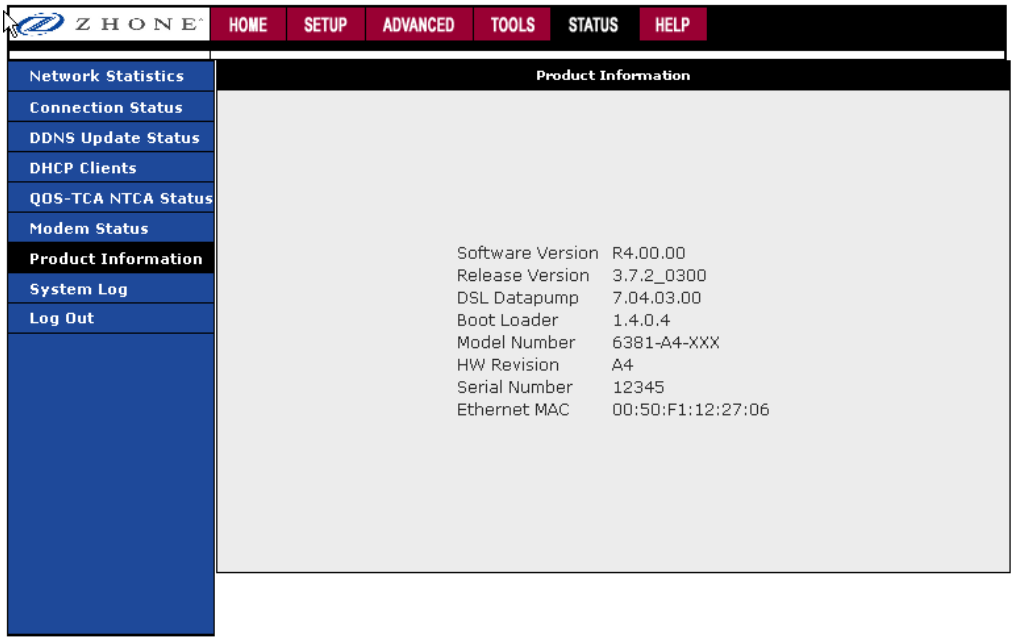
Modem Status

The modem must be connected to DSL service in order to view the modem's status.



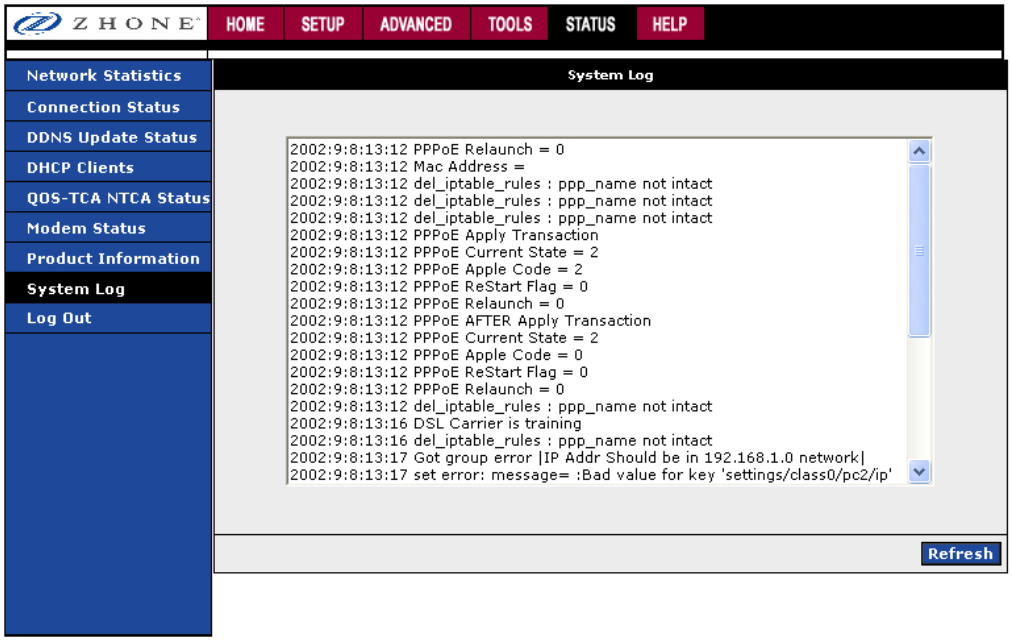
Product Information

On the Product Information page, information pertaining to the modem's software and hardware are shown.



System Log

You can display the modem's log by going to the Home screen, under the Status title, click System log. From here you can view all logged information. Depending upon the severity level, this logged info will generate log reports to a remote host (if remote logging is enabled).



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. *Make sure you are not connecting the USB and the Ethernet port to the same PC at the same time.*

4. *Check the settings on your PC. Again, refer to the quick start guide for more details*

5. *Check the router's settings.*

6. *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.*

7. *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.*

8. *Make sure NAT is enabled if you are using private addresses on the LAN ports.*

You Cannot Connect to the Router

1. *Check to see that the power LED is green and that the network cables are installed correctly.*

2. *Make sure you are not connecting the USB and the Ethernet port to the same PC at the same time.*

3. *Make sure that your PC and the router are on the same network segment. The router's default IP address is 192.168.1.1. If you are running a Windows-based PC, type ipconfig /all (or 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.*

4. *Make sure NAT is enabled if you are using private addresses on the LAN ports.*

LEDs Blink in a Sequential Pattern

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

The Status LED Continues to Blink

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

The Status LED is Always Off

1. *Make sure you have DSL service. You should receive notification from your ISP that DSL service is installed. You can usually tell if the service is installed by listening to the phone line: you will hear some high-pitched noise. If you do not hear high-pitched noise, contact your ISP.*

2. *Verify that the phone line is connected directly to the wall and to the line input on the router. If the phone line is connected to the phone side of the router or you have a splitter installed on the phone line, the DSL light will not come on.*

Diagnosing Problems using IP Utilities

Ping

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

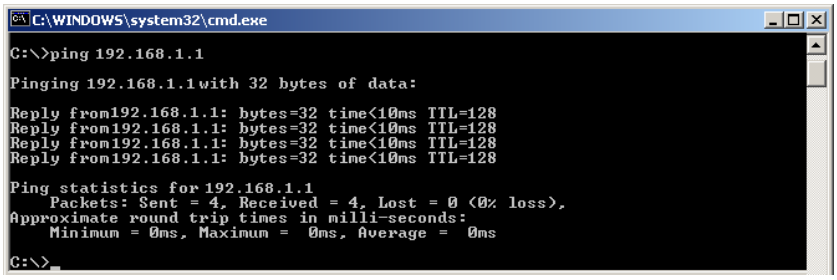
On Windows-based computers, you can execute a ping command from the Start menu.

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

   ping 192.168.1.1 or the IP address you have changed

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

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



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

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

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

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

Nslookup

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

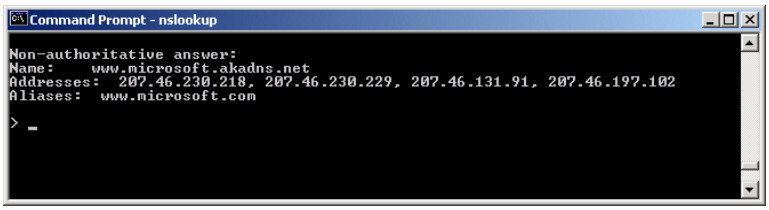
On Windows-based computers, you can execute the nslookup command from the Start menu.

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

```
Nslookup
```

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

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



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

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

Appendix A – Glossary

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

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

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