©2005 ASUSTeK COMPUTER INC. All rights reserved.

Leading Provider
of 3C Total Solutions

ASUS 4-Port Wireless Ethernet Router

User Manual

Version 1.0

Version Date: October 12, 2005
Document #: BD-AU0014-10

Table of Contents

GENERAL INFORMATION 3
Package Contents 3
Safety Instructions–Please read. 3
Front Panel View 4
Back Panel View 5
INSTALLING THE ROUTER 6
Connect the ADSL Line and Telephone 6
Connect the PC to the Router 6
Connect the Power Adapter 6
INSTALLATION DIAGRAM 7
MOUNTING THE ROUTER 8
CONFIGURING YOUR COMPUTER 9
Windows 2000 9
Windows XP 10
LOGGING INTO THE ROUTER 11
DEVICE INFO 12
Summary 12
WAN 13
STATISTICS 13
LAN Statistics 13
WAN Statistics 14
ATM Statistics 14
ADSL Statistics 15
ADSL BER Test 16
Route 17
ARP 17
QUICK SETUP 18
ATM PVC Configuration 18
ADVANCED SETUP 22
WAN 22
Connection Type 23
NAT 26
Virtual Servers 26
Port Triggering 28
DMZ Host 29
ALG 29
Firewall 30
IP Filtering–Outgoing 30
IP Filtering–Incoming 31
MAC Filtering 31
Parental Control 33
Quality of Service 34

Routing *35*
Default Gateway 35
Static Route 35
RIP 36
DNS *36*
DNS Server 36
Dynamic DNS 37
ADSL *38*
DSL Advanced Settings 39
Tone Settings 40
Port Mapping *40*
WIRELESS 42
Basic *42*
Security *42*
MAC Filter *44*
Wireless Bridge *45*
Advanced *46*
Station Info *48*
TROUBLESHOOTING–DIAGNOSTICS 49
MANAGEMENT 50
Settings *50*
Backup Settings 50
Restore User Settings 51
Restore Default 51
System Log *52*
Configure System Log 53
SNMP *54*
Internet Times *55*
Access Control *56*
Services 56
IP Addresses 56
Passwords 57
Update Software *58*
Reboot Router *58*

General Information

The 4-Port Wireless Ethernet Router features 4 LAN ports and wireless ability.

Package Contents

The package includes one of each of the following items–

- 4-Port wireless Ethernet router
- 15 VAC AC power adapter
- RJ-11 telephone cable
- RJ-45 Ethernet cable
- Splitter
- User Manual / Quick Guide

Safety Instructions–Please read.

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

- To prevent overheating, do not obstruct the ventilation openings of this equipment.

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

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

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

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

Front Panel View

LED	Mode	Indication
AP	Solid	Wireless is enabled.
	No light	Wireless is disabled.
	Blinking	There is wireless traffic.
XDSL Link	Solid	ADSL is connected.
	No light	ADSL is not connected. The ALARM led will be red.
	Blinking	The router is connected to ADSL.
XDSL ACT	Solid	ADSL is connected, and there is no ADSL traffic.
	No light	ADSL is not connected.
	Quick blinking	There is ADSL traffic.
LAN1-LAN4	Solid	Router is connected to the LAN.
	No light	No connection to the LAN. Check if the LAN cable is connected to the router.
	Blinking	LAN traffic
! (Alarm)	Solid (red)	ADSL is not connected.
	No light	ADSL is connected.
POWER	Solid	Router is powered on.
	No light	Router is not powered. Check if the router is plugged in and if the power switch is turned on.

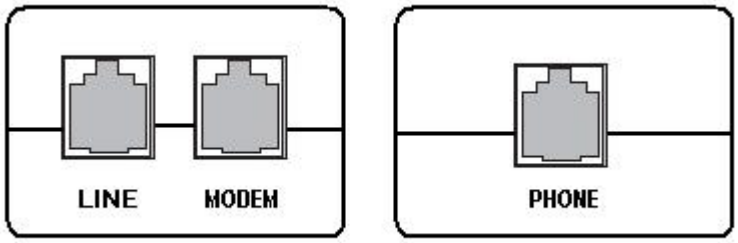
Back Panel View

Port	Description
On / Off	Press to turn the router on and off.
Power	Connects to a 15 VAC AC power adapter.
Reset	*Restart*–press the button for less than 4 seconds. *Default settings*–press the button for 4 seconds or longer.
LAN1-LAN4	RJ-45 connects the unit to an Ethernet device such as a PC or a switch.
Console	*NOTE:* To be used by maintenance professionals only. If the router needs repair, bring it to a service professional.
Line	RJ-11 cable connects to the splitter provided.

Installing the Router

Connect the ADSL Line and Telephone

An RJ-11 cable will be connected to the wall phone jack and the line-end of the splitter. Connect another RJ-11 phone wire from the modem-end of the splitter to the port labeled “line” on the router. A third RJ-11 phone wire will be needed to connect the telephone to the phone-end of the splitter.



NOTE: See connections on the installation diagram.

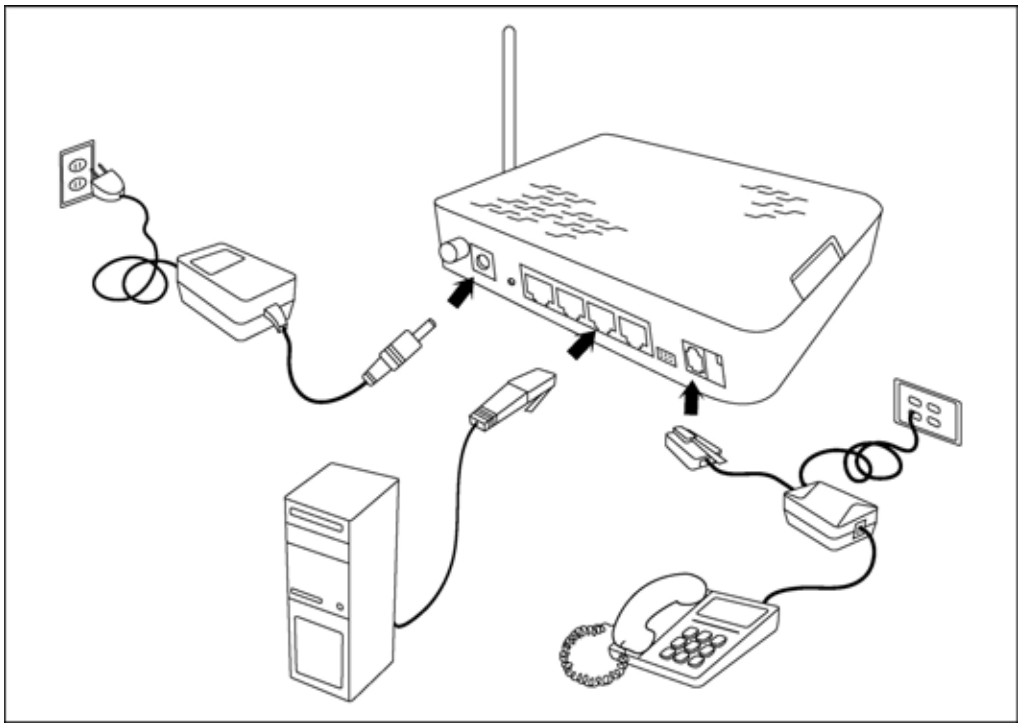
Connect the PC to the Router

Use the Ethernet cable to connect your computer directly to the router. Connect one end of the Ethernet cable to one of the ports labeled LAN on the rear panel of the router and connect the other end to the Ethernet port of your computer. Attach any additional PCs to the router using RJ-45 cables to the port labeled LAN on the rear panel of the router.

Connect the Power Adapter

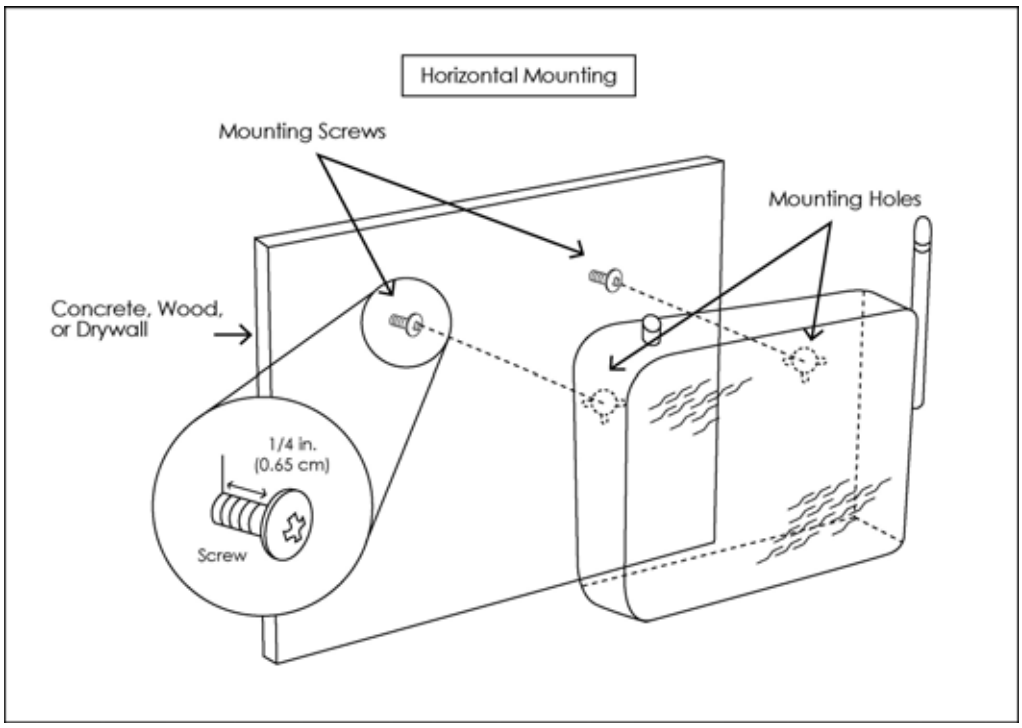
Complete the process by connecting the AC power adapter to the POWER connector on the back of the device and plug the adapter into a wall outlet or power strip. Then turn on and boot up your PC and any LAN devices, such as hubs or switches, and any computers connected to them.

Installation Diagram



Mounting the Router

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



Configuring Your Computer

Prior to accessing the router through the LAN port, note the following necessary configurations–

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

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

Windows 2000

1. In the Windows taskbar, click on the Start button and point to Settings, Control Panel, and Network and Dial-up Connections (in that order).
2. Click on Local Area Connection. When you have the Local Area Connection Status window open, click on **Properties**.
3. Listed in the window are the installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, and you can skip to Step 10.
4. If Internet Protocol (TCP/IP) does not appear as an installed component, then click on **Install**.
5. In the Select Network Component Type window, click on protocol and then the **Add** button.
6. Select Internet Protocol (TCP/IP) from the list and then click on **OK**.
7. If prompted to restart your computer with the new settings, click **OK**.

8. After your computer restarts, click on the Network and Dial-up Connections icon again, and right click on the Local Area Connection icon and then select Properties.

9. In the Local Area Connection Properties dialog box, select Internet Protocol (TCP/IP) and then click on **Properties**.

10. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled **Use the following IP address** and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.

11. Click on **OK** twice to save your changes and then close the **Control Panel**.

Windows XP

1. In the Windows taskbar, click on the Start button and point to Settings and then click Network Connections.

2. In the Network Connections window, right click on the Local Area Connection icon and click on properties.

3. Listed in the Local Area Connection window are the installed network components. Make sure the box for Internet Protocol (TCP/IP) is checked and then click on **Properties**.

4. In the Internet Protocol (TCP/IP) Properties dialog box, click in the radio button labeled **Use the following IP address** and type 192.168.1.x (where x is any number between 2 and 254) and 255.255.255.0 in the IP address field and Subnet Mask field.

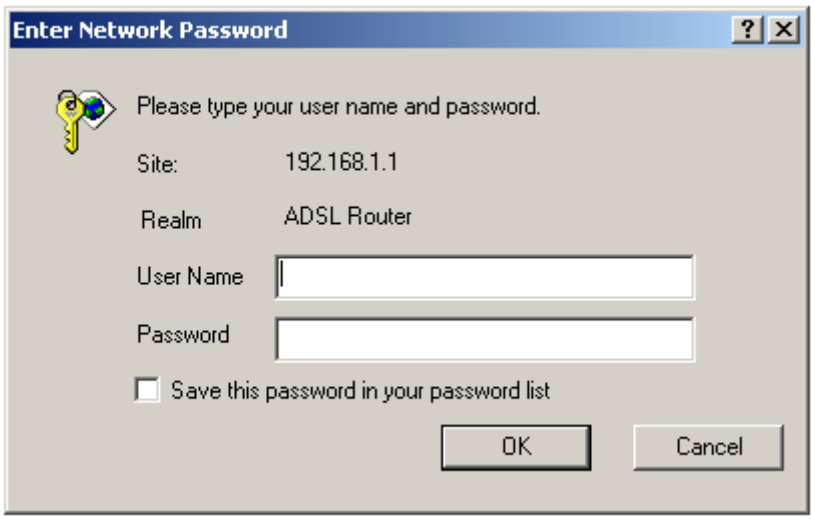
5. Click on **OK** twice to save your changes and then close the **Control Panel**.

Logging into the Router

This section explains how to log in to your router using the following steps–

1. Launch your web browser.
2. Enter the URL http://192.168.1.1 in the address bar and click on **Enter**.

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



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

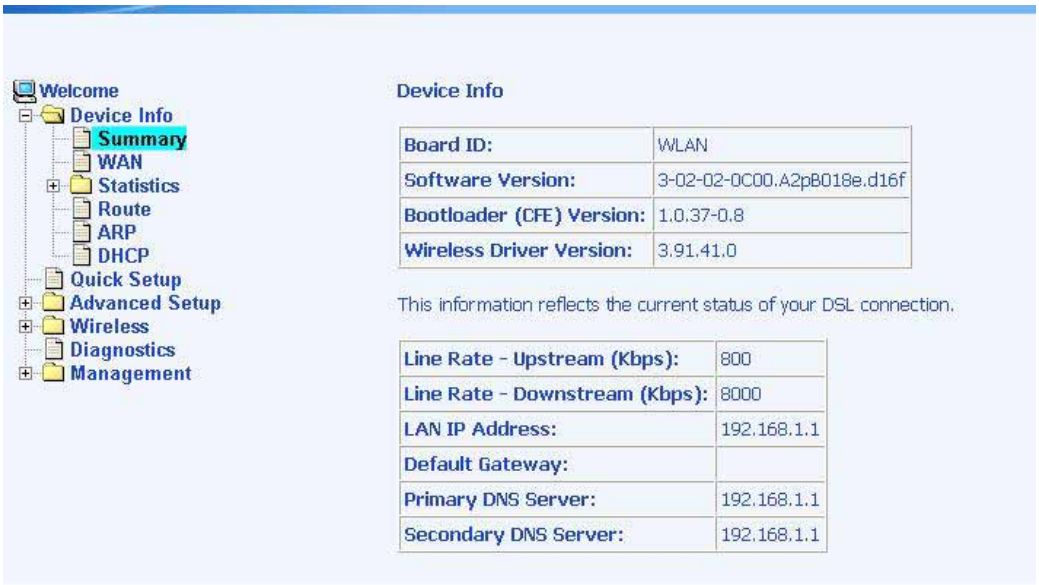
NOTE: There are two default user name and password combinations. The user / user name and password combination can display device status, but cannot change or save configurations. The admin / admin combination can perform all functions. Passwords can be changed at any time.

Device Info

This section describes the system information that can be accessed using the menu items under Device Info.

Summary

Access the general status report from the router by clicking on "**Summary**" under "**Device Info**". It shows information about the router such as the version of the software, bootloader, etc. It also displays the current status of your DSL connection as shown below–



WAN

Access the WAN status report from the router by clicking on "**WAN**" under "**Device Info**".

STATISTICS

LAN Statistics

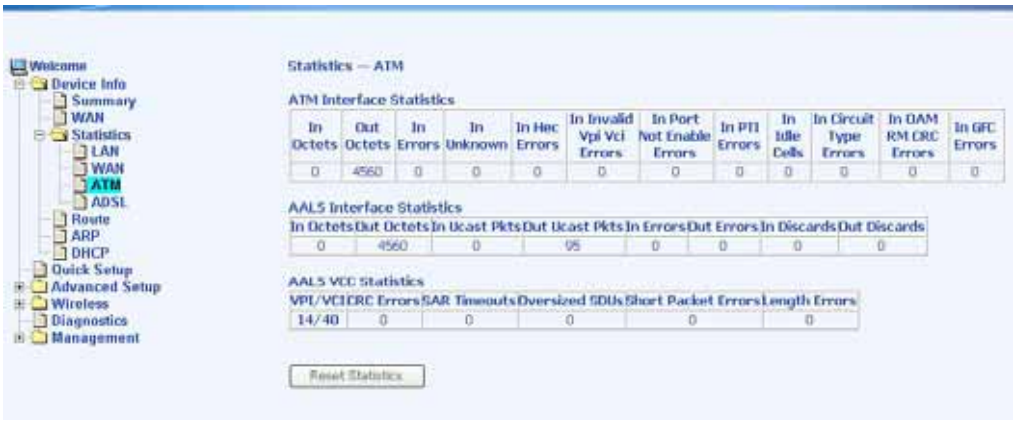
Access the LAN statistics from the router by clicking on the "LAN" item under "Statistics".

WAN Statistics

Access the WAN statistics from the router by clicking on the "**WAN**" item under "**Statistics**". The below screen shows a PPPoA WAN connection example.

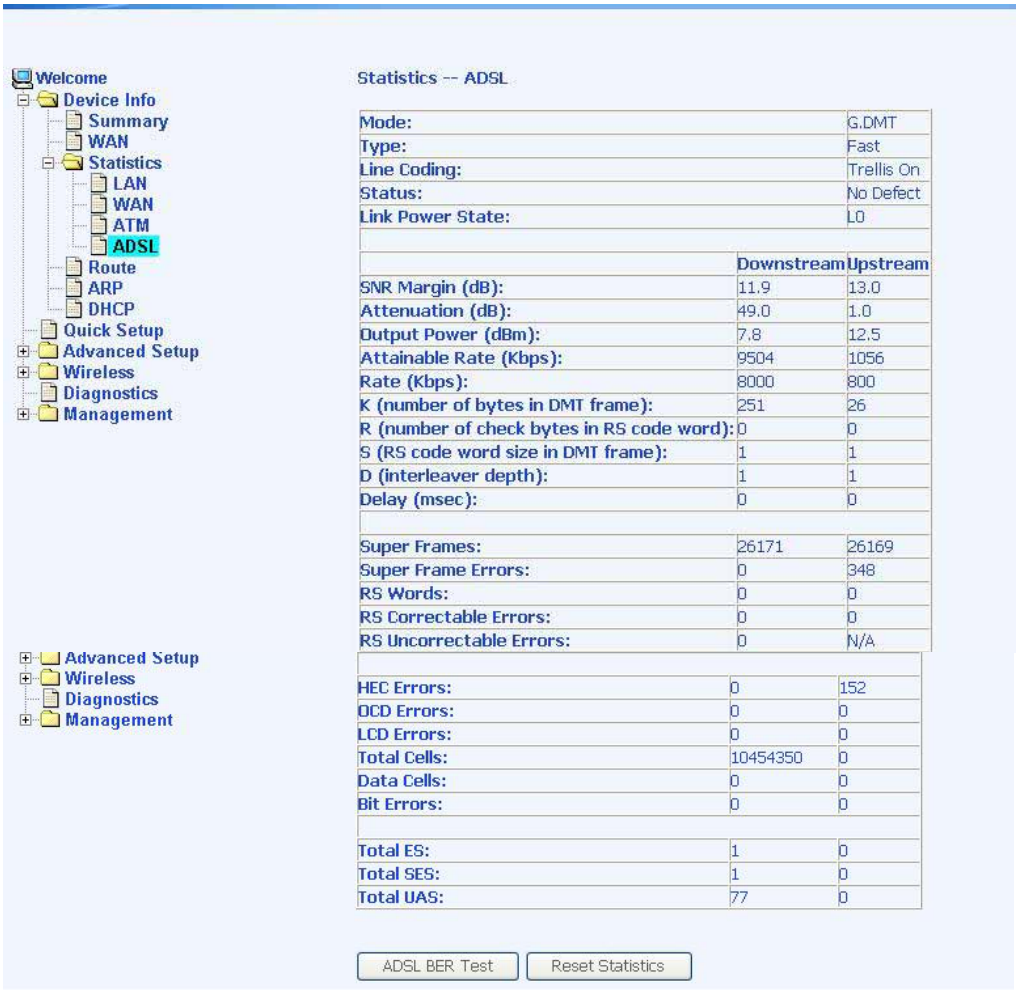
ATM Statistics

Access ATM statistics from the router by clicking on the "**ATM**" item under "**Statistics**".



ADSL Statistics

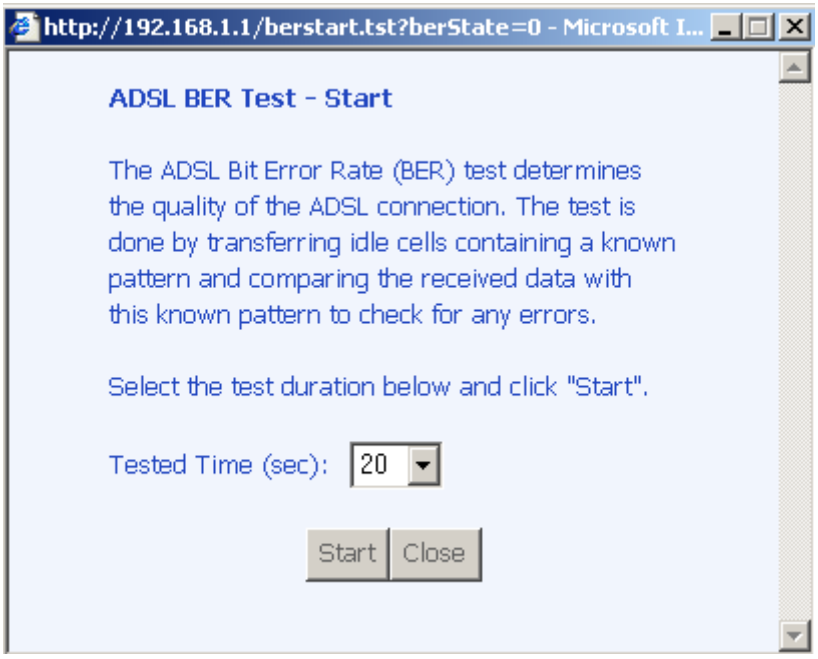
You can view ADSL statistics by clicking on the "**ADSL**" item under "**Statistics**". Information contained in this screen is useful for troubleshooting and diagnostics of connection problems.



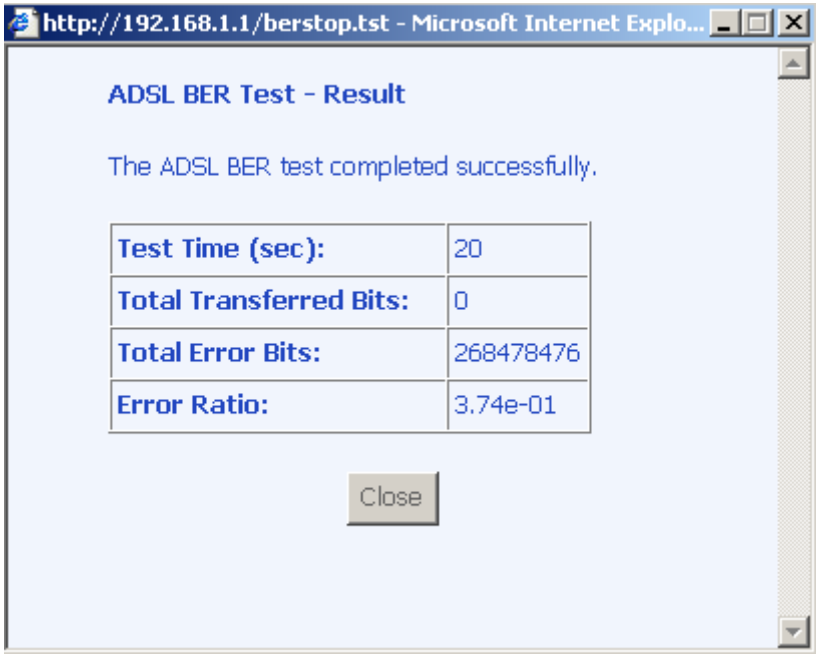
ADSL BER Test

A **Bit Error Rate Test (BER Test)** is a test that reflects the ratio of error bits to the total number transmitted.

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



Below is an ADSL BER Test result screen displaying information about the test including the error bits and ratio.



Route

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

ARP

Access the ARP status report from the router by clicking on the "**ARP**" item under "**Device Info**".

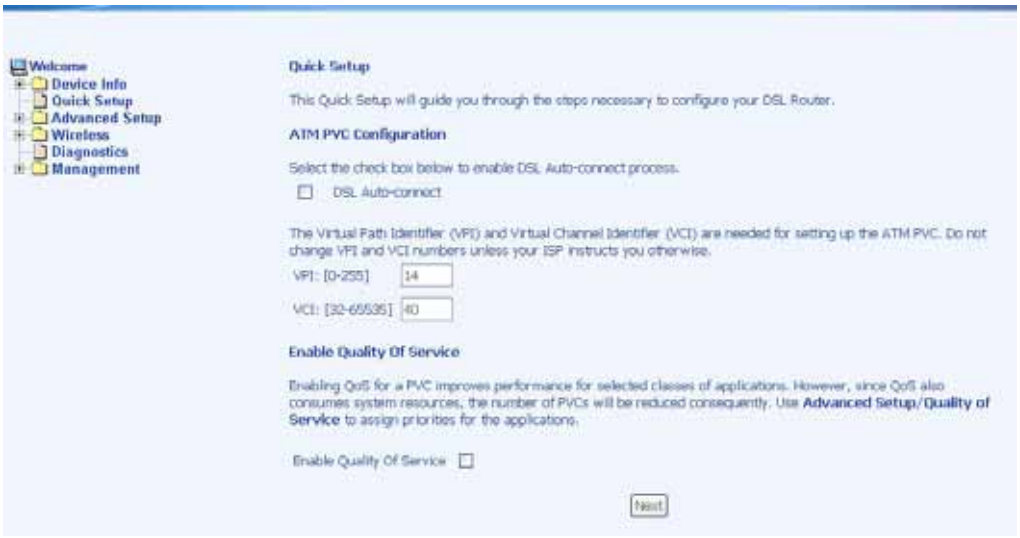
Quick Setup

This section will explain how to quickly configure the router for the main purpose of connecting to the Internet. If you need to configure any advanced functions, then those can be performed in the advanced section.

ATM PVC Configuration

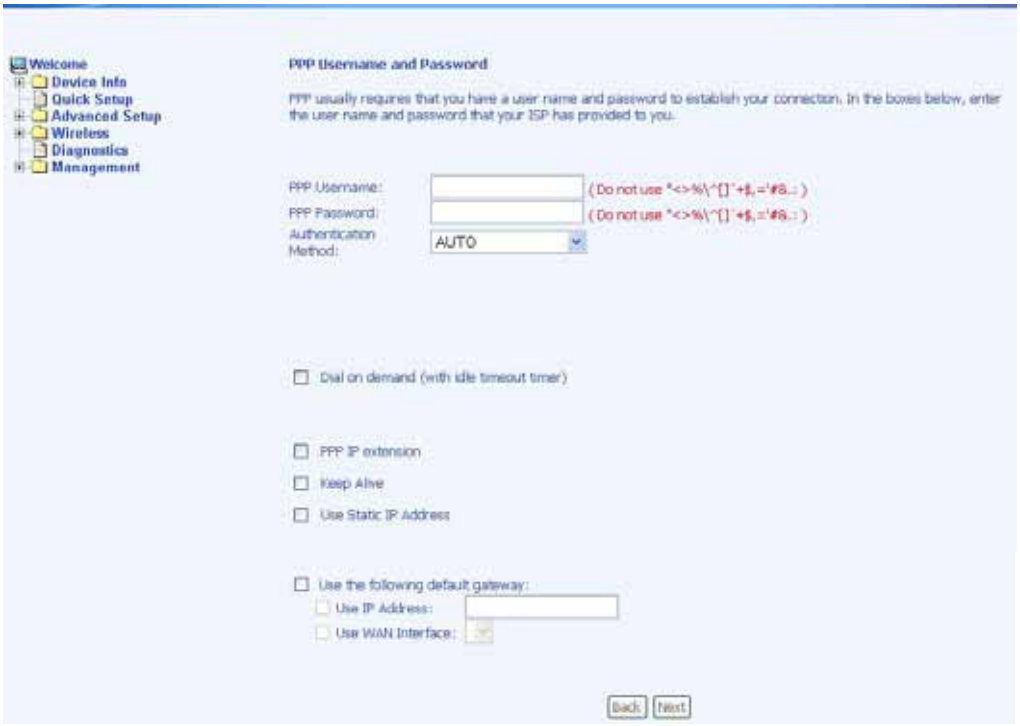
To enable the auto-connect process, click on the box labeled DSL Auto-connect, a process that will automatically detect the first usable PVC and automatically detect PPPoE, PPPoA, and Bridge Protocol (with DHCP Server available). To continue, click on the **Next** button.

If you do not use DSL Auto-connect, then you may need to change the VPI and VCI numbers. Quality of service can also be enabled on this screen.



Furthermore, if you do not use DSL Auto-connect, then you will need to select the connection type and encapsulation mode from a list as shown below.

The next screen to appear will depend on the connection type that was selected in the previous screen.



The next screen lets you decide if you want to enable NAT, firewall, IGMP multicast, and WAN service.

The following is the Device Setup screen where you enter the IP address / subnet mask as well as enable or disable DHCP server.

The last screen under the Quick Start section allows you to set up the wireless feature of the router.

When you click on Next, the summary screen shows the settings made under WAN setup.

Advanced Setup

This section of the user manual is on the advanced configurations of the router. The topics under Advanced Setup are *WAN, LAN, NAT, firewall, QoS, routing, DNS, ADSL,* and *port mapping.*

WAN

Configure the WAN settings as provided by your ISP.

Click on the **Add** button if you want to add a new rule for the WAN interface. The ATM PVC Configuration screen appears.

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

Verify the following values with your ISP before you change them.

- **VPI:** Virtual Path Identifier. The valid range is 0 to 255.
- **VCI:** Virtual Channel Identifier. The valid range is 32 to 65535.

- **Service Category:** Five classes of traffic are listed–

    - UBR Without PCR
    - UBR With PCR
    - CBR
    - Non Realtime VBR
    - Realtime VBR

Enabling QoS for a PVC improves performance for selected classes of applications. However, since QoS also consumes system resources, the number of PVCs is reduced. If you want to enable QoS service, click on the **Enable Quality Of Service** check box.

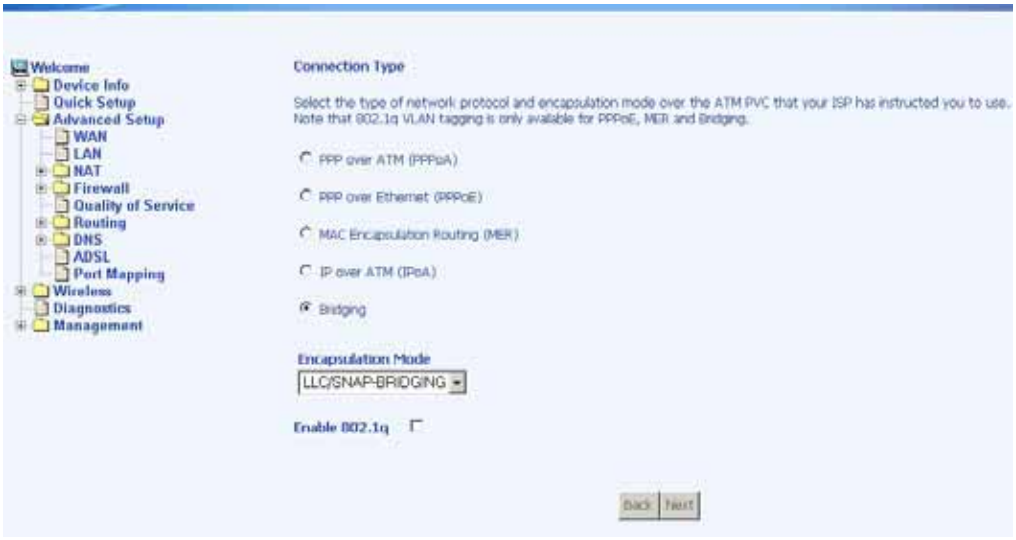
Connection Type

This screen shows the below types of network protocols and encapsulation modes–

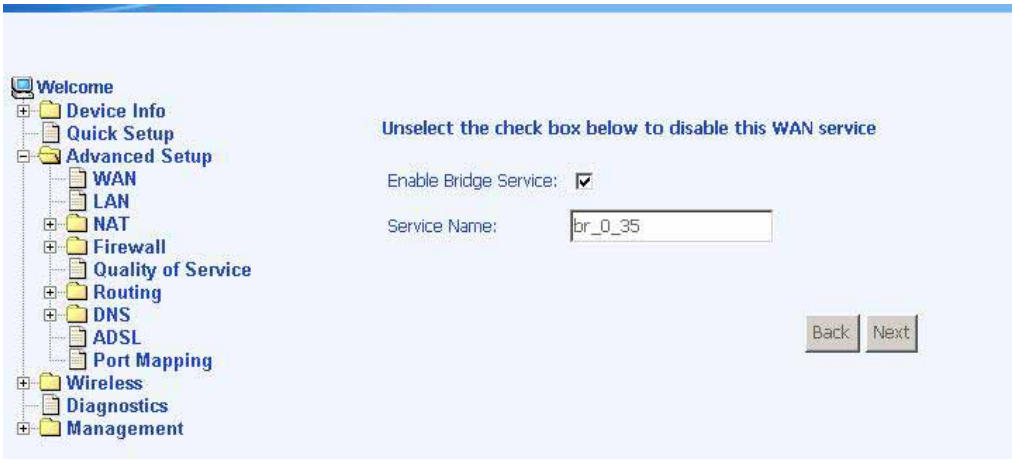
- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)
- MAC Encapsulation Routing (MER)
- IP over ATM (IpoA)
- Bridging

Select the mode that your ISP has instructed you to use and click on **Next**.

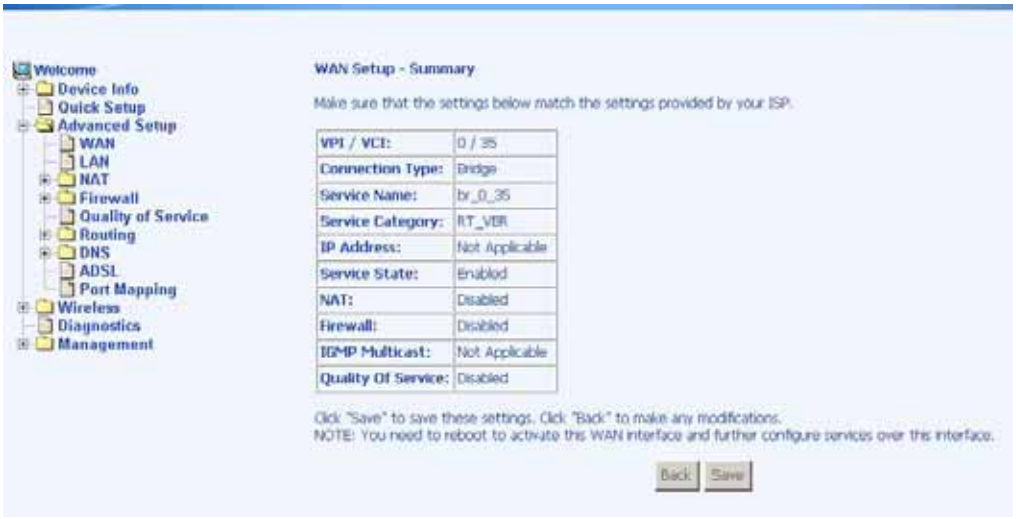
Also available is the option to enable 802.1q, a standard to allow multiple bridged networks to transparently share the same physical network link without leakage of information between networks (i.e. "trunking"). Click on the checkbox if you wish to enable this function.



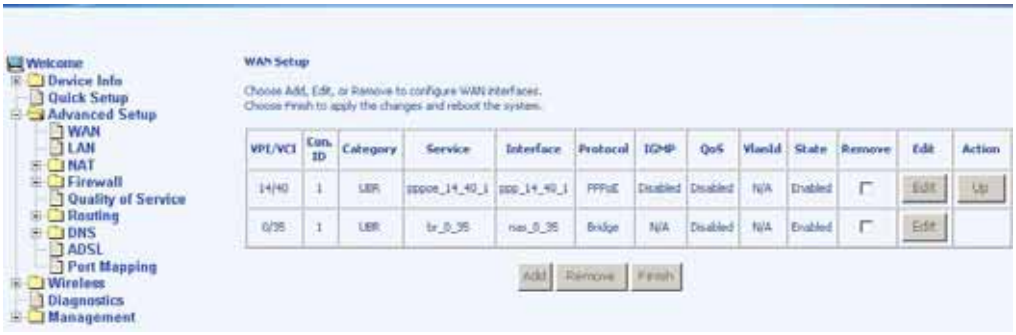
After you click on **Next**, the below screen appears allowing you disable the bridge service if desired.



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



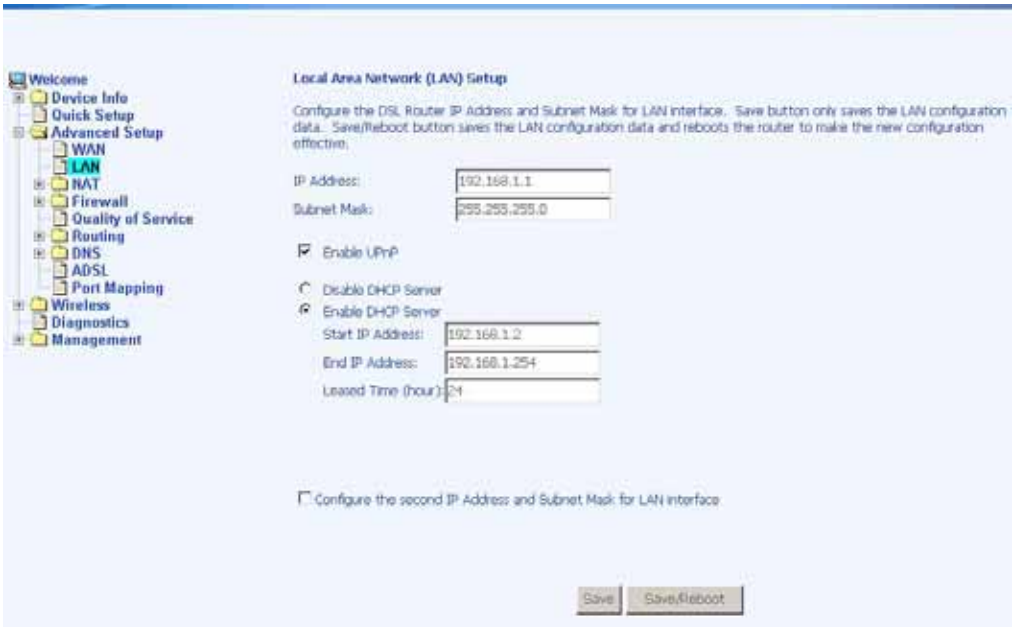
Click on the **Save** button when the settings are correct. The below screen will appear showing the WAN settings that you made. When satisfied with the settings, and no changes are necessary, click on the **Finish** button. To remove any settings, click on the **Remove** button.



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

LAN Local Area Network (LAN) Setup

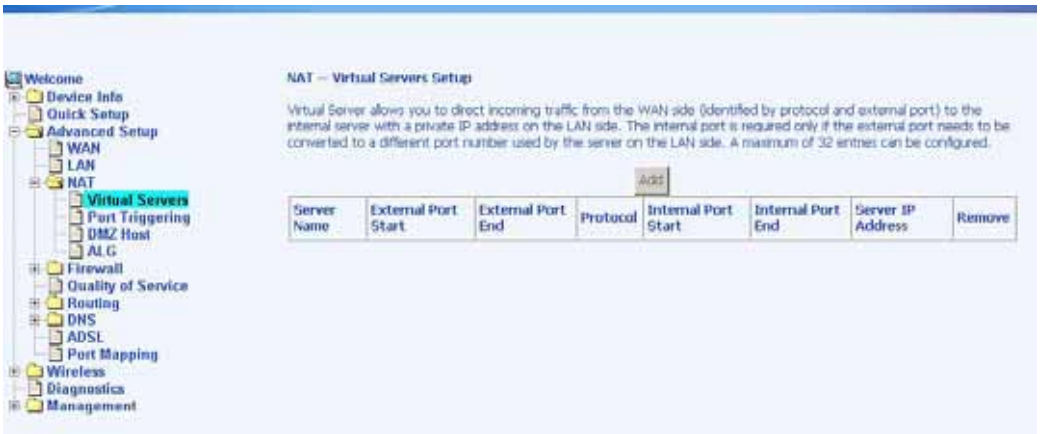
You can configure the DSL Router IP address and Subnet Mask for the LAN interface to correspond your LAN's IP Subnet. The **Save** button only saves the LAN configuration data, but does not apply the configurations. Select the **Save/Reboot** button to save the LAN configuration data and reboot the router and apply the new configurations.



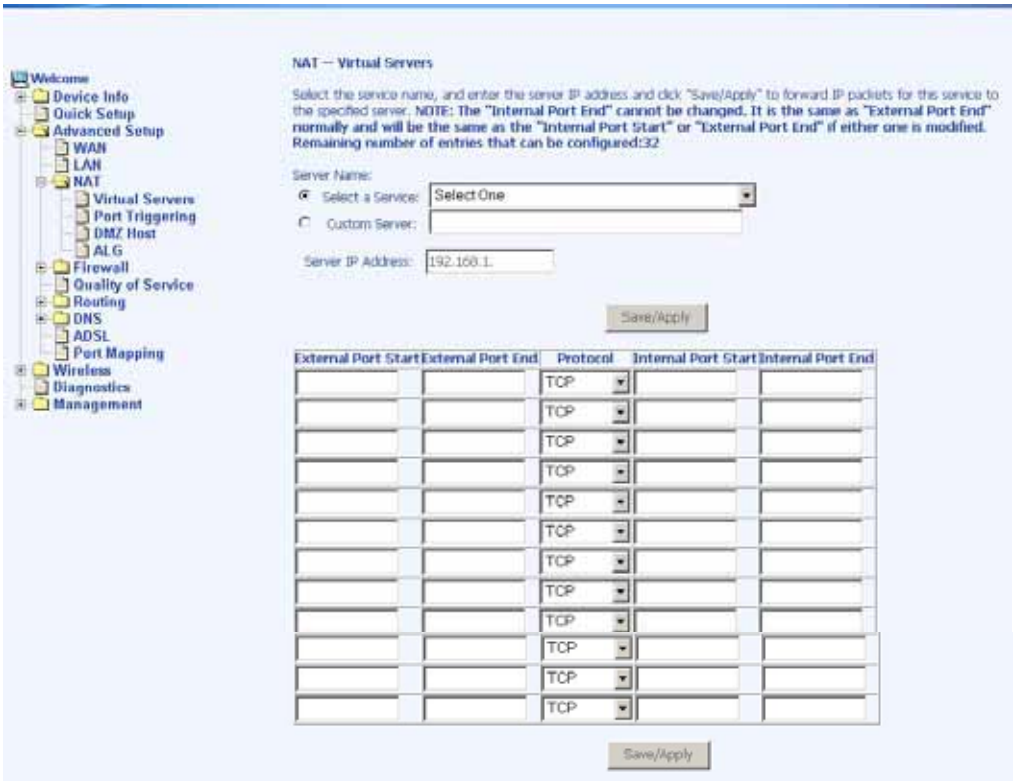
NAT

If you enable NAT (Network Address Translation), you can configure the Virtual Server, Port Triggering, and DMZ Host.

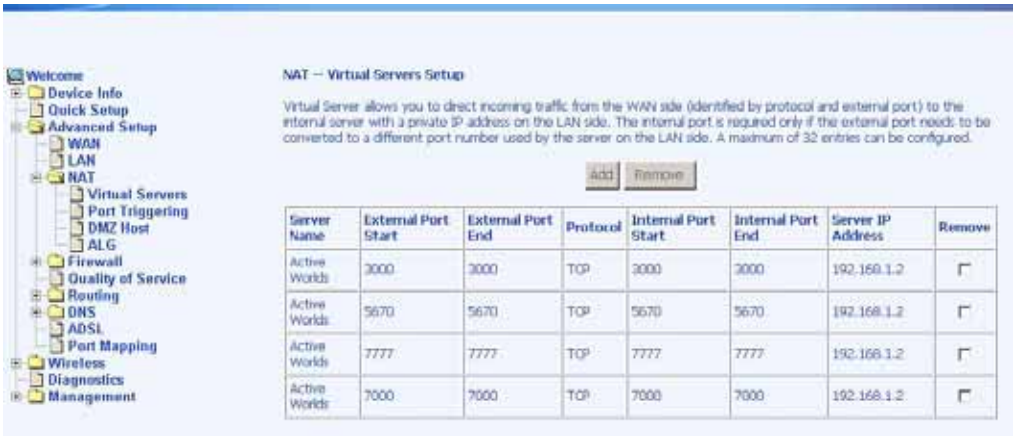
Virtual Servers



A virtual server allows you to direct incoming traffic from the WAN side to a specific IP address on the LAN side. Select the virtual server from the drop-down list and complete the server IP address, then click on the **Save / Apply** button.

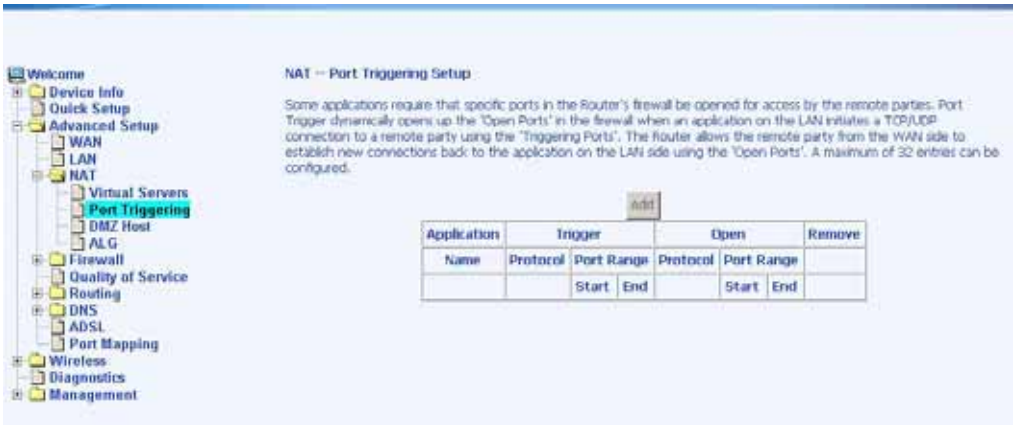


The following screen appears after you save your selection. To add additional virtual servers, click on the **Add** button. If you need to remove any of the server names, select the check box and click on the **Remove** button.

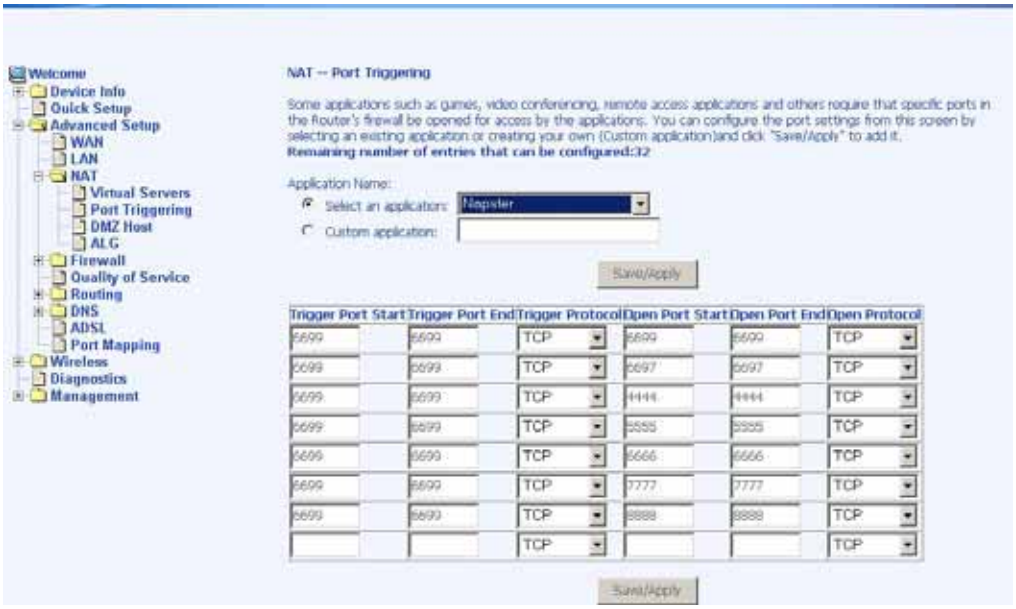


Port Triggering

Click on the **Add** button to add Port Triggering to your Internet application.



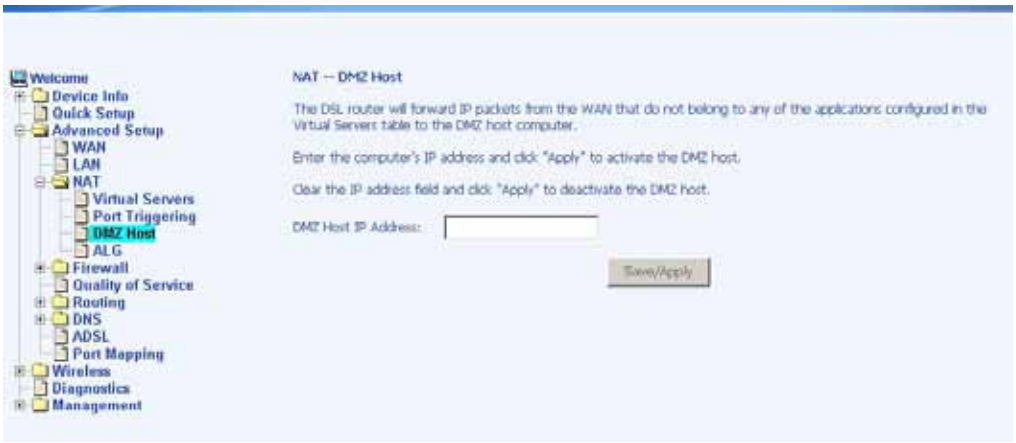
The below screen appears when you click on **Add** allowing you to select the application that you want to set the port settings for. After a selection has been made, click on the **Save / Apply** button.



The below screen appears after you save your selections. You will be able to add or remove selections made, by clicking on the **Add** and **Remove** buttons.

DMZ Host

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



ALG

The application layer is a window between various application processes to allow open information exchange. To use the Application Layer Gateway (ALG), the appropriate Application Layer Gateway definition was selected in the service configuration item.

Firewall

IP Filtering–Outgoing

The outgoing filter will block the LAN traffic from entering the WAN side. Click on the **Add** button to create filters.

The below screen will appear when you click on **Add**. Input the filter name, source information (from the LAN side), and destination information (from the WAN side). Then click on **Save / Apply**.

IP Filtering–Incoming

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

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

MAC Filtering

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

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

If you want to add a setting to the MAC filtering table, enter the Source and Destination MAC address, and select protocol type, frame direction, and WAN interface. Then click on **Save / Apply** to save it.

After you save the settings, a screen showing the settings will appear. On this screen you will be able to view and delete MAC filtering rules.

Parental Control

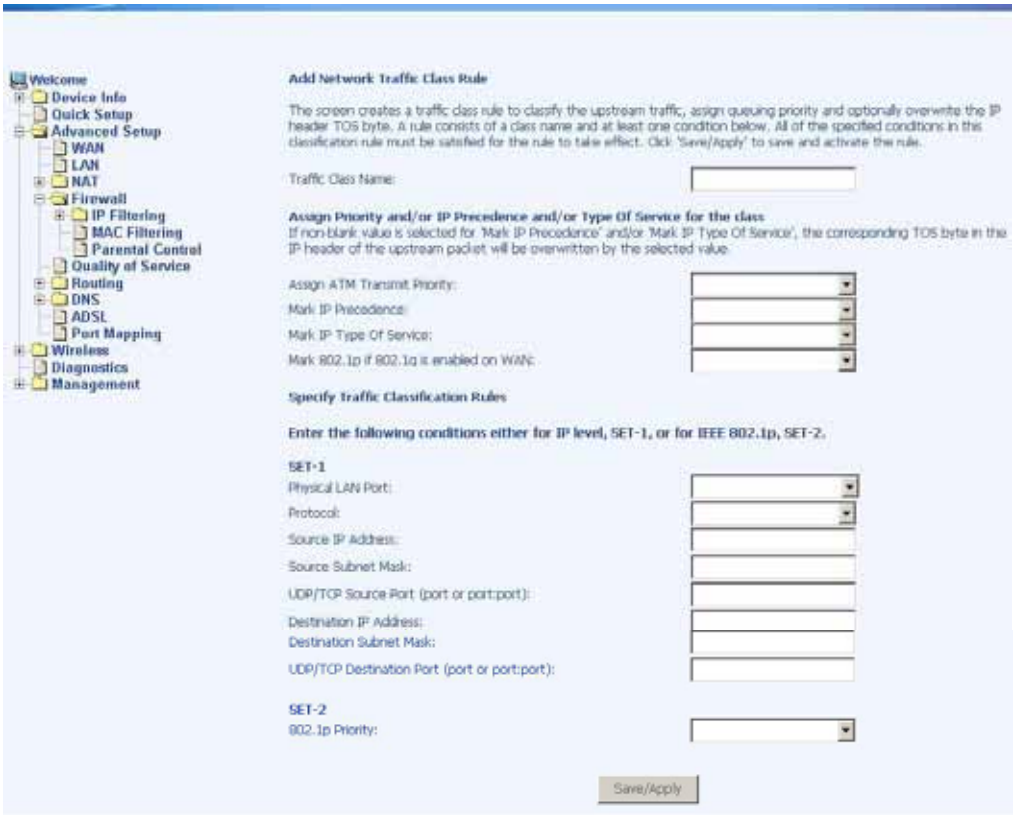
In a home setting, parents can also restrict the day of the week certain computers can access the router. Click on **Add** to set up the restrictions.

After you click on **Add**, you will see the below screen. You will be able to enter the MAC address of the PC that you wish to place on a time of day restriction. Click on **Save / Apply** to save the settings and to continue.

Quality of Service

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

On this screen you can view and delete QoS settings.



Routing

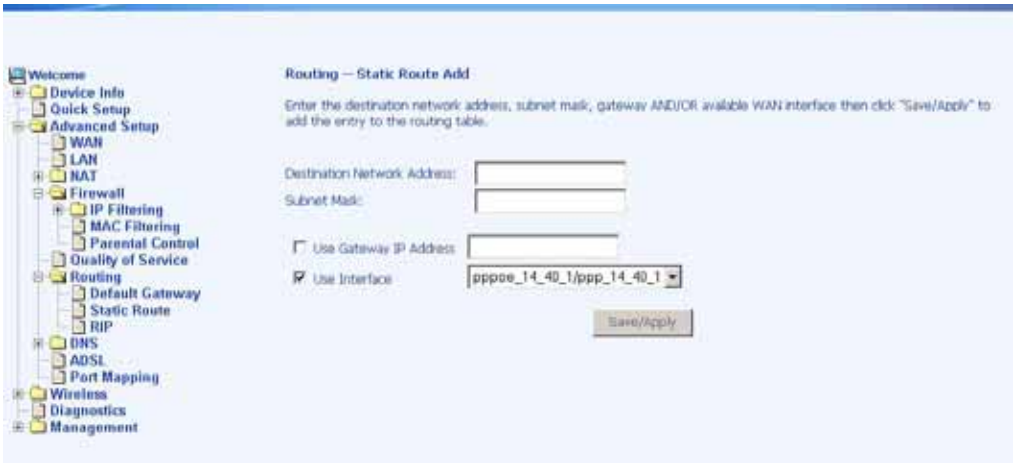
Default Gateway

You can enable automatic assigned default gateway on the Routing – Default Gateway screen. As default, the box is checked for automatic assigned default gateway to be enabled. Click the **Save / Apply** button to enable or disable this feature.

Static Route

Use the Routing – Static Route screen to add a static route to the routing table.

Enter the route information and click on **Save/Apply** to make it active. No reboot is required.



RIP

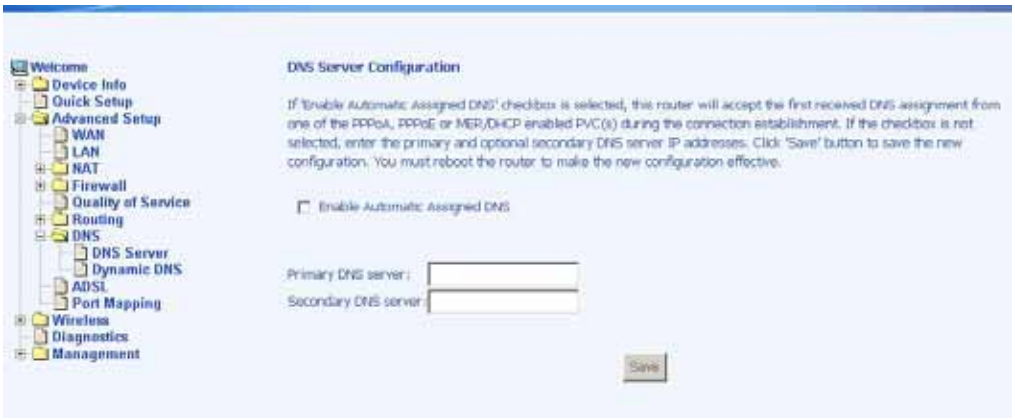
If RIP is enabled, the router operation can be configured as active or passive.

DNS

DNS Server

Use the DNS Server screen to request automatic assignment of a DNS or to specify a primary and secondary DNS.

If the automatic assigned DNS checkbox is not selected, then enter the primary and secondary DNS Server IP addresses as illustrated below.

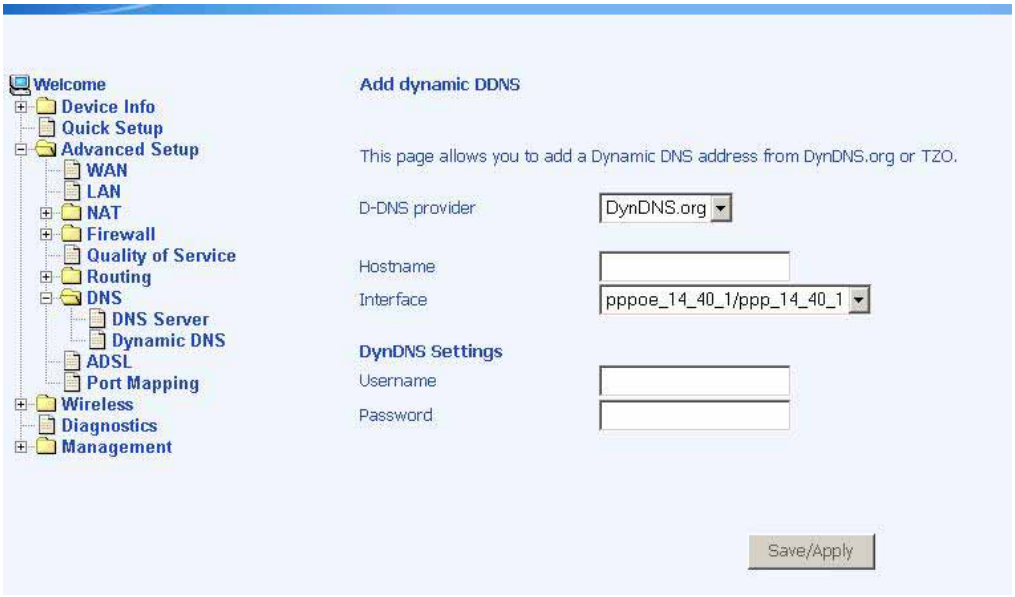


Dynamic DNS

Dynamic DNS (D-DNS) allows you to have your own permanent domain name linked to your dynamic IP address. To configure a dynamic DNS, click on **Add**. If you have already created a dynamic DNS that you want to delete, click on **Remove**.

The below screen allows you to set up the Dynamic DNS provider. Note that you will have to first register at the Dynamic

DNS site that you wish to use. Select from either *DynDNS.org* or *TZO*. Then enter the hostname and the interface that you want to establish the D-DNS address to. Enter the username / password for the D-DNS account that you have signed up for and then click on **Save / Apply**.



ADSL

There are three major items in the ADSL settings:

Modulation Methods

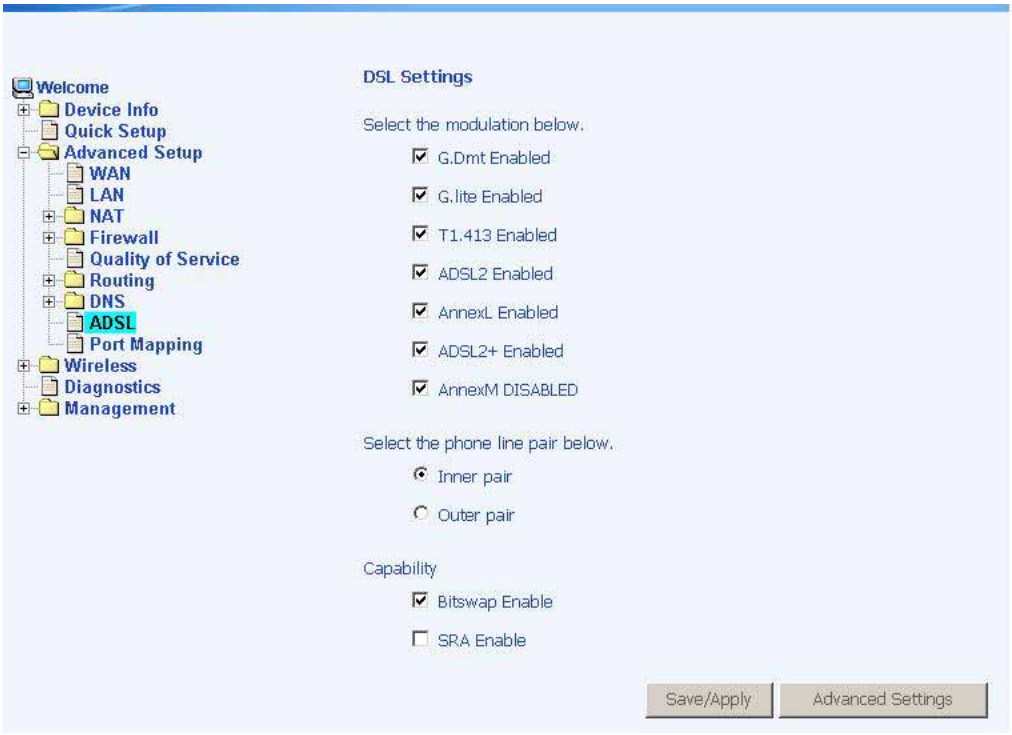
Six modulation methods for different linking speed are supported by the 6211 ADSL router: G.Dmt Enabled, G.lite Enabled, T1.413 Enabled, ADSL Enabled, Annex L Enabled, and ADSL2+ Enabled. Set this value only as directed by your ISP.

Phone Line Pair

The 6211 ADSL router supports phone lines on pins 2 and 3 or pins 1 and 4 to connect your ADSL line. If your phone system uses pins 2 and 3, attach a normal RJ11 cable to the router and select “Inner pair” on the screen; if your phone system uses pins 1 and 4, attach the phone with the supplied RJ11 cable and select “Outer pair” on the screen.

Capability

Do not change these settings unless directed by your ISP.



DSL Advanced Settings

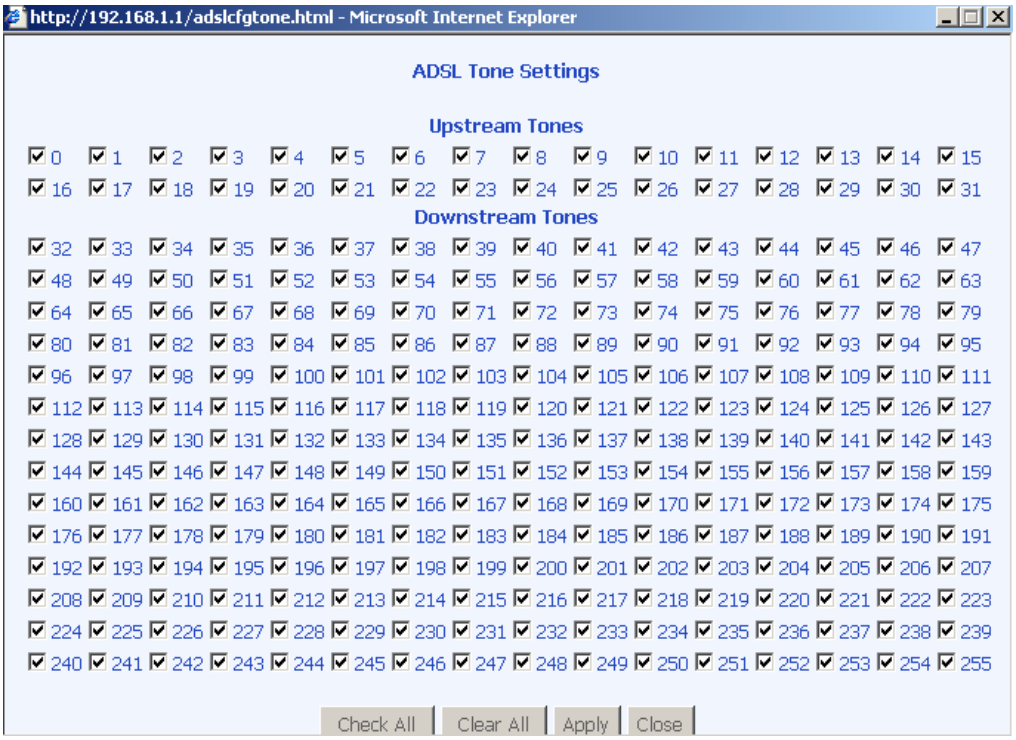
The test mode can be selected from the DSL Advanced Settings page.

Test modes are as follows–

- Normal
- Reverb
- Medley
- No retrain
- L3

Tone Settings

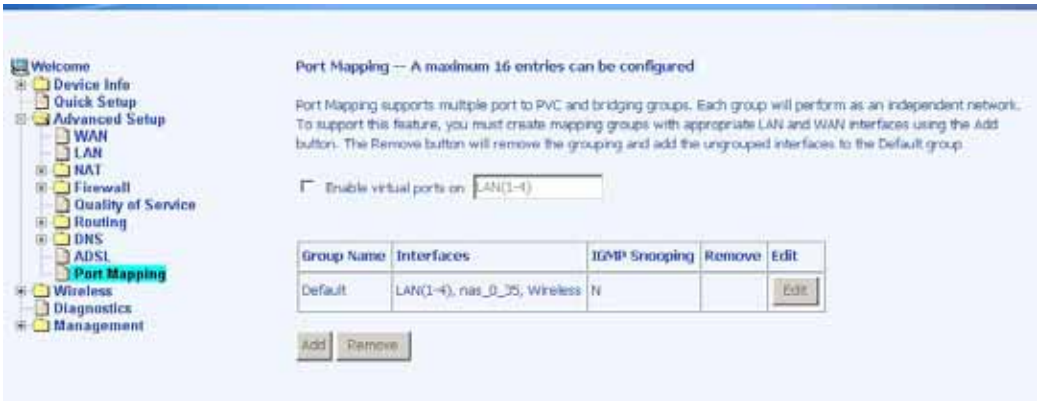
The frequency band of ADSL is split up into 256 separate tones, each spaced 4.3125 kHz apart. With each tone carrying separate data, the technique operates as if 256 separate modems were running in parallel. The tone range is from 0 to 31 for upstream and from 32 to 255 for downstream. Do not change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



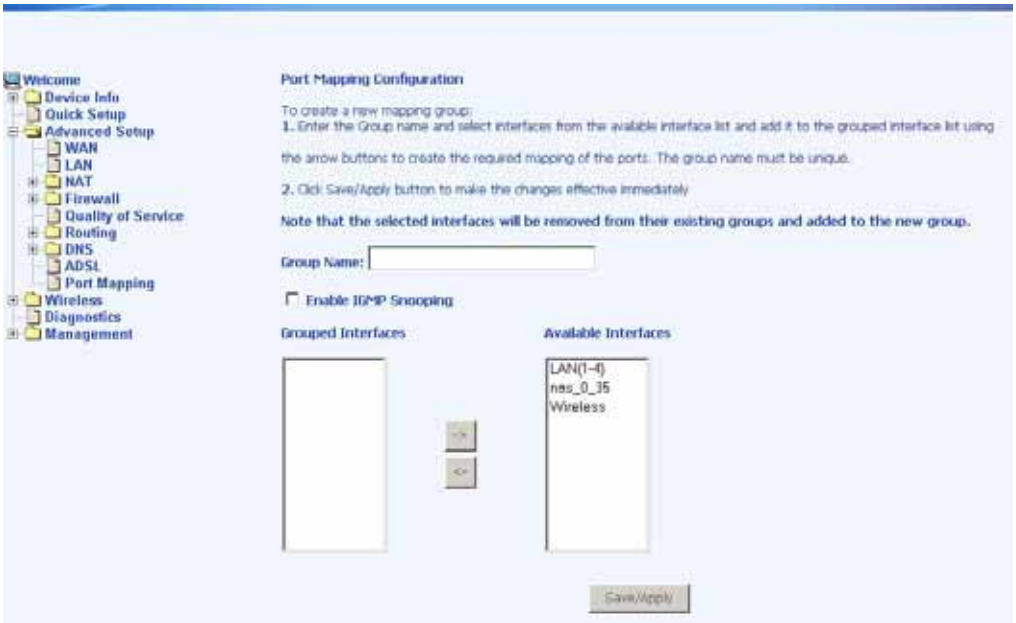
Port Mapping

Port mapping is a feature that allows you to open ports to allow certain Internet applications on the WAN side to pass through the firewall and enter your LAN. To use this feature, mapping groups need to be created. To do this, follow the below instructions–

1. Click on the **Add** button as displayed below.



2. After clicking the **Add** button, the below configuration screen appears, allowing you enter the groups and the interfaces they are associated with.



Wireless

This section allows you to configure wireless settings on your router.

Basic

The below **Wireless - Basic** screen lets you enable or disable wireless. The default setting for wireless is enabled. You can also hide the access point so others cannot see your ID on the network.

Security

The next screen is the **Wireless - Security** screen which allows you to select the network authentication method and to enable or disable WEP encryption. Note that depending on the network authentication that is selected, the screen will change accordingly so additional fields can be configured for the specific authentication method.

Network authentication methods include the following–

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

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

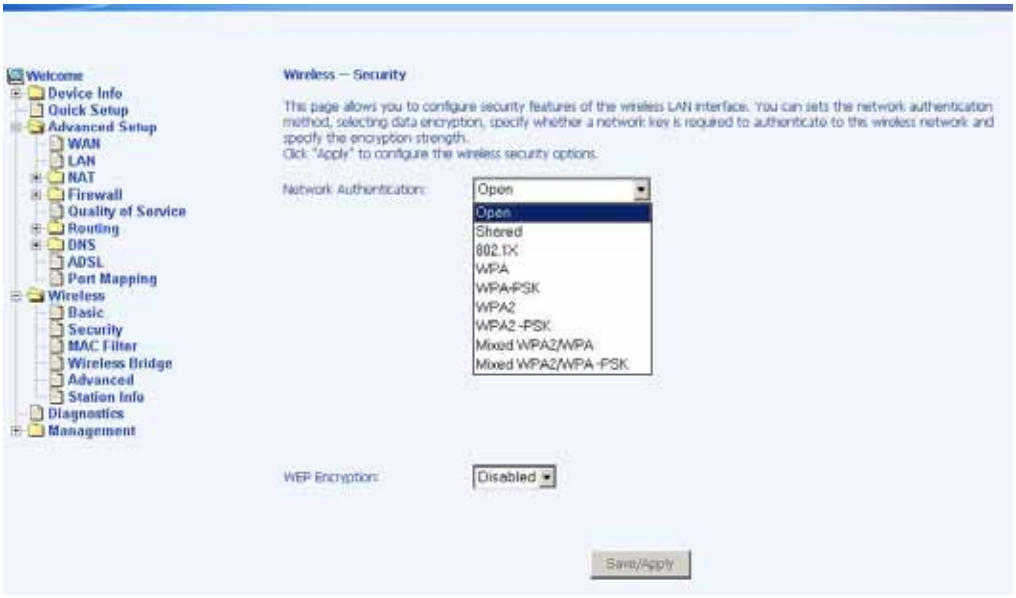
- 802.1X–requires mutual authentication between a client station and the router by including a RADIUS-based authentication server. Information about the RADIUS server such as its IP address, port and key must be entered. WEP encryption is also enabled and the encryption strength must also be selected.

- WPA–(Wi-Fi Protected Access)– usually used for the larger Enterprise environment, it uses a RADIUS server and TKIP (Temporal Key Integrity Protocol) encryption (instead of WEP encryption which is disabled). TKIP uses128-bit dynamic session keys (per user, per session, and per packet keys).
- WPA-PSK (Wi-Fi Protected Access – Pre-Shared Key)– WPA for home and SOHO environments also using the same strong TKIP encryption, per-packet key construction, and key management that WPA provides in the enterprise environment. The main difference is that the password is entered manually. A group re-key interval time is also required.
- WPA2 (Wi-Fi Protected Access 2)–second generation of WPA which uses AES (Advanced Encryption Standard) instead of TKIP as its encryption method. Network re-auth interval is the time in which another key needs to be dynamically issued.

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

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

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



MAC Filter

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

The following screen appears when you want to add a MAC address to the filter. When completed, click on the **Save / Apply** button.

Wireless Bridge

In this next screen, you can select which mode you want the router to be in, either access point or wireless bridge.

Advanced

Advanced features of the wireless LAN interface can be configured in this section.

Settings can be configured for the following–

- AP Isolation–if you select enable, then each of your wireless clients will not be able to communicate with each other.

- Band–a default setting at 2.4GHz - 802.11g

- Channel-- 802.11b and 802.11g use channels to limit interference from other devices. If you are experiencing interference with another 2.4Ghz device such as a baby monitor, security alarm, or cordless phone, then change the channel on your router.

- Multicast Rate–the rate at which a message is sent to a specified group of recipients.

- Basic Rate–the set of data transfer rates that all the stations will be capable of using to receive frames from a wireless medium.

- Fragmentation Threshold–used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.

- RTS Threshold (Request to Send Threshold)–determines the packet size of a transmission through the use of the router to help control traffic flow.

- DTIM Interval–sets the Wake-up interval for clients in power-saving mode.

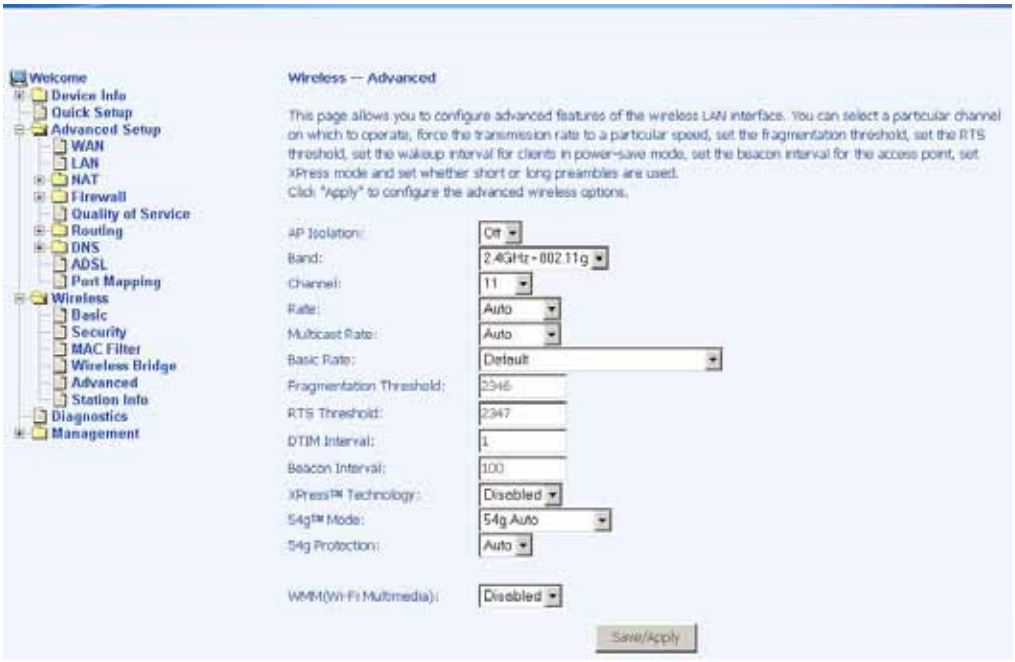
- Beacon Interval–a packet of information that is sent from a connected device to all other devices where it announces its availability and readiness. A beacon interval is a period of time (sent with the beacon) before sending the beacon again. The beacon interval may be adjusted in milliseconds (ms).

- **Xpress Technology–**a technology that utilizes standards based on framebursting to achieve higher throughput. With Xpress Technology enabled, aggregate throughput (the sum of the individual throughput speeds of each client on the network) can improve by up to 25% in 802.11g only networks and up to 75% in mixed networks comprised of 802.11g and 802.11b equipment.

- **54g Mode–** 54g is a Broadcom Wi-Fi technology.

- **54g Protection**--the 802.11g standards provide a protection method so 802.11g and 802.11b devices can co-exist in the same network without "speaking" at the same time. Do not disable 54g Protection if there is a possibility that a 802.11b device may need to use your wireless network. In Auto Mode, the wireless device will use RTS/CTS (Request to Send / Clear to Send) to improve 802.11g performance in mixed 802.11g/802.11b networks. Turn protection off to maximize 802.11g throughput under most conditions.

- **WMM (Wi-Fi Multimedia)**–feature that improves the your experience for audio, video and voice applications over a Wi-Fi network.



Station Info

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

Troubleshooting–Diagnostics

The diagnostics screen allows you to run diagnostic tests to check your DSL connection. In addition, you can test the connection to your DSL service provider.

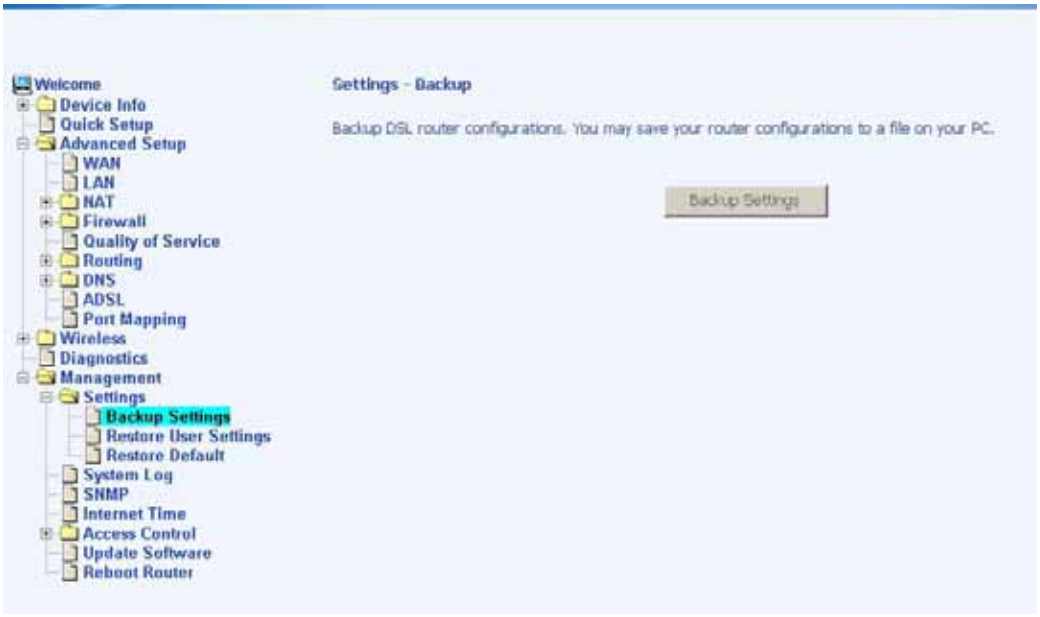
Management

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

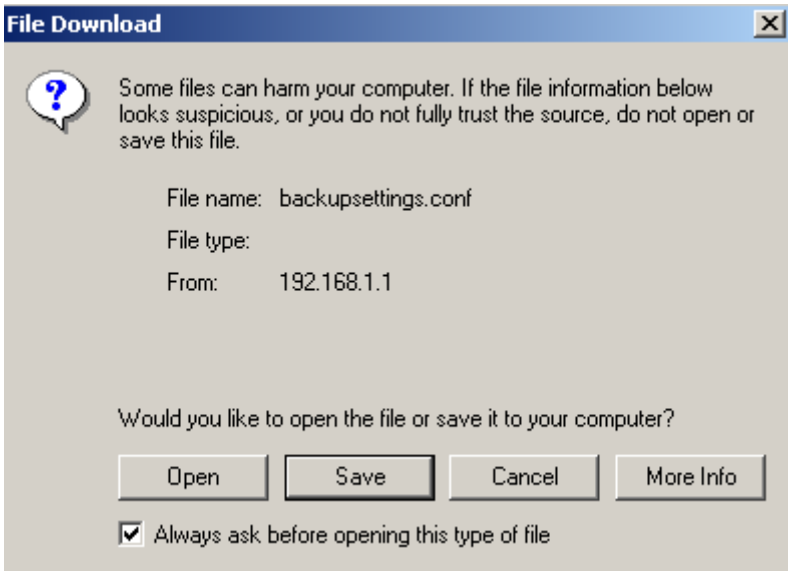
Settings

Backup Settings

To save a copy of the configurations that you have made on your router, click on the **Backup Settings** button.

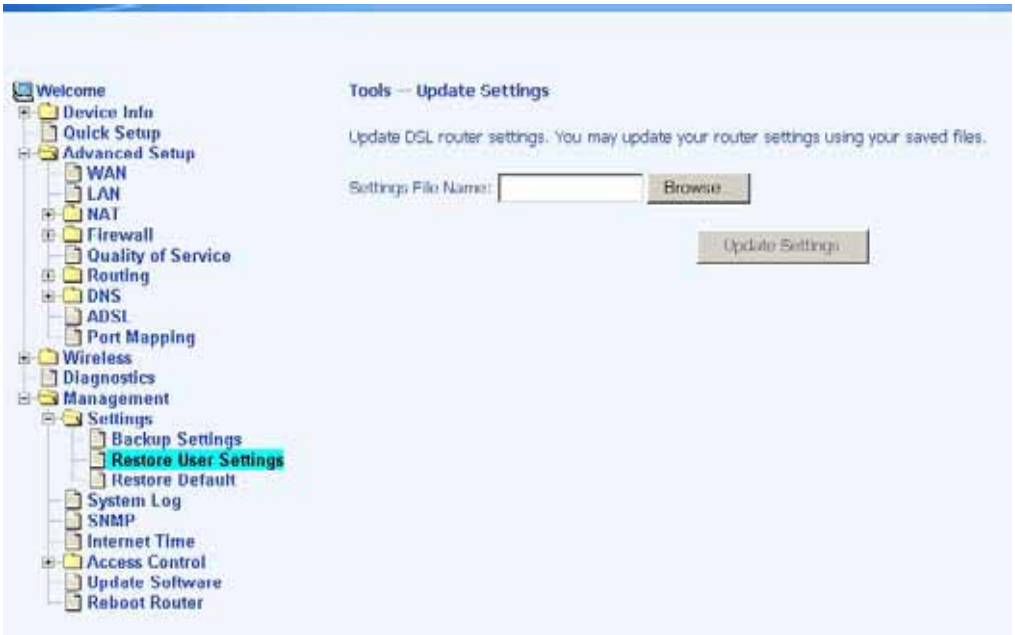


The below pop-up screen will appear with a prompt to open or save the file to your computer.



Restore User Settings

To restore saved settings, select Management→ Settings→ Restore User Settings. Then select the backup file you want to restore and click on **Update Settings**.

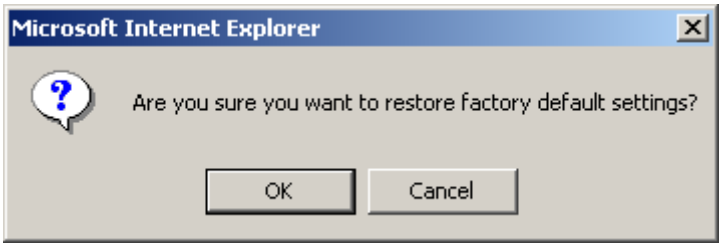


The router will restore settings and reboot to activate the restored settings.

Restore Default

Restore Default will erase all current settings and restore the router to factory default settings. To restore the router to factory default settings, select Management→Settings→Restore Default.

Reply OK to the confirmation dialog.



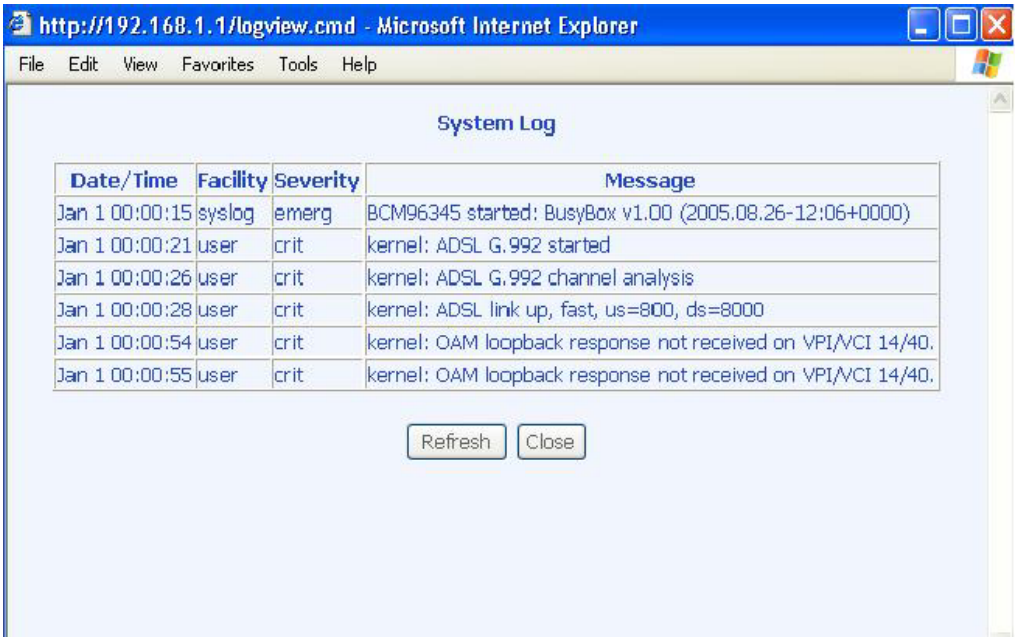
The router will restore the default settings and reboot.

System Log

The System Log dialog allows you to view the System Log and configure the System Log options.

To view the System Log click on the **View System Log** button to check the log file.

Below is a view of the **System Log**.



Configure System Log

If the log is enabled, the system will log selected events: Emergency, Alert, Critical, Error, Warning, Notice, Informational, and Debugging. All events above or equal to the selected log level will be logged and displayed.

If the selected mode is “Remote” or “Both”, events will be sent to the specified IP address and UDP port of a remote system log server. If the selected mode is “Local” or “Both”, events will be recorded in the local memory. Select the desired values and click on the “**Save/Apply**” button to configure the system log options.

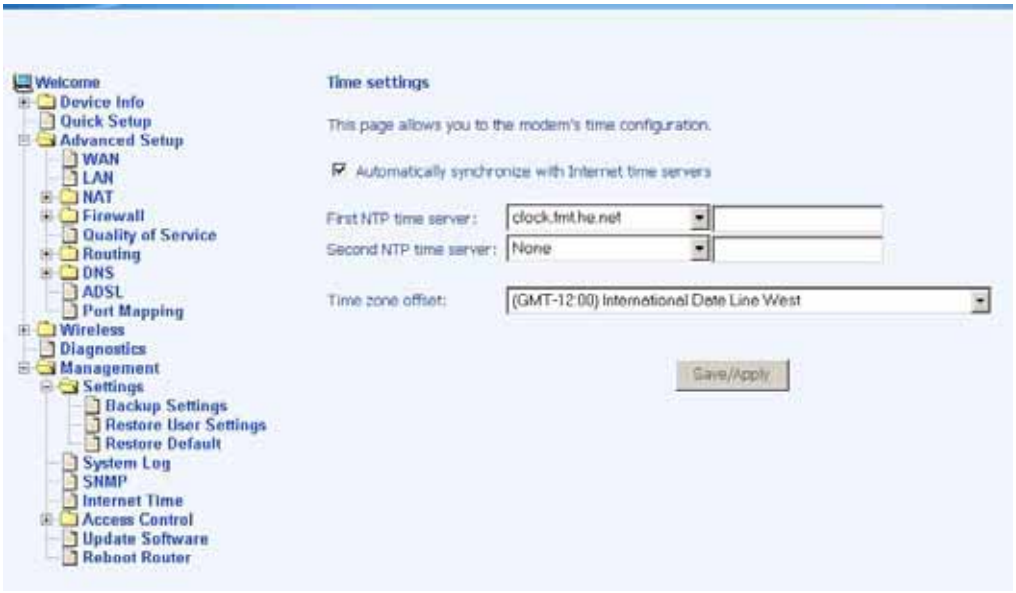
SNMP

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

Internet Times

The Time Settings page allows you to automatically synchronize your time with a timeserver on the Internet.

If you choose to automatically synchronize with Internet time servers, then click on the box and the below fields appear. Select from the list of NTP (Network Time Protocol) time servers. Then select the time zone that you are in and click on **Save / Apply** to save and complete your time settings.



Access Control

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

Services

Services that can be enabled / disabled on the LAN / WAN are FTP, HTTP, ICMP, SNMP, SSH, Telnet, and TFTP.

IP Addresses

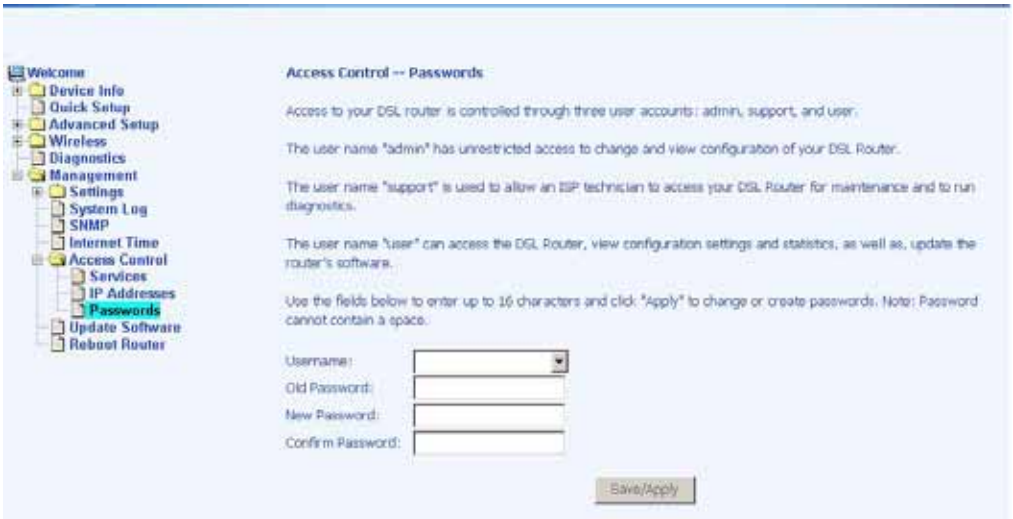
Web access to the router can be limited when Access Control Mode is enabled. The IP addresses of allowed hosts can be added using Access Control→IP Address.

Add the IP address to the IP address list by clicking on the **Add** button, then select "**Enabled**" to enable Access Control Mode.

To assign the IP address of the management station that is permitted to access the local management services, enter the IP address in the box and click on the **Save / Apply** button.

Passwords

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



Update Software

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

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

Reboot Router

Select Management→Reboot Router to reboot the router using the web interface. The router will save the current configuration and reboot itself using the new configuration.