Copyright

Trademarks

FCC Interference Statement

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 radio interference in a residential environment. This equipment can generate, use and radiate radio frequency energy and, if not installed and used in accordance with the instructions in this manual, 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 is found by turning the equipment ON and OFF, the user is encouraged to try to reduce the interference by one or more of the following measures:

- Adjust or relocate the receiving antenna
- Increase the separation between the equipment or device
- Consult a dealer or an experienced technician for assistance

CE Declaration of Conformity

This is to certify that this device complies the essential protection requirements of the European Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22). Compliance with the applicable regulations is dependent upon the use of shielded cables. It is the responsibility of the user to procure the appropriate cables.

Contents

Chapter 1 Introduction

Congratulations on your purchase of this outstanding 4 Ports 11g Wireless ADSL2/2+ Router. This device is an IEEE 802.11g Wireless and 4 Port Switch built-in ADSL2/2+ Router that allows ADSL/ADSL2/ADSL2+ connectivity while providing Wireless LAN capabilities for residential, industries and SOHO environments. Wireless-G or the so-called 11g is the upcoming 54Mbps wireless networking standard that's almost 5 times faster than the widely deployed Wireless-B or the so-called 11b products found in homes, businesses, and public wireless hotspots around the world.

ADSL2/2+ is a transmission technology used to carry user data over a single twisted-pair line between the Central Office and the Customer Premises. The downstream data rates can go up to 24 Mbps and the upstream data rates can go up to 1Mbps with length reach up to 22Kft for ADSL2/2+ connection and 54Mbps transfer data rate for the 11g connection. This device allows ADSL2/2+ connectivity while providing Wireless LAN capabilities for home or office users. This asymmetric nature lends itself to applications such as Internet access and video delivery.

With minimum setup, you can install and use the router within minutes.

1.1 Features

- **The 4 Ports 11g Wireless ADSL2/2+ Router provides the following features:**
  - Compliant to ANSI T1.413 Issue 2, ITU-T G.992.1, ITU-T G.992.2, ITU-G.992.3, ITU G.992.5 and READSL2 standards.Support all Digital Loop ITU G.992.3 annex I and J specifications.Fully compliant with Annex A/B/B (U-R2) ADSL specifications.
  - Downstream and Upstream data rates up to 24Mbps and 1Mbps.
  - Support g+ WLAN features with transmission rate up to 125Mbps (Optional).
  - IEEE 802.11g WLAN supports up to 54Mbps transmission rate.Support WEP, 802.1X and WPA based Encryption. Support RFC 1483 Bridge/Routing over ATM over ADSL.
  - Support PPPoE, PPPoA and IPoA Routing ATM over ADSL.
  - ATM Layer with Traffic Shaping QoS support (UBR, CBR, VBR-rt, VBR-nt).
  - Support UPnP functionality.
  - Web-based setup for installation and management.
  - Built-in 4*10/100 Mbps Fast Ethernet Switch port for LAN connection.
  - Compliant with IEEE 802.3/802.3u and auto-negotiation.
  - Support full-duplex 802.3 flow control.
  - Support IP Filtering, MAC Filtering, Web Filtering and IPSec Pass-Through security functionality.
  - Support Dying Gasp functionality.
  - Flash memory for firmware upgrade.
  - Hardware Reset button for fast default setting recovery.
  - HTTP Web-Based Management/Configuration.
  - LEDs indicator indicates connection status.

- **ADSL Standards**
  - Full rate ANSI T1.413 Issue2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant.
  - ITU G.992.3, ITU G.992.5 and READSL2 ADSL2/2+ standards compliant.
  - Downstream and Upstream data rates up to 24Mbps and 1Mbps.
  - Reach length up to 22Kft.
  - Support Dying Gasp functionality.

- **IEEE 802.11g Wireless Standards**
  - IEEE 802.11b/g standards compliant.
  - Support data rates up to 54Mbps (Auto-Rate Capable).
  - Support 11g+ with data transmission rate up to 125Mbps (Optional)
  - Support OFDM (64QAM, 16QAM, QPSK, BPSK) and DSSS (DBPSK, DQPSK, CCK) modulation.
  - Conforms to Wireless Ethernet Compatibility Alliance (WECA) Wireless Fidelity (Wi-Fi) Standard.
  - Support WEP/WPA/802.1X Encryption for data security.
  - Support 2.412GHZ ~ 2.484GHz frequency ranges.

- **ATM Protocols**
  - Support ATM ALL0, ALL2 & ALL5.
  - Support up to 8PVCs.
  - Support ATM UBR, CBR, VBR-rt and VBR-nt Traffic Shaping QoS.
  - Support OAM F4/F5 Loop Back.
  - Support PPPoA (RFC2364).
  - Support PPPoE (RFC2516).
  - Router/Bridged Ethernet over ATM (RFC2864 / RFC1483).
  - Classical IP over ATM (RFC2225 / RFC1577).

- **Router Mode**
  - IP Routing – RIPv1 and RIPv2.
  - Static Routing.
  - DHCP Server, Relay and Client.
  - Support DNS Relay/Server.
  - Support DMZ functionality.
  - Support NAT and NAPT (PAT) functionality with extensive ALG supported.
  - Support IPSec, L2TP, PPTP Pass-Through.
  - Support VPN Pass-Through.
  - Support SNMP functionality.
  - Support ICMP and IGMP.
  - Support PAP and CHAP PPP Authentication.

- **Bridge Mode**
  - Support Transparent Bridging (IEEE 802.1D).
  - Support RFC 2684/1483 Bridged.

- **Firewall**
  - Built in Firewall functionality.
  - Support IP Filtering.
  - Support MAC Filtering.
  - Support Web Filtering.
  - IPSec Pass-Through.
  - Protection against IP and MAC address spoofing.

- **UPnP**
  - Support UPnP functionality (Optional).

- **Ethernet Standards**
  - Built-in 4 Ports 10/100Mbps Ethernet Switch which compliant with IEEE 802.3x standards
  - Automatic MDI/MDI-X crossover for 100BASE-TX and 10BASE-T ports.
  - Auto-negotiation and speed-auto-sensing support.
  - Port based VLAN supported in any combination.

- **Web-Based Management**
  - Web-based Configuration / Management.
  - Remote / Local Management / Configuration.
  - Firmware upgrade and Reset to default via Web management.
  - Telnet, TFTP and FTP Management / Configuration.
  - SNMP MIB-II.
  - Restore factory default setting via Web or hardware reset button.
  - WAN and LAN connection statistics.
  - Configuration of static routes and routing table, NAT/NAPT and VCs.
  - Support Password Authentication.

1.2 Scope

This document provides the descriptions and usages for the 4 Ports 11g Wireless ADSL2/2+ Router's Web pages that are used in the configuration and setting process. Both basic and advanced descriptions and concepts are discussed. To help the reader understand more about these Web pages, some questions and answers (Q&A) are appended after the definition of each Web page along with the appendices at the end of the guide.

1.3 Audience

This document is prepared for use by those customers who purchase the 4 Ports 11g Wireless ADSL2/2+ Router and using the provided or embedded firmware. It assumes the reader has a basic knowledge of ADSL/ADSL2/ADSL2+, Wireless and networking.

1.4 Document Structure

Chapter 1: Introduction, provides a brief introduction to the product and user guide.

Chapter 2: Knowing The 4 Ports 11g Wireless ADSL2/2+ Router, provides device specifications and hardware connection mechanism.

Chapter 3: Setting Up TCP/IP In Windows, provides Windows system Network's configurations.

Chapter 4: Device Administration, describes the pages found under the Admin menu. These pages allow the user to view, change, edit, update, and save the 4 Ports 11g Wireless ADSL2/2+ Router's configurations or settings.

Appendix A: Router Terms, provides an introduction to basic Router Terms.

Appendix B: Frequently Asked Questions, is a compilation of useful questions regarding the 4 Ports 11g Wireless ADSL2/2+ Router.

Appendix C: Troubleshooting Guide, is a compilation of questions and answers relating to common problems dealing with Windows networking and the 4 Ports 11g Wireless ADSL2/2+ Router Configurations.

Appendix D: UPnP Setting, provides UPnP configurations procedures under Windows XP.

Appendix E: Glossary, provides definitions of terms and acronyms of this 4 Ports 11g Wireless ADSL2/2+ Router.

1.5 System Requirement

Check and confirm that your system confirm the following minimum requirements:

- Personal computer (PC/Notebook).
- Pentium II compatible processor and above.
- Ethernet LAN card or IEEE 802.11b or IEEE 802.11g Wireless adaptor installed with TCP/IP protocol.
- USB Port (Optional)
- 64 MB RAM or more.
- 50 MB of free disk space (Minimum).
- Internet Browser.
- CD-ROM Drive.

1.6 Packet Contents

The 4 Ports 11g Wireless ADSL2/2+ Router package contains the following items :

- One 4 Ports 11g Wireless ADSL2/2+ Router
- One Power Adapter
- One RJ-11 ADSL Cable
- One CAT-5 Ethernet Cable
- One detachable SMA Antenna
- One CD-ROM (Driver / Manual / Quick Setup Guide)

If any of the above items are damaged or missing, please contact your dealer immediately.

Chapter 2 Knowing The 4 Ports 11g Wireless ADSL2/2+ Router

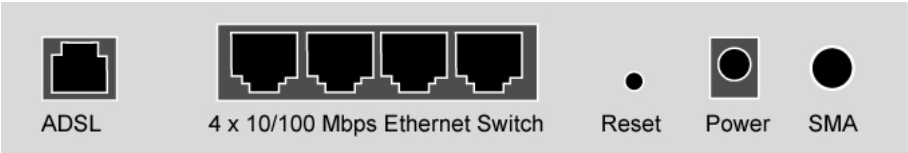
2.1 Front Panel:

The 4 Ports 11g Wireless ADSL2/2+ Router's LEDs indicators display information about the device's status.

PWR	Lights up when 4 Ports 11g Wireless ADSL2/2+ Router is powered on.
WL ACT	Lights up when Wireless system is ready.
	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is sending/receiving data.
1	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is Sending/Receiving data.
2	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is Sending/Receiving data.
3	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is Sending/Receiving data.
4	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is Sending/Receiving data.
ADSL	Lights up when a successful ADSL2/2+ connection is established.
	Blinking when 4 Ports 11g Wireless ADSL2/2+ Router is sending/receiving data.
PPP	Lights up when a PPP connection is established.

2.2 Back Panel:

The back panel of the 4 Ports 11g Wireless ADSL2/2+ Router contains ADSL, Ethernet Switches, Reset, Power Adapter connection, Power ON/OFF Switch and SMA connector.



ADSL	Port for connecting to the ADSL2/2+ Service Provider.
Ports 1~4	Four 10/100Mbps Ethernet Ports for connecting to the network devices
RESET	Restore the 4 Ports 11g Wireless ADSL2/2+ Router to factory default setting.
POWER	12V DC/1A Power adapter connector.
SMA	Detachable SMA Dipole Antenna.

All the Ethernet port of the 4 Ports 11g Wireless ADSL2/2+ Router supports auto-crossover capability.

RESET Button:
Reboot & Restore the 4 Ports 11g Wireless ADSL2/2+ Router to factory defaults.

Resetting Factory Defaults:

The reboot and restore to factory defaults feature will set the device to its factory default configuration by resetting the 4 Ports 11g Wireless ADSL2/2+ Router.

To Reset the 4 Ports 11g Wireless ADSL2/2+ Router:

- Ensure that the device is powered on.
- Press the Reset button for 5~10 seconds and release. The LED indicators will turns OFF and ON again indicates that the reset is in progress. Do not power off the device during the reset process.
- Reset is completed when the LED indicator return to steady green. The default settings are now restored.

2.3 Connection Mechanism:

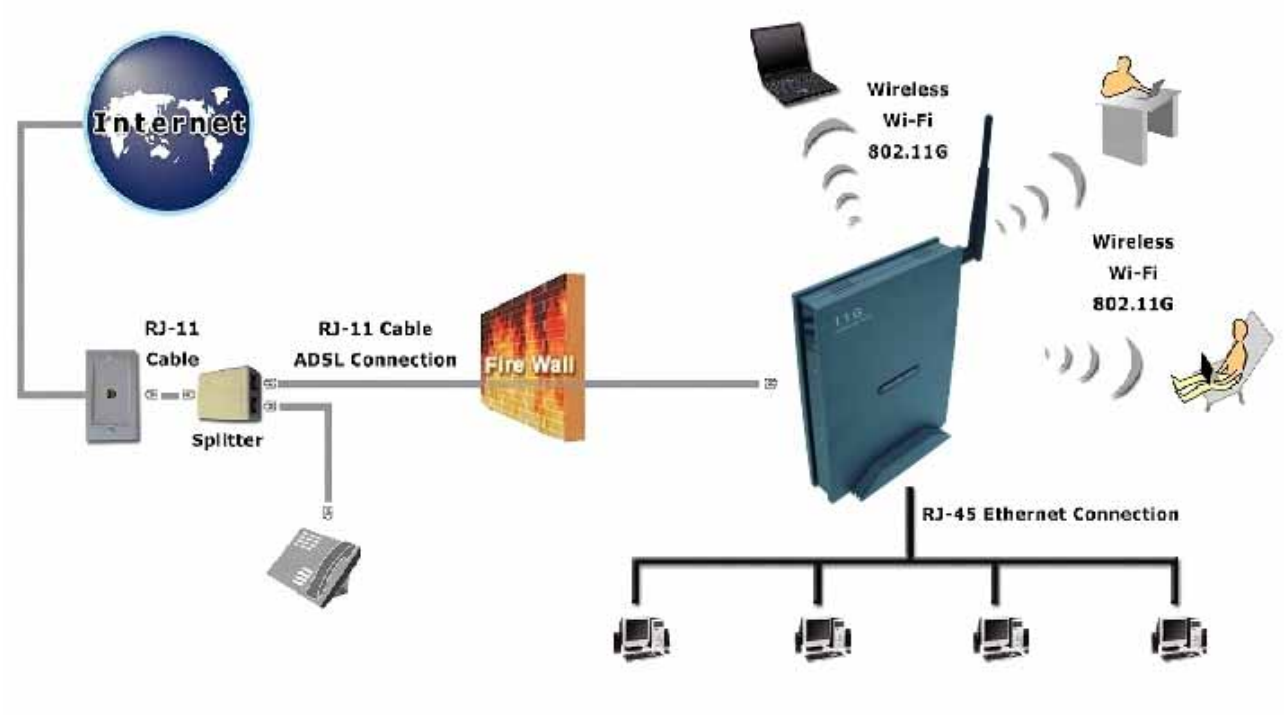
This section describes the hardware connection mechanism of 4 Ports 11g Wireless ADSL2/2+ Router on your Local Area Network (LAN) connected to the Internet, how to configure your 4 Ports 11g Wireless ADSL2/2+ Router for Internet access or how to manually configure your Internet connection.

You need to prepare the following items before you can establish an Internet connection through your 4 Ports 11g Wireless ADSL2/2+ Router:

1. A computer/notebook which must have an installed Ethernet Adaptor and an Ethernet Cable, or
2. A computer/notebook which have Wireless-b or Wireless-g wireless adaptor properly installed.
3. ADSL/ADSL2/ADSL2+ service account and configuration information provided by your Internet Service Provider (ISP). You will need one or more of the following configuration parameters to connect your 4 Ports 11g Wireless ADSL2/2+ Router to the Internet:

    a. VPI/VCI parameters
    b. Multiplexing Method or Protocol Type or Encapsulation Type
    c. Host and Domain Names
    d. ISP Login Name and Password
    e. ISP Domain Name Server (DNS) Address
    f. Fixed or Static IP Address.

Figure below shows the overall hardware connection mechanism of your 4 Ports 11g Wireless ADSL2/2+ Router.



Following are the steps to properly connect your 4 Ports 11g Wireless ADSL2/2+ Router:

1. Turn off your computer/notebook.
2. Connect the ADSL port of your 4 Ports 11g Wireless ADSL2/2+ Router to the wall jack of the ADSL/ADSL2/ADSL2+ Line with a RJ-11 cable.
3. Connect the Ethernet cable (RJ-45) from your 4 Ports 11g Wireless ADSL2/2+ Router (Switch) to the Ethernet Adaptor in your computer.
4. Connect the Power adaptor to the 4 Ports 11g Wireless ADSL2/2+ Router and plug it into a Power outlet.

The Power light will lit after turning on the 4 Ports 11g Wireless ADSL2/2+ Router.
Auto and self-diagnostic process will turn the LED indicators ON and OFF during the process.

Use the Power Adaptor exclusively in combination with the equipment supplied and do not use any other kind of power adaptor for the equipment.

5. Turn on your computer.
6. Refer to the next section to setup or configure your system's Network Adaptor.

Chapter 3 Setting up the TCP/IP in Windows

The instruction in this chapter will help you configure your computers to be able to communicate with this 4 Ports 11g Wireless ADSL2/2+ Router.

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/ Internet Protocol). Each computer/notebook on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

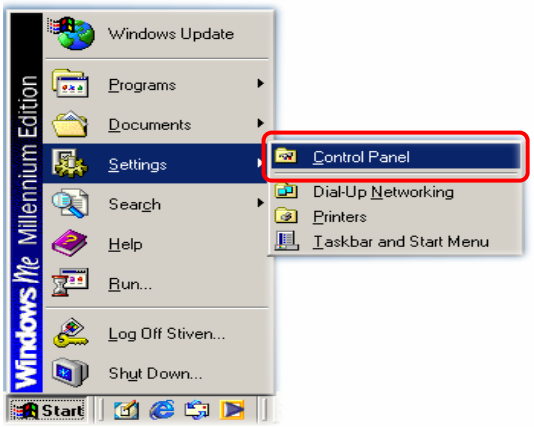
The following description assumes 4 Ports 11g Wireless ADSL2/2+ Router been set to factory default. (If not, please hold the reset button down for 5~10 seconds). The default of the 4 Ports 11g Wireless ADSL2/2+ Router's LAN IP is **192.168.1.1**.

Follow the procedures below to set your computer/notebook function as a **DHCP Client**.

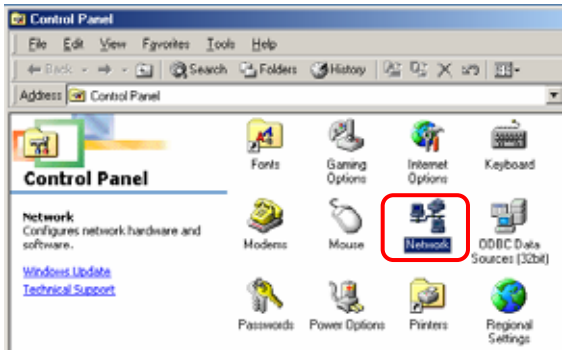
Restart and Reboot your Windows system might be necessary after setting your computer function as a DHCP Client. In order to properly activate your choice, click "OK" to restart your Windows system.

3.1 Windows ME / 98

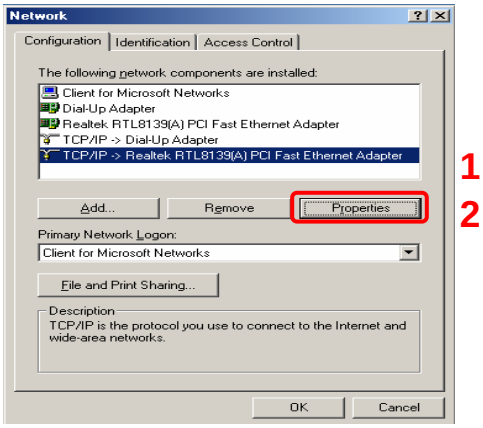
Step 1: Click **Start→Settings→Control Panel**.



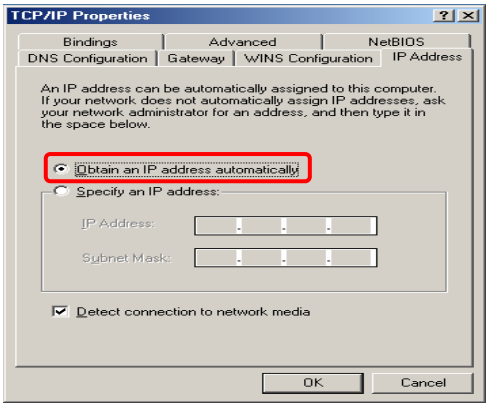
Step 2: Double-click the **Network** icon.



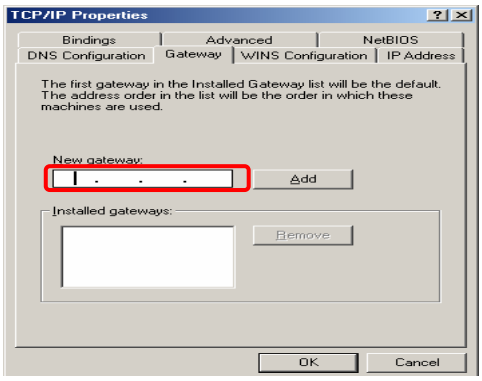
Step 3: Go to Configuration icon, select network adapter installed and click **Properties**.



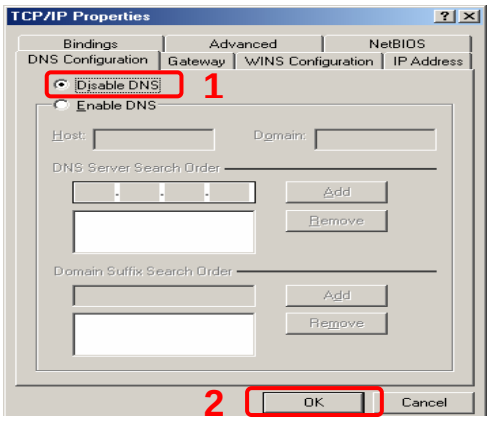
Step 4: Go to IP Address icon and select **Obtain an IP address**.



Step 5: Go to Gateway icon and erase all previous setting.

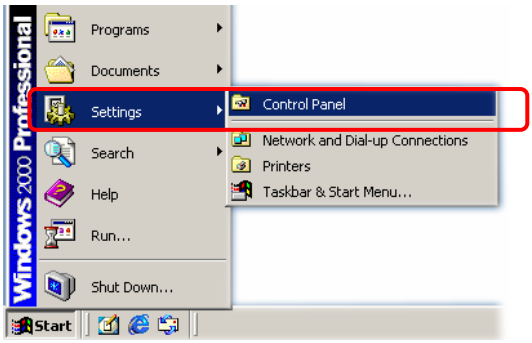


Step 6: Go to DNS Configuration icon, select **Disable DNS** and click **OK**.

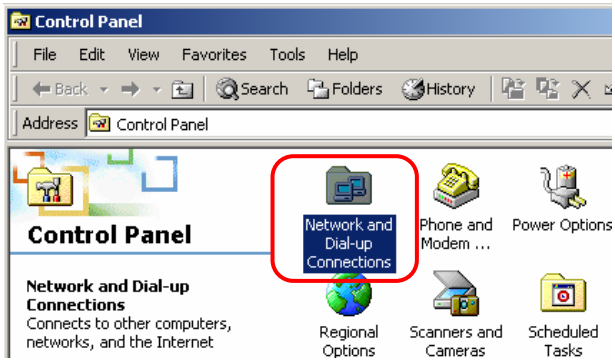


3.2 Windows 2000

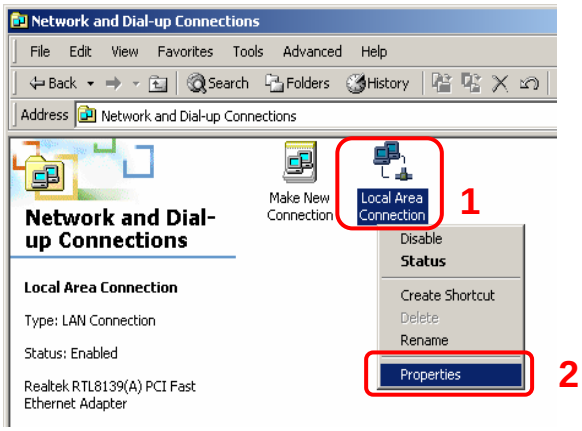
Step 1: Click **Start→Settings→Control Panel**.



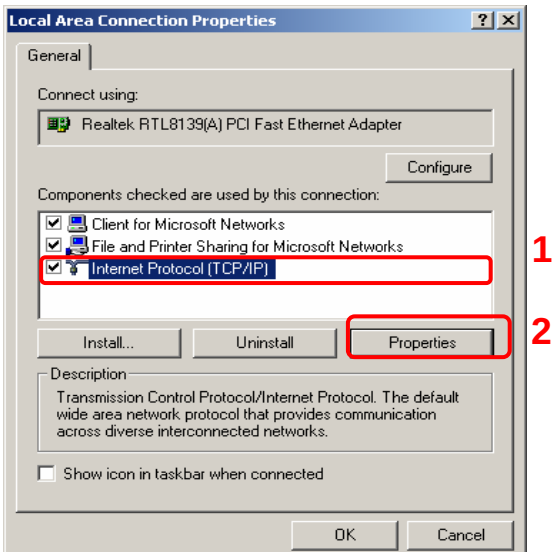
Step 2: Double-click the **Network and Dial-up Connections**.



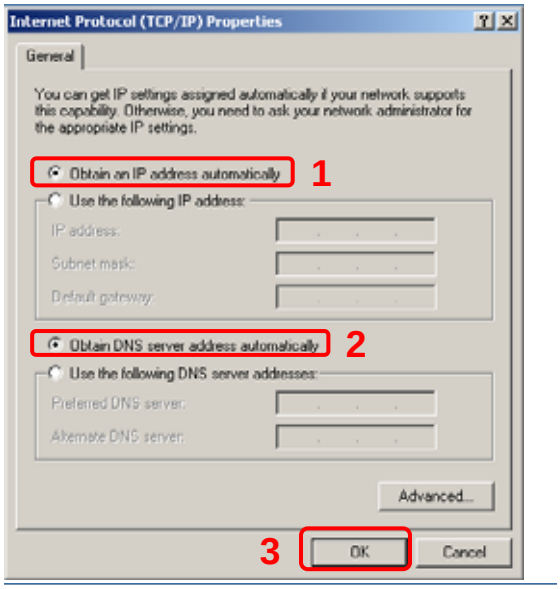
Step 3: Right Click the **Local Area Connection** and select **Properties**.



Step 4: Select **Internet Protocol (TCP/IP)** and click **Properties**.

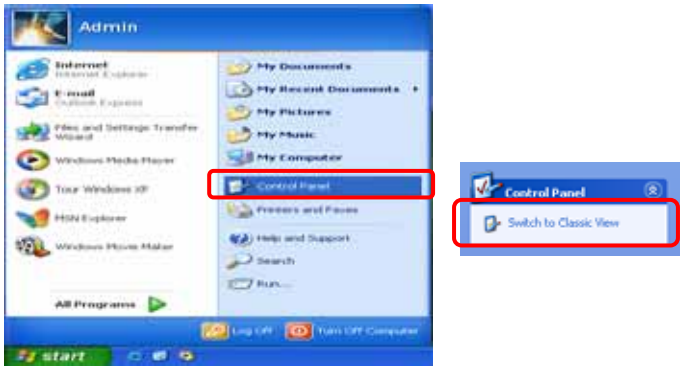


Step 5: Select **Obtain an IP address automatically** and **DNS server address automatically.** Then, click **OK**.

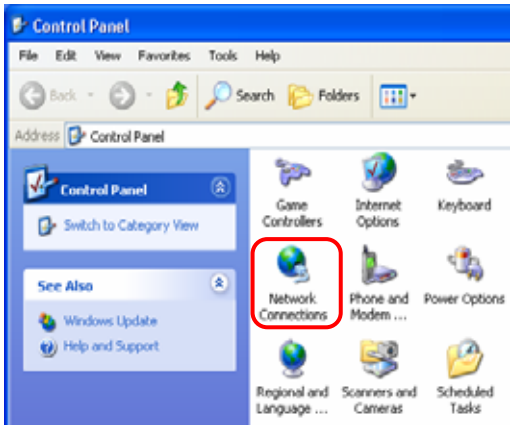


3.3 Windows XP

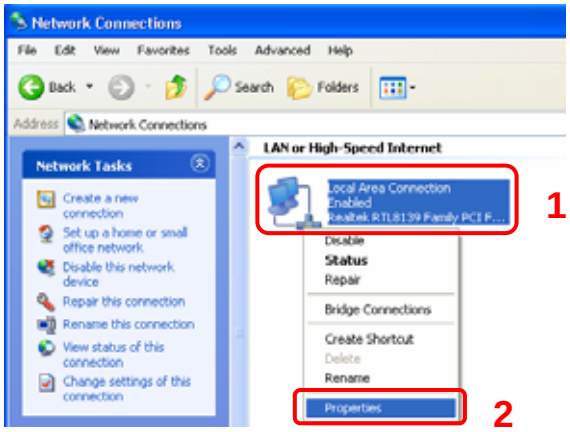
Step 1: Click **Start→Control Panel→Classic View**.



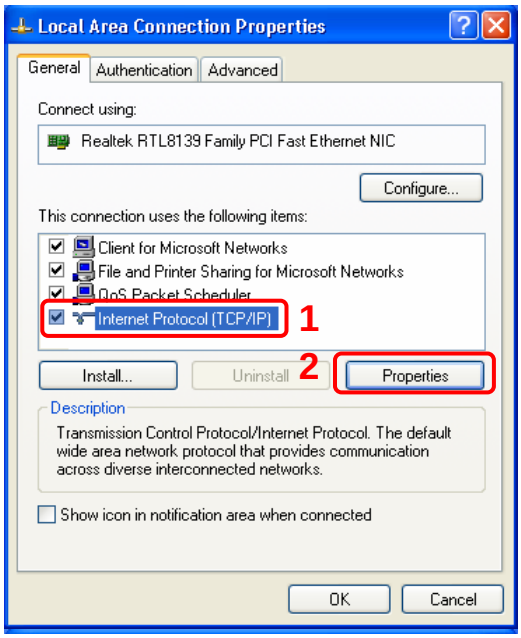
Step 2: Double-click the **Network Connections**.



Step 3: Right Click on the **Local Area Connection** and select **Properties**.

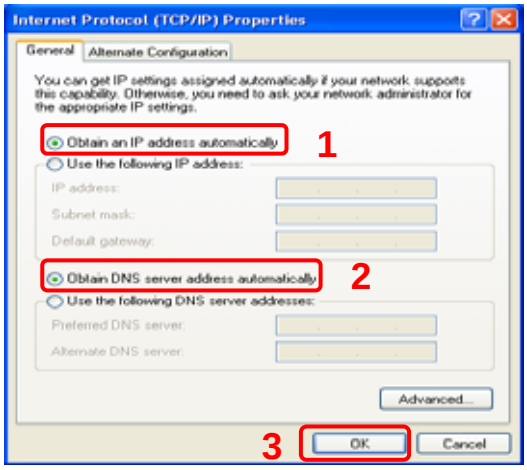


Step 4: Go to General icon, select **Internet Protocol (TCP/IP)** and click **Properties**.



Step 5: Go to General icon, select **Obtain an IP address automatically** and **DNS server address automatically**.

Then, click OK**.**



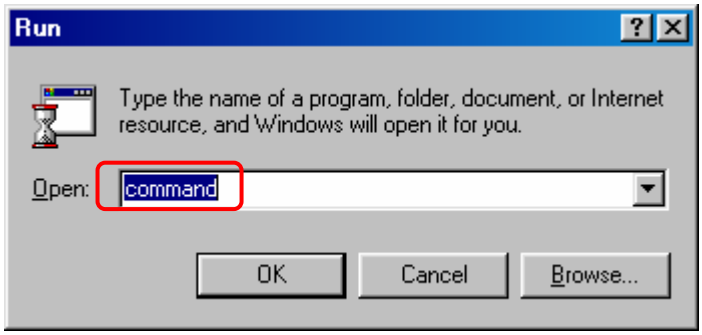
3.4 Checking TCP/IP Configuration

After your PC is configured and the system has rebooted, you can check the TCP/IP configuration using the following utility provided by your Windows system:

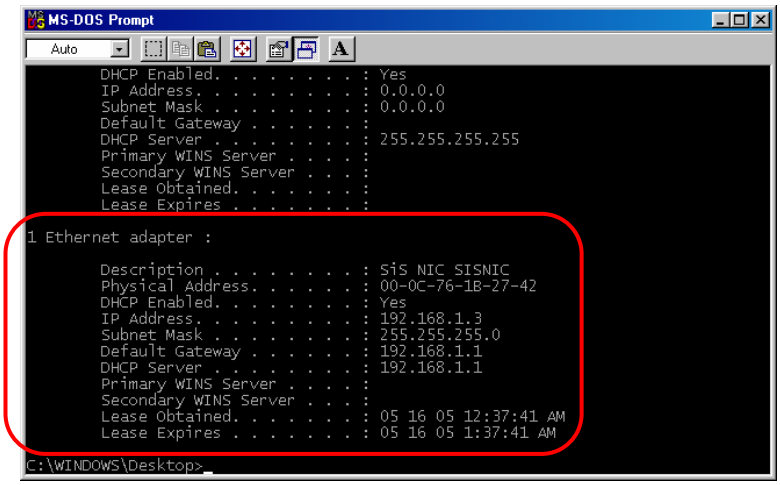
A. Windows 98/ME:

1. Click on **"Start"** and **"Run"**.

2. In the open field, enter **"Command",** then press **"OK"**.



3. All the Ethernet adapter information will be shown in the appears Windows. Check if you can get the following setting:

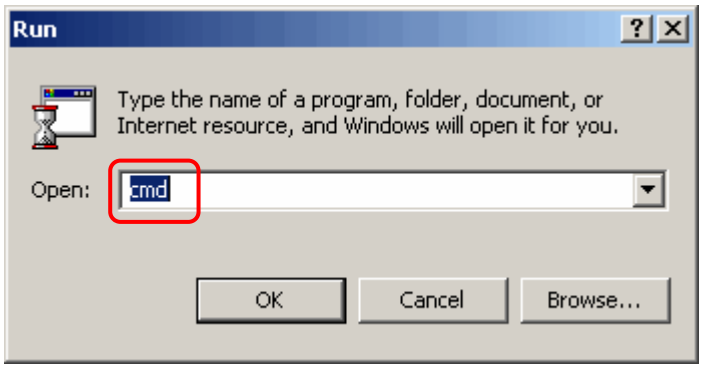


- The **IP Address** as **192.168.1.x**
- The **Subnet Mask** as **255.255.255.0**
- The **Default Gateway** as **192.168.1.1**

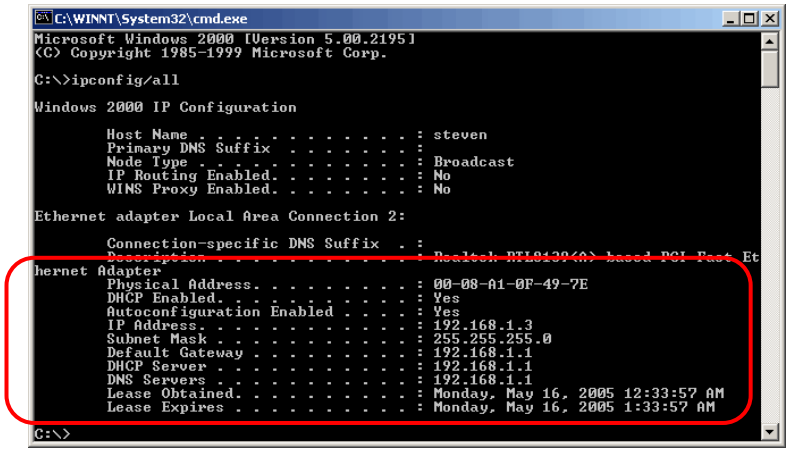
4. Type **"Exit"** to end up the MS-DOS Prompt.

B. Windows 2000:

1. Click **"Start"** and **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.



3. In the command prompt, type **"ipconfig /all"**, then press **"Enter"**.



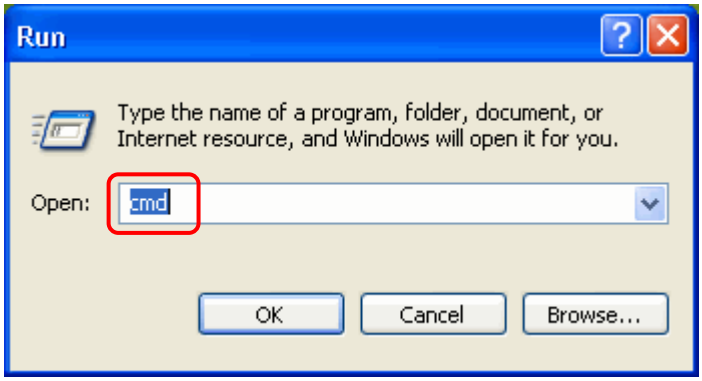
All the Ethernet adapter information will be shown in the appear Windows. Check if you can get the following setting:

- The **IP Address** as **192.168.1.x**
- The **Subnet Mask** as **255.255.255.0**
- The **Default Gateway** as **192.168.1.1**

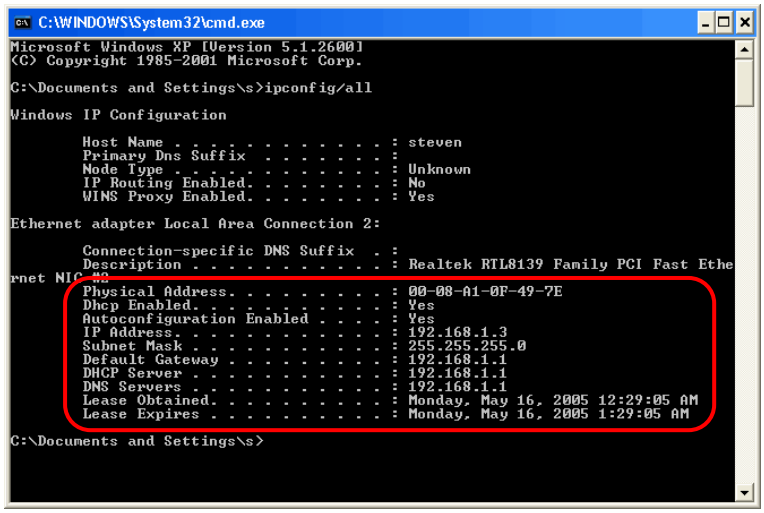
4. Type **"Exit"** to end up the process.

C. Windows XP:

1. Click **"Start"** and **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.



3. In the command prompt, type **"ipconfig /all"**, then press **"Enter"**



All the Ethernet adapter information will be shown in the appear Windows. Check if you can get the following setting:

- IP address as **192.168.1.x**
- The Subnet Mask as **255.255.255.0**
- the default gateway as **192.168.1.1**

4. Type **"Exit"** to end up the process.

Chapter 4 Device Administration

For your convenience, an Administrative Utility has been programmed into 4 Ports 11g Wireless ADSL2/2+ Router. This chapter will explain all the functions in this utility. All the 4 Ports 11g Wireless ADSL2/2+ Router based administrative tasks are performed through this web utility.

4.1 Login

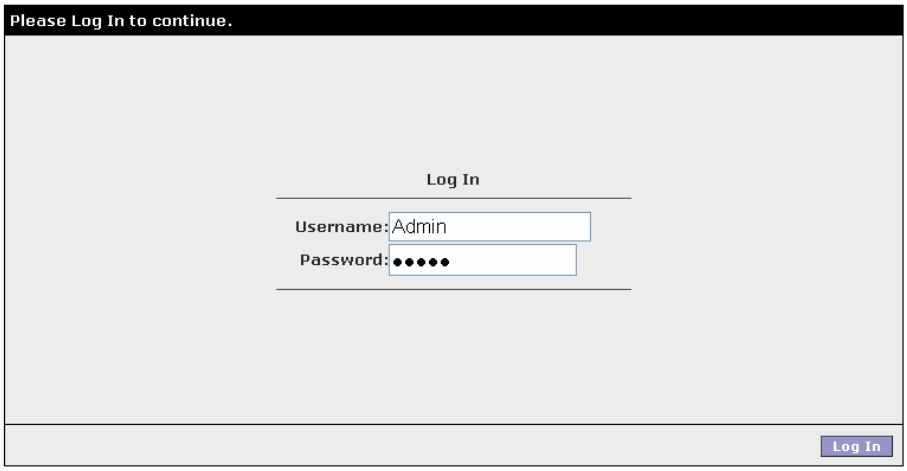
To access the 4 Ports 11g Wireless ADSL2/2+ Router Configuration screens, follow the following steps will enable you to log into the 4 Ports 11g Wireless ADSL2/2+ Router:

1. Launch the Web browser (Internet Explorer, Netscape, etc).

2. Enter the 4 Ports 11g Wireless ADSL2/2+ Router default IP address (Default Gateway) http://192.168.1.1 in the address bar then press Enter to Log in.

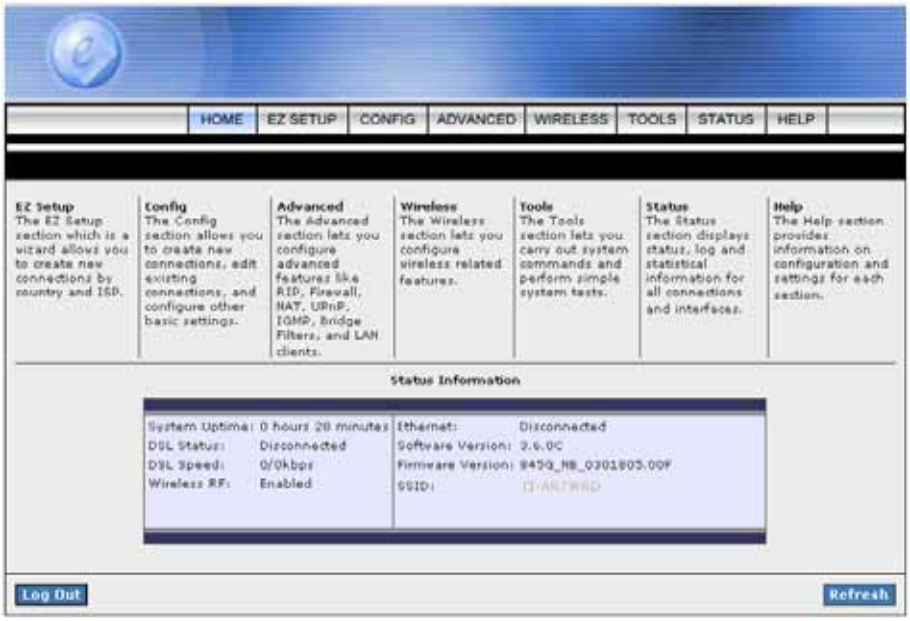
3. Entry of the username and password will be prompted. Enter the default login **"Username"** and **"Password"**: The default login Username of the administrator is **"Admin"**, and the default login Password is **"Admin"**.

☑ Note that the Username and Password are case sensitive.



"Username" and **"Password"** can be changed after login. Refer to the **Tools** configuration section for further instruction.

Upon entering the address into the web browser, the configurable **HOME** page with all the device configuration information will pop up as shown in Figure below.



- **HOME:** The **Home** section show the current 4 Ports 11g Wireless ADSL2/2+ Router's function information under different links.

- **EZ SETUP:** The **EZ Setup** is a presetting wizard which meant to help you install the 4 Ports 11g Wireless ADSL2/2+ Router quickly and easily.

- **CONFIG:** The **Config** section allows you to create new connections, edit existing connections, and configure other basic settings.

- **ADVANCED:** The **Advanced** section lets you configure advanced features like RIP, SNTP, SNMP, IP QoS, Access control, etc...

- **WIRELESS:** The **Wireless** section lets you configure wireless connection and related features.

- **TOOLS:** The **Tools** section lets you carry out system commands and perform simple system tests.

- **STATUS:** The **Status** section displays status, log and statistical information for all connections and interfaces.

- **HELP:** The **Help** section provides information on configuration and settings for each section.

- **Status Information:** Shows the current device connection status.

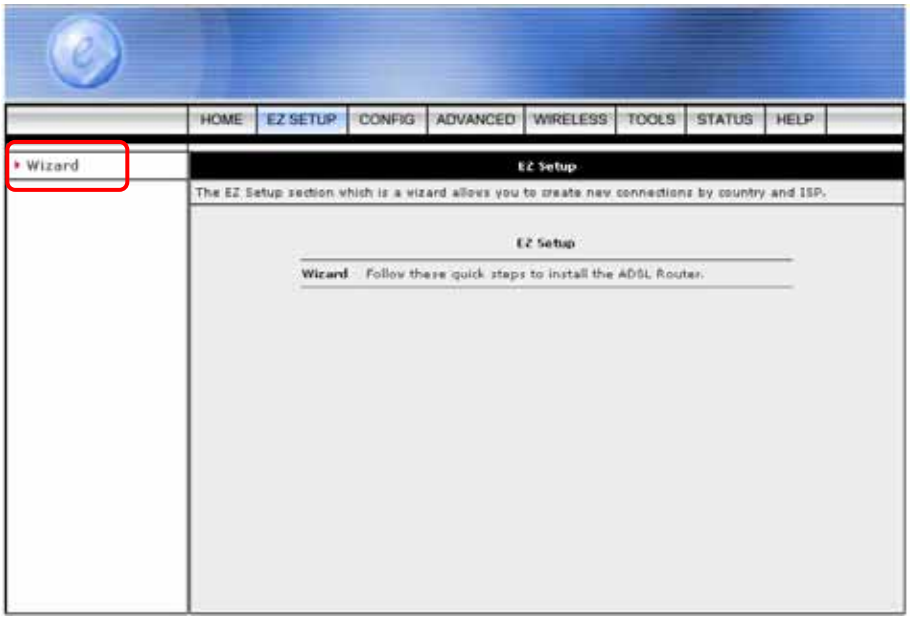
  - ☑ **System Uptime:** This field displays the time of the 4 Ports 11g Wireless ADSL2/2+ Router has been in operation.
  - ☑ **DSL Status:** Shows the 4 Ports 11g Wireless ADSL2/2+ Router connection status.
  - ☑ **DSL Speed:** This field displays the 4 Ports 11g Wireless ADSL2/2+ Router Downstream/Upstream data rate in Kbps
  - ☑ **Wireless RF:** Show the 4 Ports 11g Wireless ADSL2/2+ Router wireless system status.
  - ☑ **Ethernet:** This field displays the link up or down for the Ethernet connection.
  - ☑ **USB:** This field displays the link up or down for the USB connection (Optional).
  - ☑ **Software Version:** This field displays the 4 Ports 11g Wireless ADSL2/2+ Router's data pump code version.
  - ☑ **Firmware Version:** This field displays the 4 Ports 11g Wireless ADSL2/2+ Router's firmware version.
  - ☑ **SSID:** The Service Set Identifier (**SSID**) is a unique name for your wireless network. If you have other wireless access points in your network, they must share the same SSID. The default SSID is **TI-AR7WRD**.

- **Log Out:** Click to Log Out the Administration configuration page.

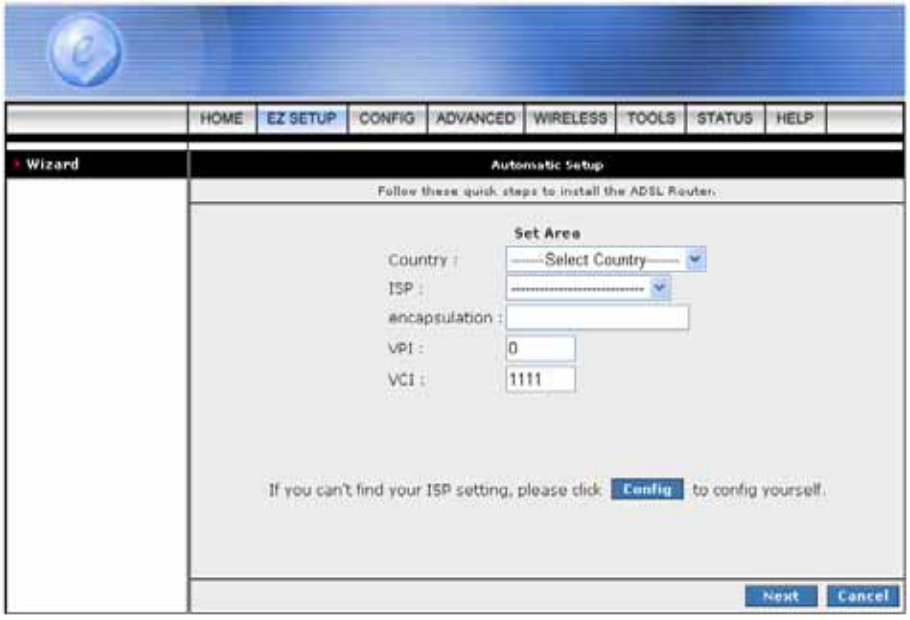
- **Refresh:** Click to Refresh current page.

4.2 EZ SETUP

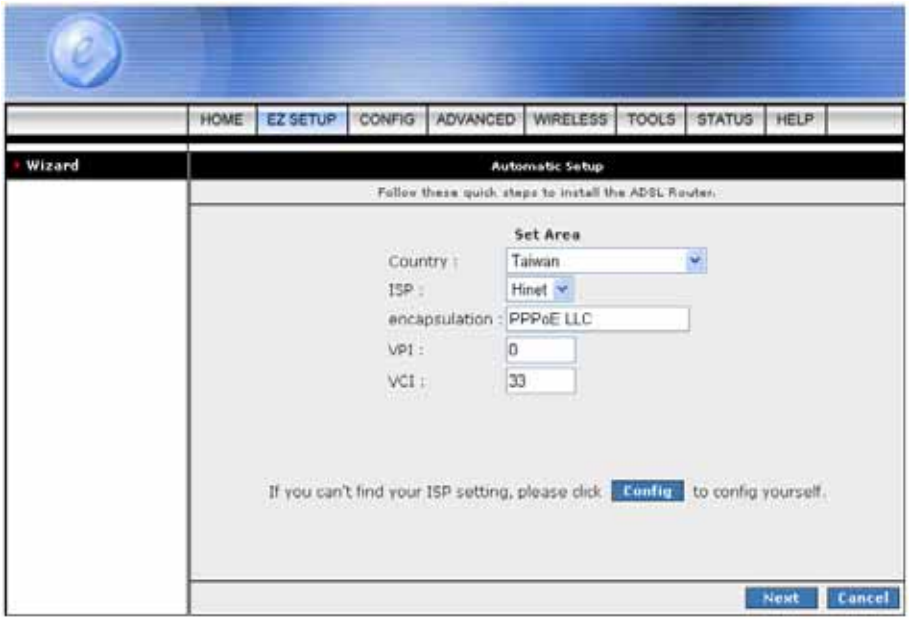
The **EZ SETUP** is a presetting wizard which meant to help you install the 4 Ports 11g Wireless ADSL2/2+ Router quickly and easily.



Click on **"Wizard"** and the following screen will pop-up. Follow the **Steps** describe below to complete your installation.



STEP 1. Select your country from the **Country** list and the ADSL service provider from the **ISP** List (If there are more than two ISP in your country) and note the **"Encapsulation"** type and **"VPI & VCI"** setting.



Click "Config" if you can't find any available parameters from the presetting country list.
Check your ISP immediately for the setting/configuration details.

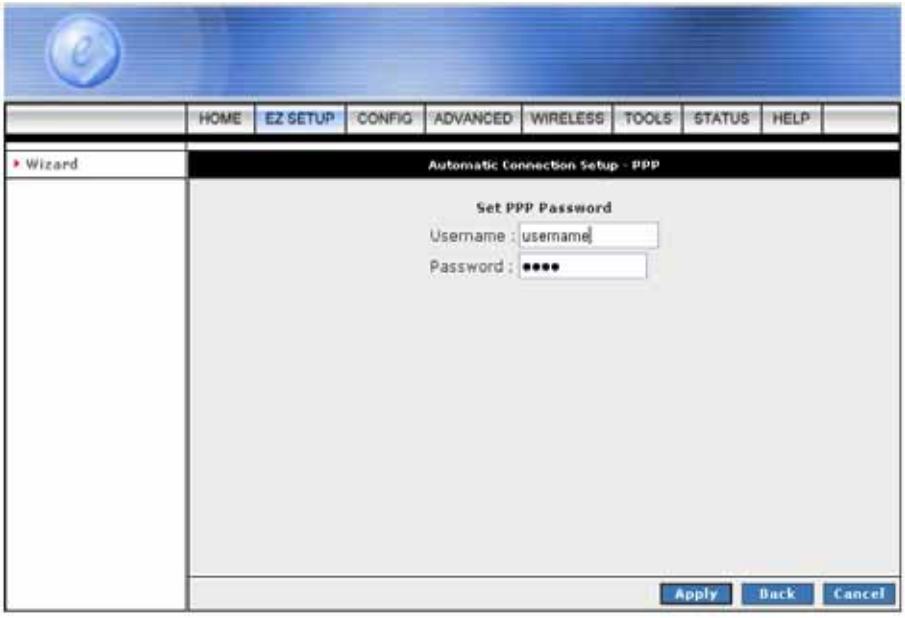
The **"Encapsulation"** type differs in each country and there are two different kinds of setup windows wizard that will pop-up:

A. For the following **"Encapsulation"** type after clicking the **"Next"** button, the pop-up setup window wizard is shown below:

☑ **PPPoA VC-Mux**

☑ **PPPoA LLC**

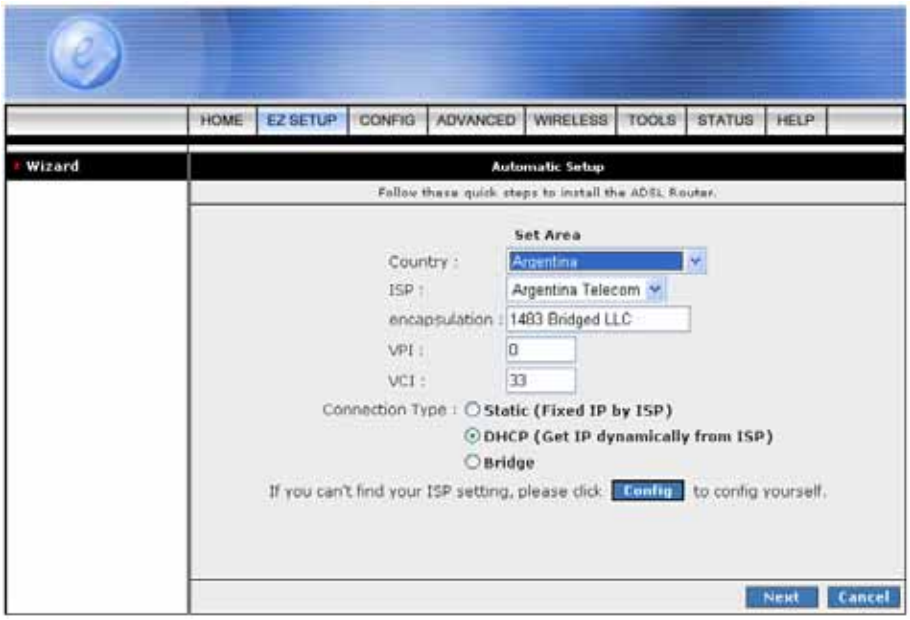
☑ **PPPoE LLC**



Manually enter your **"User Name"** and **"Password"** which will be provided by your Service Provider (ISP). Click **"Apply"** after setup.

B. For countries with the following **"Encapsulation"** type after clicking the **"Next"** button, the pop-up window is shown below:

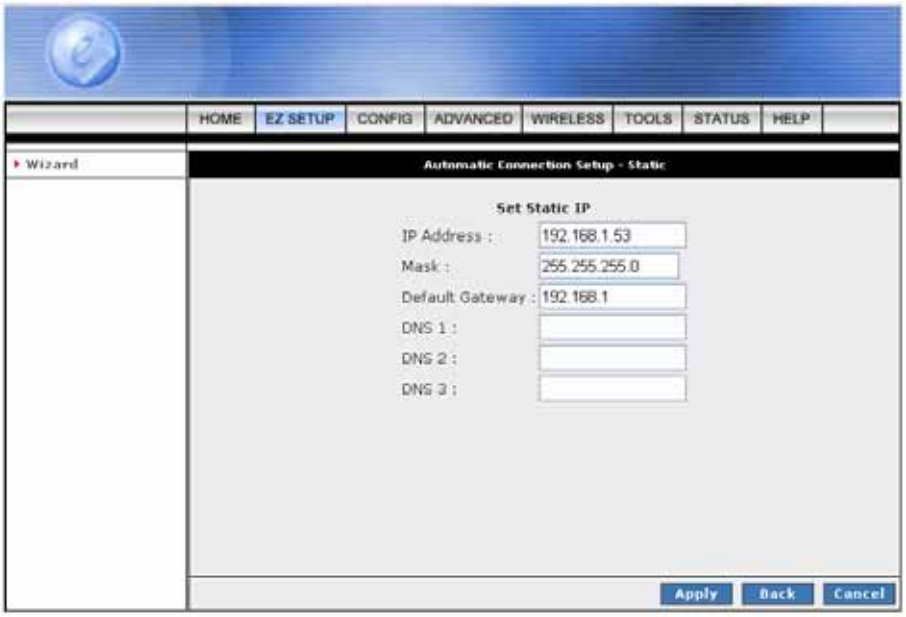
- ☑ **1483 Bridged LLC**
- ☑ **1483 Routed VC-MUX**



In this current window, you will find **THREE** different **Connection Type**:

- **Static (Fixed IP by ISP)**
- **DHCP (Get IP dynamically from ISP)**
- **Bridge**

1. **Static (Fixed IP by ISP):** Click the radio button to enable **Static (Fixed IP by ISP)** option, then click **"Next"**, the following window will pop-up:

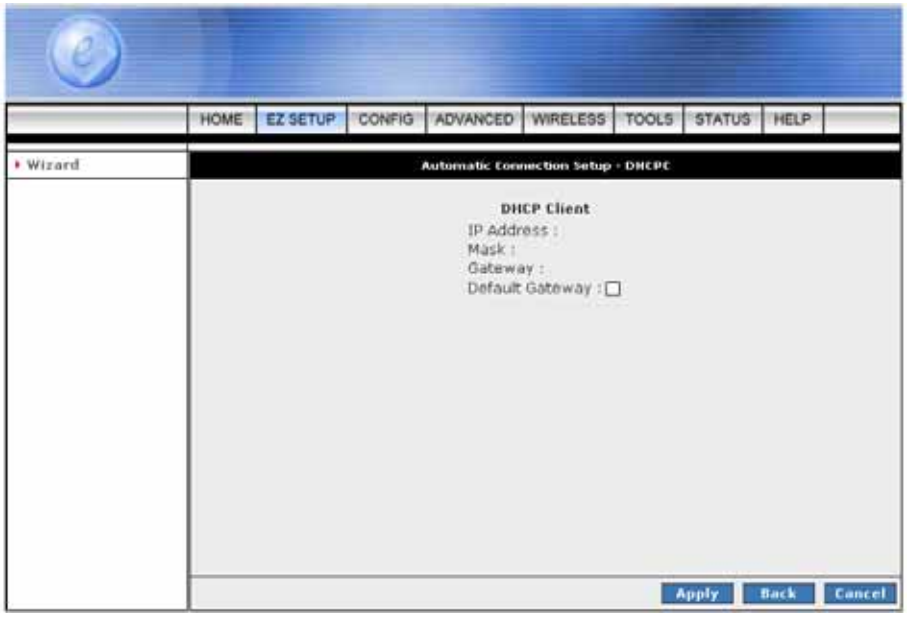


- **Set Static IP:** Static IP Settings are for users who have a Static IP Address (WAN side) from their ISP.

  - ☑ **"IP Address":** This is the static IP Address given by the ISP.
    Range for IP Address is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.
  - ☑ **"Mask":** This is the subnet mask provided by the ISP.
    Range for Subnet Mask is x.x.x.x, where 0 ≦ x ≦ 255.
  - ☑ **"Default Gateway":** This is your gateway IP address.
    Range for Gateway is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.
  - ☑ **"DNS":** This is the DNS address specify by the user or ISP. Check your ISP for setting detail.
    Range for DNS Address is x.x.x.y, where 0 ≦ x ≦ 255 and 1 ≦ y ≦ 254.

- Click **"Apply"** after your setting.

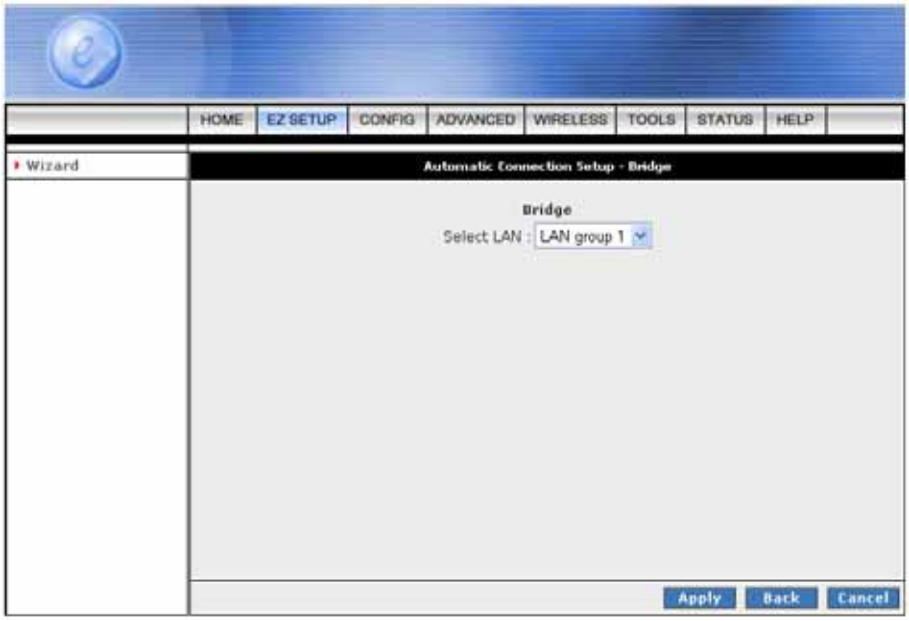
2. **DHCP (Get IP dynamically from ISP):** Click the radio button to enable **DHCP (Get IP dynamically from ISP)**. Click **"Next"** after your choice and the following window will pop-up:



- Place a check to enable the **Default Gateway**. If checked, the connection becomes the default gateway to the Internet.

- Click **"Apply"** after your setting.

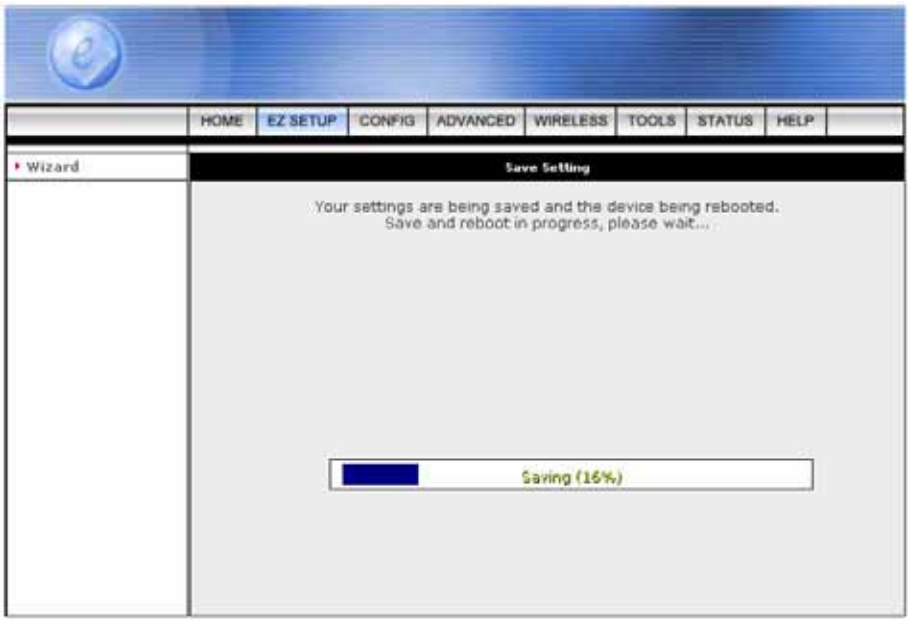
3. **Bridge:** Click the radio button to enable **Bridge** connection. Click **"Next"** after your choice and the following screen will pop-up:



- **Select LAN:** Select LAN group from the drop down manual. There are three Ethernet Bridges you can select from the drop down list or leave it in the default mode.

- Click **"Apply"** after your setting.

STEP 2. Click **"Apply"** after setup. Following windows will pop-up.



The device's system will save and activate your setting after clicking the **"Apply"** button. The following windows will pop up after the reboot process.

- Check the following items when the above window pop-up.
  - ☑ **Name:** Show the **ISP** name selected in **STEP 1**.
  - ☑ **Type:** Show the **Encapsulation** type selected in **STEP 1**.
  - ☑ **Username:** Show the **Username** manually entered in **STEP 1**.
  - ☑ **Password:** Show the **Password** manually entered in **STEP 1**.
  - ☑ **VPI:** Show the **VPI** setting as shown in **STEP 1**.
  - ☑ **VCI:** Show the **VCI** setting as shown in **STEP 1**.

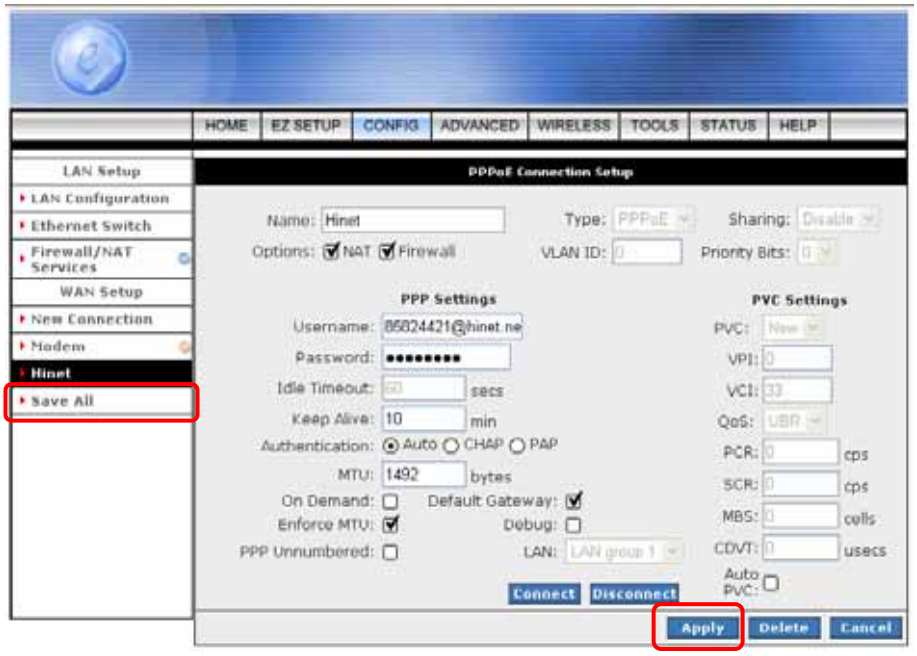
- A **Connection Profile** (Normally show the ISP Name) will be added to the left side of the configuration frame under **WAN Setup**.

NOTE: If the final setting are differ from what you'd selected in **STEP 1**, click **EZ SETUP → Wizard** and redo the setup procedures or else check your dealer immediately for technical support.

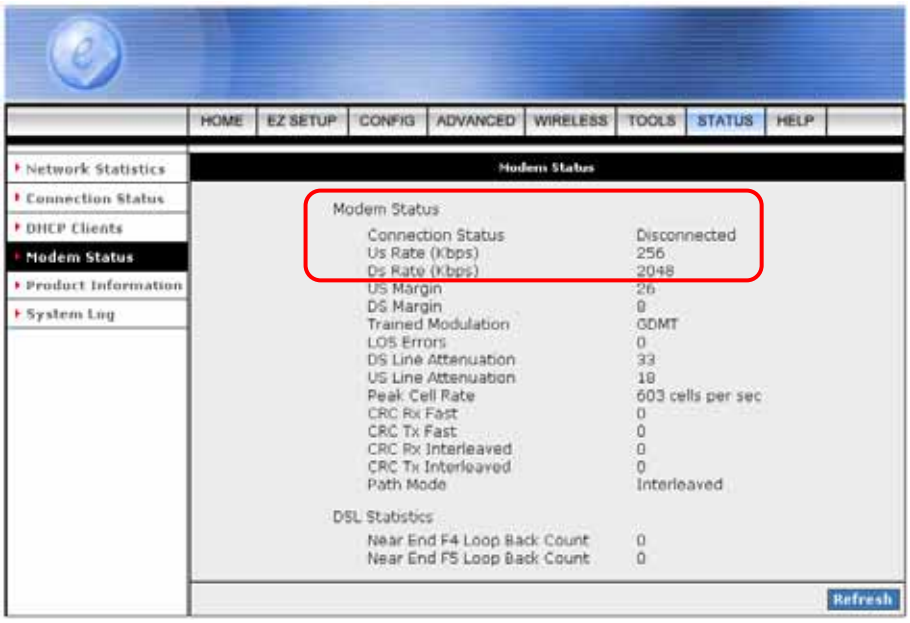
NOTE: The 4 Ports 11g Wireless ADSL2/2+ Router can be configured to maintain up to 8 Connection Profiles. Different Connection Profiles may be required if you connect to more than one ADSL service provider, or if you vary the connection type/setting you use.

Note that in many cases, only one Connection Profile will be required and only one Connection Profile in used at one time.

To complete and save the new Connection Profile, click the **Apply** button, and then click **Save All**.



STEP 3. Go to **"STATUS"** → **"Modem Status"** and the following window will pop-up. Check the **"Connection Status"**, **"Us Rate"** and **"Ds Rate"**, the numbers/data show you the actual ADSL connection speed in Kbps.



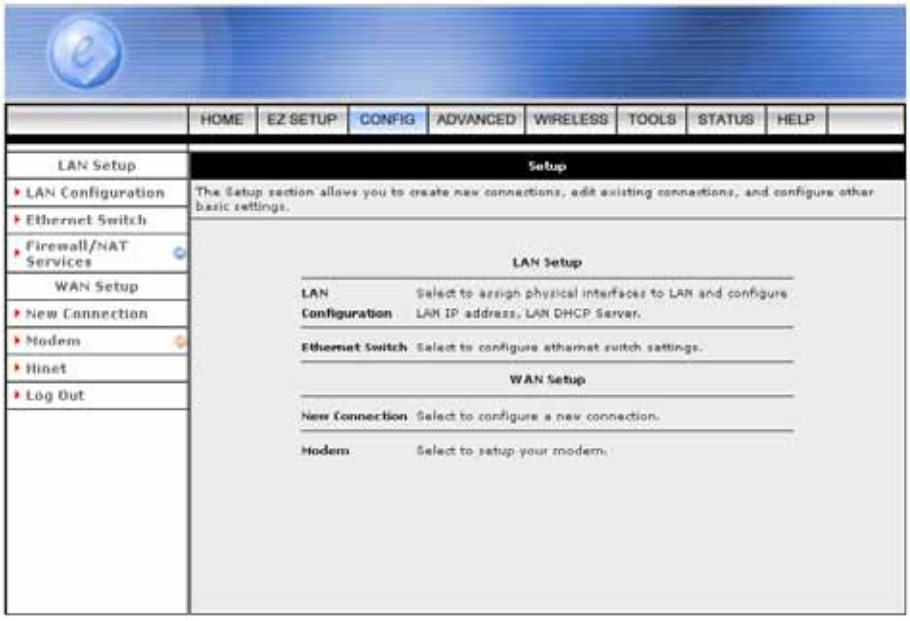
STEP 4. Launch your web browser, and enter the Google Website Address: **"www.google.com"** in the address field then press **"Enter"**.

The following Google website index page will display on your screen. This shows your ADSL connection is correctly set and access to the Internet is now available.

4.3 CONFIG

The **CONFIG** configuration page allows you to create new connections, edit existing connections, and configure other basic settings in WAN and LAN mode.

The **CONFIG** Menu is divided into two sections : **LAN Setup** and **WAN Setup**. **WAN Setup** will be dealt with first.



4.3.1 CONFIG - WAN Setup

WAN Setup: The **WAN** configuration page allows you to set the configuration for the WAN/ADSL ports. ADSL connections can be configured in a variety of ways depending on the ISP/WAN configuration, and the requirements of your home or office LAN. This 4 Ports 11g ADSL2/2+ Router supports the following ADSL connection types:

- ☑ PPPoE (RFC2516)
- ☑ PPPoA (RFC2364)
- ☑ DHCP
- ☑ Static
- ☑ Bridged (RFC1483)
- ☑ CLIP (RFC1577)

Configuring the 4 Ports 11g ADSL2/2+ Router to match these connection types may require entry of some or all of the following values:

- ☑ ISP Account Username and Password
- ☑ VPI/VCI Setting
- ☑ Encapsulation Type/Multiplexing (Either LLC or VC, check with your ISP for details)
- ☑ ADSL Handshaking Mode (Default setting is MMODE)
- ☑ Network Settings for Bridged Mode operation:

For **PPPoA** or **PPPoE** users, you need the following values from your ISP:

- ☑ Username
- ☑ Password

For Bridged Mode connections (RFC1483), you need the following information from your ISP:

- ☑ DSL Fixed Internet IP address
- ☑ Subnet Mask
- ☑ Default Gateway IP Address
- ☑ Primary DNS IP address.

The next sections will describe in detail how to set up each of these connection types and save them as Connection Profiles.

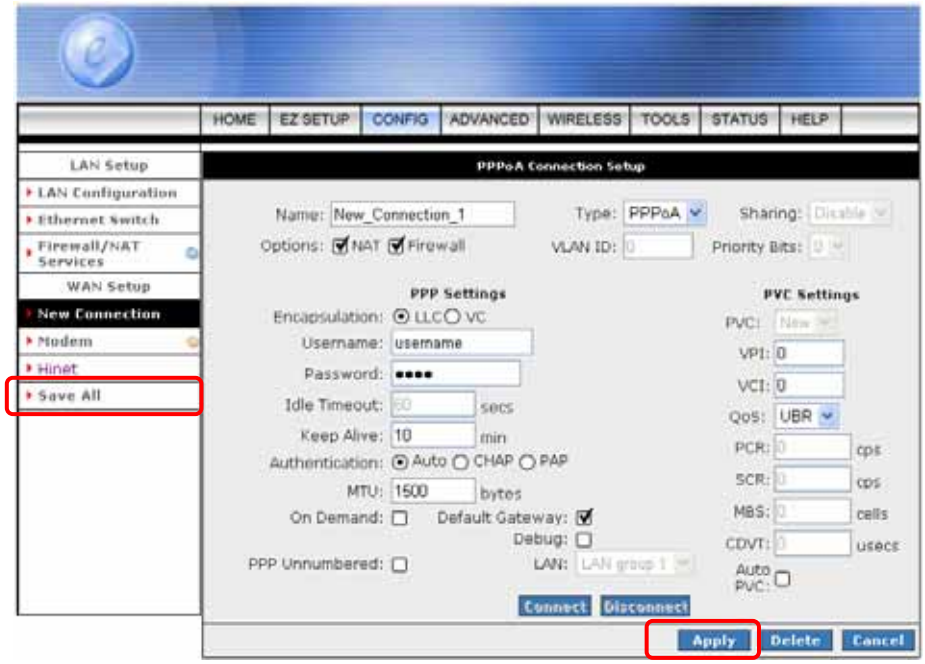
4.3.1.1 CONFIG - WAN Setup – New Connection

Click **New Connection** to setup or create a new connection profile. A **New Connection** is basically a virtual connection. This 4 Ports 11g Wireless ADSL2/2+ Router can support up to 8 different (Unique) virtual connections. If you have multiple different virtual connections, you may need to utilize the static and dynamic routing capabilities of the modem to pass data correctly.

Before you make a new WAN connection, you should make sure you have DSL connection.

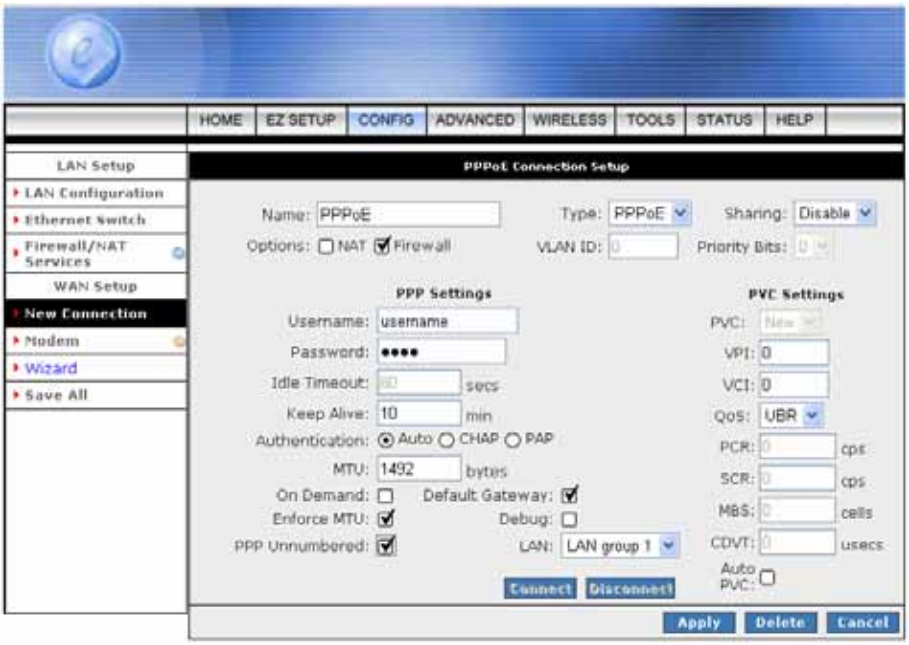
The **WAN Setup** configuration page enable the user to create, save and select connection profiles as required. (In many cases, only one connection profile will be required and only one connection profile will be used at one time).

To complete and save the new Connection Profile, click the **Apply** button, and then click **Save All**.



4.3.1.1.1 New Connection - PPPoE Connection Setup

PPPoE: When **PPPoE Mode** is selected, the following screen will pop-up. Point-to-Point Protocol (PPP) is a method of establishing a network connection between network hosts. PPPoE, also known as RFC 2516, adapts PPP to work over Ethernet for ADSL connections. PPPoE provides a mechanism for authenticating users by providing User Name and Password fields and it is a connection type provided by many ISP or Telecom.



- **Name:** Enter the PPPoE connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : **PPPoE**.
- **Sharing:** Select **"Disable"**, **"Enable"** or **"VLAN"** sharing. Default setting is **"Disable"**. The VLAN needs to be selected to create VLAN.
- **Options:** Click to enable **"NAT"** and/or **"Firewall"** functionality. Default is **"Enable"**.
- **VLAN ID:** If **"VLAN"** is selected, manually enter the **"VLAN ID"** and select **"Priority Bits"** from the drop down manual.
- **Priority Bits:** Priority is given to a VLAN connection from 0-7, 0 being the highest priority.
- **PPP Settings:**
  - ☑ **Username:** Your ISP Account ID. Check your ISP for details.
  - ☑ **Password:** Your ISP Account Password. Check your ISP for details.

- ☑ **Idle Timeout:** Specifies that PPPoE connection should disconnect if the link has no activity detected for n seconds. This field is used in conjunction with the On-Demand feature and is enabled only when the On Demand field is checked. To ensure that the link is always active, enter a 0 in this field.

- ☑ **Keep Alive:** When the On-Demand option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter 0 in this field.

- ☑ **Authentication:** The different types of available authentications are:

  - **Auto:** When auto is selected, PAP mode will run by default. However, if PAP fails, then will run as the secondary protocol. This is the default setting.

  - **PAP:** Password Authentication Procedure. Authentication is done through username and password.

  - **CHAP:** Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

- ☑ **MTU:** Maximum Transmission Unit. The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. This can be set from a minimum 128 to maximum 1500.

- ☑ **On Demand:** Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value. When checked, this field enables the Idle Timeout field.

- ☑ **Default Gateway:** If checked, this connection becomes the default gateway to the Internet.

- ☑ **Enforce MTU:** Check 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 PPP MTU. MTU (Maximum Transmission Unit) is defined as the maximum packet size (In bytes), that a particular interface can handle.

- ☑ **Debug:** Click to enable the Debug function. It is for ISP /testers to simulate packets go through from WAN side. The complete debugging information will show and listed in the System Log file.

- ☑ **PPP Unnumbered:** This is a special feature for telecommunication. It enables PPP connection to act like a bridge connection. ISP can assign blocks of public addresses to the client and make the PPP appear as pass-through from WLAn side to the LAN side.

- ☑ **LAN:** The LAN field is associated with the PPP UNunmbered field and is enabled when the PPP UNnumbered field is checked. You can specify the LAN group the packets need to go through when the PPP UNnumbered feature is activited.

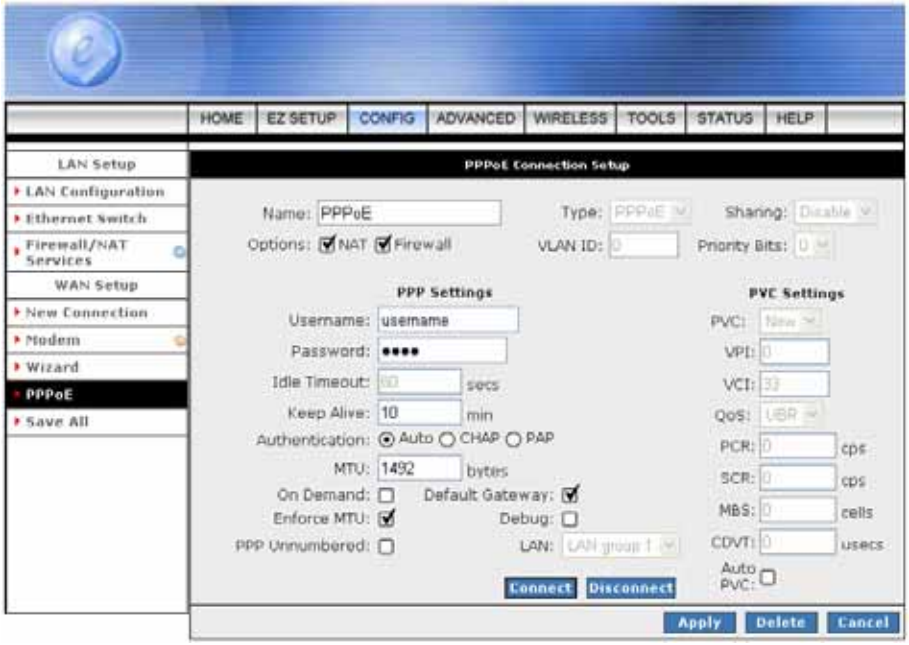
- **PVC Settings:**
  - ☑ **PVC:** This field allows you to choose the specific PVC for the PPP session.
  - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
  - ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
  - ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
  - ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
  - ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
  - ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
  - ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
  - ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports 11g Wireless ADSL2/2+ Router.
- **Connect:** Click **Connect** to attempt an ADSL connection under this connection profile.
- **Disconnect:** Click **Disconnect** to drop the ADSL connection under this connection profile.
- **Apply:** Click **Apply** to complete the connection profile's setting.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the connection profile, click **Save All** after clicking the **Apply** button.

4.3.1.1.1.1 PPPoE Configuration Procedures

1. From the **CONFIG** main page, click on **New Connection**.
2. Enter a unique name for the PPPoE connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
3. Select **PPPoE** from the **Type** drop down manual.
4. The Network Address Translation (NAT) and the Firewall options are enabled by default. Leave these in the default mode.

   Note—NAT enables the IP address on the LAN side to be translated to IP address on the WAN side. If NAT is disabled, you will not be able to go outside.
5. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

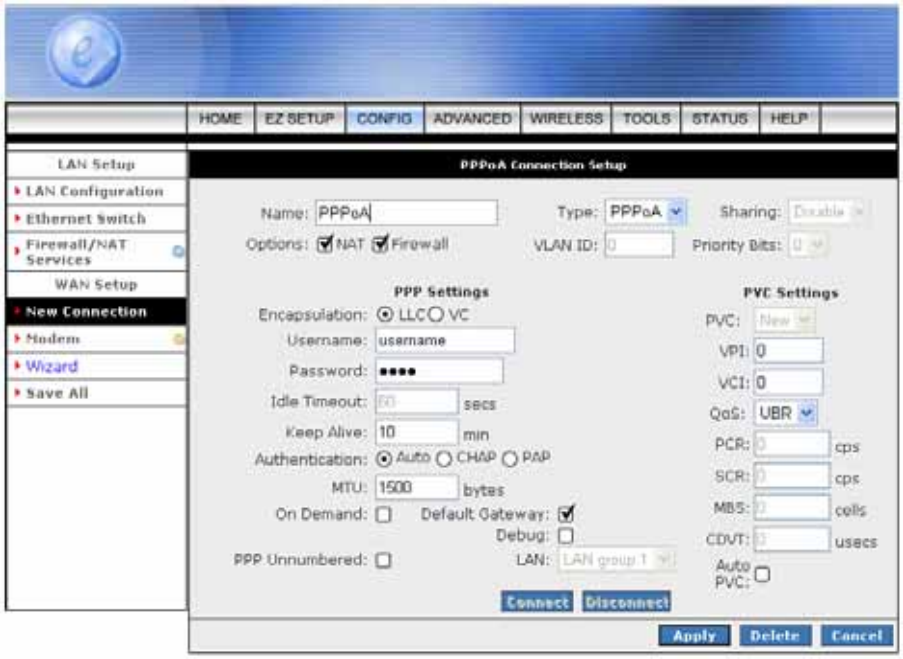
   Note—Your DSL service provider or your ISP will supply these.
6. Select the quality of service (QoS). Leave the default value if you are unsure or the ISP did not provide this information.
7. Click the **Apply** button to complete the connection setup. This will temporarily save this connection as illustrated in below. A new link has been created for this connection in the left-hand column. You can Connect/Disconnect/Apply/Delete/Cancel this connection using this screen.
8. To make the change permanent, click on **Save All**.
9. To check on the connection status, click on **Status** (at the top of the page) and select **Connection Status**.



4.3.1.1.2 New Connection - PPPoA Connection Setup

PPPoA: When **PPPoA** mode is selected, the following screen will pop-up. PPPoA is also known as RFC 2364. It is a method of encapsulating PPP packets over ATM cells which are carried over the ADSL line. PPP or Point-to-Point protocol is a method of establishing a network connection/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.



- **Name:** Enter the PPPoA connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : **PPPoA**.
- **Options:** Click to enable **"NAT"** and/or **"Firewall"** functionality. Default is **"Enable"**.
- **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 physical 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:** Your ISP Account ID. Check your ISP for details.
  - ☑ **Password:** Your ISP Account Password. Check your ISP for details.

- ☑ **Idle Timeout:** The Idle Timeout allows you to set the specific period of time, in seconds, to disconnect from the ISP if the link has no activity detected.
- ☑ **Keep Alive:** When the On-Demand option is not enabled, this value specifies the time to wait without being connected to your provider before terminating the connection. To ensure that the link is always active, enter 0 in this field.
- ☑ **Authentication:** The different types of available authentications are:
  - **Auto:** When auto is selected, PAP mode will run by default. However, if PAP fails, then will run as the secondary protocol. This is the default setting.
  - **PAP:** Password Authentication Procedure. Authentication is done through username and password.
  - **CHAP:** Challenge-Handshake Authentication Protocol. Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.
- ☑ **MTU:** Maximum Transmission Unit. The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. This can be set from a minimum 128 to maximum 1500.
- ☑ **On Demand:** Enables on-demand mode. The connection will disconnect if no activity is detected after the specified idle timeout value. When checked, this field enables the Idle Timeout field.
- ☑ **Default Gateway:** If checked, this connection becomes the default gateway to the Internet.
- ☑ **Debug:** Click to enable the Debug function. It is for ISP /testers to simulate packets go through from WAN side. The complete debugging information will show and listed in the System Log file.
- ☑ **PPP Unnumbered:** This is a special feature for telecommunication. It enables PPP connection to act like a bridge connection. ISP can assign blocks of public addresses to the client and make the PPP appear as pass-through from WLAn side to the LAN side.
- ☑ **LAN:** The LAN field is associated with the PPP UNunmbered field and is enabled when the PPP UNnumbered field is checked. You can specify the LAN group the packets need to go through when the PPP UNnumbered feature is activited.

■ **PVC Settings:**

- ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.

- ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
- ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
- ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
- ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
- ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
- ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports 11g Wireless ADSL2/2+ Router.

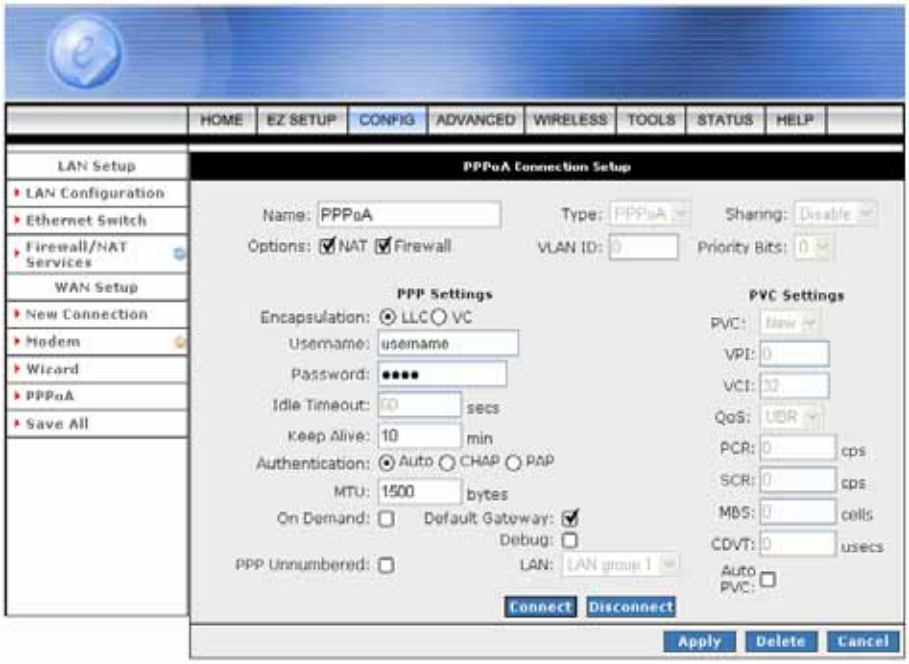
- **Connect:** Click **Connect** to attempt an ADSL connection under this connection profile.
- **Disconnect:** Click **Disconnect** to drop the ADSL connection under this connection profile.
- **Apply:** Click **Apply** to complete the connection profile's setting.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the connection profile, click **Save All** after clicking the **Apply** button.

4.3.1.1.2.1 PPPoA Configuration Procedures

1. From the Setup main page, click on **New Connection**.
2. Enter a unique name for the PPPoA connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
3. At the Type field select **PPPoA**. The PPPoA connection setup page is displayed as shown below.
4. The Network Address Translation (NAT) and the Firewall options are enabled by default. Leave these in the default mode.
5. Under **PPP Settings**, select the encapsulation type (LLC or VC).

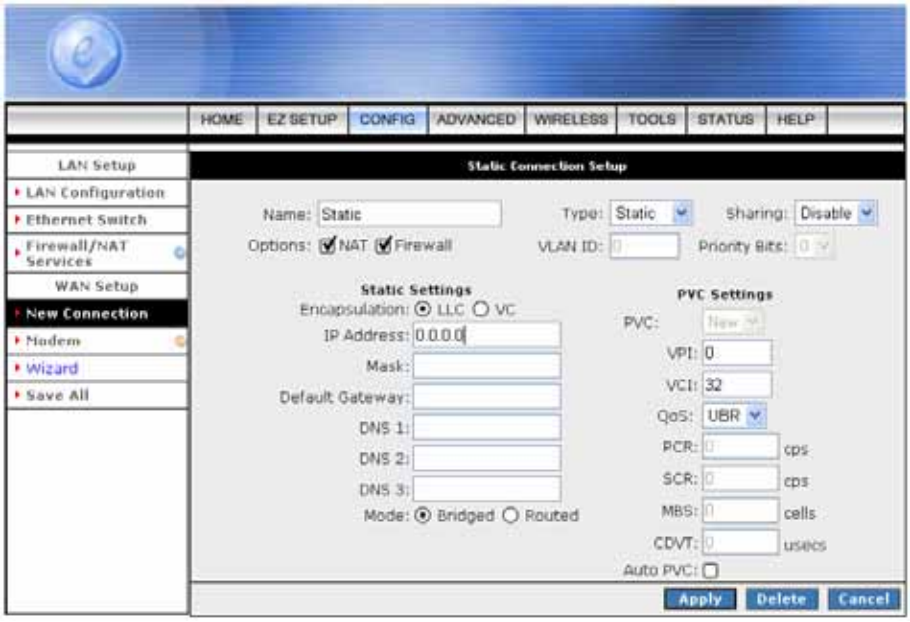
   Note—If you are not sure just use the default mode.
6. Under **PVC Settings**, enter the values of VPI and VCI settings.

   Note—Your ADSL service provider or your ISP will supply these.
7. Select the quality of service (QOS); leave the default value if you are unsure or the ISP did not provide this information.
8. Click the **Apply** button to complete the connection setup. This will temporarily save this connection as illustrated in figure below. A new link has been created for this connection in the left-hand column. You can Connect/Disconnect/Apply/Delete/Cancel this connection using this screen.
9. To make the change permanent , click on **Save All**.
10. To check on the connection status, click on **Status** (at the top of the page) and select **Connection Status**.



4.3.1.1.3 New Connection - Static Connection Setup

Static: When Static mode is selected, the following screen will pop-up. Most Internet users are provided with a dynamic IP address by their ISP for each session, however certain situations call for a Static IP address. Static is used whenever a known static IP is assigned. The accompanying information such as the Subnet mask and the gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers would enable you to have access to other web servers. Valid IP addresses range is from 0.0.0.0 to 255.255.255.255



- **Name:** Enter the Static connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : **Static**.
- **Sharing:** Select **"Disable"**, **"Enable"** or **"VLAN"** sharing. Default setting is **"Disable"**. The VLAN needs to be selected to create VLAN.
- **Options:** Click to enable **"NAT"** and/or **"Firewall"** functionality. Default is **"Enable"**.
- **VLAN ID:** If **"VLAN"** is selected, manually enter the **"VLAN ID"** and select **"Priority Bits"** from the drop down manual.
- **Priority Bits:** Priority is given to a VLAN connection from 0-7, 0 being the highest priority.

- **Static 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 physical 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).

  - ☑ **IP Address:** Enter the IP Address provided by your ISP.

  - ☑ **Mask:** Enter the Subnet mask specified by your ISP.

  - ☑ **Default Gateway:** Enter the Default Gateway as specified by the ISP.

  - ☑ **DNS:** Up to three Domain Name Server (DNS) addresses can also be specified.

  - ☑ **Mode:** For static configuration, you can also select a bridge connection or a routed connection. Since a Static IP address is typically used to host WEB servers, Bridged connection is usual however Routed is provided also. Check with ISP for confirmation.

- **PVC Settings:**

  - ☑ **PVC:** This field allows you to choose the specific PVC for the PPP session.

  - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.

  - ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.

  - ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.

  - ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.

  - ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.

  - ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.

- ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports 11g Wireless ADSL2/2+ Router.

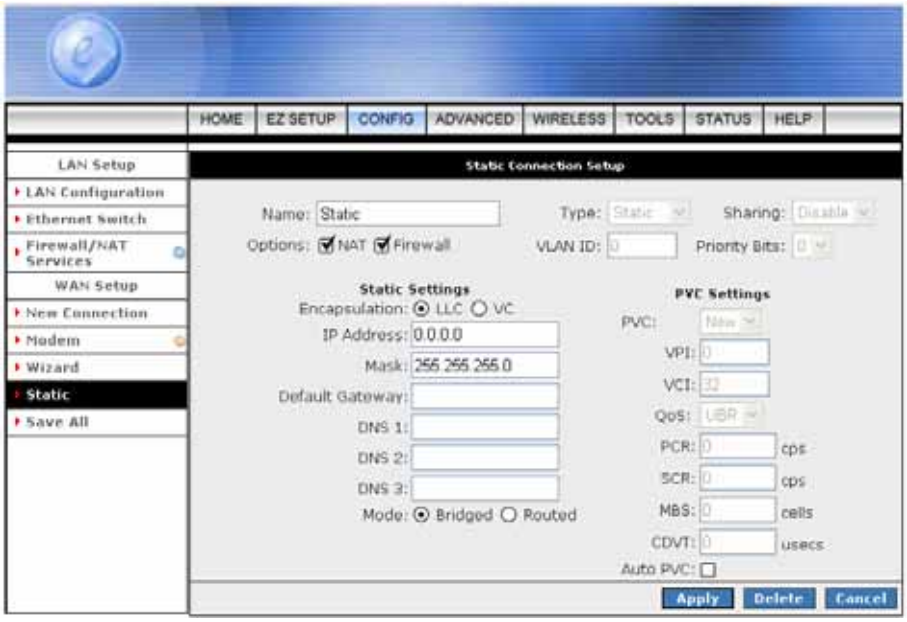
- **Apply:** Click **Apply** to complete the connection profile's setting.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the connection profile, click **Save All** after clicking the **Apply** button.

4.3.1.1.3.1 Static Configuration Procedures

1. From the Setup main page, click on **New Connection**.
2. Enter a unique name for the Static connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
3. At the **Type** field select **Static**. The Static connection setup page is displayed as shown below.
4. The Network Address Translation (NAT) and the Firewall options are enabled by default. Leave these in the default mode.
5. Under **Static Settings**, select the **Encapsulation** type (LLC or VC).

   Note—If you are not sure just use the default mode.
6. Based upon the information your ADSL/ISP provided, enter your assigned **IP address**, **Subnet Mask**, **Default Gateway** (if provided), and **Domain Name Services** (DNS) values (if provided).
7. For the static configuration, you can also select a **Bridged** connection or a **Routed** connection. Since static IP address is typically used to host WEB servers, you may want to use a bridge connection.
8. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

   Note—Your DSL service provider or your ISP will supply these.
9. Select the **Quality of Service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.
10. Click the **Apply** button to complete the connection setup. This will temporarily save this connection as illustrated in figure below. A new link has been created for this connection in the left-hand column. You can Apply/Delete/Cancel this connection using this screen.
11. To make the change permanent , click on click on **Save All**.
12. To check on the status, click on **Status** (at the top of the page) and select **Connection Status**.



4.3.1.1.4 New Connection - DHCP Connection Setup

DHCP: When DHCP mode is selected, the following screen will pop-up. Dynamic Host Configuration Protocol (DHCP) allows the ADSL Router to automatically obtain the IP address from the server. This option is commonly used in situations where the IP address is dynamically assigned and is not known prior to assignment.

- **Name:** Enter the DHCP connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : **DHCP**.
- **Sharing:** Select **"Disable"**, **"Enable"** or **"VLAN"** sharing. Default setting is **"Disable"**. The VLAN needs to be selected to create VLAN.
- **Options:** Click to enable **"NAT"** and/or **"Firewall"** functionality. Default is **"Enable"**.
- **VLAN ID:** If **"VLAN"** is selected, manually enter the **"VLAN ID"** and select **"Priority Bits"** from the drop down manual.
- **Priority Bits:** Priority is given to a VLAN connection from 0-7, 0 being the highest priority.
- **DHCP Settings:**
  - ☑ **Encapsulation:** Select the encapsulation type (LLC or VC) according to the information provided by the ISP.
  - ☑ **Default Gateway:** Click to enable the Default Gateway.

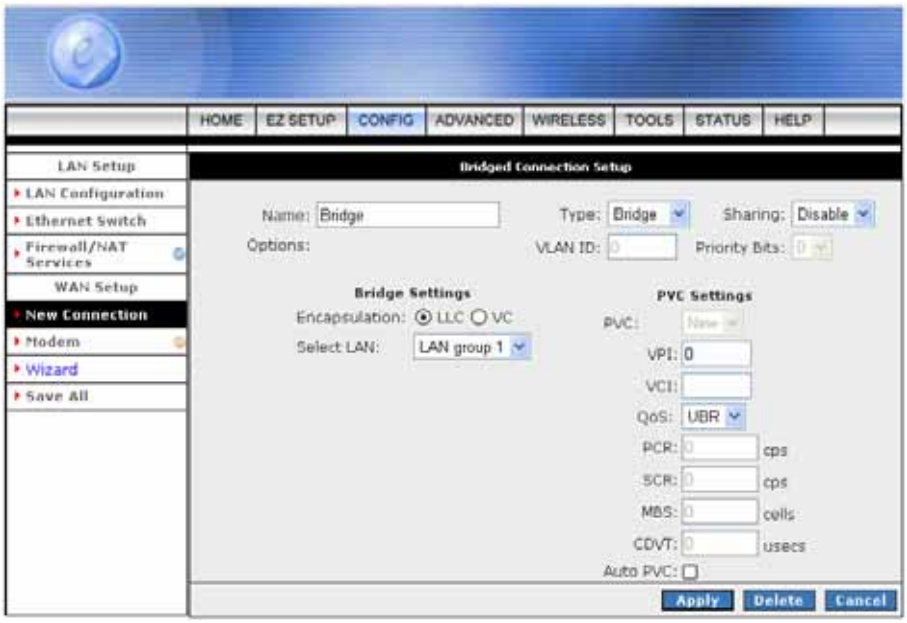
- **PVC Settings:**
  - ☑ **PVC:** This field allows you to choose the specific PVC for the PPP session.
  - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
  - ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
  - ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
  - ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
  - ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
  - ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
  - ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
  - ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports 11g Wireless ADSL2/2+ Router.
- **Renew:** Click the **Renew** button and the gateway will retrieve the IP Address, Subnet Mask, and Gateway Address.
- **Release:** Click the **Release** button to release the IP Address, Subnet Mask and Gateway Address.
- **Apply:** Click **Apply** to complete the connection profile's setting.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the connection profile, click **Save All** after clicking the **Apply** button.

4.3.1.1.4.1 DHCP Configuration Procedures

1. From the Setup main page, click on **New Connection**.
2. Enter a unique name for the Static connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
3. At the Type field select **DHCP**. The DHCP connection setup page is displayed as shown below.
4. The Network Address Translation (NAT) and the Firewall options are enabled by default. Leave these in the default mode.
5. If your ADSL line is connected and your ADSL/IPS provider is supporting DHCP, you can click the **Renew** button and the gateway will retrieve an IP address, Subnet mask, and Gateway address.
   At anytime, you can release the DHCP address by clicking on the **Release** button, and renew the DHCP address by clicking on the **Renew** button.
6. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.
   Note—Your DSL service provider or your ISP will supply these.
7. Select the **Quality of Service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.
8. Click the **Apply** button to complete the connection setup. This will temporarily save this connection as illustrated in figure below. A new link has been created for this connection in the left-hand column. You can Apply/Delete/Cancel this connection using this screen.
9. To make the change permanent , click on **Save All**.
10. To check on the status, click on **Status** (at the top of the page) and select **Connection Status**.

4.3.1.1.5 New Connection - Bridge Connection Setup

Bridge: When Bridge mode is selected, the following screen will pop-up. A Bridged connection basically disables the routing, firewall and NAT features of the 4 Ports 11g Wireless ADSL2/2+ Router. In a Bridged connection, the 4 Ports 11g Wireless ADSL2/2+ Router acts as a modem or hub, and just transmits packets between the WAN interface and the LAN interface. A Bridged connection assumes that another device is providing the routing functionality that is now disabled in the 4 Ports 11g Wireless ADSL2/2+ Router.



- **Name:** Enter the Bridge connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : **Bridge**.
- **Sharing:** Select **"Disable"**, **"Enable"** or **"VLAN"** sharing. Default setting is **"Disable"**. The VLAN needs to be selected to create VLAN.
- **Options:** Click to enable **"NAT"** and/or **"Firewall"** functionality. Default is **"Enable"**.
- **VLAN ID:** If **"VLAN"** is selected, manually enter the **"VLAN ID"** and select **"Priority Bits"** from the drop down manual.
- **Priority Bits:** Priority is given to a VLAN connection from 0-7, 0 being the highest priority.
- **Bridge Settings:**
  - ☑ **Encapsulation:** Select the encapsulation type (LLC or VC) according to the information provided by the ISP.
  - ☑ **Select LAN:** Up to three LAN Group can be specified. Select your LAN Group from the drop down manual.

- **PVC Settings:**

  - ☑ **PVC:** This field allows you to choose the specific PVC for the PPP session.
  - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.
  - ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
  - ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
  - ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
  - ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
  - ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
  - ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
  - ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports 11g Wireless ADSL2/2+ Router.

- **Apply:** Click **Apply** to complete the connection profile's setting.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the connection profile, click **Save All** after clicking the **Apply** button.

4.3.1.1.5.1 Bridge Configuration Procedures

1. From the Setup main page, click on **New Connection**.

2. Enter a unique name for the Bridge connection in the **Name** field. The name must not have spaces and cannot begin with numbers.

3. At the Type field select **Bridge**. The Bridge connection setup page is displayed as shown below.

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

5. Under **Bridge Settings**, select the encapsulation type (LLC or VC).

   Note: If you are not sure just use the default mode.

6. Under **PVC Settings**, enter the values of VPI and VCI settings.

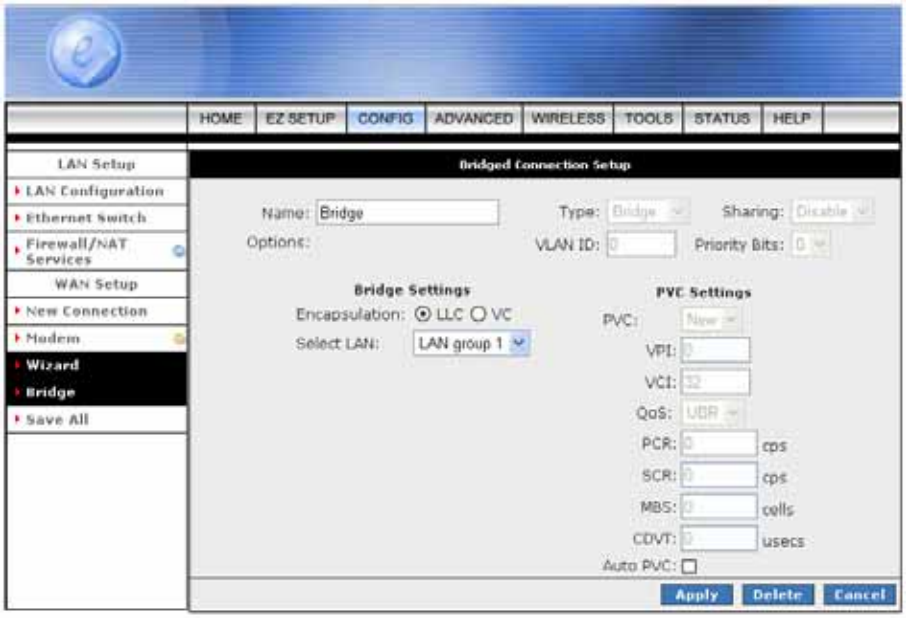
   Note: Your DSL service provider or your ISP will supply these.

7. Select the **Quality of Service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.

8. Click the **Apply** button to complete the connection setup. This will temporarily save this connection as illustrated in figure below. A new link has been created for this connection in the left-hand column. You can Apply/Delete/Cancel this connection using this screen.

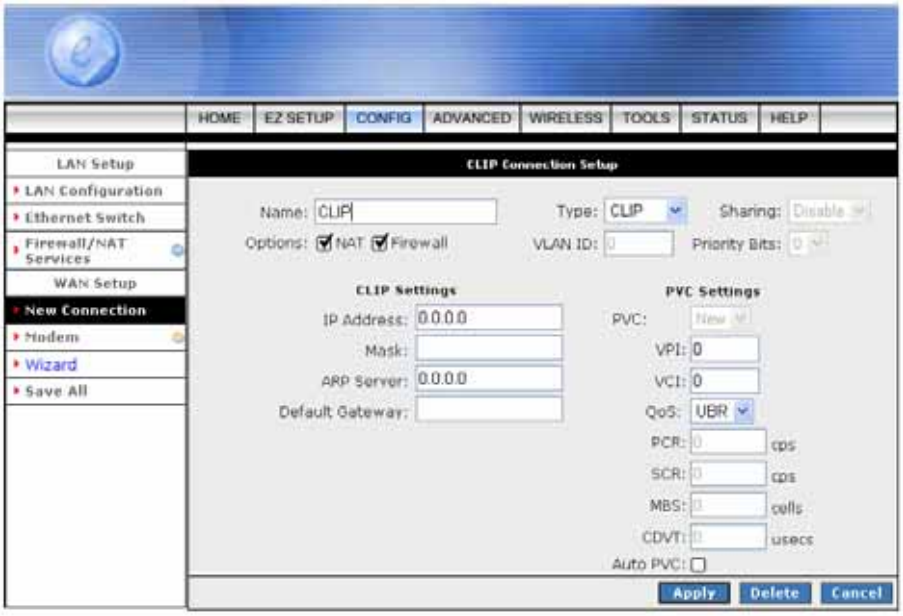
9. To make the change permanent, click on **Save All**.

10. To check on the status, click on **Status** (at the top of the page) and select **Connection Status**.



4.3.1.1.6 New Connection - CLIP Connection Setup

CLIP: When CLIP mode is selected, the following screen will pop-up. The Classical IP over ATM (CLIP) support provides the ability to transmit IP packets over an ATM network, CLIP support will encapsulate IP in an AAL5 packet data unit (PDU) frame using RFC1577and utilizes an ATM-aware version of the ARP protocol.



- **Name:** Enter the CLIP connection name. The name must be unique and must not contain spaces and must not begin with a number.
- **Type:** Connection Type : **CLIP**.
- **Options:** Click to enable **"NAT"** and/or **"Firewall"** functionality. Default is **"Enable"**.
- **CLIP Settings:**
  - ☑ **IP Address:** Enter the IP Address provided by your ISP.
  - ☑ **Mask:** Enter the Subnet mask specified by your ISP.
  - ☑ **ARP Server:** Address Resolution Protocol (ARP) server. Leave as Default (0.0.0.0) unless advised by ISP.
  - ☑ **Default Gateway:** Enter the Default Gateway as specified by the ISP.
- **PVC Settings:**
  - ☑ **VPI:** Virtual Path Identifier is a virtual path used for cell routing that is identified by an eight bit field in the ATM cell header. The VPI field specifies this eight bit identifier for routing.

- ☑ **VCI:** A Virtual Channel Identifier is a virtual channel that is identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel. The VCI field specifies this 16 bit numerical tag that determines the destination.
- ☑ **QoS:** Select the Quality of Service (QoS) type. If in doubt leave as default.
- ☑ **PCR:** Peak Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the rate cells per second that the source device may never exceed. Available only when VBR QoS is chosen.
- ☑ **SCR:** Security Cell Rate. This is an ATM (Asynchronous Transfer Mode) term to describe the security cell transmitted per second.
- ☑ **MBS:** Maximum Burst Size. A term used in ATM (Asynchronous Transfer Mode) to specify the maximum number of cells which can be transmitted at the contracted PCR (Peak Cell Rate). Available only when VBR QoS is chosen.
- ☑ **CDVT:** Cell Delay Variation Time. The Cell Delay Variation is a term used in ATM (Asynchronous Transfer Mode) to describe the time difference that is acceptable between cells being presented at the receiving host. Available only when VBR QoS is chosen.
- ☑ **Auto PVC:** Click to enable Auto PVC features. Auto PVC allows detection of virtual channels via the built-in mechanism for communicating ATM Layer information from DSLAM to the 4 Ports 11g Wireless ADSL2/2+ Router.

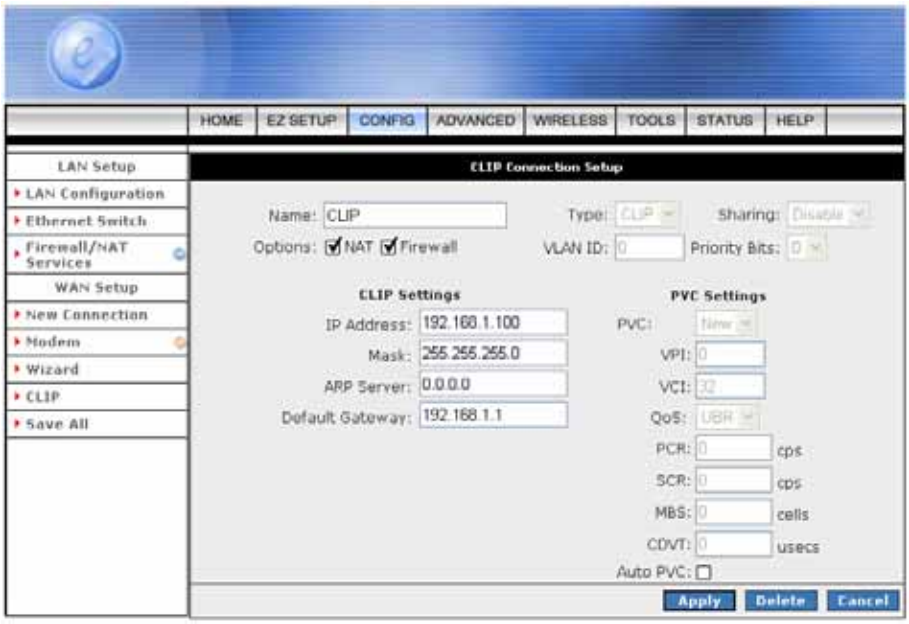
- **Apply:** Click **Apply** to complete the connection profile's setting.
- **Delete:** Click **Delete** to delete a connection.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the connection profile, click **Save All** after clicking the **Apply** button.

4.3.1.1.6.1 CLIP Configuration Procedures

1. From the Setup main page, click on **New Connection**.
2. Enter a unique name for the Static connection in the **Name** field. The name must not have spaces and cannot begin with numbers.
3. At the Type field select **CLIP**. The CLIP connection setup page is displayed as shown in figure below.
4. The Network Address Translation (NAT) and the Firewall options are enabled by default. Leave these in the default mode.
5. Based upon the information your ADSL/ISP provided, enter your assigned **IP address**, **Mask**, **ARP server**, and **Default Gateway**.
6. Under **PVC Settings**, enter the values of **VPI** and **VCI** settings.

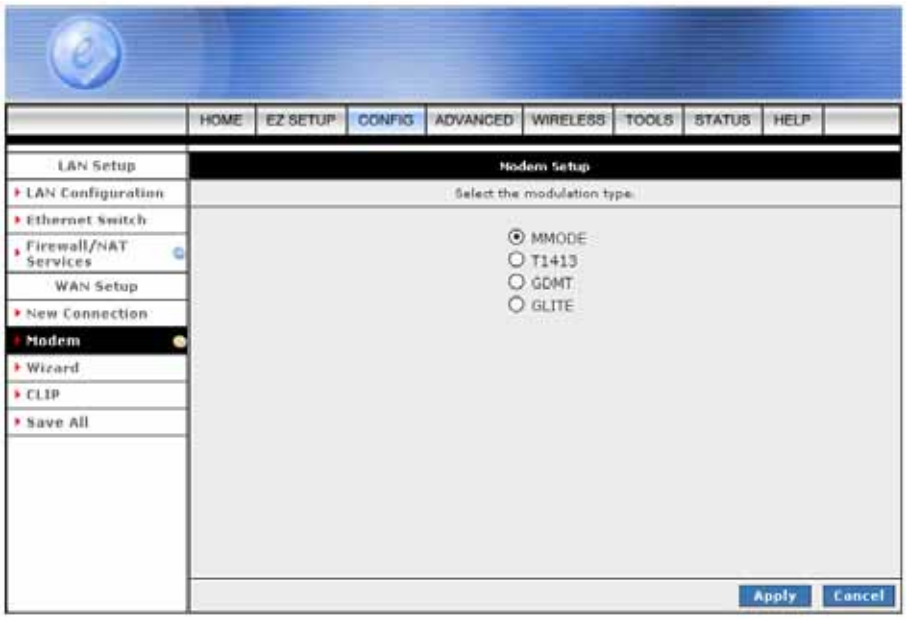
   Note: Your DSL service provider or your ISP will supply these.

7. Select the **quality of service** (QOS); leave the default value if you are unsure or the ISP did not provide this information.
8. Click the **apply** button to complete the connection setup. This will temporarily save this connection as illustrated in figure below. A new link has been created for this connection in the left-hand column. You can Apply/Delete/Cancel this connection using this screen.
9. To make the change permanent , click on **Save All**.
10. To check on the status, click on **Status** (at the top of the page) and select **Connection Status**.



4.3.1.2 CONFIG - WAN Setup - Modem

Modem: This field allows you to select from the following ADSL handshake protocols. Check your ISP for the connection type.



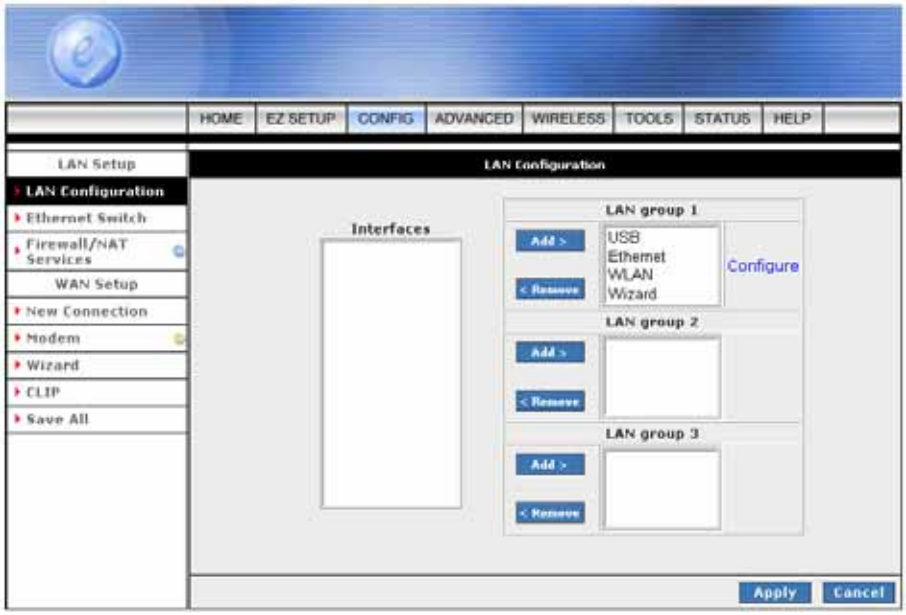
- **MMODE:** Multiple Mode (Default).
- **T1413:** T1.413 Mode.
- **GDMT:** G.dmt Mode.
- **GLITE:** G.Lite Mode.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2 CONFIG - LAN Setup

The **LAN Configuration** page allow you to select or assign physical interfaces to LAN group and configure LAN IP Address and DHCP functionality.

4.3.2.1 LAN Setup - LAN Configuration

Click LAN Configuration and the following screen will be shown.

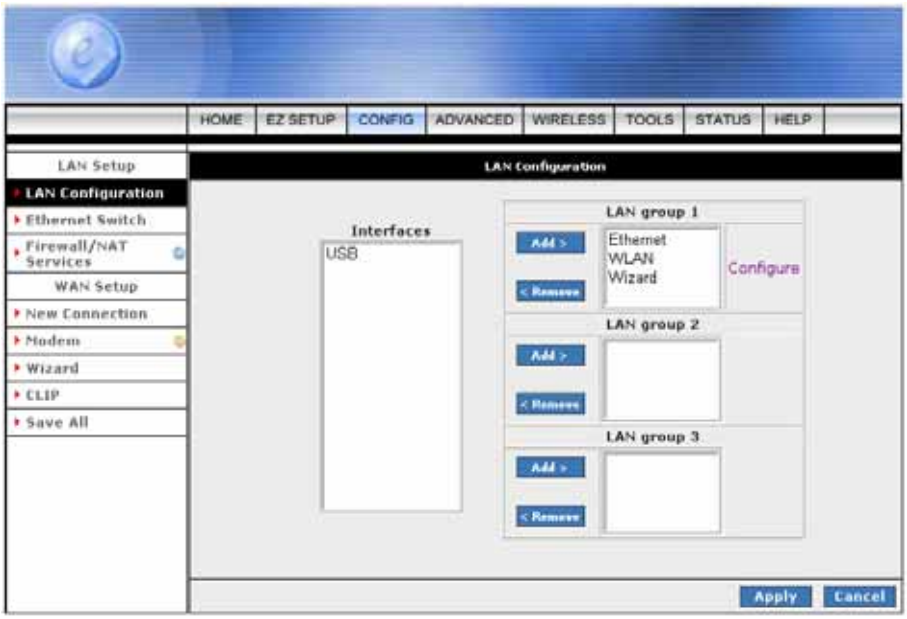


- Click **Add** or **Remove** Interfaces from list under the different LAN Group. The LAN Group features only supported under **Bridge Mode** setting. Interfaces under the same LAN Group (WLAN, Ethernet and USB) will have the ability to communicate with each other. Different LAN Group are prohibited to communicate with one another.
- Click **Configure** for detail LAN Group setting. Refer to next section (4.3.2.1.2) for detail LAN Configuration or Setting.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

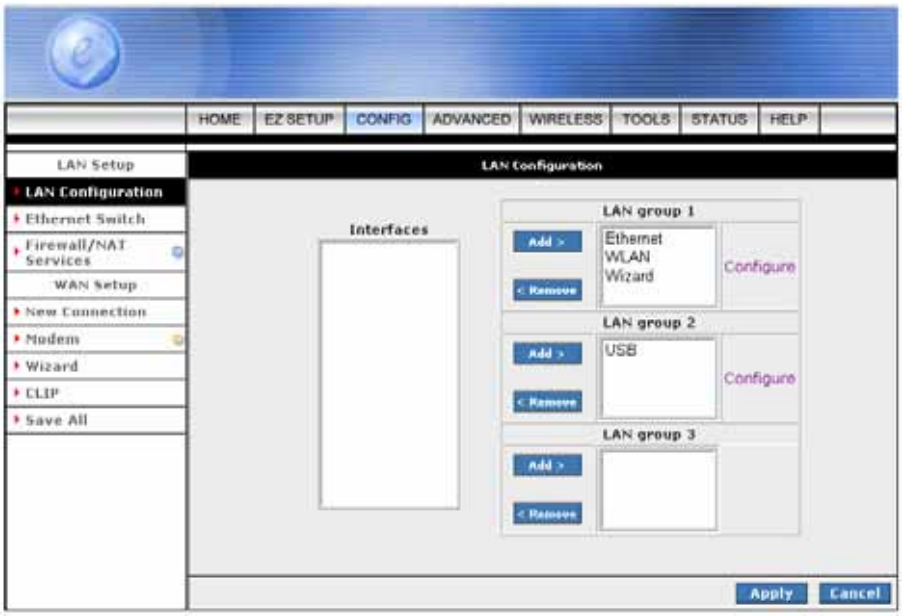
4.3.2.1.1 LAN Configuration Procedures

1. Select **USB** interface in LAN Group and click **Remove**. **USB** moves to the Interface box on the left as shown in figure below.

   Note—You can configure the USB interface and/or WLAN interface to a different LAN group. However, the Ethernet interface is default in LAN group 1 and cannot be moved.



2. Select **USB** in the Interface box and click **Add** next to LAN group 2. **USB** moves to LAN group 2 as shown in figure below. The Configure link for LAN group 2 has also been generated, which allows additional configurations for the defined LAN group.



3. Click **Apply** to temporarily save the changes.
4. To make the change permanent, click on **Save All**.

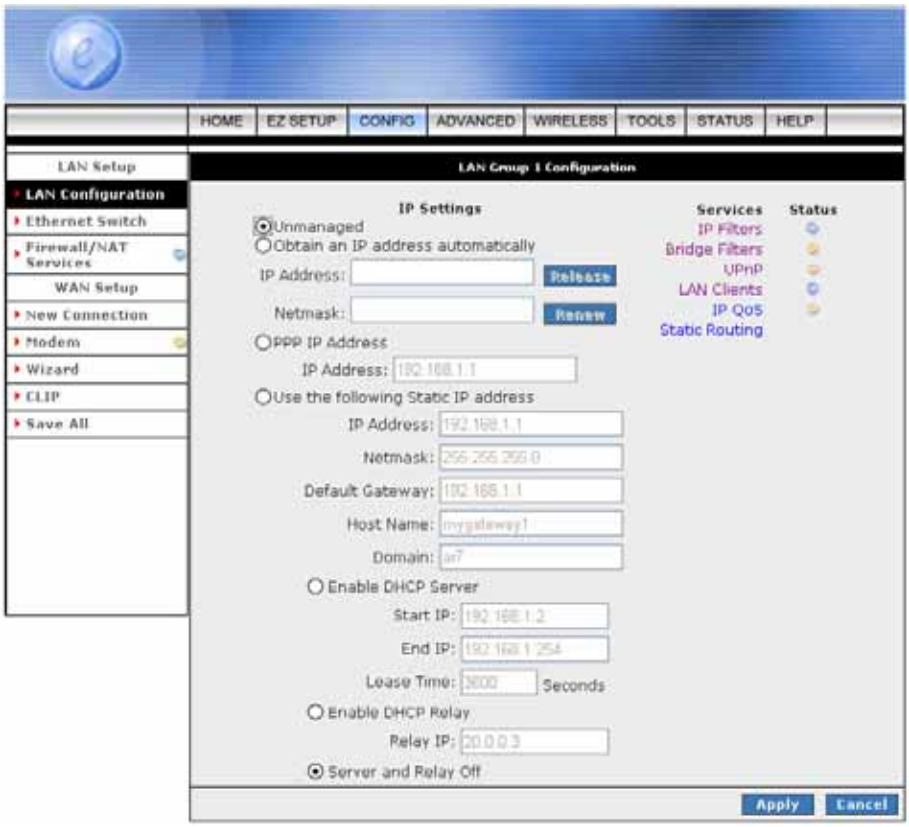
4.3.2.1.2 LAN Configuration - Unmanaged

The LAN Group Configuration screen allows you to configure settings for each defined LAN group. Notice that you can also view the status of advanced services that can be applied to this LAN group.

Unmanaged: Click the **Unmanaged** radio button, the following configuration screen will pop-up. All filling items are hidden except the **Server and Relay Off** (Unchangeable) radio button will turn on.

Unmanaged is a state when the LAN group is not configured and no IP address has been assigned to the bridge.

Click the **Services** items will guides you to detail setting. Refer to **ADVANCED** section for setting/configuration details.



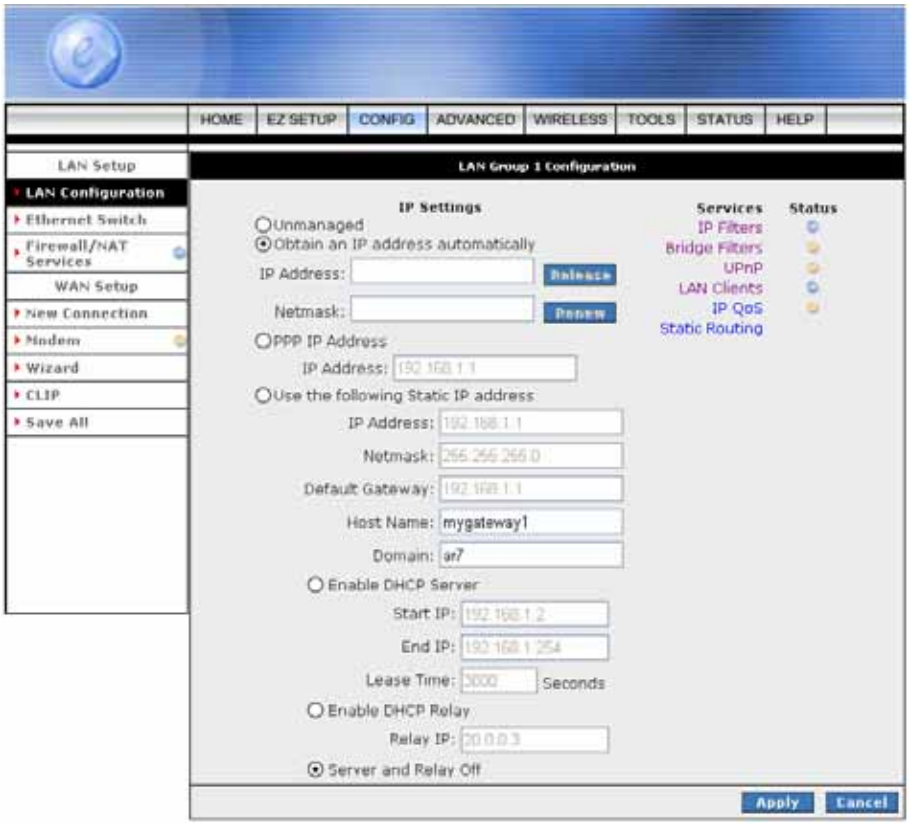
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2.1.3 LAN Configuration – Obtain an IP Address Automatically

Obtain an IP address automatically: The following configuration screen will pop-up. All filling items will be hidden except **Host Name**, **Domain Name** and **Server and Relay Off** (Unchangeable) radio button will turn on.

When this function is enabled, your 4 Ports 11g Wireless ADSL2/2+ Router acts like a client and can request IP address from the DHCP server.

Click **Services** selection items will guides you to detail setting. Refer to **ADVANCED** section for setting/configuration details.



- **Host Name:** Can be any alpha-numeric expression that does not contain spaces.

- **Domain Name:** Used in conjunction with the host name to uniquely identify the gateway. To access the 4 Ports 11g Wireless ADSL2/2+ Router's web pages, the user can type **192.168.1.1** (The default IP Address) or type **mygateway1.ar7** in the Web browser's address bar.

- **Apply:** Click **Apply** to complete the setting.

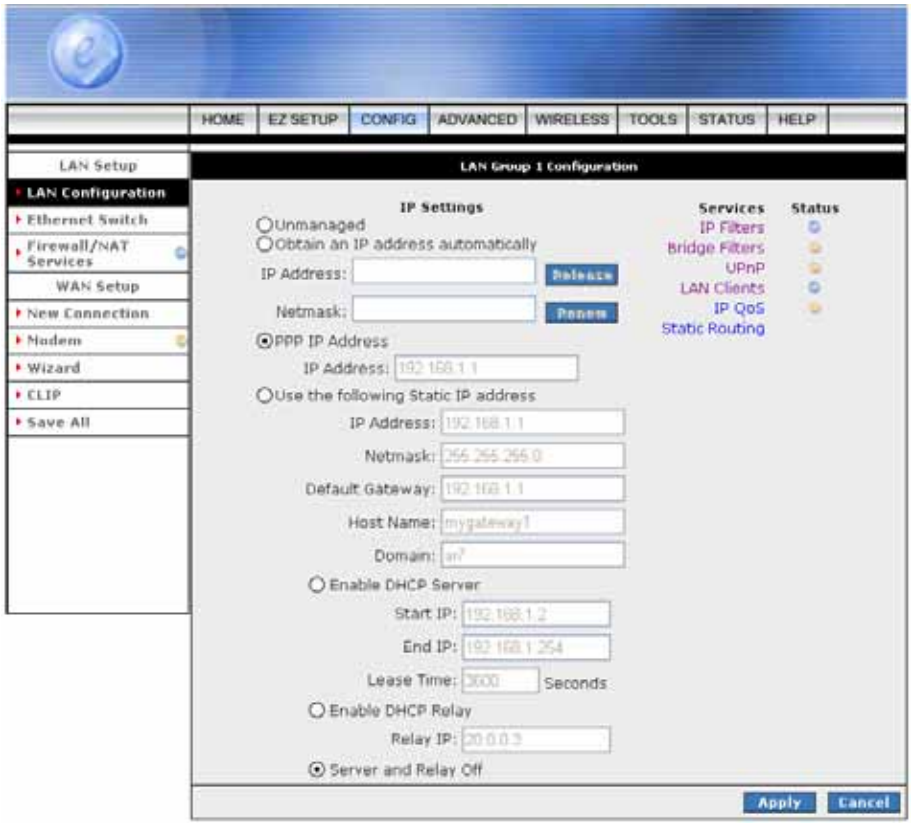
- **Cancel:** Click **Cancel** to ignore all the changes.

- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2.1.4 LAN Configuration – PPP IP Address

PPP IP Address: Click the **PPP IP Address** radio button, the following configuration screen will pop-up. All filling items are hidden except the **Server and Relay Off** (Unchangeable) radio button will turn on.

Click the **Services** items will guides you to detail setting. Refer to **ADVANCED** section for setting/configuration details.

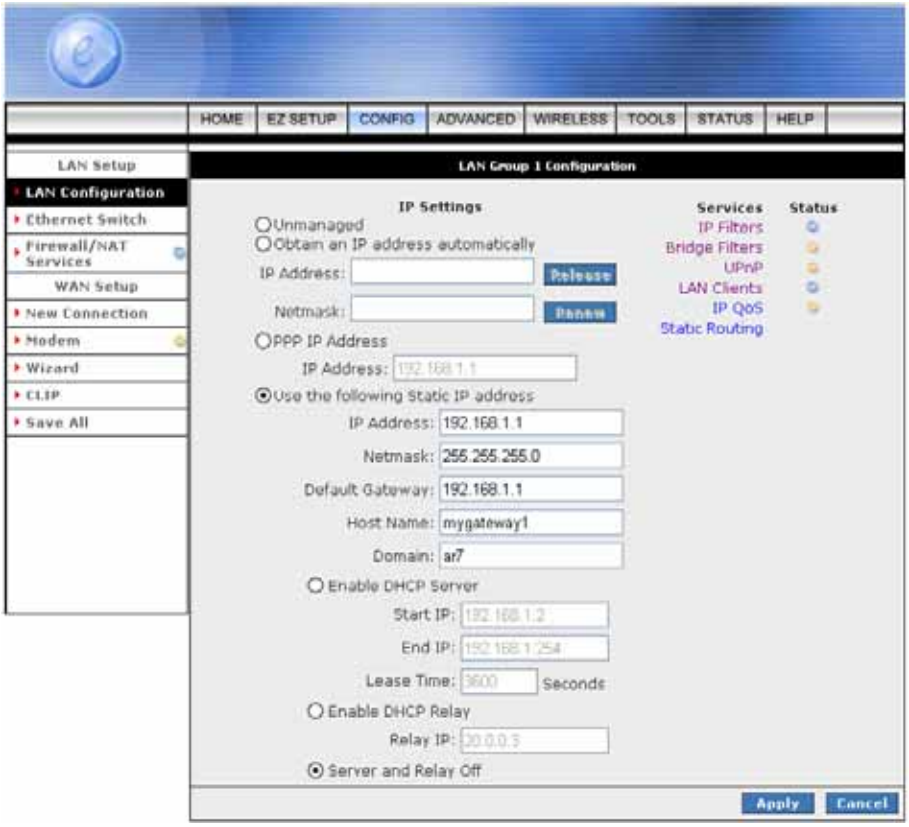


- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.2.1.5 LAN Configuration – Use The Following Static IP Address

Use the following Static IP address: The following configuration screen will pop-up.

Click the radio button to select **Enable DHCP Server** or **Enable DHCP Relay** or **Server and Relay Off**. Manually enter the necessary items based on each selection.



- **IP Address:** The 4 Ports 11g Wireless ADSL2/2+ Router's default IP address is 192.168.1.1.
- **Netmask:** The 4 Ports 11g Wireless ADSL2/2+ Router's default subnet mask is 255.255.255.0. This subnet will allow the gateway to support 254 users. If you want to support a larger number of users you can change the subnet mask. The DHCP server is defaulted to only give out 255 IP addresses. Remember that if you change your 4 Ports 11g Wireless ADSL2/2+ Router's IP address and you have DHCP enabled, the DHCP configuration must reside within the same subnet
- **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 will provide you with the default gateway Address.
- **Host Name:** Can be any alpha-numeric expression that does not contain spaces.
- **Domain:** Used in conjunction with the host name to uniquely identify the gateway.

- **Enable DHCP Server:** Click the radio button to enable the DHCP Server. By default, your Ports 11g Wireless ADSL2/2+ Router has 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; if you plug a second DHCP server into the network, you will experience network errors and the network will not function correctly.

  - ☑ **Start IP:** The Start IP Address indicates the beginning of the range at which the DHCP server starts issuing IP addresses.

    This value must be greater than the Routers IP address value. If the Routers IP address is 192.168.1.1 (The default) than 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 gateways IP address. In other words, if the gateways IP address is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.128.1.2/192.128.1.100, you will not be able to communicate to the gateway if your PC has DHCP enabled.

  - ☑ **End IP:** The End IP Address indicates the end of the IP address range.

    The ending address must not exceed a Subnet Limit of 253; hence the maximum value that can be entered in this example is 192.168.1.254.

    If the DHCP server runs out of DHCP addresses, users will not get access to network resources. If this happens you can increase the Ending IP address (to the limit of 255) 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 gateways IP address. In other words, if the gateways IP address is 192.168.1.1 (default) and you change the DHCP start/end IP addresses to be 192.128.1.2/192.128.1.100, you will not be able to communicate to the gateway if your PC has DHCP enabled.

  - ☑ **Lease Time:** Lease Time is the amount of time a network user will be allowed connection to the 4 Ports 11g Wireless ADSL2/2+ Router with their current Dynamic IP address. The amount of time is in units of minutes; the default value is 3600 minutes (60 hours).

- **Enable DHCP Relay:** Click the radio button to enable the DHCP Relay. When the gateway is configured as DHCP server, it assigns the IP addresses to the LAN clients. When the gateway is configured as DHCP relay, it is responsible for forwarding the requests and responses negotiating between the DHCP clients and the server.

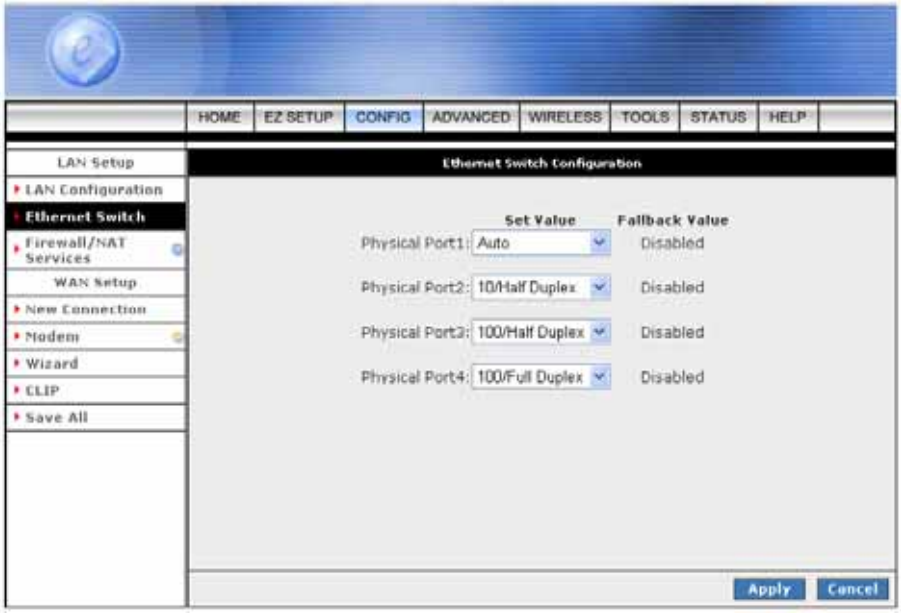
  - ☑ **Relay IP:** This is the IP Address given by the ISP.

- **Server and Relay Off:** Click the radio button to enable. By turning off the DHCP server and relay the network administrator must carefully 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 and your Gateway must be on the same subnet as all the other computers.

- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.3 LAN Setup - Ethernet Switch

The **Ethernet Switch** page allows you to set the LAN port into the following modes (Default is **"Auto"**). Ethernet Switch port settings can be configured to meet the requirements of your LAN configuration.



- **Auto:** The 4 Ports 11g Wireless ADSL2/2+ Router will automatically sense which mode to use, selecting between 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex, and 10 Mbps Half Duplex. Default setting is **"Auto"**.

- **10/Half Duplex:** Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 10Mbps.

- **10/Full Duplex:** Data can be transferred and received simultaneously at the transfer rate of 10Mbps.

- **100/Half Duplex:** Data cannot be transferred and received at the same time. For example, data can be sent, and once the transmission is complete, data can be received. This is done at a transfer rate of 100Mbps.

- **100/Full Duplex:** Data can be transferred and received simultaneously at the transfer rate of 100Mbps.

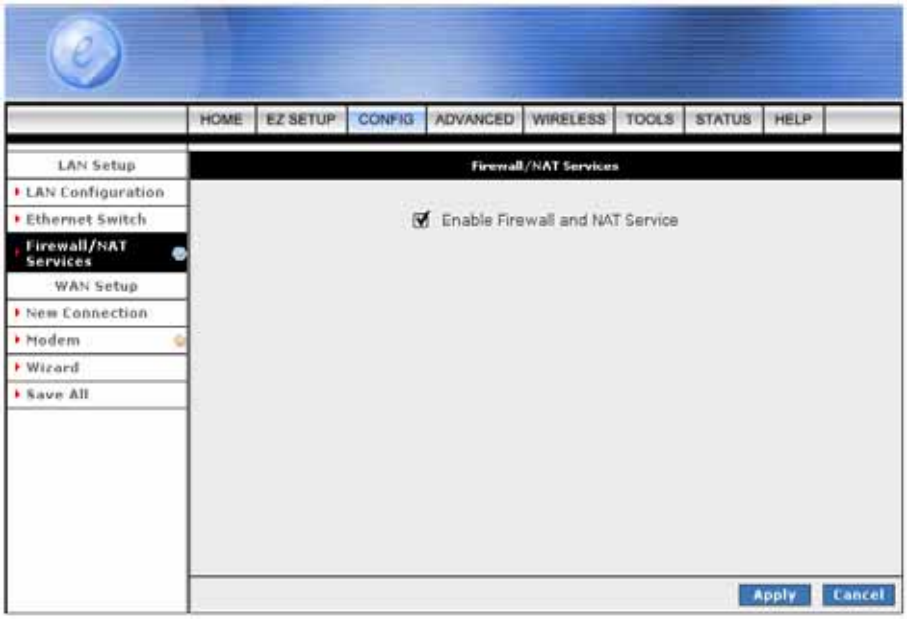
- **Apply:** Click **Apply** to complete the setting.

- **Cancel:** Click **Cancel** to ignore all the changes.

- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.3.4 LAN Setup - Firewall/NAT Services

Firewall/NAT Services: Place a check to **"Enable"** the most basic Firewall and NAT Service to secure your system. The 4 Ports 11g Wireless ADSL2/2+ Router is equipped with advanced Firewall features to provide security from malicious attack, hacking or eavesdropping across the Internet. It's strongly recommend that you enable this feature for security purpose. The default setting is **"Enable"**.



- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4 ADVANCED

The Advanced Menu provides access to advanced networking, management and routing capabilities.

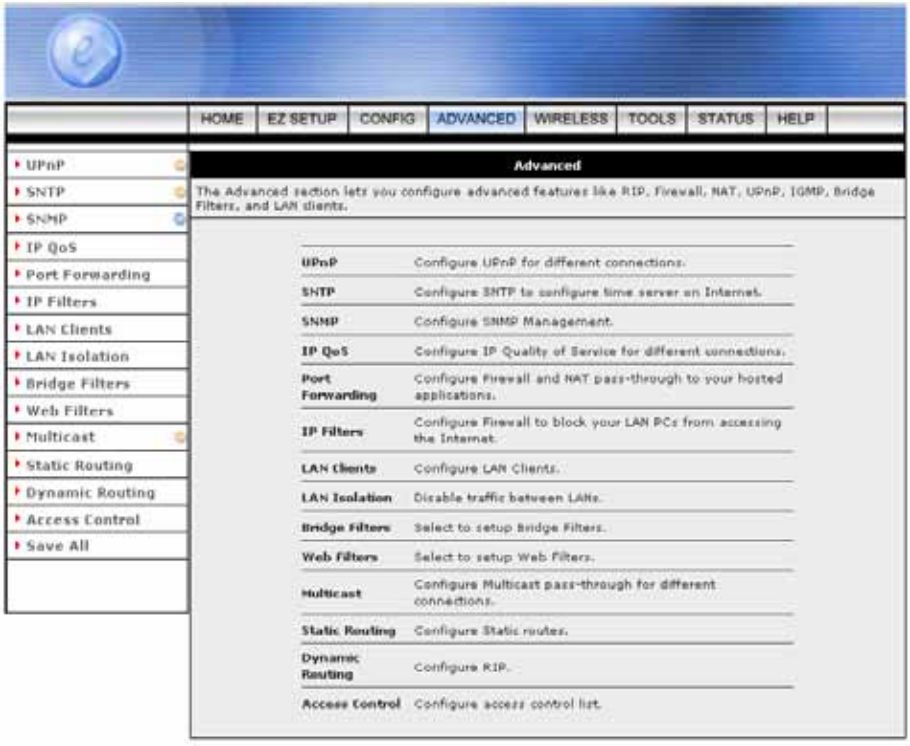
Click the **ADVANCED** tab and the following screen will pop-up.

The Advanced tab allows you to perform advanced configuration functions for existing connections including:

- Enabling and disabling of key features including voice, UPnP, SNTP, SNMP, IP QoS, RIP, access control and multicasting.
- Assignment of IP QoS weighting to connections.
- Management of LAN port interfaces, packet flow, and filtering.

At least one WAN connection must be configured before implementing advanced WAN configuration features.

At least on LAN group must be defined before implementing advanced LAN configuration features.



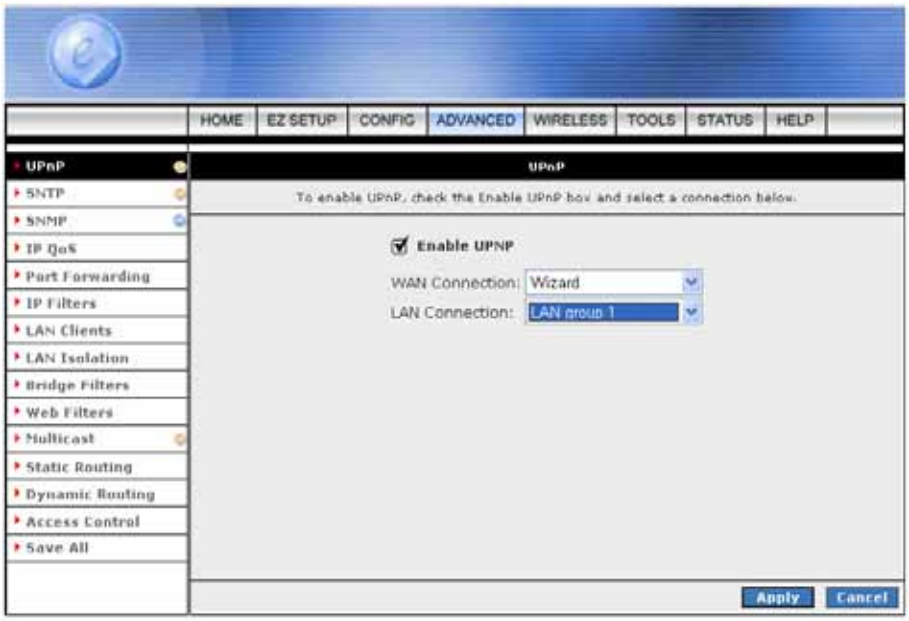
- **UPnP:** Configure UPnP for different connections.
- **SNTP:** Configure SNTP to configure time server on Internet.
- **SNMP:** Configure SNMP Management.
- **IP QoS:** Configure IP Quality of Service for different connections.
- **Port Forwarding:** Configure Firewall and NAT pass-through to your hosted applications.
- **IP Filters:** Configure Firewall to block your LAN PCs from accessing the Internet.
- **LAN Clients:** Configure LAN Clients.
- **LAN Isolation:** Disable traffic between LANs.

- **Bridge Filters:** Select to setup Bridge Filters.
- **Web Filters:** Select to setup Web Filters.
- **Multicast:** Configure Multicast pass-through for different connections.
- **Static Routing:** Configure Static routes.
- **Dynamic Routing:** Configure RIP.
- **Access Control:** Configure access control list.

4.4.1 ADVANCED - UPnP

UPnP: Universal Plug and Play is a protocol which automates connectivity between network devices, including computers, game consoles, digital cameras and other systems which connect via TCP/IP. Applications which implement the UPnP protocol are able to negotiate a connection with a UPnP-enabled device without requiring manual device configuration.

UPnP (Universal Plug and Play), NAT (Network Address Translation) and Firewall Traversal allow traffic to pass through the router for applications using the UPnP protocol. UPnP can be enabled/disabled across Multiple LAN segments. This feature requires one active ADSL connection. In presence of multiple ADSL connections, select the one over which the incoming traffic will be present.



- **Enable UPNP:** Place a check to enable the UPnP feature.
- **WAN Connection:** Select the required **WAN Connection Profile** by clicking on the drop down button adjacent to the Connection Profile name.
- **LAN Connection:** Select the **LAN Group** fro the drop down manual.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

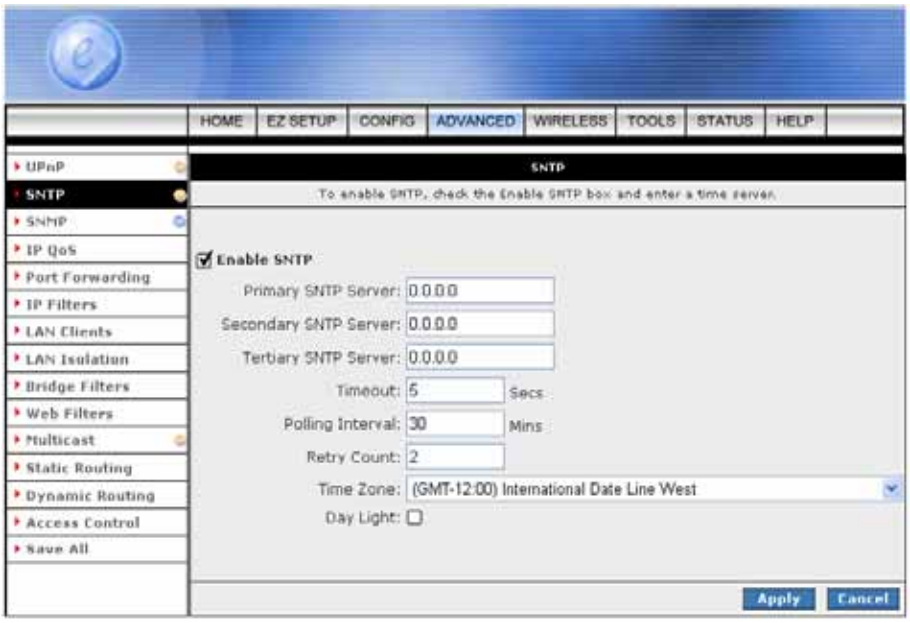
4.4.1.1 UpnP Configuration Procedures

1. Check **Enable UPnP**. This enables the WAN Connection and LAN Connection fields.
2. Select the **WAN Connection** and **LAN Connection** that will utilize UPnP from the drop-down lists.
3. Click **Apply** to temporarily save the setting.
4. To make the change permanent, click on **Save All**.

4.4.2 ADVANCED - SNTP

SNTP: SNTP (Simple Network Timing Protocol) is a protocol used to synchronize the system time to the public SNTP servers. It uses the UDP protocol on port 123 to communicate between clients and servers. Place a check at Enable SNTP to enable the SNTP functionality.

When the SNTP feature is enabled, your 4 Ports 11g Wireless ADSL2/2+ Router will start querying for the time clock information from the primary SNTP server. If it fails to get a valid response within the “Timeout” period, it will try for “Retry” number of times, before moving to the Secondary SNTP server. If it fails to get a valid response from Secondary STNP server within valid retry times, it starts querying Tertiary SNTP server. If it fails to get a valid response from all the servers, then the program stops. When a valid response is received from one of the server, the program sleeps for “Polling Interval” amount of minutes, before starting the whole process again.



- **Enable SNTP:** Place a check to enable SNTP feature.
- **Primary SNTP Server:** The IP address or the host name of the primary SNTP server.
- **Secondary SNTP Server:** The IP address or the host name of the secondary SNTP server.
- **Tertiary SNTP Server:** The IP address or the host name of the tertiary SNTP server.
- **Timeout:** A time limit for an operation. If the 4 Ports 11g Wireless ADSL2/2+ Router failed to connect to a SNTP server within the “Timeout” period, it will retry the connection.
- **Polling Interval:** The length of time (In Minutes) the 4 Ports 11g Wireless ADSL2/2+ Router retrieves the time from the SNTP Server. Time between a successful connection with a SNTP server and a new attempt to connect to an SNTP server.

- **Retry Count:** Enter the Retry Count to access the SNTP Server. The number of times the 4 Ports 11g Wireless ADSL2/2+ Router will try to connect to an SNTP server before it try to connect to the next server in line.
- **Time Zone:** This specifies the time zone (Geographical location).
- **Day Light:** Place a check at the Day Light to activate Daylight Savings Time.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.2.1 SNTP Configuration Procedure

1. Check **Enable SNTP**.

2. Use as a reference and configure the following fields:

   - Primary SNTP Server
   - Secondary SNTP Server
   - Tertiary SNTP Server
   - Timeout
   - Polling Interval
   - Retry Count
   - Time Zone
   - Day Light

3. Click **Apply** to temporarily save the setting.

4. To make the change permanent, click on **Save All**.

4.4.3 ADVANCED - SNMP

SNMP: Simple Network Management Protocol (**SNMP**) is a troubleshooting and management protocol, which uses the UDP protocol on port 161 to communicate between clients and servers.

SNMP uses a manager MIB (management information base) agent solution to fulfill the network management needs. The agent is a separate station that can request data from an SNMP agent in each of the different managed system in the network.

The agent uses the MIBs as dictionaries of manageable objects. Each SNMP-managed device has at least one agent that can respond to the queries from the NMS. The SNMP agent supports GETS, SETS, and TRAPS for 4 groups with MIB-II: System, Interface, IP, and ICMP.

- **SNMP Agent:** Click to enable the **SNMP Agent**. An SNMP agent is a node that resides on the network, typically a computer or a router. The SNMP agent is controlled and configured by the NMS by sending SNMP messages between one another. SNMP agents are logged and identified in a Management Information Base (MIB), in which they are identified by an object identifier (OID).
- **SNMP Traps:** Click to enable the **SNMP Traps**. SNMP traps are used to notify network managers of significant events that have taken place in the network. These traps are sent to the SNMP NMS (NMS Server located at Trap IP) through the specified Ports.
- **Name:** An administratively-assigned name for the 4 Ports 11g Wireless ADSL2/2+ Router. By convention, this is the node's fully-qualified domain name.
- **Location:** The physical location of the 4 Ports 11g Wireless ADSL2/2+ Router.

- **Contact:** Contact person and/or contact information for the 4 Ports 11g Wireless ADSL2/2+ Router.
- **Vendor OID:** Vendor Object Identifier. Private MIDBs fit under OID 1.3.6.1.4.1. The enterprise number of this device is 294.

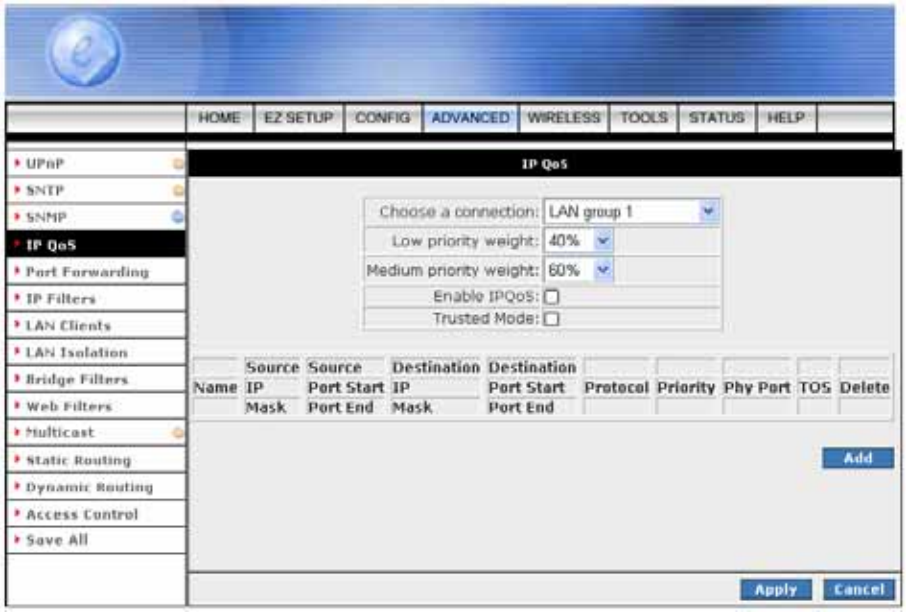
  Note: The System Name, System Contact, and System Location can be up to 127 characters.
- **Community:** SNMP defines a community to be a relationship between an SNMP agent and one or more SNMP managers. Once the clear-text community name corresponds to a community known to the receiving SNMP entity, the sending SNMP entity is considered to be authenticated as a member of that community and is granted different levels of access: read-only or read-write.
  - ☑ **Name:** Name of community. SNMP supports up to 3 communities including the default community name of "Public".
  - ☑ **Access Right:** Two options are offered:
    - ◆ **ReadOnly:** Allows a GET or a GETNEXT operation to all objects with access rights of READ-ONLY in the MIB.
    - ◆ **ReadWrite:** Allows a GET or a GETNEXT operation to all objects with access rights of READ-WRITE in the MIB.
- **Traps:** Trap is event notification. There are 4 standard traps supported in this 4 Ports 11g Wireless ADSL2/2+ Router: WarmStartTrap, LinkUpTrap, LinkDownTrap, and AuthenticationFailureTrap.
  - ☑ **Destination IP:** Destination IP address of trap. Trap can be sent to 3 different destinations.
  - ☑ **Trap Community:** Community name of the trap.
  - ☑ **Trap Version:** Two trap versions/formats are supported: SNMPv1 & SNMPv2C.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.4 ADVANCED - IP QoS

IP QoS: IP Quality of Service (QoS) prioritize data streams to ensure that basic connectivity is maintained when running multiple services over one connection.

When QoS is enabled in the 4 Ports 11g Wireless ADSL2/2+ Router, the designated machine, application or person would have precedence over peers when competing for bandwidth. The IP QoS Setup page allows you to configure QoS for a connection, view previously configured QoS rules, add a new rule, or delete an existing rule.

Each output device has three priority queues associated with transmit data. The **high priority** queues have strict priority over the **medium priority** and **low priority** queues, and therefore can exhaust all available bandwidth. The web UI will allow you to select the weights of the medium and low priority queues in increments of 10% so that that the sum of the weights of the 2 queues is equal to 100%. These queues will be serviced on a Round Robin priority basis according to the weights assigned, after the high priority queues have been completely serviced.



- **Choose a connection:** This field allows you choose a connection from the list of available connections.
- **Priority weight :** There are 2 Priority Weight to select from the drop down manual. These 2 fields will allow you to select the weights of the Medium and Low priority queues in increments of 10%, so that that the sum of the weights of these 2 queues is equal to 100%.
- **Enable IPQoS:** This field allows you to enable/disable IP QoS for the chosen connection.

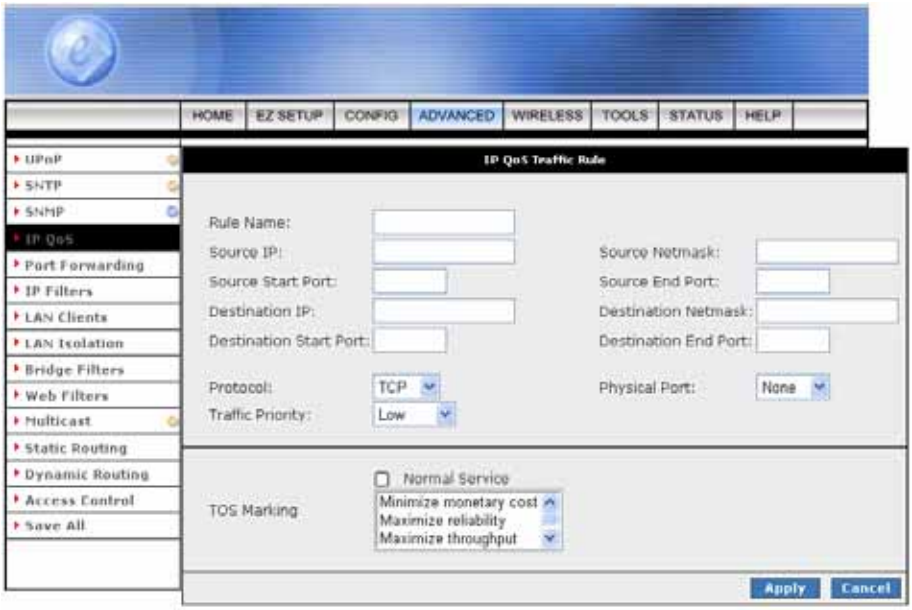
  Note: If IP QoS is enabled and no rules are defined, a default rule is applied to the connection. The default rule puts all the traffic to be transmitted in the Low Priority queue.

- **Trusted Mode:** Click to enable Trusted Mode. The 4 Ports 11g Wireless ADSL2/2+ Router has two primary modes of operation with regard to queue traffic prioritization - Trusted and Un-Trusted. This field allows you to choose the mode - Trusted (Checked) and Un-Trusted (Unchecked). In "Trusted Mode" all the rules will be applied first, regardless of the setting of the TOS bits. After the rules have been exhausted the existing TOS bit settings will be honored. The "Un-Trusted" mode will match first against all rules as in "Trusted" mode. The difference is that if there is no match then a default rule will be used. The default rule will have an associated queuing priority – Low.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.4.1 IP QoS Rule Setup

The IP QoS Rule Setup page allows you to define a traffic rule for a specified connection. Use the following procedures to access the IP QoS Rule Setup Page.

1. From the IP QoS Setup page, **Choose A Connection** filed, select the specific connection you want to define the IP QoS traffic rules.
2. Check **Enable IP QoS**.
3. Click **Add**.
4. Click **Apply** to temporarily save the setting.
5. To make the change permanent , click on **Save All**.



The Rules configuration page will allow you to define IP matching fields to associate with the priority queues associated with the named connections selected above in the "QoS Setup Page" section.
There will be three primary fields for you to select:

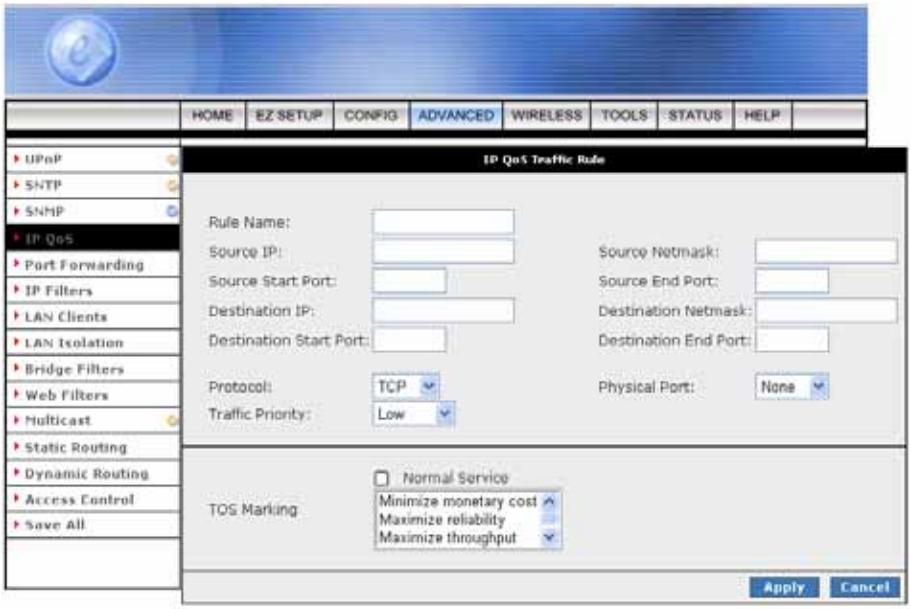
- A Trusted mode check box.
- A traffic priority choice (High, Medium, Low).
- An IP rules matching selection area.

The 4 Ports 11g Wireless ADSL2/2+ Router has two primary modes of operation with regard to queue traffic prioritization: Trusted and Un-trusted. The Web UI will provide one check box to enable trusted mode. In "Trusted mode" all rules will be applied first, regardless of the setting of the TOS bits. After the rules have been exhausted the existing TOS bit settings will be honored. If the "Trusted mode" box is unchecked this will indicate the "Un-trusted mode." "Un-trusted" mode will match first against all rules as in "Trusted" mode. The difference is that if there is no match then a default rule will be used. The default rule will have an associated queuing priority - Low.

Rule definitions will be defined by you, by allowing you to select matching based on Source IP and Netmask, Destination IP and Netmask, IP Protocol, Source Port range, Destination Port range, and Incoming Mac Port (Switched LAN Port). These selections will define a rule and be associated with a particular queue priority: High, Medium, and Low. There is another option to choose a particular TOS marking. The allowed options are - No change, Normal service, Minimize monitory cost, Maximize reliability, Maximize throughput and Minimize delay.

4.4.4.2 Create IP QoS Traffic Rule

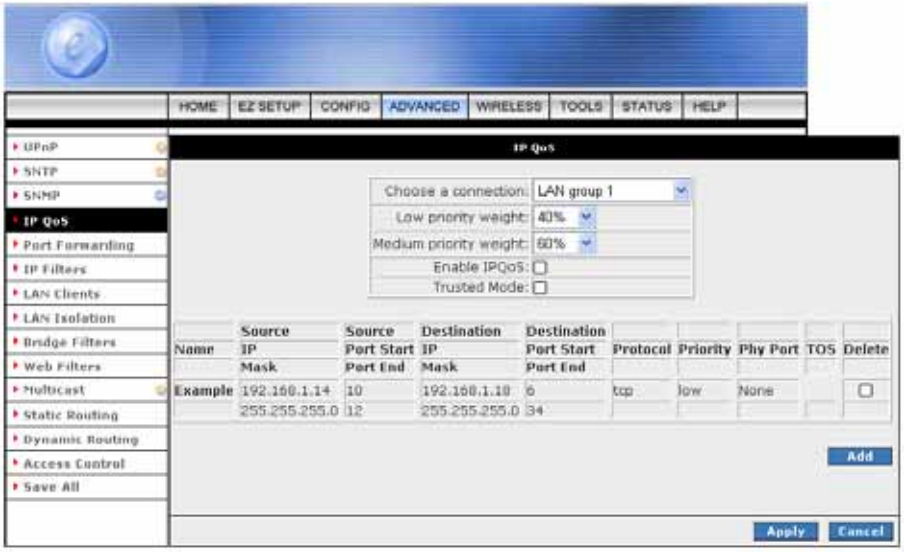
1. Use the terms describe below as a reference, and enter the required fields on the IP QoS Setup page.
2. Click **Apply** to temporarily save the setting.
3. To make the change permanent, click on **Save All**.



- **Rule Name:** Name of the traffic rule.
- **Source IP**: The IP address of the traffic source.
- **Source Netmask**: The Netmask of the source.
- **Source Start Port**: The start port of the source.
- **Source End Port**: The end port of the source.
- **Destination IP**: The IP address of the traffic destination.
- **Destination Netmask**: The Netmask of the destination.
- **Destination Start Port**: The start port of the destination.
- **Destination End Port**: The end port of the destination.
- **Protocol**: Select the protocol from the drop down manual. The protocols supported are TCP, UDP, ICMP and ANY.
- **Physical Port**: The selections are none, Port 1 through 4, USB, and WLAN.
- **Traffic Priority**: The Traffic Priority field corresponds to the Priority Queue (High/Medium/Low) for this traffic. The possible options for Protocol are: ANY, ICMP, TCP, and UDP. Wildcard(*) entries are allowed for IP Address/Netmask and Port range fields.
- **Normal Service:** The packets matching the rule should be treated as normal packets. Normal packets do not require any special treatment along the path. Implementation wise, normal packets will have ToS byte of 0 in the IP Header.
- **TOS Marking:** The TOS marking field allows you to assign a TOS value to this traffic. The values for the TOS marking can be: No Change, Normal Service, Minimize monetary cost, Maximize reliability, Maximize throughput, and Minimize delay.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.4.3 Delete a Traffic Rule

The traffic rule “Example” has been created as illustrated in figure below:

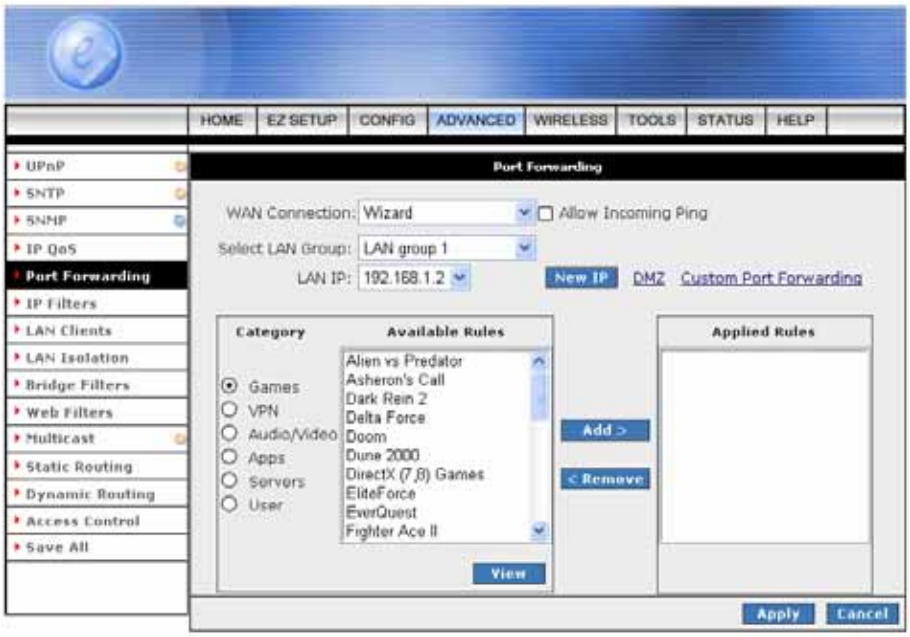


1. Check **Delete** next to the traffic rule you want to delete.
2. Click **Apply** to temporarily save the setting.
3. To make the change permanent, click on **Save All**.

4.4.5 ADVANCED - Port Forwarding

Port Forwarding (or Virtual Server) allows you to direct incoming traffic to specific PCs based on a service 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. Port Forwarding is configurable per LAN segment.

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/delete your own Port Forwarding rules.

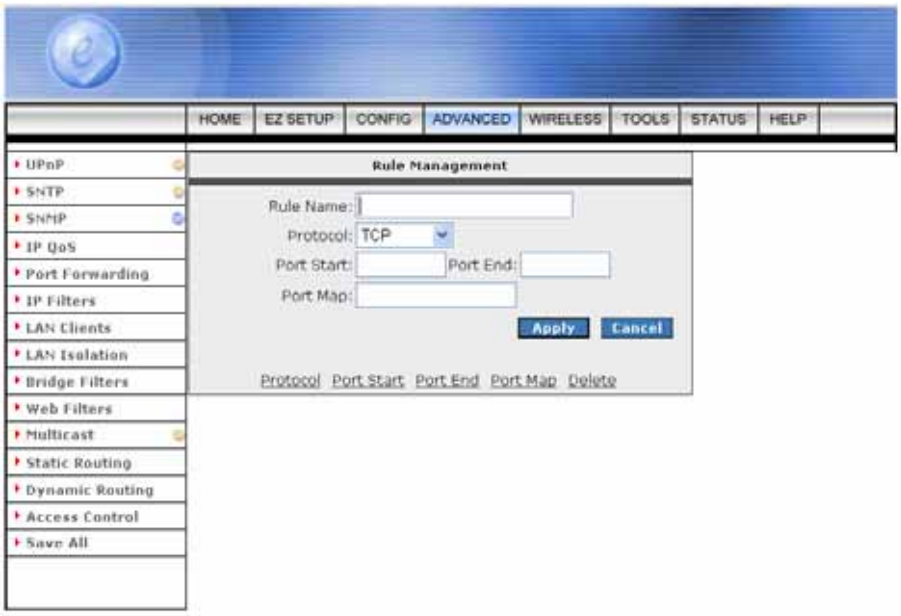


- **WAN Connection:** Select the WAN connection you are going to apply the port forwarding feature.
- **Allow Incoming Ping:** Place a check to enable the incoming ping.
- **Select LAN Group:** Select the LAN Group you are going to apply the port forwarding feature.
- **LAN IP:** Select the IP address that will host the service.
- **Allow Incoming Ping:** Enabling incoming ping (ICMP) requests on the Port Forwarding page allows the router to respond to a ping from the Internet.
- **DMZ:** Demilitarized Zone. DMZ More information on DMZ is available in the “DMZ Setting” sextion.
- **Custom Port Forwarding:** This link takes you to the Custom Port Forwarding screen, more is discussed in “Custom Port Forwarding” section.
- **Category:** Custom and user-defined categories.
- **Available Rules:** Predefined and/or user-defined IP filtering rules for each category.
- **Applied Rules:** The IP filtering rules you select to apply for each given category.

4.4.5.1 Port Forwarding Configuration Procedure

1. From the Port Forwarding configuration screen, select **WAN Connection**, **LAN Group**, and **LAN IP**. If the desired LAN IP is not available in the LAP IP drop-down menu, you can add it using the LAN Client screen, which can be accessed by clicking **NEW IP**.
2. Select the available rules for a given category, click **View** to view the rule associated with a predefined filter (Figure below), click **Add** to apply the rule for this category.

3. If a rule is not in the list, you can create your own in the user category. With User category selected, click **Add**. The Rule Management screen will populate for you to create new rules. The rule(s) you create will be available in the User category. You will be able to Edit/Delete the rule(s) you create.

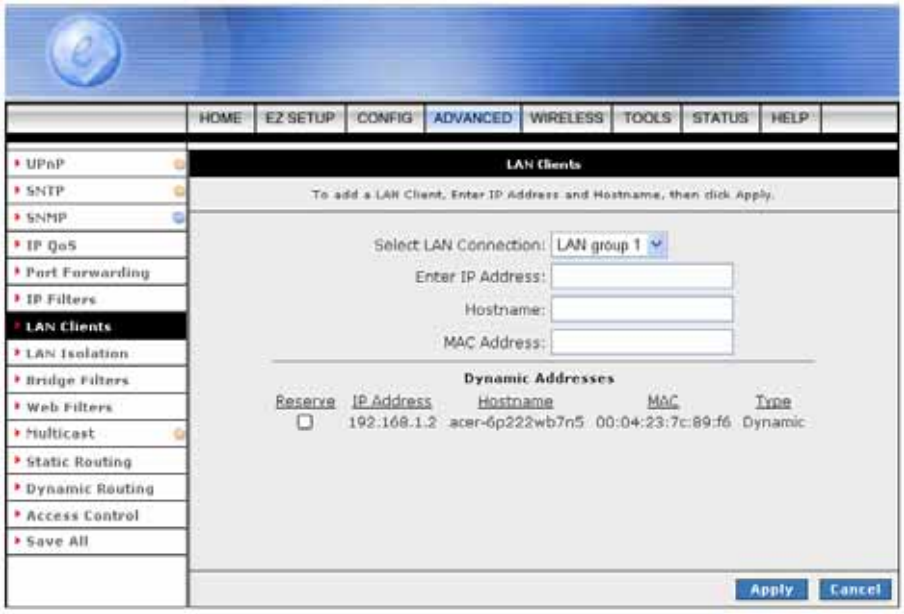


4. Repeat adding rules to each category.
5. Click **Apply** when you finish to temporarily save the settings.
6. To make the change permanent, click on **Save All**.

4.4.5.2 Port Forwarding – New IP

New IP: If you wish to manually add a LAN client so that you can apply rules to it, click on the **New IP** button. The following screen will pop-up. Refer to **ADVANCED ➔ LAN Clients** setting for more details.

Enter the **IP Address**, **Hostname** and **MAC Address** as shown then click **Apply** to save your setting.

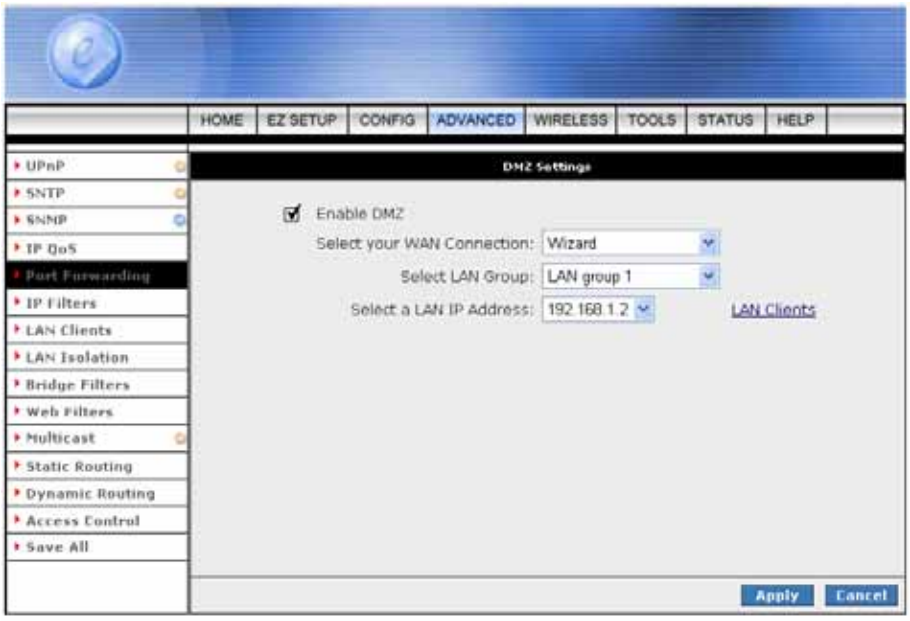


4.4.5.3 Port Forwarding – DMZ

DMZ: A DMZ (Demilitarized Zone) is added between a protected network and an external network, in order to provide an additional layer of security.

Setting a computer on your local network as DMZ (DeMilitarized Zone) forwards any network traffic that is not redirected to another computer via the port forwarding feature to the computer's IP address. This opens the access to the DMZ computer from the Internet. This function is disabled by default.

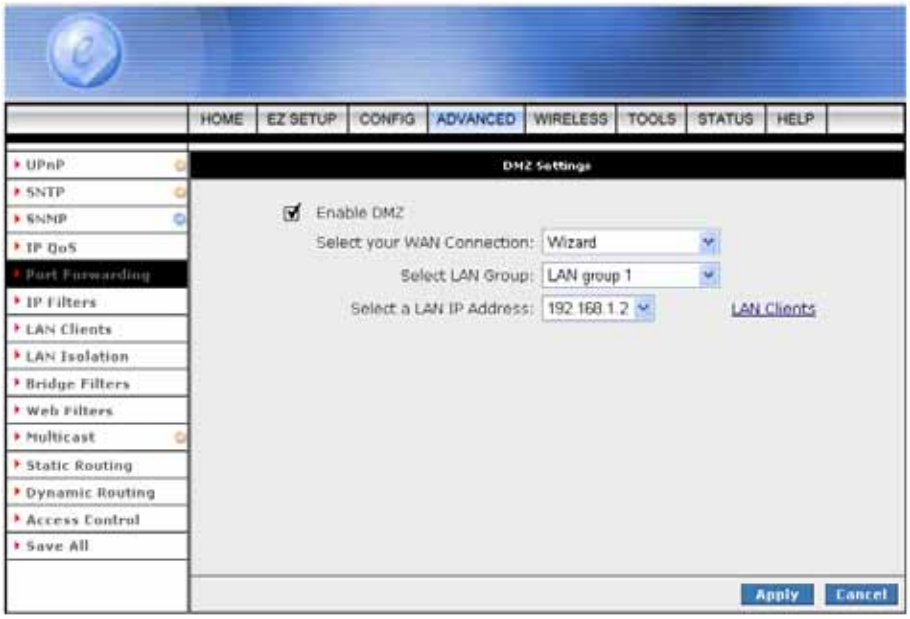
The following screen will pop-up after clicking the DMZ button. Place a check to enable the DMZ functionality. Select the **WAN Connection**, **LAN Group** and **LAN IP Address** from the drop down manual. Click **Apply** to save and activate your setting.



- **Enable DMZ:** Enable/disables the Demilitarized Zone feature. This field is unchecked by default.
- **Select your WAN Connection:** Select the WAN Group you are going to apply the DMZ feature.
- **Select LAN Group:** Select the LAN Group you are going to apply the DMZ feature.
- **Select a LAN IP Address:** Select the LAN IP address you are going to use as the DMZ host. This computer will be exposed to the Internet. Be aware that this feature may expose your local network to security risks.
- **LAN Clients:** This link will take you to the LAN Clients screen, more information on LAN Clients can be found in “LAN Clients” configuration section.

4.4.5.3.1 DMZ Configuration Procedure

1. From the Port Forwarding Configuration screen, click the **DMZ** link. You will be taken to the DMZ settings screen as shown below.



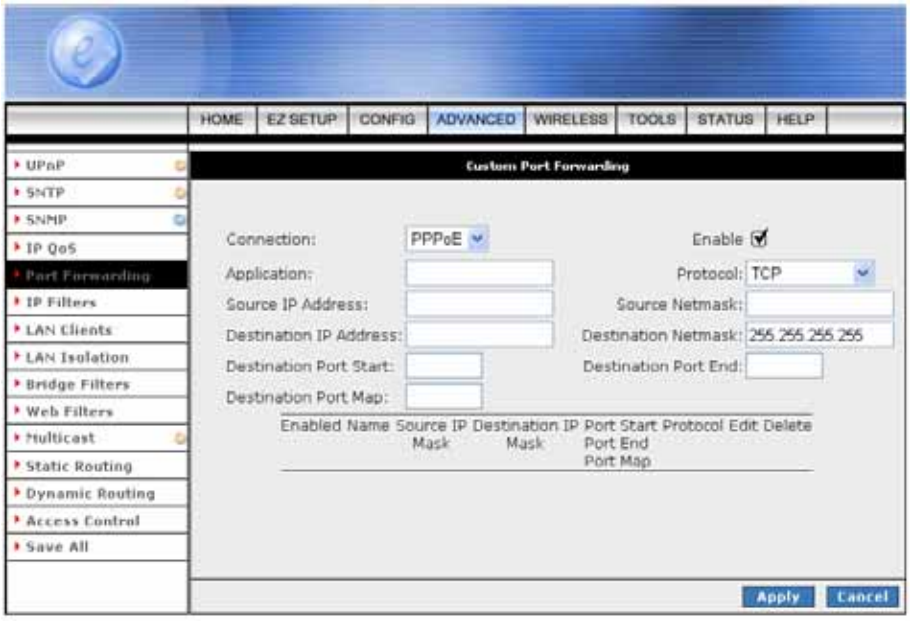
2. Check the **Enable DMZ** box on the DMZ setting screen.
3. Select the **WAN Group**, **LAN Group**, and **LAN IP Address**. DMZ is configurable per LAN segment.
4. Click **Apply** when you finish to temporarily save the settings.

   Note—You can click on “LAN Clients” link to access the LAN Clients screen.
5. To make the change permanent, click on **Save All**.

4.4.5.4 Port Forwarding – Custom Port Forwarding

Custom Port Forwarding: If there is no pre-defined Port Forwarding Rule for a particular application, a user rule can be created which defines the required Ports, Protocols and Port forwarding rules. Click the Custom Port Forwarding button and the following screen will pop-up.

The Custom Port Forwarding screen allows you to create up to 20 custom port forwarding entries to support specific services or applications; such as Concurrent NAT/NAPT operation.



To create a custom rule you will need to know the specific port number and port type that the application requires. Some applications specify a range of ports in which case you will need to know both the starting and ending port numbers in the range, which are mapped by the start port and end port fields.

The Port Map specifies the internal port that the data will be directed to on the LAN Client. When dealing with port ranges, the Internal Port will be the same as the first port in the range. When you simply want to forward a single port from outside to inside, then all three fields (Port Start, Port End and Port Map) will have the same port number.

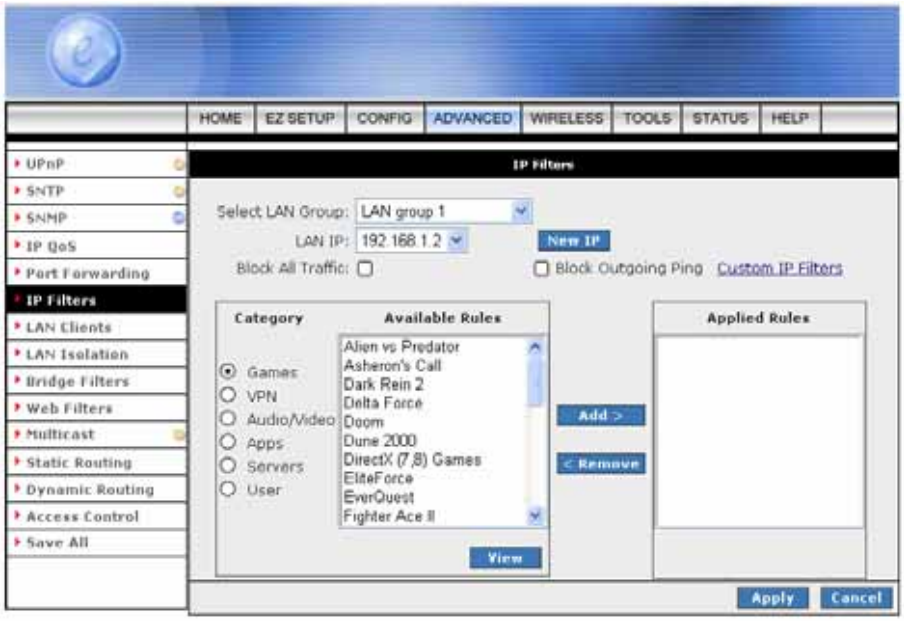
- **Connection:** Select the WAN connection you are going to apply the custom Port Forwarding rule.
- **Enable:** The Enable button is checked by default, meaning this rule is applied when you click on the Apply button.
- **Application:** Name of the application your port(s) will be opened for.
- **Protocol:** 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 will be 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:** Since it is for incoming traffic, the destination IP address is on your LAN side.
- **Destination Netmask:** The destination netmask on your LAN side.
- **Destination Port Start:** The starting port number that will be made open for this application.
- **Destination Port End:** The ending port number that will be made open for this application.
- **Destination Port Map:** Destination port mapped on the LAN (destination) side to which packets will be forwarded.

4.4.6 ADVANCED - 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 this 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/delete your own IP filter rules.



- **Select LAN Group:** Select the LAN Group you are going to apply the IP Filters feature.
- **LAN IP:** Select the IP address in the given LAN group that you are going to apply the IP Filters feature.
- **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 PC has a virus that attempts a Ping-of-Death Denial of Service attack.
- **Custom IP Filters:** This link takes you to the Custom IP Filter screen, more is discussed in "Custom IP Filters Screen" section.
- **Available Rules:** Predefined and/or user-defined IP filtering rules for each category.
- **Applied Rules:** The IP filtering rules you elelct to apply for each given category.

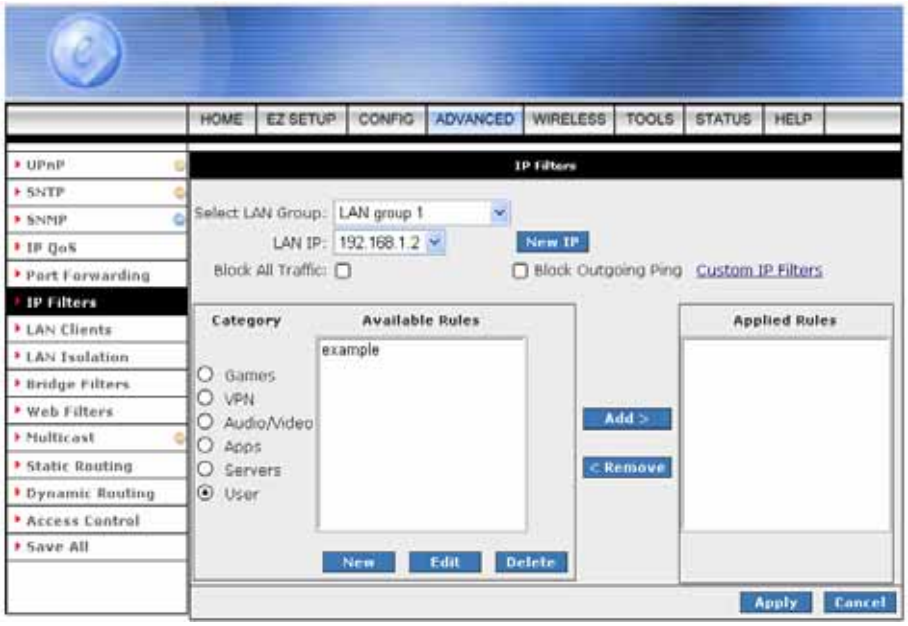
4.4.6.1 IP Filters Configuration Procedure

1. From the IP Filters configuration screen, select LAN Group and LAN IP.

   If the desired LAN IP is not available in the LAP IP drop-down menu, you can add it using the LAN Client screen, which can be accessed by clicking **NEW IP**.

2. Select the available rules for a given category, click **View** to view the rule associated with a predefined filter, click **Add** to apply the rule for this category.

3. If a rule is not in the list, you can create your own in the user category. With User category selected, click **Add**. The Rule Management screen will populate for you to create new rules. The rule(s) you create will be available in the User category. You will be able to Edit/Delete the rule(s) you create.



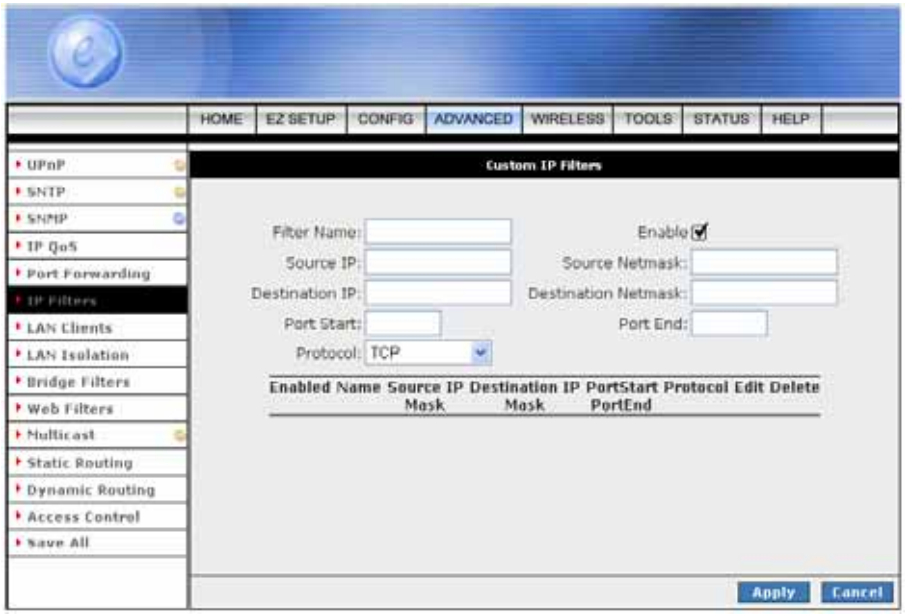
4. Repeat adding rules for each category.
5. Click **Apply** when you finish to temporarily save the settings.
6. To make the change permanent, click on **Save All**.

4.4.6.2 IP Filters – Custom IP Filters

Customer IP Filters are different from Port forwards, or Block All traffic because they allow greater scopes of IP addresses to be included in the block.

The Custom IP Filters function allows creation of 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
- TCP
- UDP
- TCP and UDP
- ICMP
- Any



- **Filter Name:** Name of the IP filter rule you are about to create.
- **Enable:** The Enable button is checked by default, meaning this rule is applied when you click on the Apply button.
- **Source IP:** Since IP filtering is for outgoing traffic, the source IP is the IP address on your LAN side that you want to block network traffic from.
- **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 the access. Enter “0..0.0.0” for all.

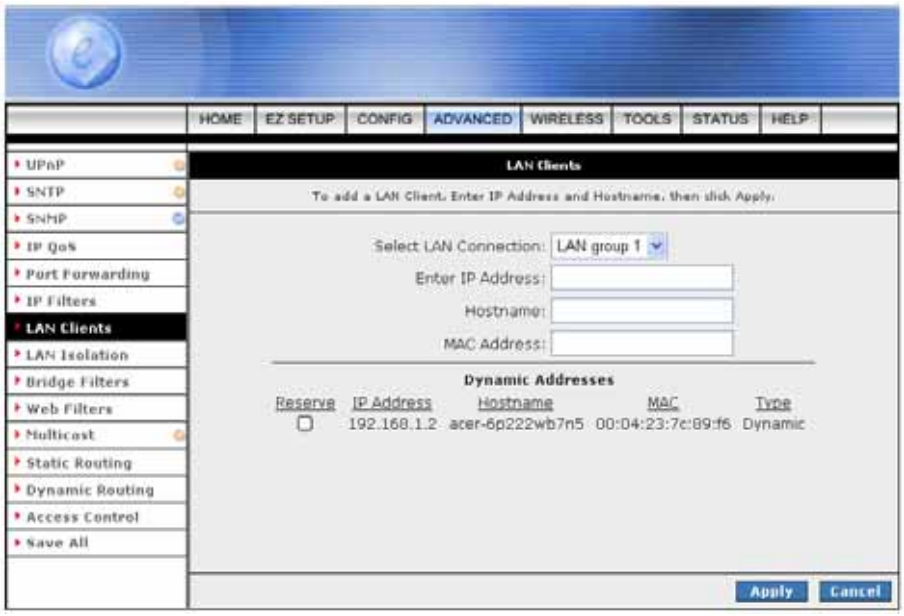
- **Destination Netmask:** Netmask of the destination IP. Enter “255.255.255.255” for all.
- **Port Stat:** The starting port number that will be blocked for this application.
- **Port End:** The ending port number that will be blocked for this application.
- **Protocol:** There are five options available: TCP, UDP, TCP and UDP, ICMP, and Any.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.7 ADVANCED - LAN Clients

The LAN Clients feature allows you to see all the PCs on the LAN segment. Each PC is qualified to be either "dynamic" (PC obtained a lease from this router) or "static" (PC has a manually configured IP address).

You can add a "static" IP address(belonging to the network segment of the router LAN IP address). Any existing static entry falling within DHCP server's range can be deleted and the IP address would be made available for future allocation.

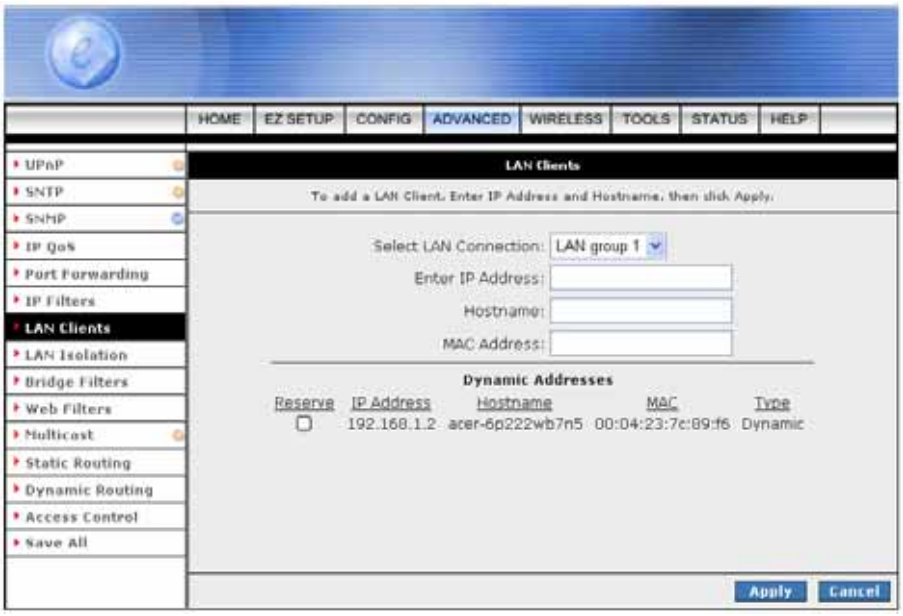
Enter the IP Address, Hostname and MAC Address as shown. Click Apply to activate your setting.



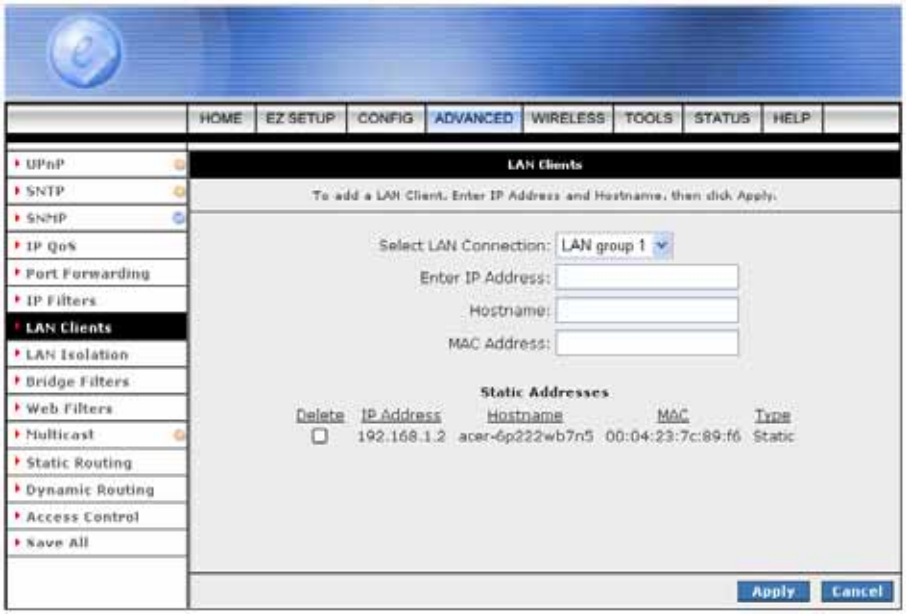
- **Select LAN Connection:** Select the LAN connection you want to add the client to.
- **Enter IP Address:** Assign the dynamic IP address to the host here. This is a mandatory field.
- **Hostname:** Hostname of the client. This field is optional.
- **MAC Address:** MAC address of the PC. This field is optional.

4.4.7.1 LAN Clients Configuration Procedure

1. From the LAN Clients screen, select **LAN Connection,** and enter **IP Address, Hostname, and MAC Address**.
2. Click **Apply**. The IP address is allocated and it shows up in the list of LAN clients as a "dynamic" entry.



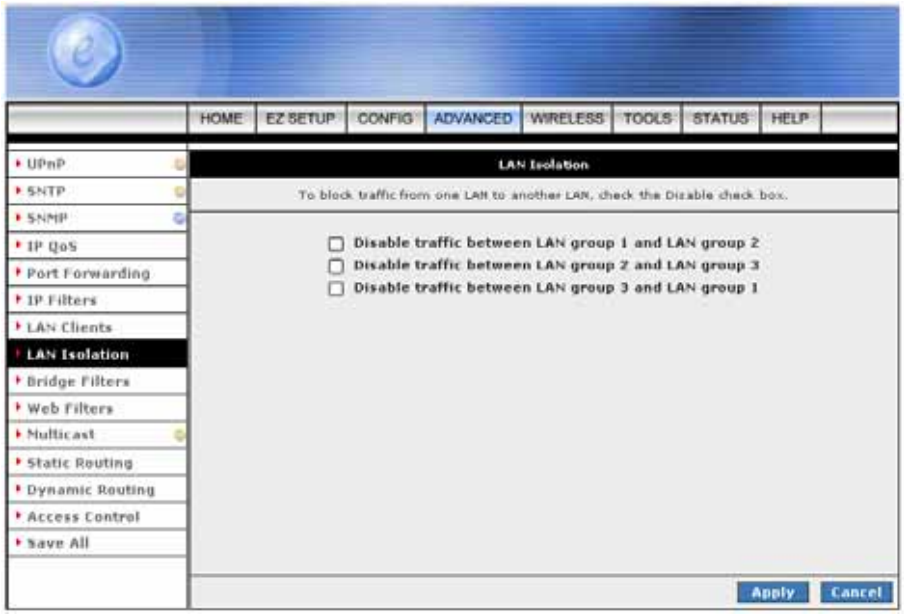
3. You can convert the dynamic entry into static by clicking **Reserve**, then **Apply**. As shown in below, the IP is now changed to static address. You can delete this entry using the **Delete** checkbox.



4. When you finish, click **Apply** to temporarily save the settings.
5. To make the change permanent, click on **Save All**.

4.4.8 ADVANCED - LAN Isolation

LAN Isolation allows you to disable the flow of packets between up to three-user-defined LAN groups (WLAN, USB, and Ethernet). This allows you to secure information in private portions of the LAN from other, publicly accessible LAN segments.



4.4.8.1 LAN Isolation Configuration Procedure

1. Check the traffic between the two LAN groups that you want to disable the packets flow.
2. Click **Apply** to temporarily save the settings.
3. To make the change permanent, click on **Save All**.

4.4.9 ADVANCED - Bridge Filters

Bridge Filtering allows packets to be forwarded or blocked, depending on the MAC address. The **Bridge Filtering** configuration page allows you to set the configuration of MAC filtering.

Bridge Filter (Or sometimes known as MAC Filter) enable rules to be defined which allow or deny data to pass through the Router based on the source and destination MAC address and data type of each data frame.

Most of the Bridge Filter Rule is to specify which computers on a network are allowed Internet access; or to determine which particular computers are allowed to access services provided by the Router. Twenty filter rules are supported with bridge filtering.

- **Enable Bridge Filters:** Place a tick at the check box to enable the Bridge Filters functionality. If the check box is selected, Bridge Filtering is enabled according to the list of Bridge Filter Rules that has been created. If the box is de-selected, Bridge Filtering will not be enabled, even if Bridge Filter Rules have been created.
- **Enable Bridge Filter Management Interface:** Place a check to enable the Bridge Filter Management Interface. There are three interface provided for the setting, Ethernet, USB and Wireless Interface.
- **Select LAN:** Select your LAN group.
- **Bridge Filter Management Interface:** You can choose from Ethernet, USB, and 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 would be considered also 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.

- **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:** Select t **Allow** or **Deny** for the rule.
- **Delete:** Place a check adjacent to the Bridge Filter Rule and click Apply to Delete the Bridge Filter Rule.
- **Add:** Click **Add** button to add the rule to the list of rules.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.9.1 Bridge Filters Configuration Procedure

1. Check **Enable Bridge Filters**.
2. To add a rule, enter source MAC address, destination MAC address and frame type with desired filtering type, and click **Add**.

   You can also edit a rule that you created using the **Edit** checkbox.

   You can delete a rule using **Delete**.
3. Click **Apply** to temporarily save the settings.
4. To make the change permanent, click on **Save All**.

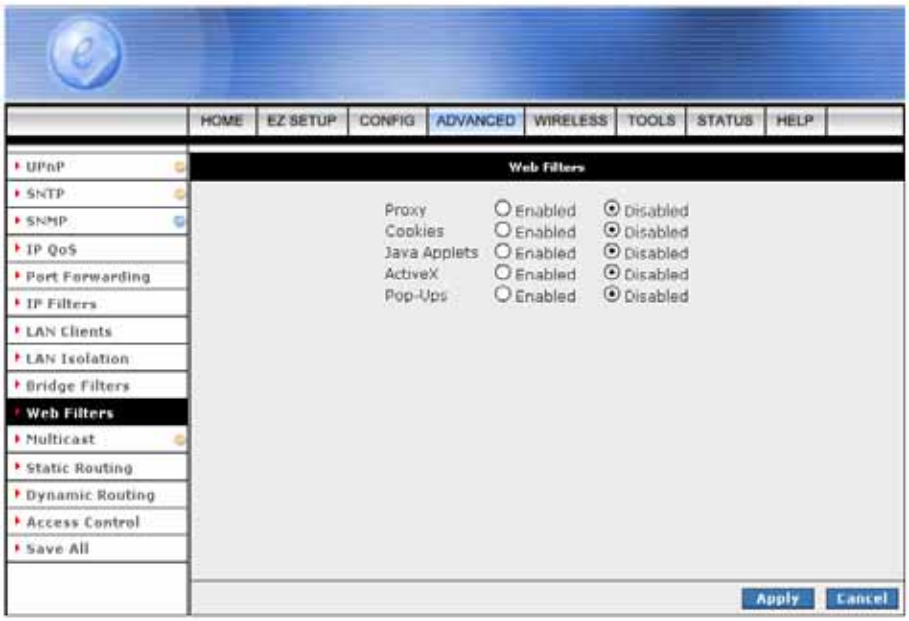
4.4.10 ADVANCED – Web Filters

Web Filter is a tool that have the ability to filter Internet content. Using an easy, category-based listing, you can control exactly what website content can or can not be accessed. Click the radio button to Enable or Disable the filter rules to ensure an accurate representation of the world of information reachable on the Internet.

The following content types are disabled by default:

- Proxy Server
- Cookies
- Java Applets
- ActiveX Controls
- Pop-Ups

To enable, simply check **Enabled**, then click **Apply**.



- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

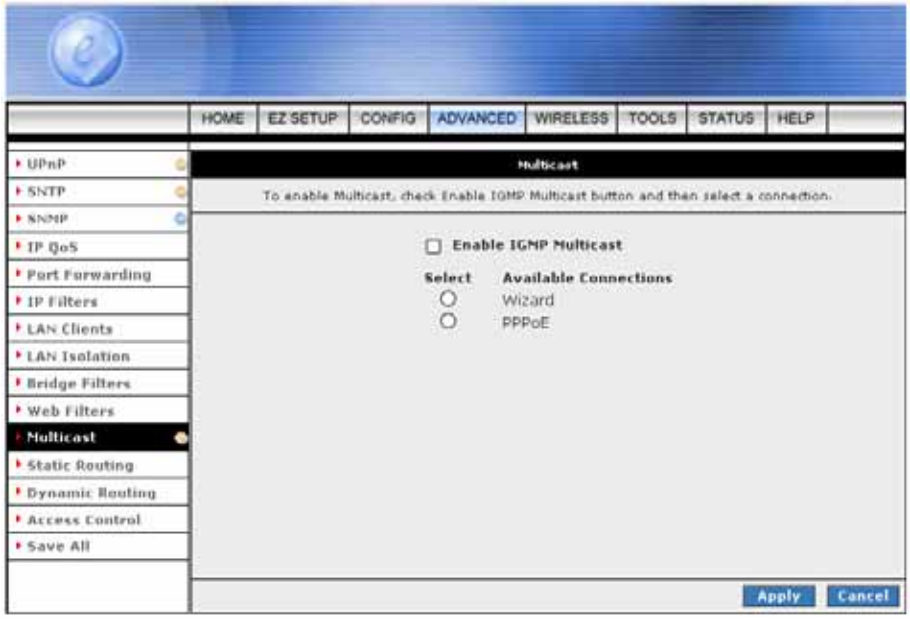
4.4.11 ADVANCED - Multicast

Multicasting is a form of limited broadcast. UDP is used to send datagram to all hosts that belong to what is called a “Host group”. A host group is a set of zero or more hosts identified by the same destination IP address. The following statements apply to host groups:

- 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 datagram to the host group.

Multicasting is useful when 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 stream from multicast servers. This 4 Ports 11g Wireless ADSL2/2+ Router support an IGMP (Internet Group Management Protocol) proxy that handles IGMP messages. When enabled, the router will act as a proxy for a PC making requests to join and leave multicast groups.



- **Enable IGMP Multicast:** Click to enable IGMP Multicast and then select a connection listed.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

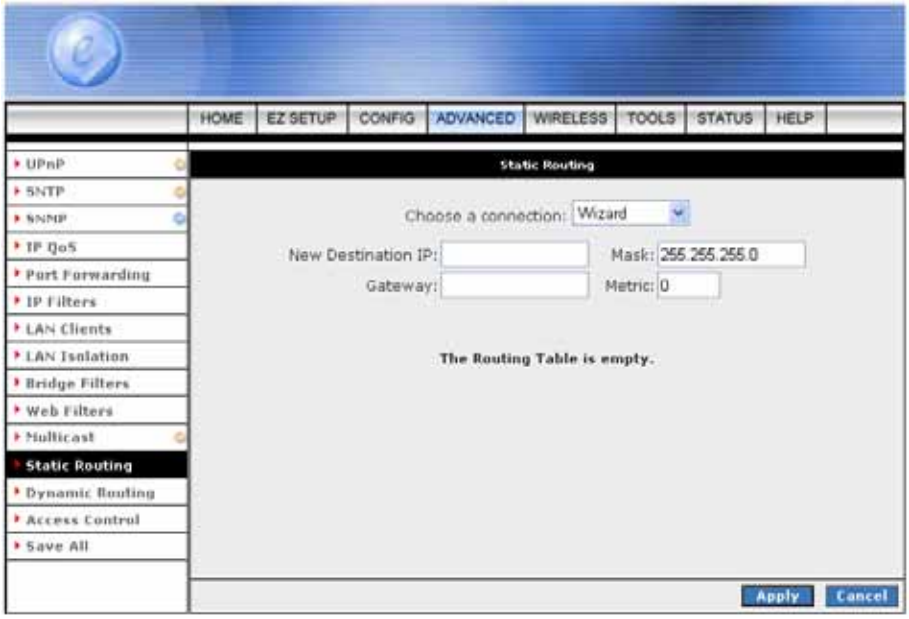
4.4.11.1 Multicast Configuration Procedure

1. Check **Enable IGMP Multicast**.
2. Select the WAN connection from the **Available Connections** list.

   Note—Only one WAN connection can be enabled for Multicast. This is usually the default connection the ISP provides.
3. Click **Apply** to temporarily save the settings.
4. To make the change permanent, click on **Save All**.

4.4.12 ADVANCED – Static Routing

If the Router is required to serve more than one network, you will need to set up a Static Route between the networks. Static routing can be used to allow users from one IP domain to access the Internet through the Router in another domain. A Static Route provides the defined pathway that network information must travel to reach the specific host or network which is providing Internet access. Up to 16 routes can be added.



- **Configuring Static Routing:** If the Router is connected to more than one network, it may be necessary to set up a static route between them. A static route is a pre-determined pathway that network information must travel to reach a specific host or network. Follow the following steps to create a Static Route:

  - ☑ **Choose a Connection:** Presents list of saved Connections. Select appropriate connection from the list.
  - ☑ **The New Destination IP:** The network IP address of the subnet. (You can also enter the IP address of each individual station in the subnet).
  - ☑ **Mask:** The Subnet Mask identifies which portion of an IP address is the network portion, and which portion is the host portion. The subnet mask defaults is 255.25.255.0
  - ☑ **Gateway:** The LAN through which the subnet communicates with the WAN/LAN.
  - ☑ **Metric:** It defines the number of hop(s) the between network nodes that data packets will travel. The default value is "0", which means the subnet is directly one level down the local LAN network.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

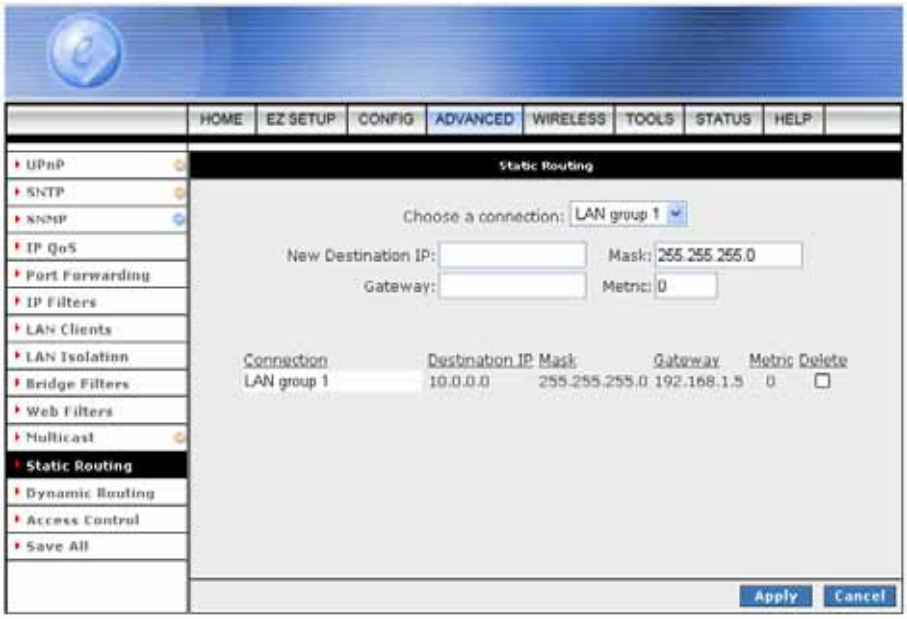
4.4.12.1 Static Routing Configuration Procedure

1. From the **Choose a connection** drop-down menu, select your LAN connection "LAN group 1" (For example).
2. Enter/leave the following parameters:
   - ☑ **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 router a new subnet with an IP of 10.0.0.0 and a netmask of 255.255.255.0 has been added and will access this 4 Ports 11g Wireless ADSL2/2+ Router via station 192.168.1.5.

   The metric is 0 since the subnet is one level down the LAN.

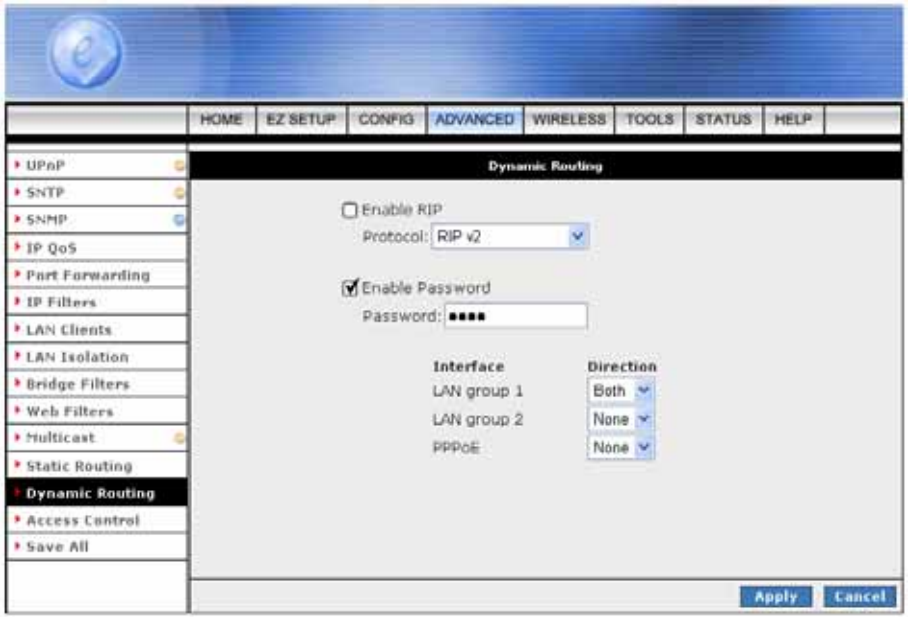
3. Click **Apply** to temporarily save the settings. You have added the subnet to the routing table (Figure below). The fours stations in the subnet will be able to send/receive packets. You can add up to 16 entries. You can also delete any entry using the **Delete** checkbox.



4. Click **Apply** again when you finish making all the changes.
5. To make the change permanent, click on **Save All**.

4.4.13 ADVANCED – Dynamic Routing

The dynamic routing feature enables the 4 Ports 11g Wireless ADSL2/2+ Router to dynamically define routes for subnet(s) on the WAN/LAN side. Dynamic Routing uses RIP (Routing Information Protocol) for exchanging routing information with other routers in the network. It is supported across both WAN and LAN interfaces. When RIP (Routing Information Protocol) is enabled the router builds its own routing tables utilizing request and response packets. A request packet tells the router to build a list of its routing table contents with the network/host IP to which the table belongs, Netmask for the network and RIP host. After obtaining this information, the router will send a response to the machine that sent the original request. RIP will also update the main routing table.



- **Enable RIP:** If this box is checked, Dynamic Routing is enabled.
- **Protocol:** Select the protocol from the drop-down manual. The choice is dependent upon the network environment. 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.
  - ☑ **RIPv1:** RIP Version 1: One of the first dynamic routing protocols introduced used in the Internet, RIPv1 was developed to distribute network reach ability information for what is now considered simple topologies.
  - ☑ **RIPv2:** RIP Version 2: Shares the same basic concepts and algorithms as RIPv1 with added features such as subnet masks, authentication, external route tags, next hop addresses, and multicasting in addition to broadcasting.
- **Enable Password:** This is an optional field. RIP version v2/Compatibility allows you to provide simple plaintext password based authentication to RIP packets. This field is disabled if RIP v1 protocol is selected.
- **Password:** The 16 character long plain text password.

- **Direction:** Normally when RIP is enabled on a router it dynamically learns/provides routes on all it's configured interfaces. This parameter allows you to select the interfaces on which RIP is expected to learn and distribute routing information. This feature allows the user to control how and which routes get distributed through the network e.g. by selecting “In Only” mode, it prevent routes to the private LAN networks from being sent over to the WAN side router. The following four direction options are available:
  - ☑ **Both:** Receive updates on the interface and also send it's routing table to other routers connected to that interface.
  - ☑ **In:** Receive routing updates from other routers connected to that interface but NOT send routing updates on that interface.
  - ☑ **Out:** Send routing updates but not receive updates on this interface from the other routers connected to that interface.
  - ☑ **None:** Ignores this interface and not send or receive routing updates through this interface.

- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.4.13.1 Dynamic Routing Configuration Procedure

1. Check **Enable RIP**.
2. Select the RIP Protocol **RIP v2** for training purpose. The **Enable Password** field is enabled.

   Note—The same RIP protocol should be used to enable dynamic routing on all routers on the network.
3. Check **Enable Password** and enter a password. This is an optional field for additional security.
4. For LAN group 1 and LAN Group 2, leave “Both” checked in the **Direction** field.
5. Click **Apply** to temporarily save the settings.
6. Click **Apply** again when you finish making all the changes.
7. To make the change permanent, click on **Save All**.

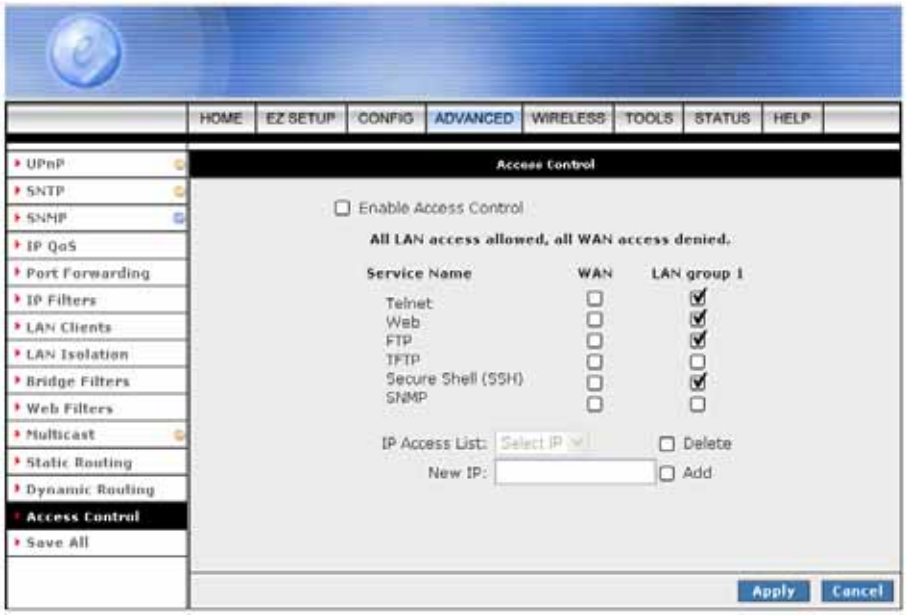
4.4.14 ADVANCED – Access Control

Access control allows you to open the access from the Internet (WAN) or LAN to the following management ports of the 4 Ports 11g Wireless ADSL2/2+ Router:

- Telnet
- Web
- FTP
- TFTP
- Secure Shell (SSH)
- SNMP

Figure below illustrates the default Access Control screen. The Access Control is disabled by default, remote management from the WAN side IP addresses is denied, most services from the LAN side IP addresses are enabled.

Access Control, when enabled, supports up to 16 IP addresses with controlled (allow/deny) WAN and/or LAN access.



- **Enable Access Control:** Check this box to enable selective access from the WAN to your LAN for applications of the class indicated by the relevant check boxes. If Access Control is not enabled, the individual check boxes cannot be checked.

  The default configuration enables Telnet, Web, FTP and SSH access from LAN to WAN. If Access Control is enabled, and an enable WAN checkbox is selected, then the WAN access to the matching service is enabled.

- **IP Access List:** This enables you to specify which LAN/WAN IP addresses are allowed access to the 4 Ports 11g Wireless ADSL2/2+ Router configuration services specified.
- **Delete:** Delete the IP Access List from the drop down manual.
- **Add:** Add new IP Access to the list.
- **Apply:** The following dialog box will pop-up when clicking the Apply button indicates that you should not disable LAN Web Access or else you might not be able to connect to the device. Click **OK** to confirm your setting.

- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

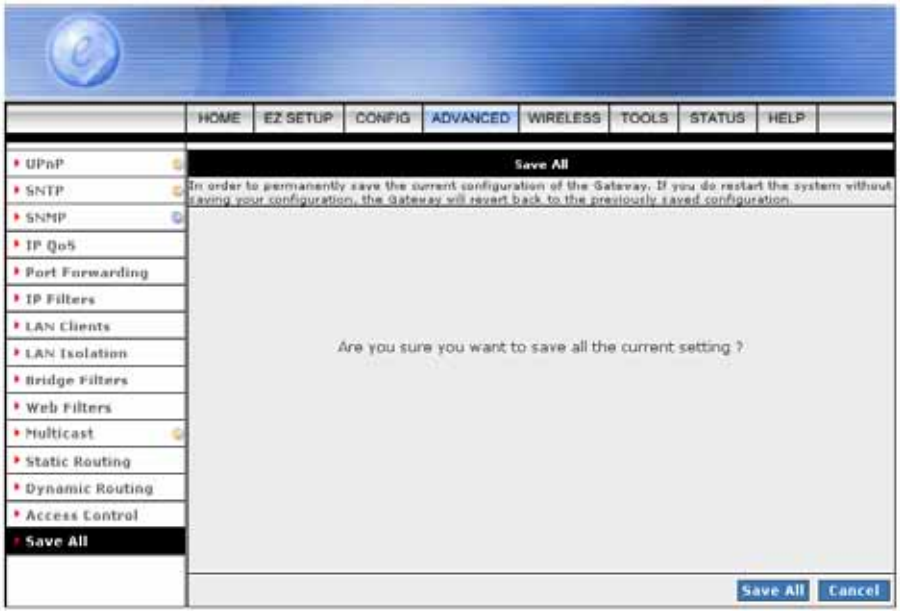
4.4.14.1 Access Control Configuration Procedure

Use the following procedure to enable Access Control and add an WAN IP address and a LAN IP address to the access control list.

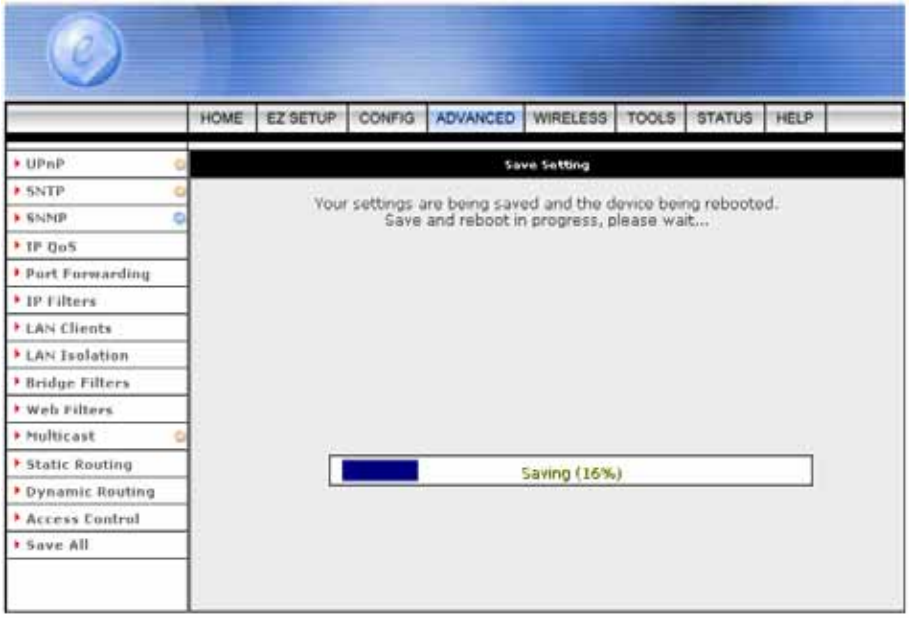
1. Check **Enable Access Control** to enable the feature. This will enable the IP Access List field.
2. You can select an IP from the IP Access List, or enter a new IP and check **Add**.
3. Change the LAN and/or WAN configurations of the IP address.
4. Click **Apply** to temporarily save the settings on screen.
5. To make the change permanent, click on **Save All**.

4.4.15 ADVANCED – Save All

This button enables you to permanently save the current configuration of this 4 Ports 11g Wireless ADSL2/2+ Router. If you restart the system without saying your configuration, this 4 Ports 11g Wireless ADSL2/2+ Router will revert back to the previously saved configuration.



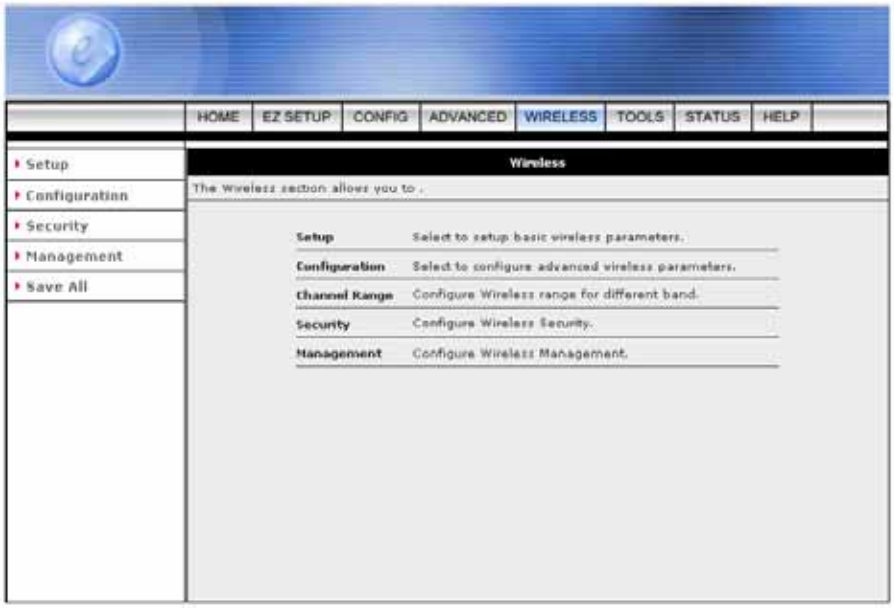
- **Save All:** Click **Save All** to confirm the setting. The following window will be shown.



- **Cancel:** Click **Cancel** to ignore all the changes.

4.5 WIRELESS

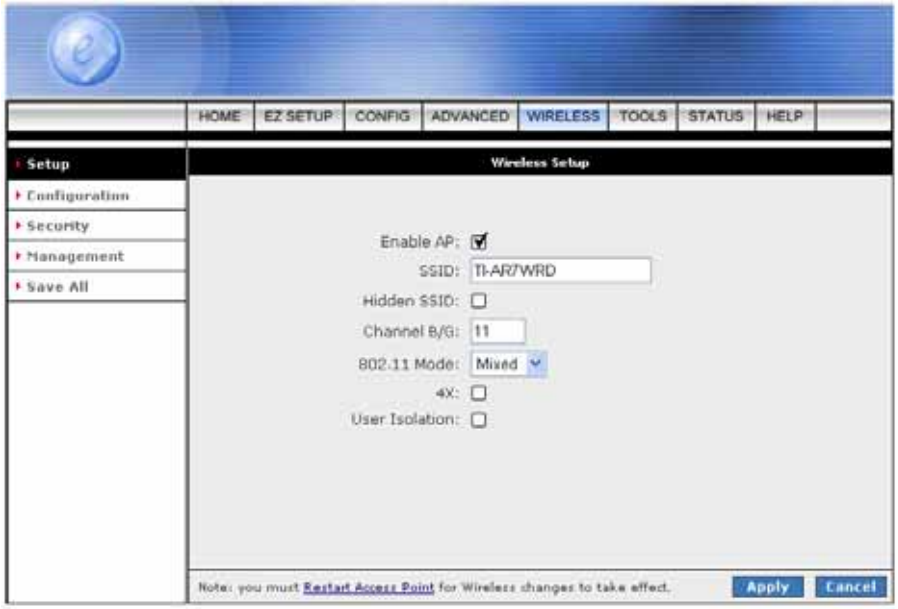
The Wireless configuration page describe the detail instruction on Setup, Configuration, Channel Range, Security and Management for 11g Wireless user.



4.5.1 WIRELESS - Setup

The Setup configuration page describe the basic wireless setting for the 4 Ports 11g Wireless ADSL2/2+ Router.

This screen provides basic local and Wireless networks parameter settings.



- **Enable AP:** Place a check to Enable or Disable the Wireless Access Point built in the 4 Ports 11g Wireless ADSL2/2+ Router. The Wireless Access Point must be enabled to allow wireless stations to access the Internet.

- **SSID:** The Service Set Identifier, also known as the Wireless Network name. The Service Set Identifier (SSID) is a unique name for your wireless network. If you have other wireless access points in your network, they must share the same SSID.

  The default SSID is **TI-AR7WRD**, but it is strongly recommends that you change your network Name to a different value for security purpose. The SSID can be up to 31 characters.

- **Hidden SSID:** Enables/disables the Hidden SSID feature. The AP (Access Point) will not transmit beacon and thus will not be seen by any other station.

- **Channel B/G:** The channel on which the AP and the wireless stations will communicate. Different domain will have different ranges of channels. For FCC in 2.4GHz, the default is 11. The channel can be selected according to the band selection.

- **802.11 Mode:** The default is **"Mixed"**, which allows both 802.11g and 802.11b wireless stations to access this device. You can select from the following mode:

  ☑ **Mixed mode:** The legacy SR IE contains the 802.11b legacy supported rates and the additional OFDM supported rates. Extended SR IE contains the extended supported rates, if present. Beacon & Probe Response Frames are sent in "11b" rate.

- ☑ **11b only Mode:** The legacy SR IE contains only the 802.11b legacy supported rates. The extended SR IE is not present.
- ☑ **11b+ Mode:** Similar to the "802.11b-only" mode except that 22Mbps PBCC rate/modulation is included, which is TI proprietary.
- ☑ **11g only Mode:** The legacy SR IE contains only the OFDM additional supported rates. The extended SR IE contains the extended supported rates, if present.

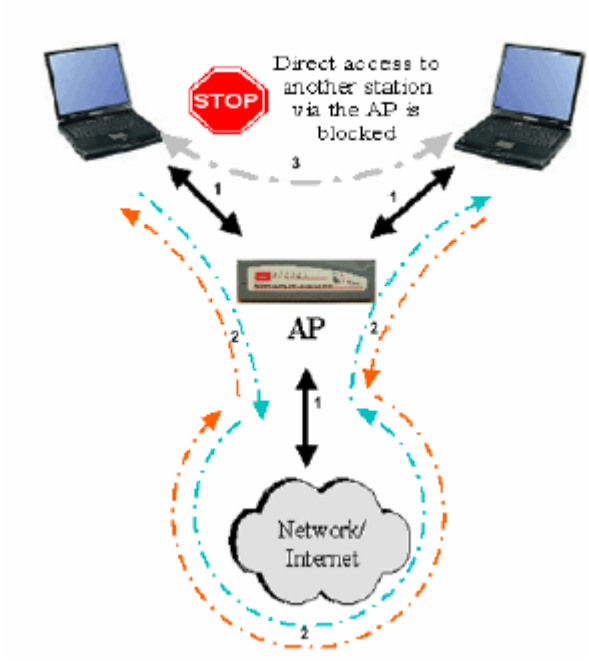
- **4X:** Same as TI's "11b+" mode, which enables/disables the 4x feature. This function is TI proprietary and is only available when both TI wireless station card and TI ADSL2/2+ modem are used.
- **User Isolation:** If enabled, Wireless Stations will not be able to communicate with each other or with stations on the wired network. This feature normally should be disabled.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.1.1 WIRELESS – Setup – User Isolation

When User Isolation is enabled, wireless users will not be able to directly access other wireless users. Access can be controlled by the AP. This is enabled on the network side.

Figure below demonstrates the User Isolation feature.

1. AP disabled BSS (Basic Service Set) bridging
2. All data sent to WAN (Wide Area Network)
3. Enable/Disable flag



4.5.1.2 How to set up and test basic wireless connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

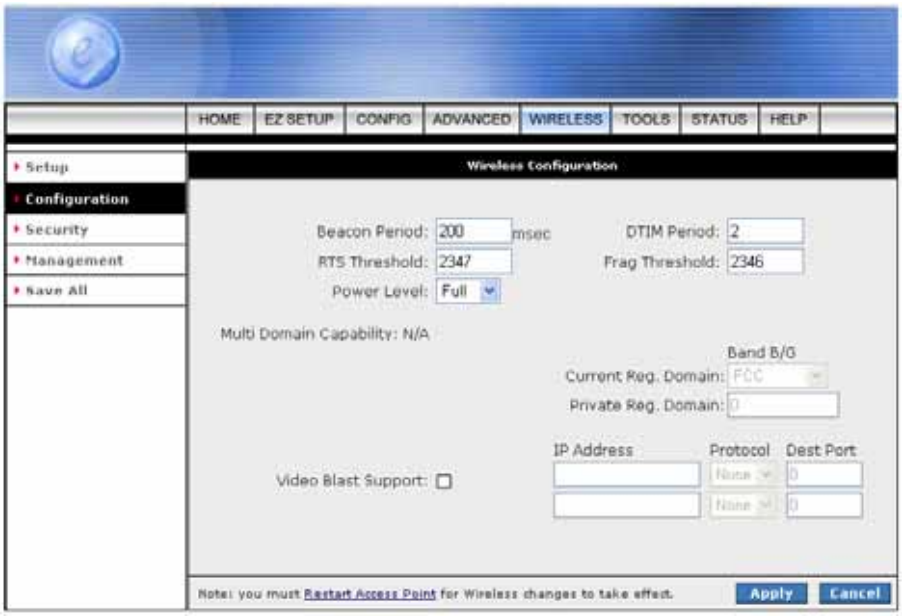
1. Log in to the 4 Ports 11g Wireless ADSL2/2+ Router default IP address http://192.168.1.1 with its default username: **Admin** and default password: **Admin**, or using whatever IP Address and Username and Password you have set up.
2. Click the **WIRELESS** → **Setup** link in the main menu of the 4 Ports 11g Wireless ADSL2/2+ Router.
3. Click to **Enable AP** feature.
4. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is **TI-AR7WRD**.

   Note: The SSID of any wireless access adapters must match the SSID you configure in the 4 Ports 11g Wireless ADSL2/2+ Router . If they do not match, you will not get a wireless connection to the 4 Ports 11g Wireless ADSL2/2+ Router.
5. Uncheck the **Hidden SSID**.
6. Set the **Channel B/G**. The default channel is 11. This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point.
7. Set the 802.11 Mode as its default, **Mixed**.
8. Uncheck the **User Isolation** feature.
9. Click **Apply** to complete the setting.
10. To complete and save the setting, click **Save All** after clicking the **Apply** button.
11. Configure and test your computers for wireless connectivity. Program the wireless adapter of your computers to have the same SSID and channel that you configured in the 4 Ports 11g Wireless ADSL2/2+ Router. Check whether they have a wireless link and are able to obtain an IP address by DHCP from the 4 Ports 11g Wireless ADSL2/2+ Router.

    Once your computers have basic wireless connectivity to the 4 Ports 11g Wireless ADSL2/2+ Router, then you can configure the advanced wireless security functions of the firewall.

4.5.2 WIRELESS - Configuration

The Configuration page describes how to configure the wireless features of your 4 Ports 11g Wireless ADSL2/2+ Router.



- **Beacon Period:** Enter a value between 1 ~ 65535 milliseconds. The Beacon Interval value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the 4 Ports 11g Wireless ADSL2/2+ Router to synchronize the wireless network. The default value is 200.

- **DTIM Period:** This value, between 1 ~ 65535, indicates the interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the 4 Ports 11g Wireless ADSL2/2+ Router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages. The default value is 2.

- **RTS Threshold:** The range is 0 ~ 3000 bytes. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The 4 Ports 11g Wireless ADSL2/2+ Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. This default setting is 2347. However, when 4x is enabled on the setup page, the RTS threshold value changes to 4096.

- **Frag Threshold:** The Fragmentation Threshold. The range is 256 ~ 2346 bytes. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the Fragmentation Threshold. Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended. This default setting is 2346. However, when 4x is enabled on the setup page, the fragmentation threshold value changes to 4096.

- **Power Level:** Select “Full”, “50%”, “25%”, “12%” or “6%” Power Level from the drop down manual. The default is **“Full”**.

- **Video Blast Support:** Place a check to enable the Video Blast functionality. Check the following items when Video Blast features is enabled. When checked, priority is given to video in the traffic to and from the specified IP. Noted that this feature is only available if TI wireless station card and TI’s ADSL2/2+ modem are used.

  - ☑ **IP Address:** The LAN-side IP with the preferred bandwidth. This field is related to the Video Blast Support and is enabled when Video Blast Support is checked. You can enter up to two IPs for the Video Blast Support features.

  - ☑ **Protocol:** The protocol used by the IP address. This field is related to the Video Blast Support and is enabled when Video Blast Support is checked. There are three options: None, TCP, and UDP. You will need to select TCP or UDP for each IP.

  - ☑ **Dest Port:** The port number used by the IP address. This field is related to the Video Blast Support and is enabled when Video Blast Support is checked.

- **Apply:** Click **Apply** to complete the setting.

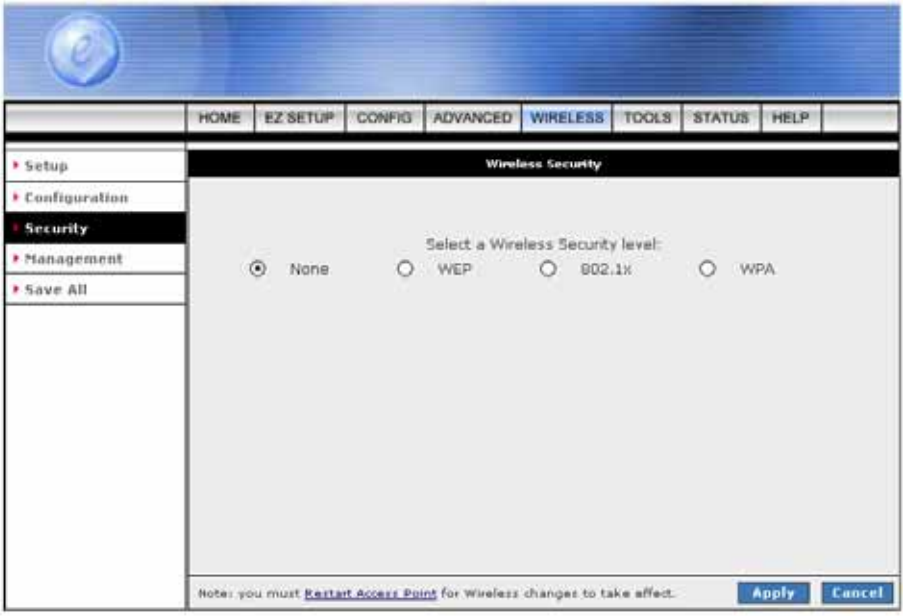
- **Cancel:** Click **Cancel** to ignore all the changes.

- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.3 WIRELESS - Security

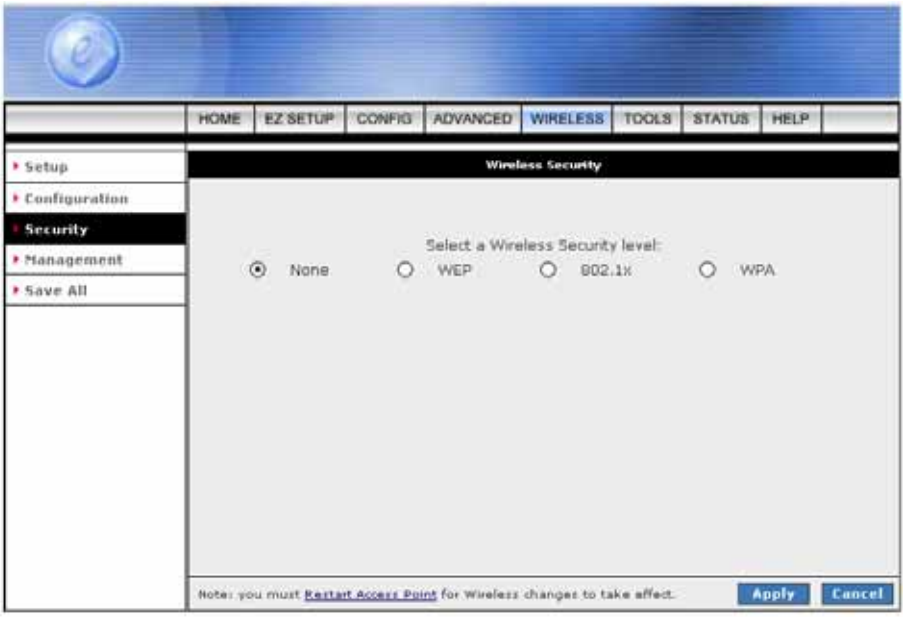
The Security page describes how to configure the Wireless Security Level of your 4 Ports 11g Wireless ADSL2/2+ Router. There are four security level provided by this 4 Ports 11g Wireless ADSL2/2+ Router : **"None"**, **"WEP"**, **"802.1x"** and **"WPA"**.

- ☑ **None:** No security used.
- ☑ **WEP (Wired Equivalent Privacy):** Enable legacy stations to connect the AP.
- ☑ **802.1x:** Enable stations with 802.1x capability to connect the AP.
- ☑ **WPA (Wi-Fi Protected Access)**: Enable stations with WPA capability to connect the AP.



4.5.3.1 WIRELESS – Security - None

None: Wireless security is not used. No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.



- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

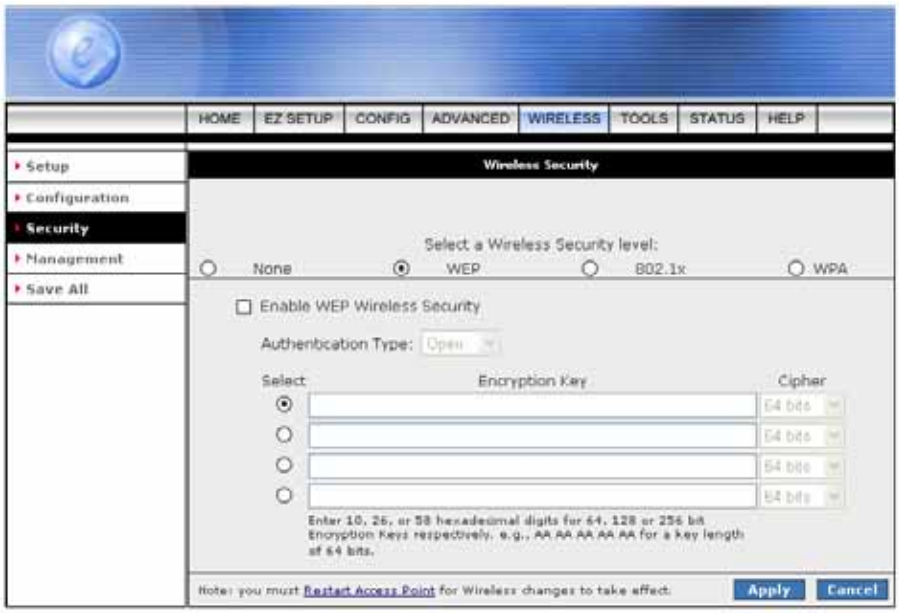
4.5.3.2 WIRELESS – Security - WEP

WEP: Wired Equivalent Privacy. WEP is a security protocol for wireless local area networks defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

The 4 Ports 11g Wireless ADSL2/2+ Router supports 3 levels of WEP encryption:

- ☑ 64 Bit encryption
- ☑ 128Bit encryption
- ☑ 256 Bit encryption

With WEP, the receiving station must use the same key for decryption. Each radio NIC and access point, therefore, must be manually configured with the same key. Figure below illustrates the default setting of the WEP Wireless Security screen.



- **Enable WEP Wireless Security:** Place a check to enable WEP Security.
- **Authentication Type:** Authentication algorithm to use when the security configuration is set to Legacy. When the security configuration is set to 802.1x or WPA, the authentication algorithm is always open. This field is enabled when the WEP security field is checked. There are three options:
  - ☑ **Open:** In open-system authentication, the access point accepts any station without verifying its identify.
  - ☑ **Shared:** Shared-key authentication requires a shared key (WEP encryption key) be distributed to the stations before attempting authentication.

- ☑ **Both:** If both is selected, the access point will perform shared-key authentication, then open-system authentication.

- **Encryption Key:** This field is enabled when the WEP security field is checked. The key's value that is used when the security configuration is set to legacy. The key length must match the WEP cipher. This field is not used when the security configuration is set to 802.1x or WPA.

  - ☑ For 64 bit WEP, enter 10 Hexadecimal digits (any combination of 0-9, A-F).
  - ☑ For 128 bit WEP, enter 26 Hexadecimal digits (any combination of 0-9, A-F).
  - ☑ For 256 bit WEP, enter 58 Hexadecimal digits (any combination of 0-9, A-F).

- **WEP Cipher:** This field is enabled when the WEP security field is checked. You can select from 64 bits, 128 bits, and 256 bits. The WEP cipher that is used when the security configuration is set to Legacy or 802.1x. This field is not used when the security configuration is set to WPA.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

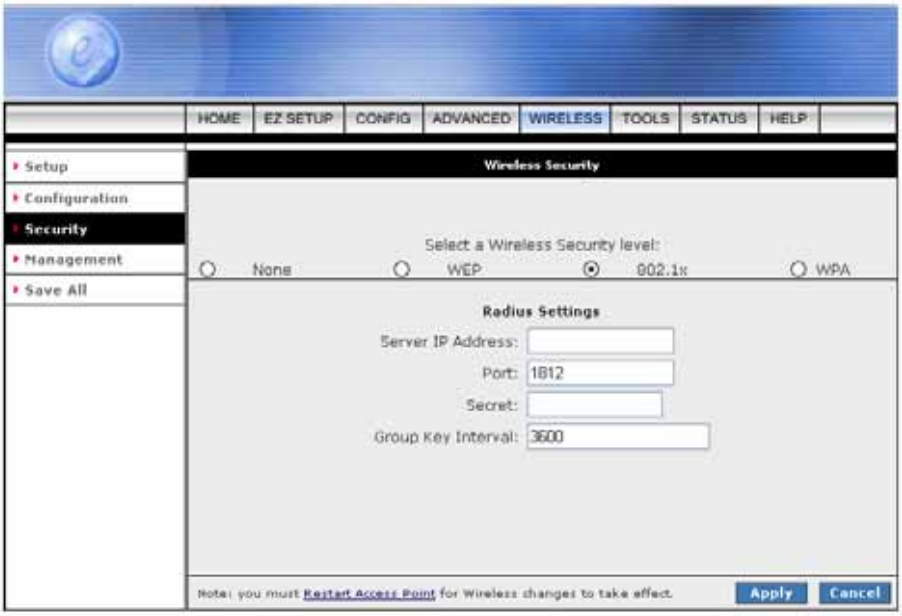
4.5.3.2.1 How to configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the 4 Ports 11g Wireless ADSL2/2+ Router at its default LAN address of *http://192.168.1.1* with its default Username : **Admin** and default password : **Admin**.
2. Click the WIRELESS configuration link in the main menu of the 4 Ports 11g Wireless ADSL2/2+ Router.
3. Go to the Security page.
4. Select the Wireless Security Level.
5. Click Enable WEP Wireless Security.
6. Select the Authentication Type.
7. Select the Encryption Type (64 bits, 128 bits or 256 bits).
8. Enter the Encryption Keys. Manually enter hexadecimal digits (any combination of 0-9, a-f, or A-F).
9. Select the radio button for the key you want to make active. Be sure you clearly understand how the WEP key settings are configured in your wireless adapter.
10. Click **Apply** to complete the setting.
11. To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.3.3 WIRELESS – Security – 802.1x

802.1x is a security protocol for Wireless Local Area Networks (WLAN). It is a port-based network access control that keeps the network port disconnected until authentication is completed. 802.1x is based on Extensible Authentication protocol (EAP). EAP messages from the authenticator to the authentication server typically use the RADIUS (Remote Authentication Dial-In User Service) protocol. Figure below illustrates the default setting of the 802.1x Wireless Security screen.



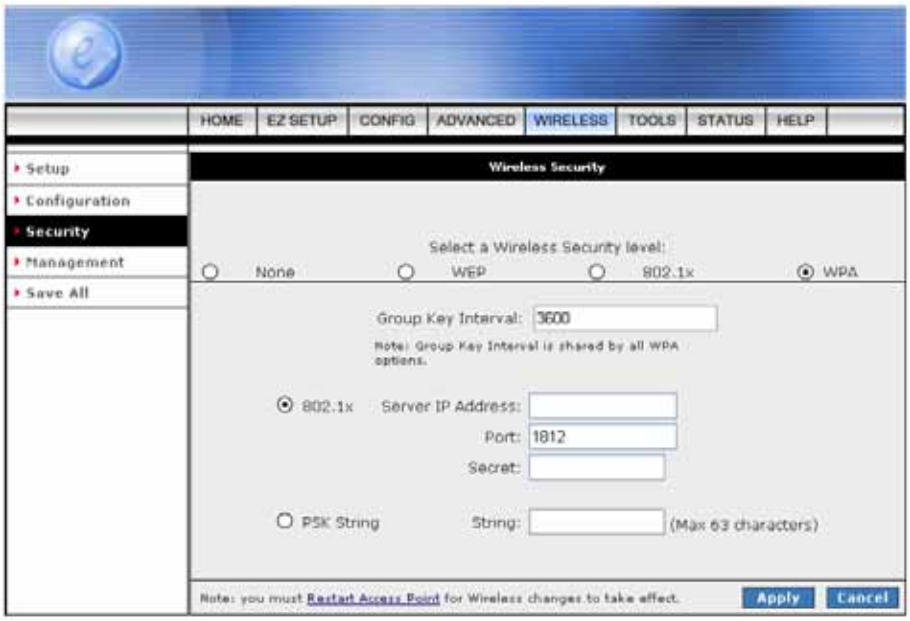
- **Server IP Address:** The LAN-side RADIUS (Remote Authentication Dial-In User Service) server's IP address.
- **Port:** The RADUIS server's port.
- **Secret:** Enter the Radius shared key. The secret that the AP shares with the RADIUS server. You can enter up to 63 characters in this field.
- **Group Key Interval:** The group key interval that is used to distribute the group key to 802.1x and WPA stations.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.3.4 WIRELESS – Security - WPA

WPA (Wi-Fi Protected Access) is a security protocol for Wireless Local Area Networks (WLAN). WPA uses a sophisticated key hierarchy that generates new encryption keys each time a mobile device establishes itself with an access point.

Protocols including 802.1X, EAP and RADIUS are used for strong authentication. Like WEP, keys can still be entered manually (preshared keys); however, using a RADIUS authentication server provides automatic key generation and enterprise-wide authentication. Figure below illustrates the default setting of the WPA (Wi-Fi Protected Access) Wireless Security screen.

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client.

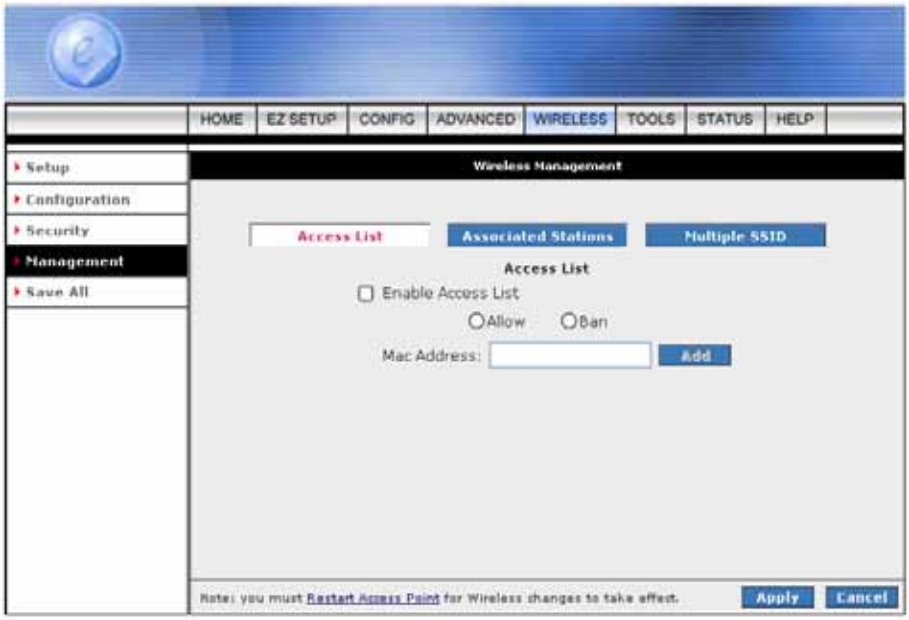


- **Group Key Interval:** Type a numeric value (In seconds) of the time lapse in changing the key in the **"Group Key Interval"** box.
- **802.1x:** When selected, the WPA stations authenticate with the RADIUS server using EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) over 802.1x.
- **Port:** The RADUIS server's port.
- **Secret:** The secret that the AP shares with the RADIUS server.
- **PSK String:** Pre-Shared Key String. When selected, the WPA stations do not authenticate with the RADIUS server using EAP-TLS. Instead they share a pre-shared secret with the AP (ASCII format). The PSK string needs to be entered in the first time configuration with each station.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.4 WIRELESS - Management

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. The **Management** function gives another level of security to your 4 Ports 11g Wireless ADSL2/2+ Router. It allows you to create an allowed access list or a banned access list (not both), and view a list of stations associated with your access point.

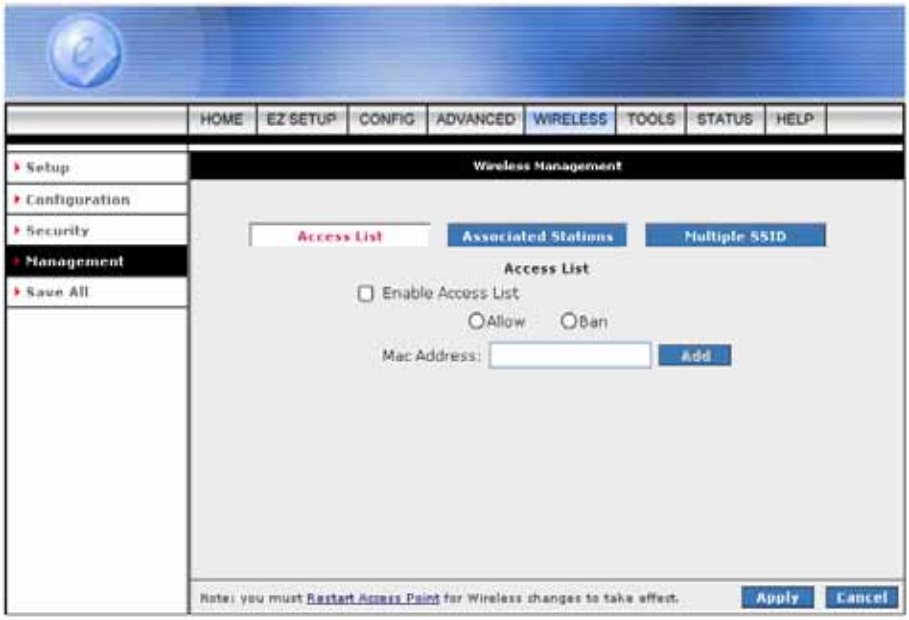
Click on **WIRELESS** then **Management**, the following screen will pop-up.



4.5.4.1 WIRELESS – Management – Access List

Access List: By default, any wireless computer that is configured with the correct wireless network name or SSID will be allowed access to your wireless network. For increased security, you can restrict access to the wireless network to only specific computers based on their MAC addresses.

You can create an **"Allow"** or **"Ban"** access list from the Access List screen by performing the following procedures describe in next section.



- **Enable Access List:** Select **Allow** or **Ban** to setup your Access List.
- **MAC Address:** Enter the MAC Address of the wireless network that are Allow or Ban to access your 4 Ports 11g Wireless ADSL2/2+ Router. Then click **Add** to include to your Access List.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.4.1.1 Access List Configuration Procedure

1. Check **Enable Access List**.

2. Select **Allow** to create an allowed access list or **Ban** to create a banned list.

   Note—You can not create both.

3. Enter a MAC (Medium Access Control) address of an allowed or banned station, then click the **Add** button. This station will appear in your allowed or banned access list.

4. Repeat this step for each station.

5. To save your settings or make the change permanent, click on **Save All**.

4.5.4.2 WIRELESS – Management – Associated Stations

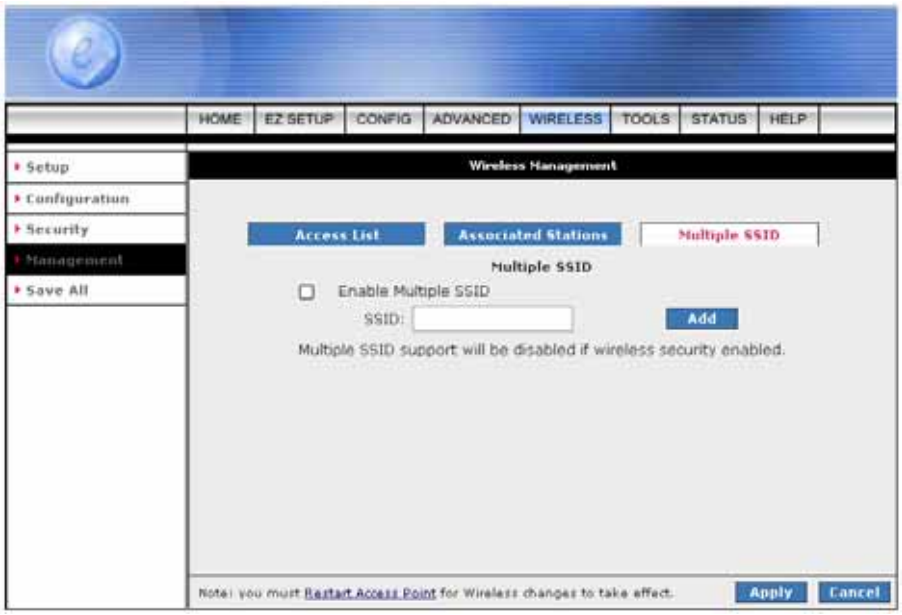
By clicking on the **Associated Stations** button under the **Management** option, you are taken to the Associated Stations screen (Figure below). This screen allows you to see a list of all associated stations with the access point. You can ban any station(s) on the list by clicking on the Ban Station button next to the MAC Address. To save your settings, click on **Save All** after clicking the **Apply** button.

- **Ban Station:** Click and select the Ban Station from the list.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.4.3 WIRELESS – Management – Multiple SSID

Multiple SSID: Click on Multiple SSID and the following screen will pop-up. By default, any wireless PC that is configured with the correct SSID will be allowed access to your wireless network.

An SSID is a 32 character (maximum) alphanumeric key identifying the name of the wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

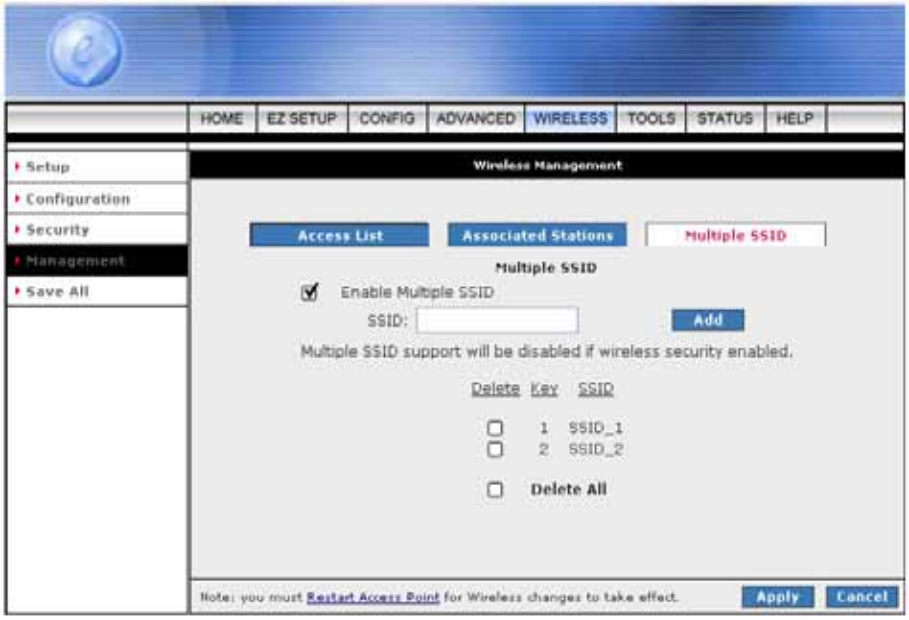


- **Enable Multiple SSID:** Place a check to Enable Multiple SSID. Enter the SSID that are authorized to access the 4 Ports 11g Wireless ADSL2/2+ Router and click the **Add** button to add your entry.
- **SSID:** Manually enter the SSID. An SSID is a 32 character (maximum) alphanumeric key identifying the name of the wireless local area network.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.5.4.3.1 Multiple SSID Configuration Procedure

1. Check **Enable Multiple SSID**.
2. Enter the name of the first SSID in the **SSID** field, then click the **Add** button.

   Repeat this step for each additional SSID. The SSIDs will appear as shown in figure below.

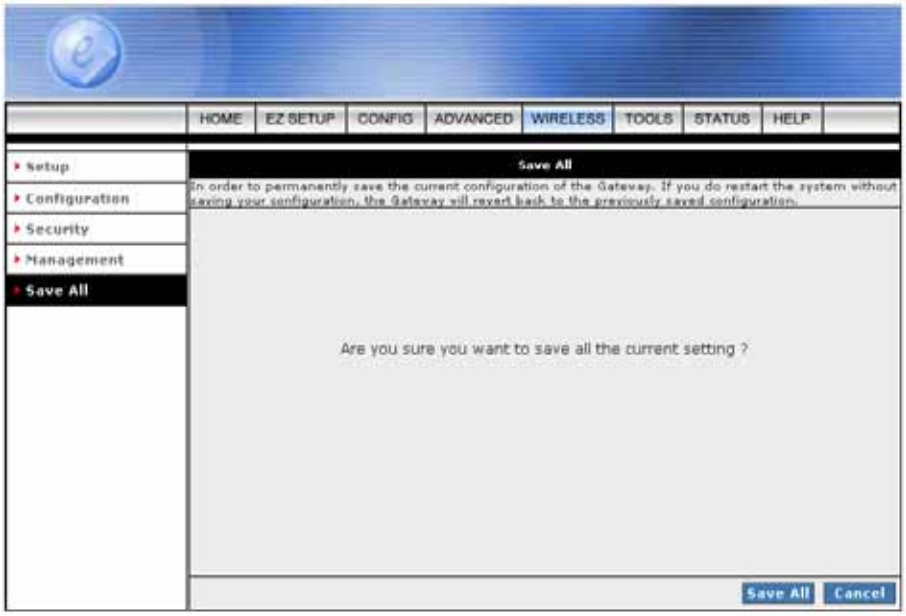


3. To delete an SSID, check the SSID, then click **Delete** in the popup window.

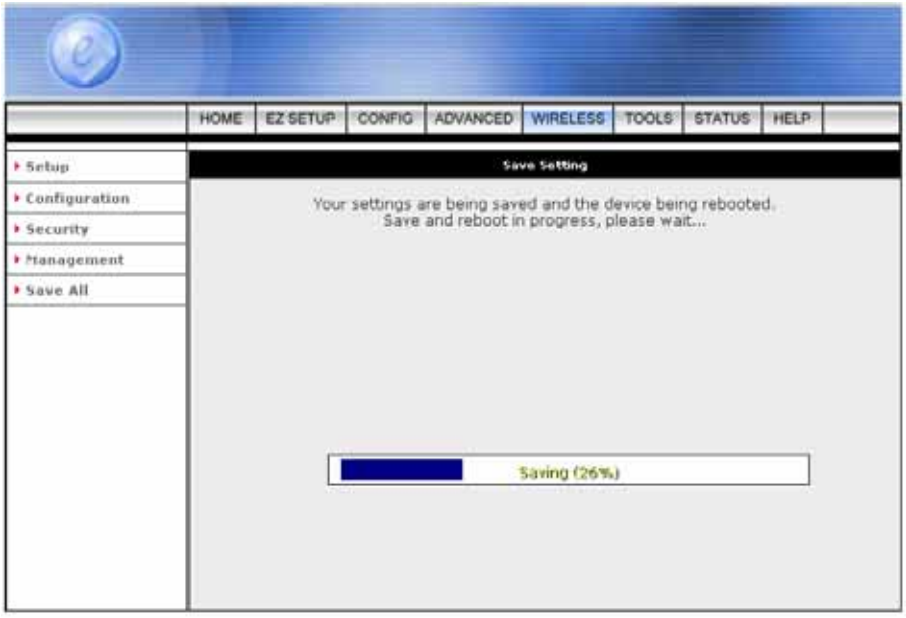
   To delete all SSIDs, check **Delete All**.
4. To save your settings, click **Save All** after clicking the **Apply** button.

4.5.5 WIRELESS – Save All

This button enables you to permanently save the current configuration of this 4 Ports 11g Wireless ADSL2/2+ Router. If you restart the system without saying your configuration, this 4 Ports 11g Wireless ADSL2/2+ Router will revert back to the previously saved configuration.



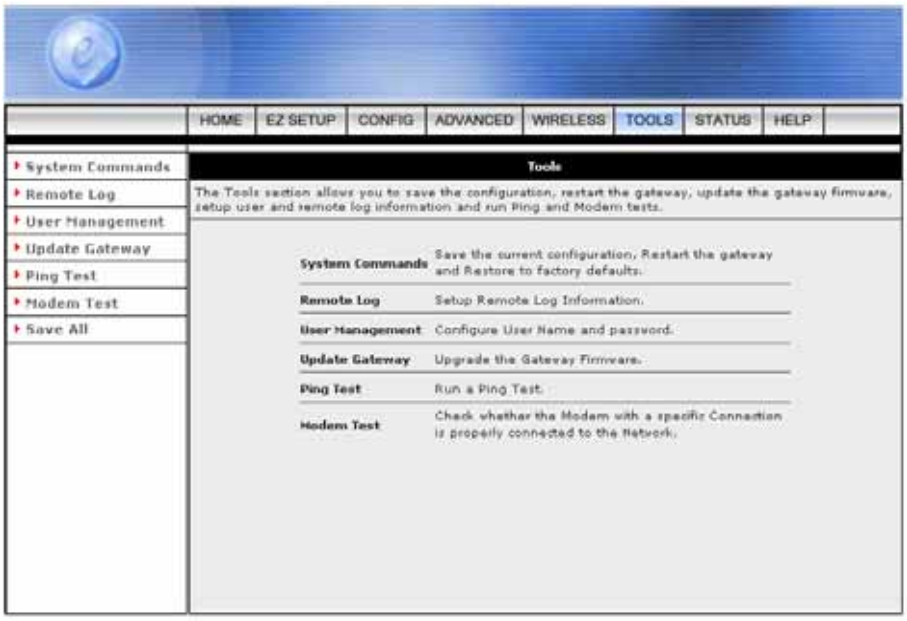
- **Save All:** Click **Save All** to confirm the setting. The following window will be shown.



4.6 TOOLS

Figure below shows the **TOOLS** main screen, which can be accessed by clicking on the **TOOLS** tab from the top of the screen. This screen provides access to the following tools screens:

- ☑ System Commands
- ☑ Remote Log
- ☑ User Management
- ☑ Update Gateway
- ☑ Ping Test
- ☑ Modem Test
- ☑ Save All



- **System Commands:** Save the current configuration, restart the 4 Ports 11g Wireless ADSL2/2+ Router and restore to factory defaults setting.
- **Remote Log:** Setup Remote Log Information.
- **User Management:** Configure user name and password.
- **Update Gateway:** Upgrade the 4 Ports 11g Wireless ADSL2/2+ Router firmware.
- **Ping Test:** Run a ping test.
- **Modem Test:** Check whether the modem with a specific connection is properly connected to the network.
- **Save All:** Save the device setting.

4.6.1 TOOLS - System Commands

Figure below shows the default System Commands screen, which can be accessed by clicking on the System Commands link.

- **Restart:** This button enables you to restart the system. If you have not saved your configurations, the 4 Ports 11g Wireless ADSL2/2+ Router will revert back to the previously save configuration upon re-starting.

  Note: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

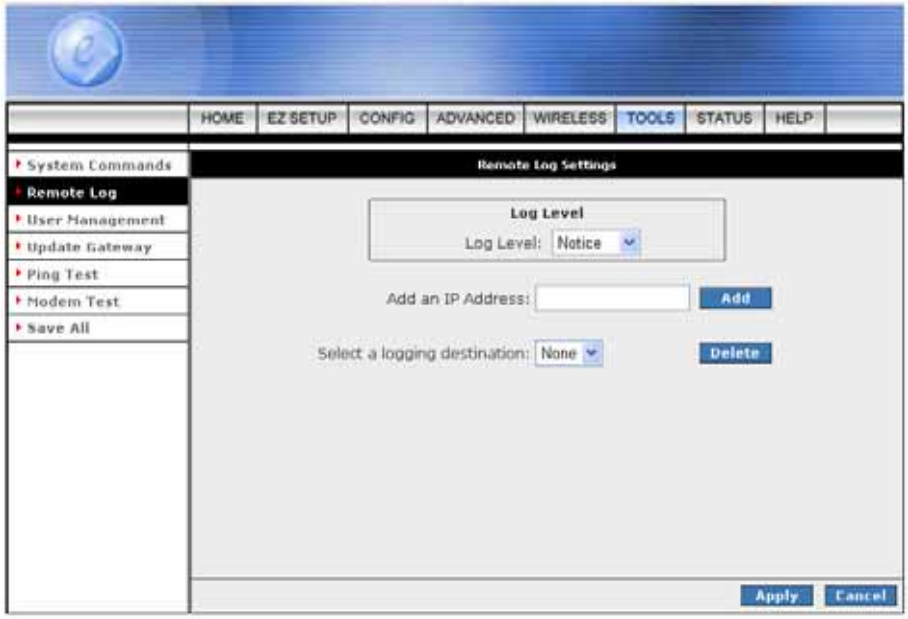
- **Restart Access Point:** Use this button to restart the Wireless Access Point. It is important to Restart the Access Point any time when changing the Wireless Setting.

- **Restore Defaults:** Use this button to restore factory default configurations.

  Note: You will be redirected to the 4 Ports 11g Wireless ADSL2/2+ Router Homepage after the unit has successfully been restored to factory default configurations.

4.6.2 TOOLS - Remote Log

Figure below shows the default **Remote Log** screen. The remote log feature will forward all logged information to the 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 and are rated at that level or higher are logged to the destination.



- **Log Level:** The default log level is **"Notice"**. There are eight log levels in the order of its severity:
  - ☑ **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:** Critical conditions, such as hard drive errors.
  - ☑ **Error:** Error conditions that generally have less serious consequences than errors in the emergency, 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 message. Specify the level only when so directed by a technical support representative.

Note: when you select a log level, all log information within this severity level and level(s) above (meaning, more severe levels) will be sent to the remote PC.

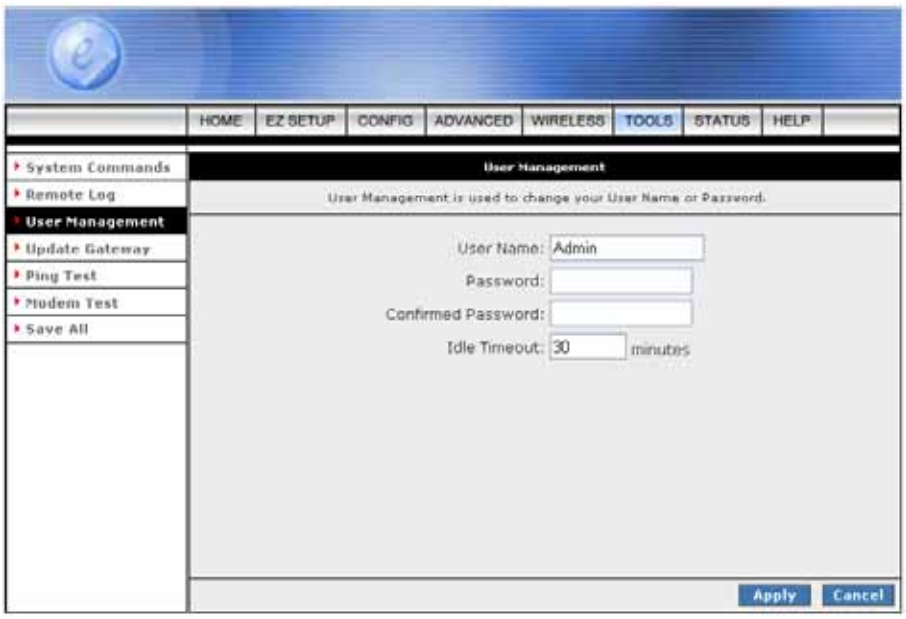
- **Add an IP Address:** You can also enter additional IP address to which you want the log information be forwarded to other than the remote PC. Any IP address you add here will show up in the drop-down list of the next field: Select a logging destination.
- **Select a logging destination:** You can select a destination IP to which the log information will be sent from the drop-down list. You can customize the list using the Add and/or Delete buttons.
- **Delete:** Delete the logging destination IP Address from the drop down list.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.6.3 TOOLS - User Management

User Management: The User Management page enables you to change your User Name and/or Password. It is recommended that you change the User Name and password from the default Admin to ensure the security of the 4 Ports 11g Wireless ADSL2/2+ Router.

For security reasons, the router has its own user name and password. Also, after a period of inactivity for a set length of time, the administrator login will automatically disconnect. When prompted, enter the router User Name: **Admin** and the router Password: **Admin** to log in.

NOTE: If you forget your user name and password, access to the 4 Ports 11g Wireless ADSL2/2+ Router can only be gained by resetting the unit to factory defaults. Pressing the **"Reset"** button for 10 seconds, the LED indicators will turns OFF and ON again indicates that the Reset process is successfully done.



- **User Name: "Admin"** is your default user name. You can enter your new user name here.
- **Password: "Admin"** is your default password. You can enter your new password here.

  Note: If you forget your password, you can press and hold the reset to factory default button for 10 seconds (or more). The 4 Ports 11g Wireless ADSL2/2+ Router will reset to its factory default configuration and all custom configuration will be lost.

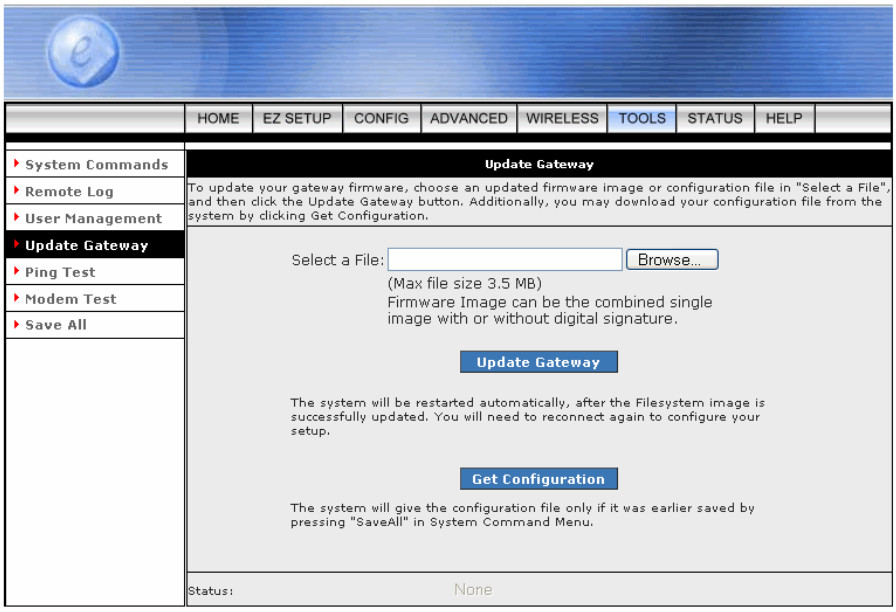
- **Confirm Password:** Enter your new password here again to confirm.
- **Idle Timeout:** The default is 30 minutes. You will need to log back onto the 4 Ports 11g Wireless ADSL2/2+ Router if it is been inactive for 30 minutes. You can change the timeout here.
- **Apply:** Click **Apply** to complete the setting.
- **Cancel:** Click **Cancel** to ignore all the changes.
- To complete and save the setting, click **Save All** after clicking the **Apply** button.

4.6.4 TOOLS - Update Gateway

Update Gateway: Firmware is the software that controls the 4 Ports 11g Wireless ADSL2/2+ Router and also provides the user interface that is subject of this manual. The Firmware resides in the 4 Ports 11g Wireless ADSL2/2+ Router internal Flash memory; currently loaded firmware version can be found under **STATUS → Product Information**.

Note: It is recommends that you back up your configuration before doing a firmware upgrade. After the upgrade is complete, you may need to restore your configuration settings.

To access Firmware Updates, click on **TOOLS → Update Gateway**. The following window screen will pop-up.



- **Select a File:** Click on the **Browse…** button to locate the Firmware or update image file from your computer's hard drive.
- **Update Gateway:** Click the **Update Gateway** button to upgrade your 4 Ports 11g Wireless ADSL2/2+ Router. The system will be restarted automatically after the Firmware/Image is successfully uploaded. You will need to reconnect again to configure your setup.
- **Get Configuration:** You may download your configuration file from the system by clicking **Get Configuration**. Follow the instruction and save your configuration file in your hard drive.

Note: When uploading Firmware/Configuration File to the 4 Ports 11g Wireless ADSL2/2+ Router, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the upgrading process. When the upload is complete, your 4 Ports 11g Wireless ADSL2/2+ Router will automatically reboot and restart. The upgrade process will typically take about 1~2 minutes.

4.6.4.1 Update Gateway Procedure

Use the following procedures to update firmware for your 4 Ports 11g Wireless ADSL2/2+ Router.

1. Click **Browse** and select the file to update. The file name will appear in the Select a File field.
   Note—The file size should not exceed 3.5MB.

2. Click **Update Gateway**. The status of the uploading will appear at the bottom of the screen. When the upload is finished, the 4 Ports 11g Wireless ADSL2/2+ Router will reboot and you will be prompt to log in again.

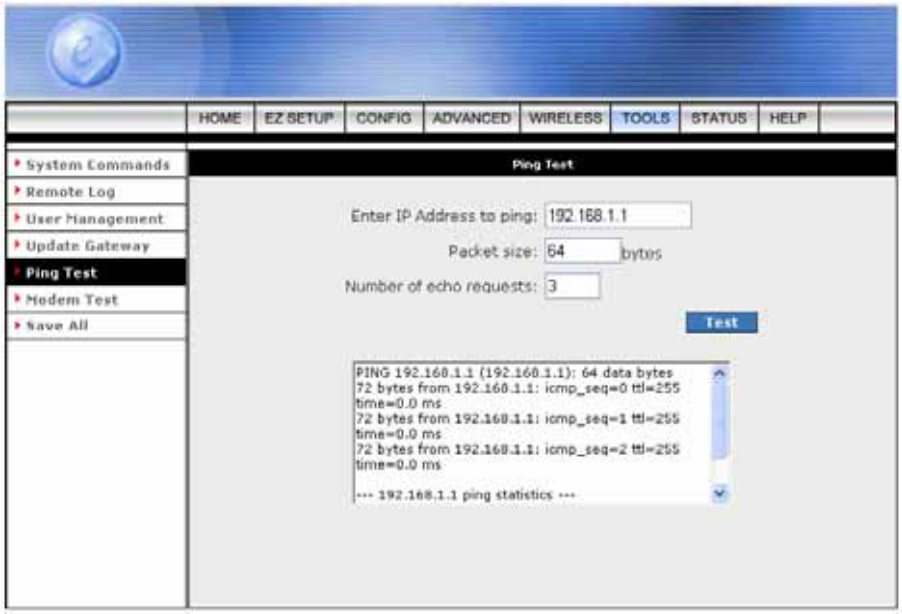
3. Enter your **Username** and **Password** to log back in.

4. If you want to make sure the firmware is properly upgraded, go to **Status /Product Information** and check on the Wireless Firmware version information on the Product Information screen

5. If you would like a copy of the configuration file (config.bin) saved to the 4 Ports 11g Wireless ADSL2/2+ Router flash, click **Get Configuration** to download it.

4.6.5 TOOLS - Ping Test

Once you have your 4 Ports 11g Wireless ADSL2/2+ Router configured, it is a good idea to make sure you can Ping the network. Figure below shows the default Ping Test screen, which can be accessed by clicking on the Ping Test link from the left of the Tools screen. If you have your PC connected to the 4 Ports 11g Wireless ADSL2/2+ Router via the default DHCP configuration, you should be able to Ping the network address 192.168.1.1. If the pings for both the WAN side and the LAN side are complete, and your have the proper protocol configures, you should be able to surf the Internet.



- **Enter IP Address to ping:** Enter the IP address that you want to ping. The default is set to the default IP address of you AR7 is “192.168.1.1”.
- **Packet size**: You can define the packet size of the ping test. The default is 64 bytes.
- **Number of echo requests**: You can define how many times the IP address will be pinged. The default is 3 times.
- **Test**: Click Test to start the ping test. The result will be shown in the window underneath.

4.6.5.1 Ping Test Procedure

1. Click **Ping Test** from the **Tools** menu to access the Ping Test screen.

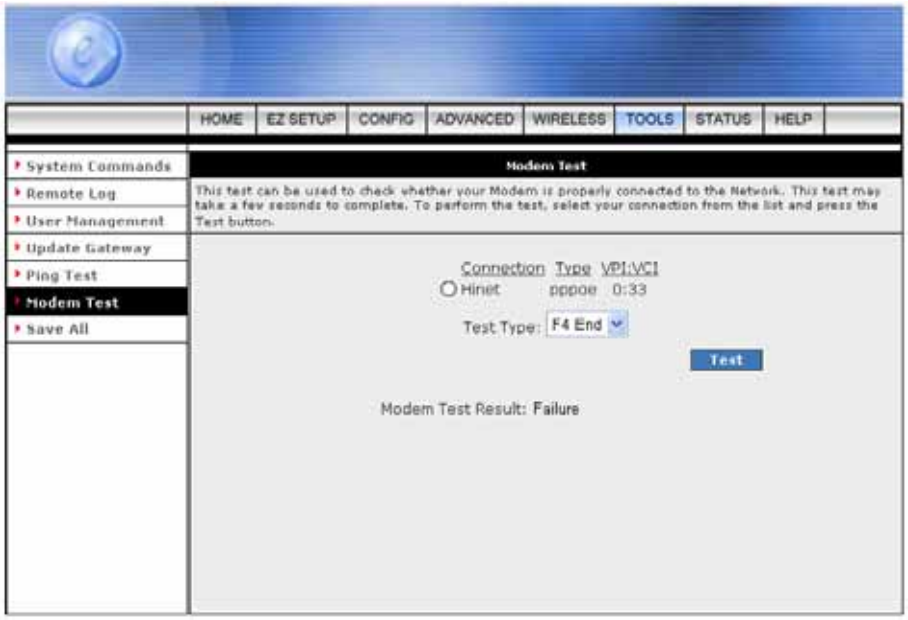
2. Change or leave the default settings of the following fields:
   - Enter IP Address to ping
   - Packet size
   - Number of echo requests

3. Click **Test**.

4. The ping results will be displayed in the box on the screen. If the ping test was successful, it means that the TCP/IP protocol is up and running. If the Ping test failed, the TCP/IP protocol is not loaded for some reason, you should restart the 4 Ports 11g Wireless ADSL2/2+ Router.

4.6.6 TOOLS - Modem Test

The **Modem Test** is used to check weather your Modem is properly connected to the WAN network. This test may take a few seconds to complete. Before running this test, make sure you have at least one WAN connection configured and have valid ADSL link; if the ADSL link is not connected, the test will fail. Figure below illustrates the Modem Test screen with one WAN connections (Hinet) pre-configured.



- **Connection:** The WAN connections you have available.

  Note: You will not be able to perform a modem test without any WAN connection configured.

- **Type:** The type of the WAN connection.

- **VPI/VCI:** Virtual Path identifier/Virtual Channel Identifier.

- **Test Type:** There are 4 test types:

  ☑ **F4 End:** F4 end to end.

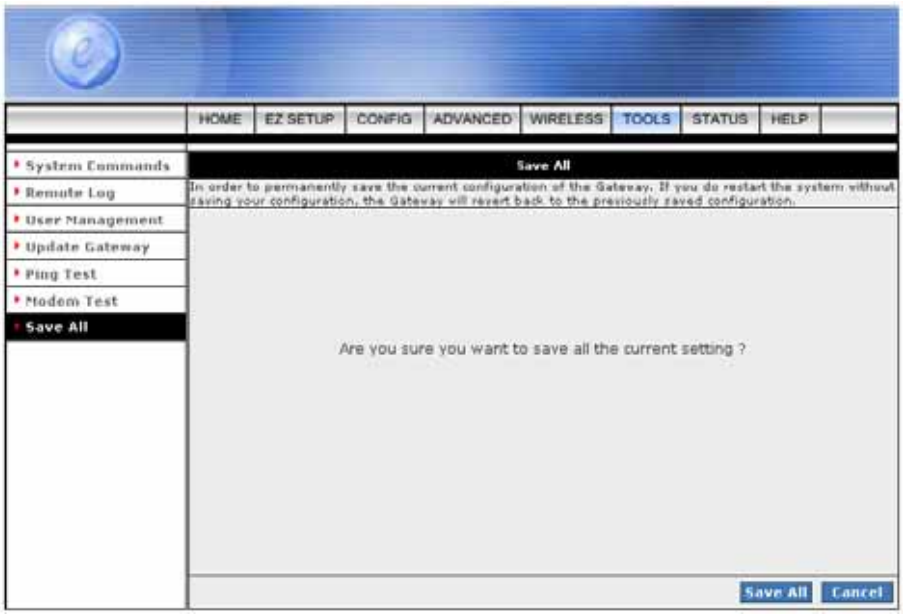
  ☑ **F4 Seg:** F4 segment.

  ☑ **F5 End:** F5 end to end.

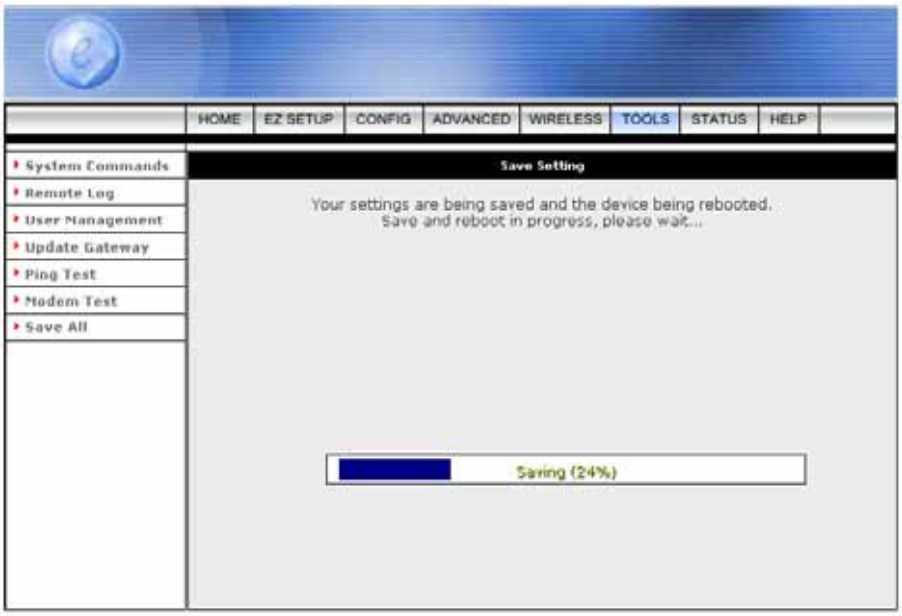
  ☑ **F5 Seg:** F5 segment.

4.6.7 TOOLS – Save All

This button enables you to permanently save the current configuration of this 4 Ports 11g Wireless ADSL2/2+ Router. If you restart the system without saying your configuration, this 4 Ports 11g Wireless ADSL2/2+ Router will revert back to the previously saved configuration.



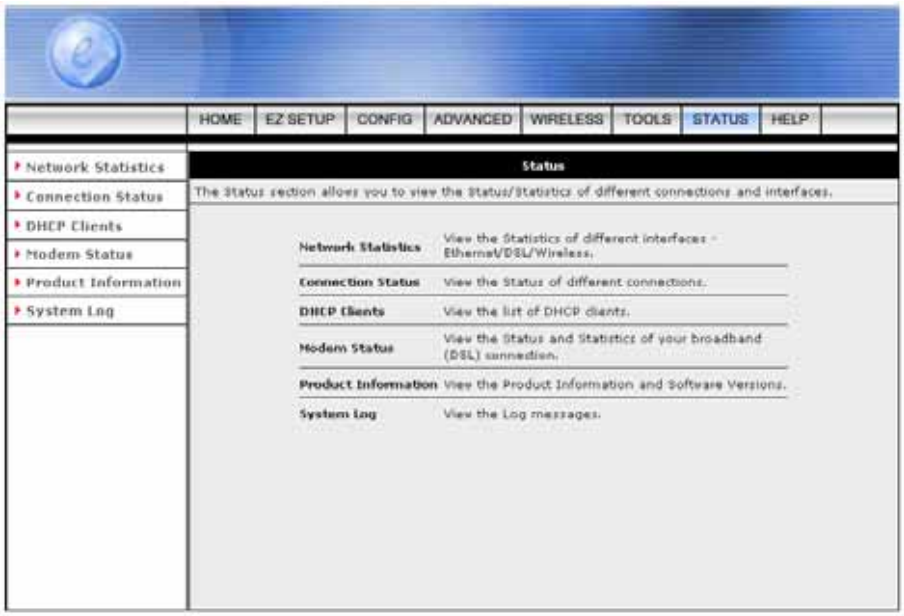
- **Save All:** Click **Save All** to confirm the setting. The following window will be shown.



4.7 STATUS

Figure shows the Status main screen, which can be accessed by clicking on the **STATUS** tab from the top of the screen. This screen provides access to the following status screens:

- Network Statistics
- Connection Status
- DHCP Clients
- Modem Status
- Product Information
- System Log

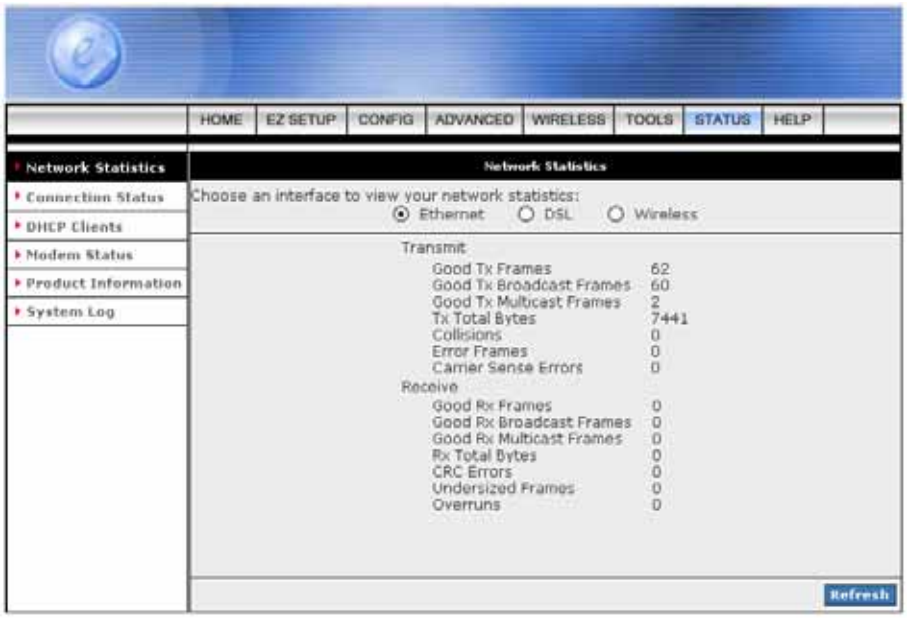


4.7.1 STATUS - Network Statistics

The Network Statistics show the Select Network Interface type to peruse statistics for each type of connection. Click Ethernet, USB (Optional), DSL or Wireless to view your Network Statistics.

4.7.1.1 STATUS - Network Statistics - Ethernet

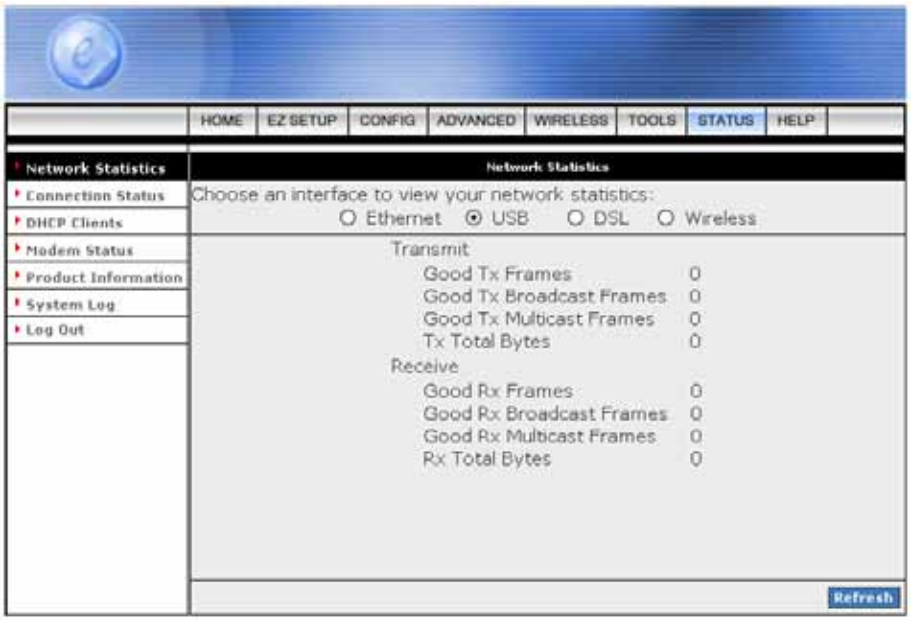
Ethernet: Shows the Transmit/Receive Frames, Error Frames, Collision and CRC Errors information of the Ethernet Interface. The traffic counter will reset if the device is rebooted.



- **Refresh:** Click **Refresh** button to reload Web browser.

4.7.1.2 STATUS - Network Statistics – USB (Optional)

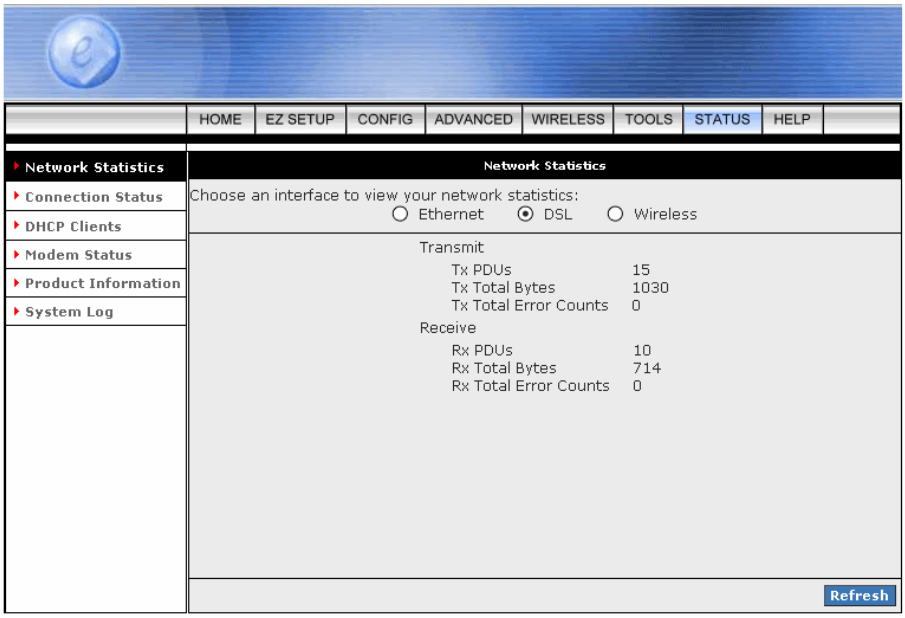
USB: Shows the Transmit/Receive Frames and Total Bytes Receive/Transmit information of the USB Interface. The traffic counter will reset if the device is rebooted.



- **Refresh:** Click **Refresh** button to reload Web browser.

4.7.1.3 STATUS - Network Statistics - DSL

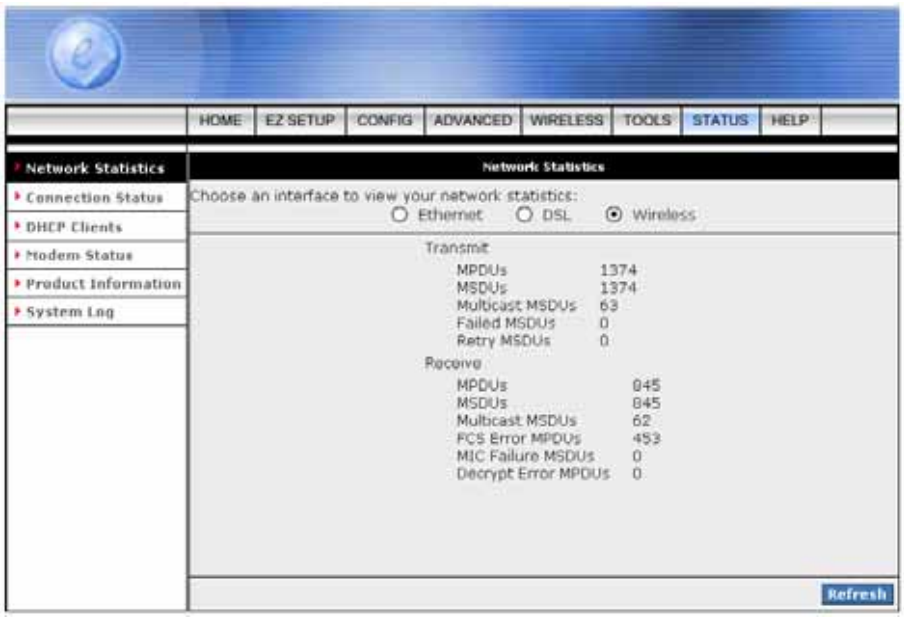
DSL: Shows the Total Bytes Receive/Transmit and Error Count information of the ADSL (WAN) Interface. The traffic counter will reset if the device is rebooted.



- **Refresh:** Click **Refresh** button to reload Web browser.

4.7.1.4 STATUS - Network Statistics - Wireless

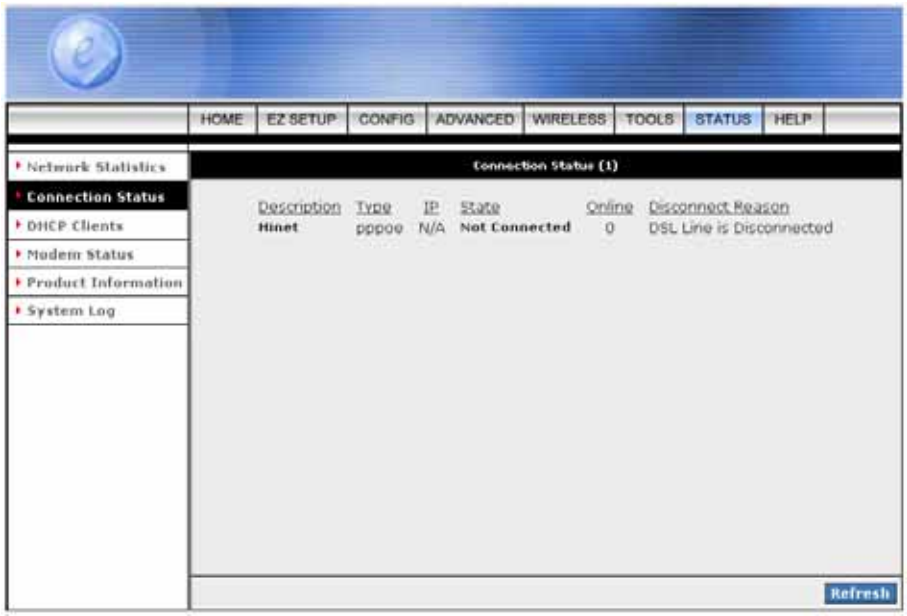
Wireless: Shows the packets transmit/receive information through the Wireless Interface. The traffic counter will reset if the device is rebooted.



- **Refresh:** Click **Refresh** button to reload Web browser.

4.7.2 STATUS – Connection Status

You can view your the status of your different connections from the Connection Status screen. To access, click on the **Connection Status** link from the **STATUS** main screen.

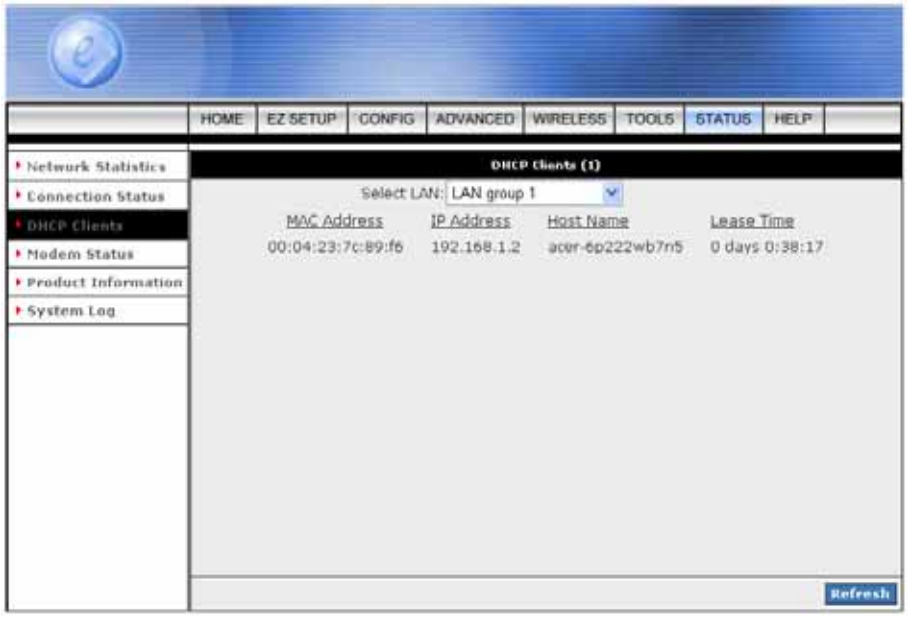


- **Refresh:** Click **Refresh** button to reload Web browser.

4.7.3 STATUS - DHCP Clients

If you have enabled the DHCP server, you can view a list of the DHCP clients from the DHCP Clients screen. From the **STATUS** main screen, click the **DHCP Clients** link, select the LAN connection, and the following information of the DHCP LAN Clients will be displayed:

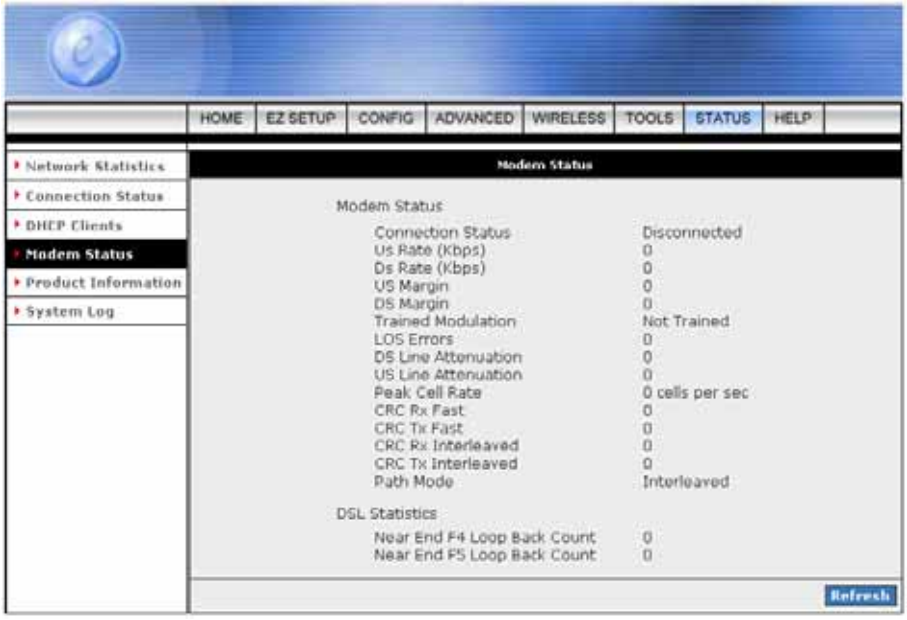
- MAC Address
- IP Address
- Host Name
- Lease Time



- **Refresh:** Click **Refresh** button to reload Web browser.

4.7.4 STATUS - Modem Status

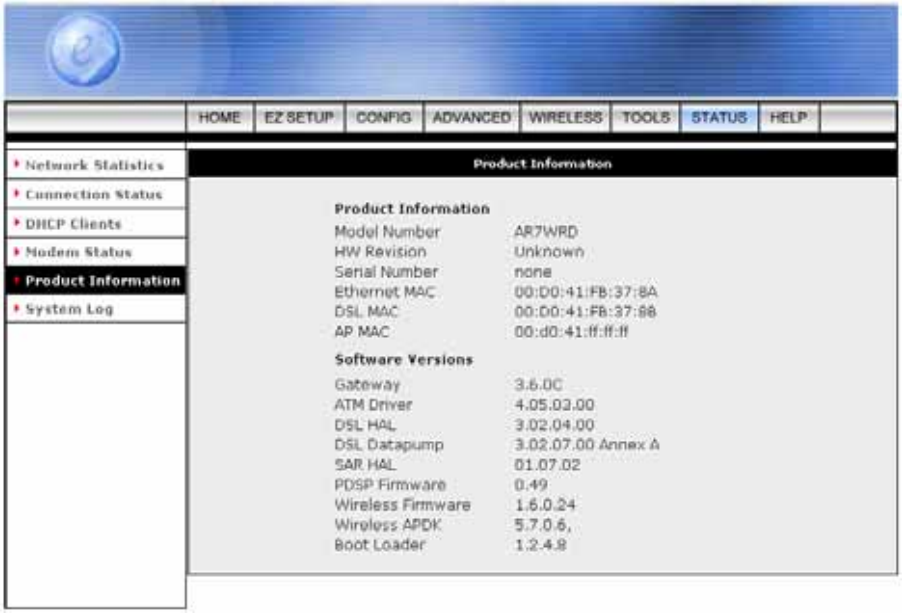
The **Modem Status** page shows the 4 Ports 11g Wireless ADSL2/2+ physical layer or link status. The information displayed on this page is either inherent to the 4 Ports 11g Wireless ADSL2/2+ Router or set by the ADSL Central Office (CO) DSLAM, neither of which cannot be changed by the user.



- **Refresh:** Click **Refresh** button to reload Web browser.

4.7.5 STATUS - Product Information

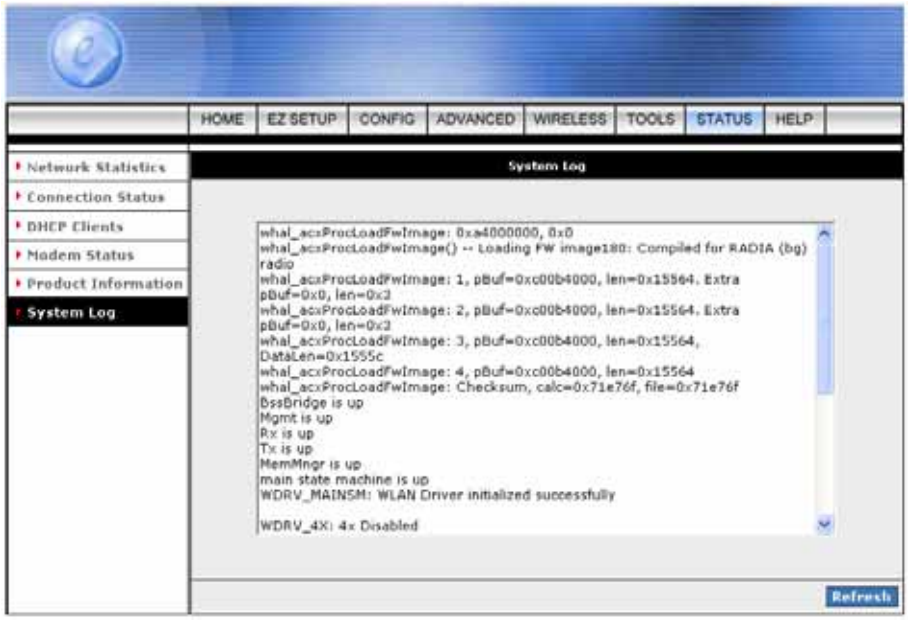
The **Product Information** show the complete information and various parameters of the 4 Ports 11g Wireless ADSL2/2+ Router including Software Versions.



4.7.6 STATUS - System Log

You can display your 4 Ports 11g Wireless ADSL2/2+ Router's log by clicking on the **System Log** link from the **STATUS** Main screen. The **System Log** screen allows you to view all logged information. Depending upon the severity level, the logged information will generate log reports to a remote host (if remote logging is enabled).

This page contains information that is dynamic and will refresh every 5~10 seconds..

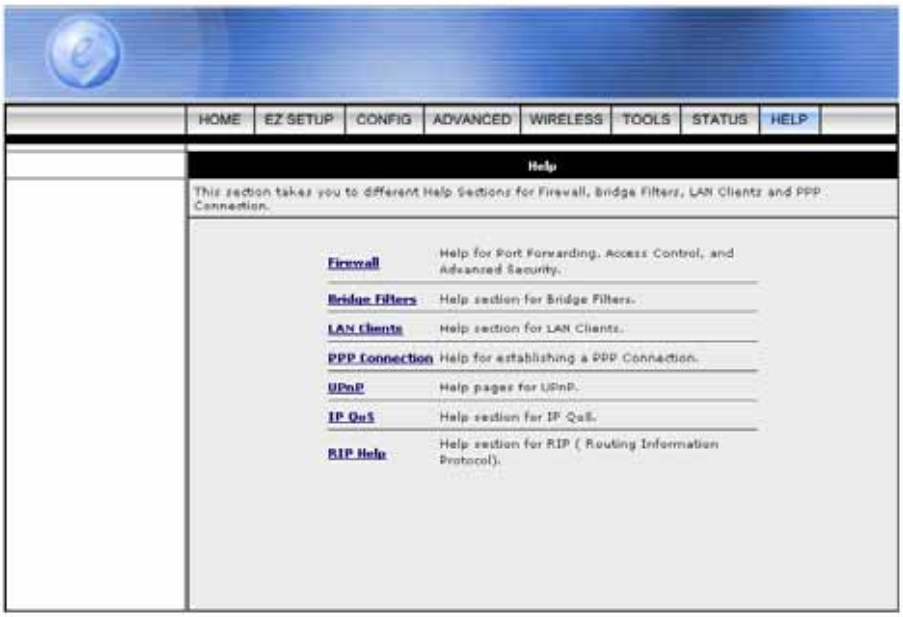


- **Refresh:** Click **Refresh** button to reload Web browser.

4.8 HELP

Figure below shows the **HELP** main screen, which can be accessed by clicking on the **HELP** tab from the top of the screen. The help screens provide help information on the following advanced features:

- Firewall (Port forwarding, Access Control, and Advanced Security)
- Bridge Filters
- LAN Clients
- PPP Connection
- UPnP
- IP QoS
- RIP (Routing Information Protocol)



Appendix A: Router Terms

What is a firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

What is NAT?

NAT stands for Network Address Translation. Another name for it is Connection Sharing. What does this mean? Your ISP provides you with a single network address for you to access the Internet through. However, you may have several machines on your local network that want to access the Internet at the same time. The router provides NAT functionality that converts your local network addresses to the single network address provided by your ISP. It keeps track of all these connections and makes sure that the correct information gets to the correct local machine.

Occasionally, there are certain programs that don't work well through NAT. Some games, and some specialty applications have a bit of trouble. The router contains special functionality to handle the vast majority of these troublesome programs and games. NAT does cause problems when you want to run a SERVER though. When running a server, please see the DMZ section below.

What is a DMZ?

DMZ really stands for Demilitarized Zone. It is a way of separating out part of your local network so that is more open to the Internet. Suppose that you want to run a web-server, or a game server. Normal servers like these are blocked from working by the NAT functionality. The solution is to "isolate" the single local computer into a DMZ. This makes the single computer look like it is directly on the Internet, and others can access this machine.

Your machine isn't really directly connected to the Internet, and it really has an internal local network address. When you provide the servers network address to others, you must provide the address of the router. The router "fakes" the connection to your machine.

You should use the DMZ when you want to run a server that others will access from the Internet. Internal programs and servers (like print servers, etc) should NOT be connected to the DMZ

What is a Gateway?

The Internet is so large that a single network cannot handle all of the traffic and still deliver a reasonable level of service. To overcome this limitation, the network is broken down into smaller segments or subnets that can deliver good performance for the stations attached to that segment. This segmentation solves the problem of supporting a large number of stations, but introduces the problem of getting traffic from one subnet to another.

To accomplish this, devices called routers or gateways are placed between segments. If a machine wishes to contact another device on the same segment, it transmits to that station directly using a simple discovery technique. If the target station does not exist on the same segment as the source station, then the source actually has no idea how to get to the target.

One of the configuration parameters transmitted to each network device is its default gateway. This address is configured by the network administrators and it informs each personal computer or other network device where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside of this area, it is usually because of an incorrectly configured default gateway.

Appendix B: Frequently Asked Questions

The Frequently Asked Questions addresses common questions regarding 4 Ports 11g Wireless ADSL2/2+ Router settings.

Some of these questions are also found throughout the guide, in the sections to which they reference.

1. **How do I determine if a link between the Ethernet card (NIC) and the 4 Ports 11g Wireless ADSL2/2+ Router has been established?**

Ans. A ping test would determine if a connection is established between your 4 Ports 11g Wireless ADSL2/2+ Router and computer. Using, the ping command, ping the IP address of the 4 Ports 11g Wireless ADSL2/2+ Router, in this case, 192.168.1.1 (default). For more information on Ping Testing, refer to Appendix C: Troubleshooting Guide. Alternatively, if the Ethernet LINK LED is solidly on, then the Ethernet link is established.

2. **How do I determine if a link between the 4 Ports 11g Wireless ADSL2/2+ Router and the Internet has been established?**

Ans. Similar to the previous question, a ping test would determine whether or not a connection is established. However, this time use a URL instead of and IP Address, such as www.google.com. Alternatively, if the ADSL LED is solidly on, then the ADSL link is established.

3. **How can I find/verify my 4 Ports 11g Wireless ADSL2/2+ Router and/or computer Ethernet MAC Address?**

Ans. Refer to Chapter 3 and 4 for details.

4. **What is ad-hoc mode?**

Ans. When a wireless network is set to ad-hoc mode, the wireless-equipped computers are configured. To communicate directly with each other, peer-to-peer without the use of an access point.

5. **What is infrastructure mode?**

Ans. When a wireless network is set to infrastructure mode, the wireless network is configured to communicate with a network through a wireless access point.

6. **What is roaming?**

Ans. Roaming is the ability of a portable computer user to communicate continuously while moving freely throughout an area greater than that covered by a single access point. Before using the roaming function, the computer must make sure that it is the same channel number with the access point of dedicated coverage area.

7. What is ISM band?

Ans. The FCC and their counterparts outside of the U.S. have set aside bandwidth for unlicensed use in the ISM (Industrial, Scientific and Medical) band. Spectrum in the vicinity of 2.4 GHz, in particular, is being made available worldwide. This presents a truly revolutionary opportunity to place convenient high-speed wireless capabilities in the hands of users around the globe.

8. What is MAC Address?

Ans. Short for **Me**dia **A**ccess **C**ontrol **Address.** It is a hardware address that uniquely identifies each node of a Ethernet networking device. This address is usually permanent.

9. What is IEEE 802.11b standard?

Ans. IEEE 802.11b is an extension standards to 802.11 that applies to Wireless LAN and provides 11Mbps transmission speed in the 2.4 GHz band.

10. What is IEEE 802.11g standard?

Ans. IEEE 802.11g is an extension standards to 802.11 that applies to Wireless LAN and provides 54Mbps transmission speed in the 2.4 GHz band.

11. What is NAT (Network Address Translation) and what is it used for?

Ans. NAT translates multiple IP Address on the private LAN to one public IP Address (in WAN) that is sent out to the Internet. NAT adds a level security since the IP address of a PC connected to the private LAN is never transmitted on the Internet.

12. What can I do when I am not able to get the web configuration screen for this 4 Ports 11g Wireless ADSL2/2+ Router?

Ans. Remove the proxy settings on your Internet Browsers or remove the dial-up settings on your browser.

13. What is DMZ (DeMilitarized zone)?

Ans. DMZ allows one IP Address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. It is recommended that you set your computer with a static IP if you want to use DMZ features.

14. What is BSS ID?

Ans. A specific Ad-Hoc LAN is called a Basic Service Set (BSS). Computers in a BSS must be configured with the same BSS ID.

15. What is SSID?

Ans. Short for Service Set Identifier. SSID is a 32 character unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS. The SSID differentiates one WLAN from another, so all Access Point and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID.

16. What is WEP?

Ans. Short for **W**ired **E**quivalent **P**rivacy. WEP is a security protocol for wireless local area networks defined in the 802.11b standard. WEP is designed to provide the same level of security as that of a wired LAN. WEP aims to provide security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

***17.* What is WPA?**

Ans. Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.

18. What is the maximum IP addresses supported by this 4 Ports 11g Wireless ADSL2/2+ Router?

Ans. The 4 Ports 11g Wireless ADSL2/2+ Router can support up to 253 IP addresses.

Appendix C: Troubleshooting Guide

The Troubleshooting Guide provides answers to common problems regarding the 4 Ports 11g Wireless ADSL2/2+ Router settings, connections, and computer settings.

1. The 4 Ports 11g Wireless ADSL2/2+ Router does not work (None of the LEDs light up)

Ans. Check the following:

1. Make sure that the 4 Ports 11g Wireless ADSL2/2+ Router is plugged into a power socket.
2. Make sure that you are using the correct power supply for your 4 Ports 11g Wireless ADSL2/2+ Router device.
3. Make sure the power switch on the 4 Ports 11g Wireless ADSL2/2+ Router is turned on

2. I changed the LAN IP Address in the LAN configuration page and my PC is no longer able to detect the 4 Ports 11g Wireless ADSL2/2+ Router.

Ans. After changing the LAN IP Address of the 4 Ports 11g Wireless ADSL2/2+ Router, proceed to the following step before a PC is able to recognize the 4 Ports 11g Wireless ADSL2/2+ Router:

1. Click **"Start"** → **"Run"**.
2. In the open field, enter **"cmd"** then click **"OK"**.
3. In the command prompt, type **"ipconfig/release"** then press **"Enter"**.
4. Type **"ipconfig / renew"** then press **"Enter"**.
5. Type **"ipconfig ?"** for more usage of the command.

3. No wireless connectivity.

Ans. Check the following:

1. Make sure both wireless client adapter and the 4 Ports 11g Wireless ADSL2/2+ Router is allowed to connect through wireless channels as defined for local regulatory domain.
2. Make sure that the WLAN client is configured for the correct wireless settings (SSID, WEP).

4. Poor wireless connectivity or reach.

Ans. Check the following:

1. Choose automatic channel selection or be careful to select a DSSS channel that doesn't interfere with other radio channels.
2. Check the location of the 4 Ports 11g Wireless ADSL2/2+ Router in the building.
3. Make sure both WLAN client adapter and the 4 Ports 11g Wireless ADSL2/2+ Router are allowed to connect through wireless channels as defined for local regulatory domain.

5. LAN (Link/Act) LED does not light up.

Ans. Check the following:

1. Make sure that the LAN cables are securely connected to the 10/100Base-T port.
2. Make sure that you are using the correct cable type for your Ethernet equipment.
3. Make sure the computer's Ethernet port is configured for auto-negotiation.

6. Failed to configure the 4 Ports 11g Wireless ADSL2/2+ Router through web browser (By a client PC in LAN)

Ans. Check the following:

1. Check the hardware connection of the 4 Ports 11g Wireless ADSL2/2+ Router's LAN port. The LED will lit when a proper connection is made.
2. Check your Windows TCP/IP setting (Refer to Chapter 3 for setting details).
3. Open the Windows System Command Prompt:
   - For Windows 9x/ME: Manually enter **winipcfg**, then press **Enter**.
   - For Windows 2000/XP: Manually enter **ipconfig/all**, then press **Enter**.
4. You should have the following information listed on your Window System:
   - **IP Address: 192.168.1.x**
   - **Submask: 255.255.255.0**
   - **Default Gateway IP: 192.168.1.1**

7. I forgot or lost my Administrator Password.

Ans. Reset the 4 Ports 11g Wireless ADSL2/2+ Router to factory default by pressing the **"Reset"** button for 10 seconds.

If you are still getting prompted for a password when saving settings:

1. Access the Router's web interface by going to **http://192.1681.1.**
2. Enter the default **"username"** and **"password"** then click **"Enter"** to log in.
3. Click on **"TOOLS"** then click "**User Management"**.
4. Enter a new **"Password"** and new **"Username"** in the **"Username"** and "**Password"** field, and enter the same password in the second field to confirm the password.
5. Click **"Apply"** after your setting.

8. I need to upgrade the Firmware.

Ans. Check with your local dealer for technical support before upgrading your 4 Ports 11g Wireless ADSL2/2+ Router. Before proceed the upgrading process, check the following details:

1. Download the latest Firmware and save at your pointed location.
2. Read the firmware release note carefully before proceed the upgrading process.
3. Refer to **TOOLS → Update Gateway** section for the upgrading process.

9. Testing LAN path to your 4 Ports 11g Wireless ADSL2/2+ Router.

Ans. To verify whether the LAN path from your PC to your 4 Ports 11g Wireless ADSL2/2+ Router is properly connected, you can **"Ping"** the 4 Ports 11g Wireless ADSL2/2+ Router with the following procedures:

1. From the Windows toolbar, click **"Start"** and select **"Run".**
2. In the open field, type **"Ping 192.168.1.1"** and click **"OK"**
3. If the path is working, you should see the message in the following format:

   Reply from 192.168.1.1 bytes = 32 time < 10ms TTL = 60
4. If the path is not working, you should see the following message:

   Request timed out

If the path is not functioning correctly:

1. Make sure the LAN port LED indicator is on.
2. Check whether you are using the correct LAN cable.
3. Check your Ethernet Adaptor installation and configurations.
4. Verify that the IP address for your 4 Ports 11g Wireless ADSL2/2+ Router and your workstation are correct and that the addresses are on the same subnet.

10. Failed to connect with the 4 Ports 11g Wireless ADSL2/2+ Router via Wireless LAN card.

Ans. Ensure that the WL ACT LED indicator of the 4 Ports 11g Wireless ADSL2/2+ Router is correctly illuminated.

1. Check whether your Wireless LAN setting (e.g. SSID, Channel Number) is the same as your 4 Ports 11g Wireless ADSL2/2+ Router.
2. Check whether you'd used the same WEP Key Encryption for both your Wireless LAN and your 4 Ports 11g Wireless ADSL2/2+ Router.

Appendix D: UPnP Setting on Windows XP

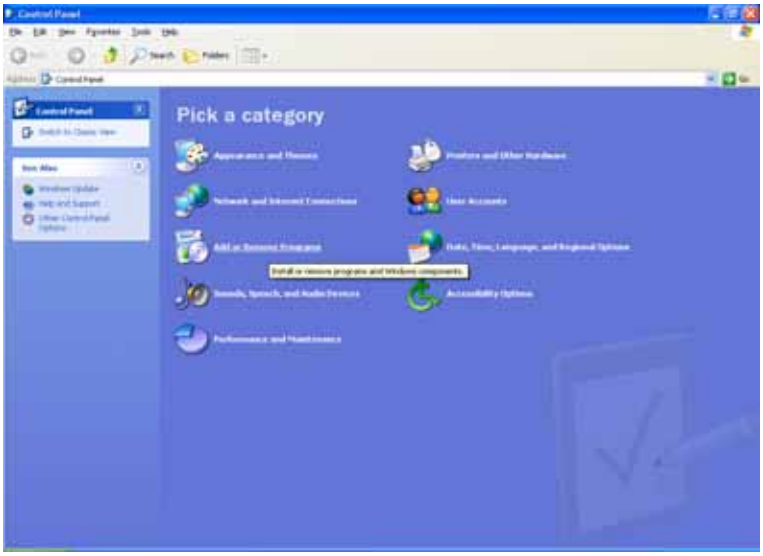
D.1 Adding UPnP:

If you are running Microsoft Windows XP, it is recommended to add the UPnP component to your system.

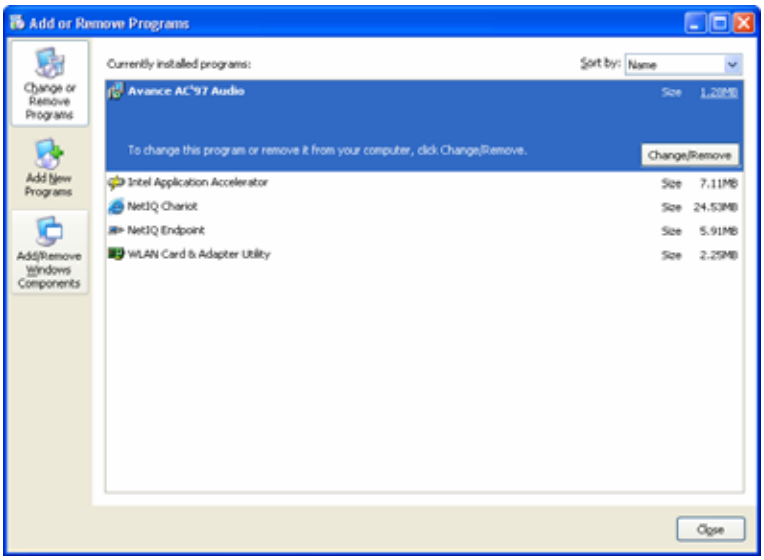
Proceed as follows:

1. Click **"Start"** → **"Settings"** then **"Control Panel"**.

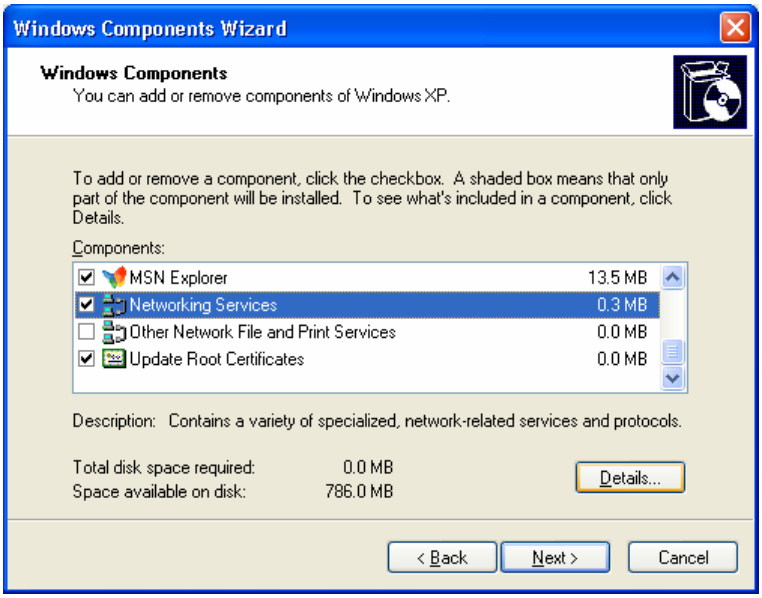
2. The **"Control Panel"** window appears. Click **"Add or Remove Programs"**.



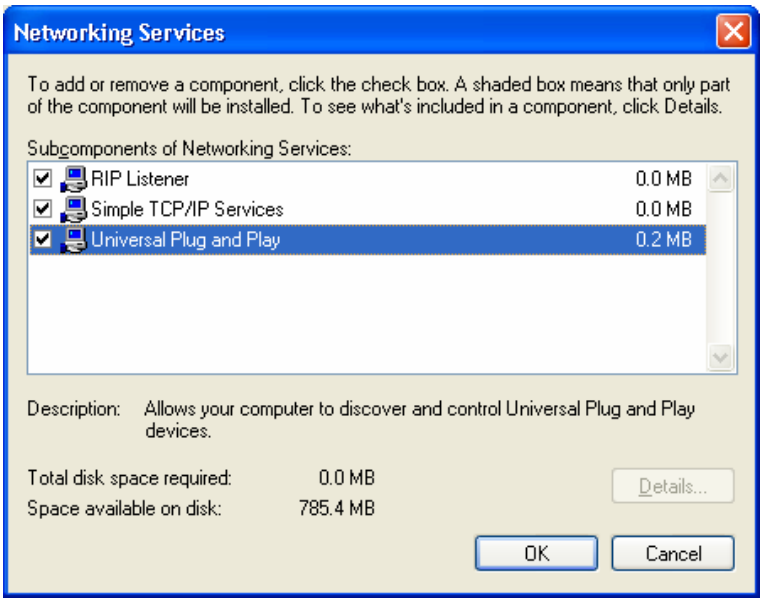
3. The **"Add or Remove Programs"** window appears. Click **"Add/Remove Windows Components"**.



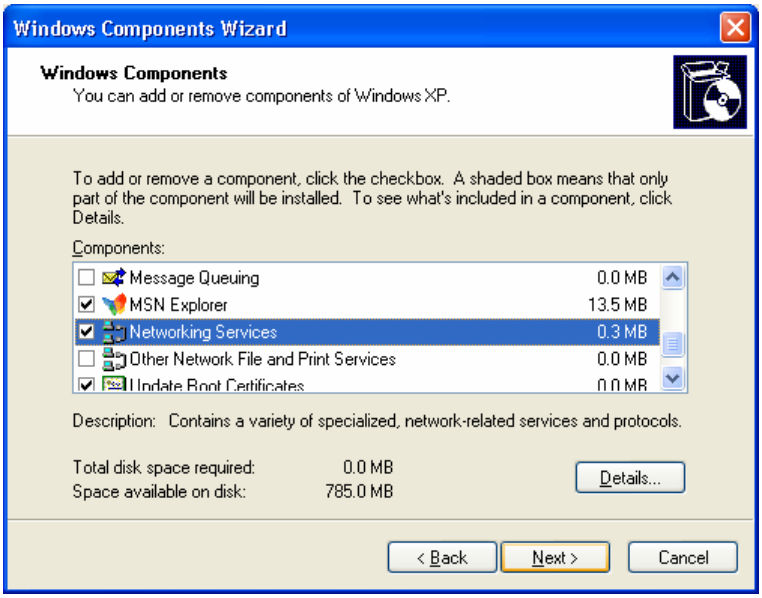
4. The **"Windows Components Wizard"** appears. Select **"Networking Services"** in the Components list and click **"Details"**.



5. The **"Networking Services"** window appears. Select **"Universal Plug and Play"** and click **"OK"**.



6. Click **"Next"** to start the installation and follow the instructions in the Windows Components Wizard.



Note : ***System may ask for original Windows XP CD-ROM. Insert the CD-ROM and direct Windows to the proper location of the CD-ROM.***

Restart your Windows system to activate your setting might be necessary. Click "OK" to restart your Windows system.

7. A **"Completing the Windows Components Wizard"** will appears indicating the installation was successful. Click **"Finish"** to quit.

Appendix E: Glossary

The Glossary provides an explanation of terms and acronyms discussed in this user guide.

10BASE-T: IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx: IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.11b: IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11g: IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHz.

802.11x: 802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management. The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys.

AP: Access Point: A station that transmits and receives data in a WLAN (Wireless Local Area Network). An access point acts as a bridge for wireless devices into a LAN.

ATM: Asynchronous Transfer Mode: A method of transfer in which data is organized into 53-byte cell units. ATM cells are processed asynchronously in relation to other cells.

BC: Broadcast: Communication in which a sender transmits to everyone in the network.

BER: Bit Error Rate: Percentage of Bits that contain errors relative to the total number of bits transmitted.

Bridge: A device that connects two networks and decides which network the data should go to.

Bridge Mode: Bridge Mode is used when there is one PC connected to the LAN-side Ethernet or USB port. IEEE 802.1D method of transport bridging is used to bridge between the WAN (ADSL) side and the LAN (Ethernet or USB) side, i.e., to store and forward.

CBR: Constant Bit Rate: A constant transfer rate that is ideal for streaming (executing while still downloading) data, such as audio or video files.

Cell: A unit of transmission in ATM, consisting of a fixed-size frame containing a 5-octet header and a 48-octet payload.

CHAP: Challenge Handshake Authentication Protocol: Typically more secure than PAP, CHAP uses username and password in combination with a randomly generated challenge string which has to be authenticated using a one-way hashing function.

CLP: Cell Loss Priority: ATM cells have two levels of priority, CLP0 and CLP1. CLP0 is of higher priority, and in times of high traffic congestion, CLP1 error cells may be discarded to preserve the Cell Loss Ratio of the CLP0 cells.

CO: Central Office: In a local loop, a Central Office is where home and office phone lines come together and go through switching equipment to connect them to other Central Offices. The distance from the Central Office determines whether or not an ADSL signal can be supported in a given line.

CPE: Customer Premises Equipment. This specifies equipment on the customer, or LAN, side.

CRC: Cyclic Redundancy Checking: A method for checking errors in a data transmission between two computers. CRC applies a polynomial function (16 or 32-bit) to a block of data. The result of that polynomial is appended to the data transmission. Upon receipt, the destination computer applies the same polynomial to the block of data. If the host and destination computer share the same result, the transmission was successful. Otherwise, the sender is notified to re-send the data block.

DHCP: Dynamic Host Configuration Protocol: A communications protocol that allows network administrators to manage and assign IP addresses to computers within the network. DHCP provides a unique address to a computer in the network which enables it to connect to the Internet through Internet Protocol (IP). DHCP can lease and IP address or provide a permanent static address to those computers who need it (servers, etc.).

DMZ: Demilitarized Zone: A computer Host or network that acts as a neutral zone between a private network and a public network. A DMZ prevents users outside of the private network from getting direct access to a server or any computer within the private network. The outside user sends requests to the DMZ, and the DMZ initiates sessions in the public network based on these requests. A DMZ cannot initiate a session in the private network, it can only forward packets to the private network as they are requested.

DNS: Domain Name System: A method to locate and translate Domain Names into Internet Protocol (IP) addresses, where a Domain Name is a simple and meaningful name for an Internet address.

DSL: Digital Subscriber Line: A technology that provides broadband connections over standard phone lines.

DSLAM: Digital Subscriber Line Access Multiplexer: Using multiplexing techniques, a DSLAM receives signals from customer DSL lines and places the signals on a high-speed backbone line. DSLAMs are typically located at a telephone company's CO (Central Office).

Encapsulation: The inclusion of one data structure within another. For example, packets can be encapsulated in an ATM frame during transfer.

FEC: Forward Error Correction: An error correction technique in which a data packet is processed through an algorithm that adds extra error correcting bits to the packet. If the transmitted message is received in error, these bits are used to correct the errored bits without retransmission.

Firewall: A firewall is a method of implementing common as well as user defined security policies in an effort to keep intruders out. Firewalls work by analyzing and filtering out IP packets that violate a set of rules defined by the firewall administrator. The firewall is located at the point of entry for the network. All data inbound and outbound must pass through the firewall for inspection.

Fragmentation: Breaking a packet up into smaller packets that is caused either by the transmission medium being unable to support the original size of the packet or the receiving computer not being able to receive a packet of that size. Fragmentation occurs when the sender's MTU is larger than the receiver's MRU.

FTP: File Transfer Protocol. A standardized internet protocol which is the simplest way to transfer files from one computer to another over the internet. FTP uses the Internet's TCP/IP protocols to function.

Full Duplex: Data transmission can be transmitted and received on the same signal medium and at the same time. Full Duplex lines are bidirectional.

G.dmt: Formally G.992.1, G.dmt is a form of ADSL that uses Discrete MultiTone (DMT) technology. G.dmt incorporates a splitter in its design.

G.lite: Formally G.992.2, G.lite is a standard way to install ADSL service. G.lite enables connections speeds up to 1.5 Mbps downstream and 128 kbps upstream. G.lite does not need a splitter at the user end because splitting is preformed at the remote end (telephone company).

Gateway: A point on the network which is an entrance to another network. For example, a router is a gateway that connects a LAN to a WAN.

Half Duplex: Data transmission can be transmitted and received on the same signal medium, but not simultaneously. Half Duplex lines are bidirectional.

HEC: Headed Error Control: ATM error checking by using a CRC algorithm on the fifth octet in the ATM cell header to generate a check character. Using HEC, either a single bit error in the header can be corrected or multiple bit errors in the header can be detected.

HNP: Home Network Processor

Host: In context of Internet Protocol, a host computer is one that has full two way access to other computers on the Internet.

IAD: Integrated Access Device: A device that multiplexes and demultiplexes communications in the CPE

onto and out of a single telephone line for transmission to the CO.

IP: Internet Protocol: The method by which information is sent from one computer to another through the Internet. Each of these host computers have a unique IP address which distinguishes it from all the other computers on the internet. Each packet of data sent includes the sender's IP address and the receiver's IP address.

LAN: Local Area Network: A group of computers, typically covering a small geographic area, that share devices such as printers, hard disk drives, scanners, and optical drives. Computers in a LAN typically share an internet connection through some sort of router that connects the computers to a WAN.

LLC: Logical Link Control: Provides an interface point to the MAC sublayer. LLC Encapsulation is needed when several protocols are carried over the same Virtual Circuit.

MAC Address: Media Access Control Address: A unique hardware number on a computer or device that identifies it and relates it to the IP address of that device.

MC: Multicast: Communication involving a single sender and multiple specific receivers in a network.

MRU: Maximum Receive Unit: MRU: Maximum Receive Unit (MRU) is the largest size packet that can be received by the modem. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU). In the normal negotiation, the peer will accept this MRU and will not send packet with information field larger than this value.

MSS: Maximum Segment Size: The largest size of data that TCP will send in a single, unfragmented IP packet. When a connection is established between a LAN client and a host in the WAN side, the LAN client and the WAN host will indicate their Maximum Segment Size during the TCP connection handshake.

MTU: Maximum Transmission Unit: The largest size packet that can be sent by the modem. If the network stack of any packet is larger than the MTU value, then the packet will be fragmented before the transmission. During the PPP negotiation, the peer of the PPP connection will indicate its MRU and will accept any value up to that size. The actual MTU of the PPP connection will be set to the smaller of the two (MTU and the peer's MRU).

NAPT: Network Address and Port Translation: An extension of NAT, NAPT maps many private internal addresses into one IP address. The outside network (WAN) can see this one IP address but it cannot see the individual device IP addresses translated by the NAPT.

NAT: Network Address Translation: The translation of an IP address of one network to a different IP address known by another network. This gives an outside (WAN) network the ability to distinguish a device on the inside (LAN) network, as the inside network has a private set of IP address assigned by the DHCP server not known to the outside network.

PAP: Password Authentication Protocol: An authentication protocol in which authorization is done through a user name and password.

PDU: Protocol Data Unit: A frame of data transmitted through the data link layer 2.

Ping: Packet Internet Groper: A utility used to determine whether a particular device is online or connected to a network by sending test packets and waiting for a response.

PPP: Point-to-Point Protocol: A method of transporting and encapsulating IP packets between the user PC and the ISP. PPP is full duplex protocol that is transmitted through a serial interface.

Proxy: A device that closes a straight connection from an outside network (WAN) to an inside network (LAN). All transmissions must go through the proxy to get into or out of the LAN. This makes the internal addresses of the devices in the LAN private.

PVC: Permanent Virtual Circuit: A software defined logical connection in a network; A Virtual Circuit that is permanently available to the user.

RIP: Routing Information Protocol: A management protocol that ensures that all hosts in a particular network share the same information about routing paths. In a RIP, a host computer will send its entire routing table to another host computer every X seconds, where X is the supply interval. The receiving host computer will in turn repeat the same process by sending the same information to another host computer. The process is repeated until all host computers in a given network share the same routing knowledge.

RIPv1: RIP Version 1: One of the first dynamic routing protocols introduced used in the internet, RIPv1 was developed to distribute network reach ability information for what is now considered simple topologies.

RIPv2: RIP Version 2: Shares the same basic concepts and algorithms as RIPv1 with added features such as subnet masks, authentication, external route tags, next hop addresses, and multicasting in addition to broadcasting.

Router Mode: Router Mode is used when there is more than one PC connected to the LAN-side Ethernet and/or USB port. This enables the ADSL WAN access to be shared with multiple nodes on the LAN. Network Address Translation (NAT) is supported so that one WAN-side IP address can be shared among multiple LAN-side devices. DHCP is used to serve each LAN-side device and IP address.

SNAP: SubNetwork Attachment Point.

SNMP: Simple Network Management Protocol: Used to govern network management and monitor devices on the network. SNMP is formally described in RFC 1157.

SNR: Signal-to-Noise Ratio: Measured in decibels, SNR is a calculated ratio of signal strength to background noise. The higher this ratio, the better the signal quality.

Subnet Mask: Short for SubNetwork Mask, subnet mask is a technique used by the IP protocol to filter messages into a particular network segment, called a subnet. The subnet mask consists of a binary pattern that is stored in the client computer, server, or router. This pattern is compared with the incoming IP address to determine whether to accept or reject the packet.

TCP: Transfer Control Protocol: Works together with Internet Protocol for sending data between computers over the Internet. TCP keeps track of the packets, making sure that they are routed efficiently.

TFTP: Trivial File Transfer Protocol: A simple version of FTP protocol that has no password authentication or directory structure capability.

Trellis Code: An advanced method of FEC (Forward Error Correction). When enabled, it makes for better error checking at the cost of slower packet transmission. Setting Trellis Code to Disabled will cause increased packet transmission with decreased error correction.

TTL: Time To Live: A value in an IP packet that indicates whether or not the packet has been propagating through the network too long and should be discarded.

UBR: Unspecified Bit Rate: A transfer mode that is usually used in file transfers, email, etc. UBR can vary depending on the data type.

USB: Universal Serial Bus: A standard interface between a computer and a peripheral (printer, external drives, digital cameras, scanners, network interface devices, modems, etc.) that allows a transfer rate of 12Mbps.

UDP: User Datagram Protocol: A protocol that is used instead of TCP when reliable delivery is not required. Unlike TCP, UDP does not require an acknowledgement (handshake) from the receiving end. UDP sends packets in one-way transmissions.

VBR-nrt: Variable Bit Rate – non real time: With VBR-nrt, cell transfer is variable upon certain criteria.

VC: Virtual Circuit: A virtual circuit is a circuit in a network that appears to be a physically discrete path, but is actually a managed collection of circuit resources that allocates specific circuits as needed to satisfy traffic requirements.

VCI: Virtual Channel Identifier: A virtual channel identified by a unique numerical tag that is defined by a 16-bit field in the ATM cell header. The purpose of the virtual channel is to identify where the cell should travel.

VC-Mux: Virtual Circuit based Multiplexing: In VC Based Multiplexing, the interconnect protocol of the carried network is identified implicitly by the VC (Virtual Circuit) connecting the two ATM stations (each protocol must be carried over a separate VC).

VPI: Virtual Path Identifier: Virtual path for cell routing indicated by an eight bit field in the ATM cell header.

WAN: Wide Area Network: A WAN covers a large geographical area. A WAN is consisted of LANs and the Internet is consisted of WANs.

WPA: Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that increase the level of data protection and access control for existing and future wireless LAN systems.