USER MANUAL

DSL-2640B

VERSION 1.0

D-Link®

BROADBAND

Table of Contents

General Information

The D-Link DSL-2640B is an ADSL2+ wireless router, that combines a DSL router and wireless solution in a single device. The DSL-2640B also has four addional 10/100Mbps ethernet ports to connect non-wireless computers. This user manual provides you with a simple and easy-to-understand format to install and configure your router.

Package Contents

- ADSL2/2+ 4-Port Wireless Router
- 12VDC, 1A DC CEC-compliant switching power adapter
- RJ-11 telephone cable
- RJ-45 Ethernet cable
- Quick Install Guide
- Documentation CD-ROM (QIG + user manual)

Note: *Using a power supply with a different voltage rating than the one included with the DSL-2640B will cause damage and void the warranty for this product.*

Important Safety Instructions

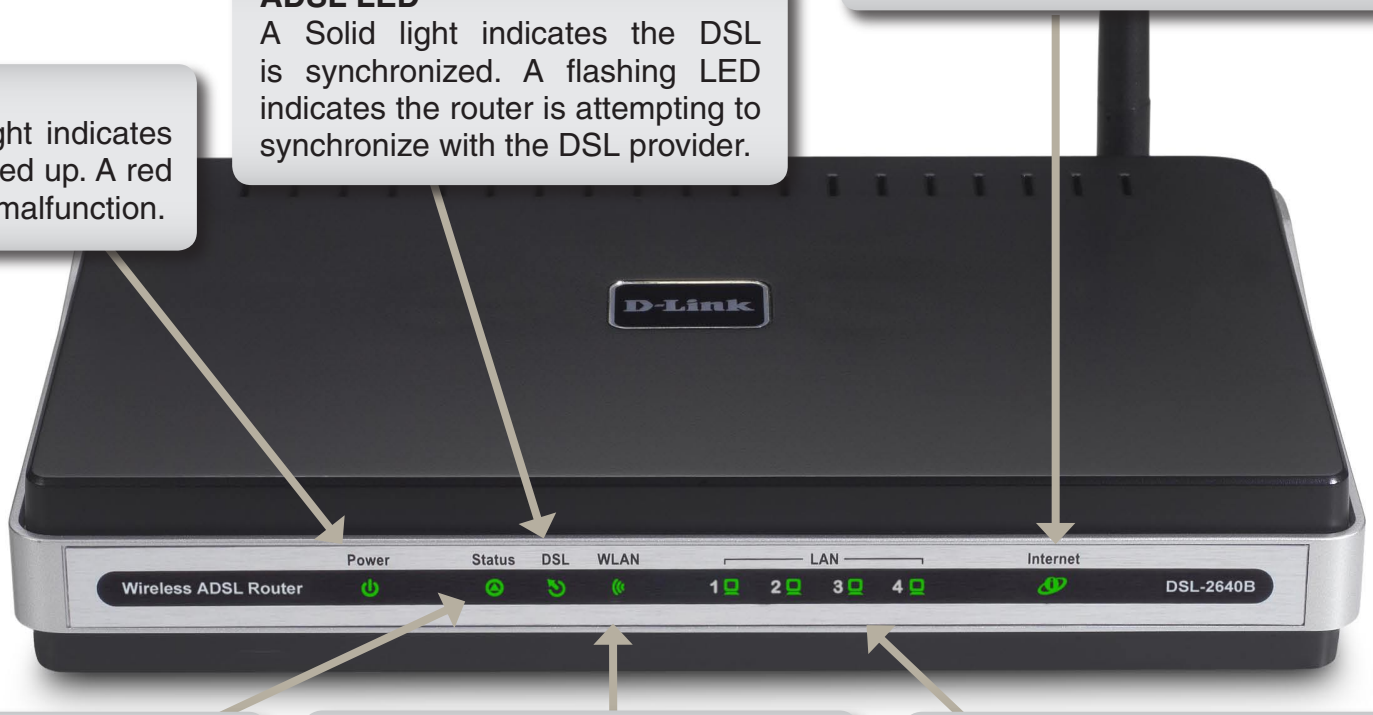
- Place your router on a flat surface close to the cables in a location with sufficient ventilation.
- To prevent overheating, do not obstruct the ventilation openings of this equipment.
- Plug this equipment into a surge protector to reduce the risk of damage from power surges and lightning strikes.
- 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

Internet LED
A solid green light indicates that the router has an IP address and is connected to the Internet. A red light indicates that the router does not have an IP address or authentication has failed. No light indicates that an ADSL connection is not present or the router is in bridge mode.

ADSL LED
A Solid light indicates the DSL is synchronized. A flashing LED indicates the router is attempting to synchronize with the DSL provider.

Power LED
A solid green light indicates the unit is powered up. A red light indicates a malfunction.

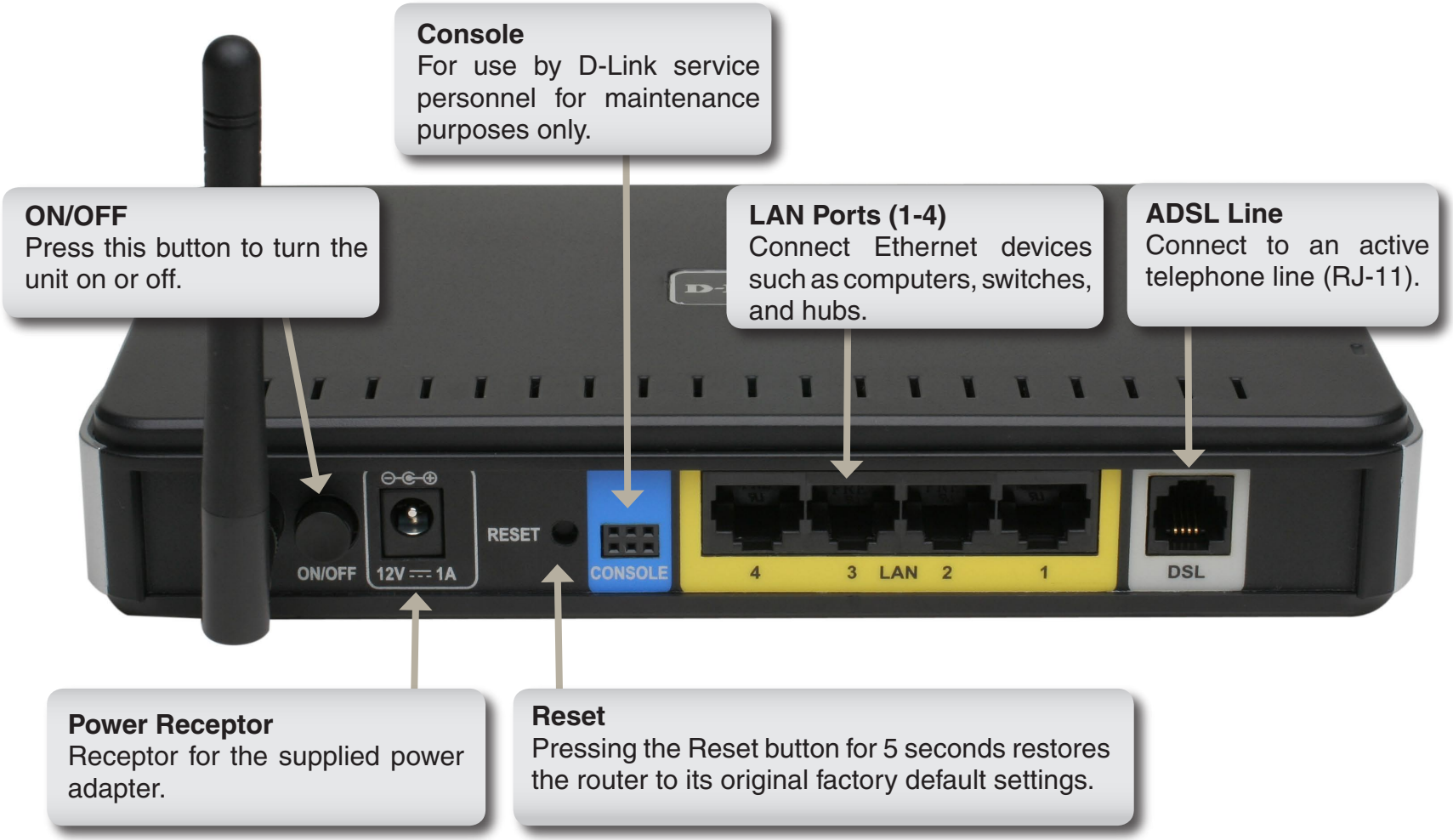


Status LED
A blinking light indicates traffic is passing through.

WLAN LED
A solid green light indicates the wireless is operational. A flashing green light indicates wireless traffic is passing through the router.

Local Network LEDs
A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

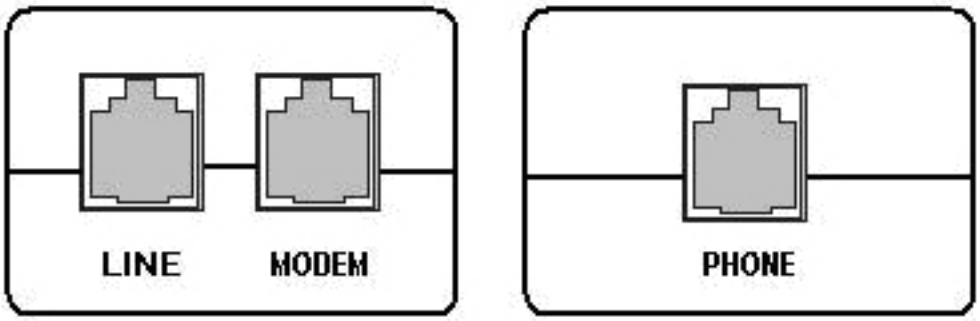
Rear Panel View



Installing the Router

Connect the ADSL and Telephone Lines

- Connect an RJ-11 cable between the wall phone jack and the line-end of the splitter (see diagram below).
- Attach another RJ-11 phone cable to the router-end of the splitter and the **ADSL** port on the rear panel of the router.
- The phone-end of the splitter will be connected to the telephone using a third RJ-11 phone cable.



NOTE: See connections on the installation diagram.

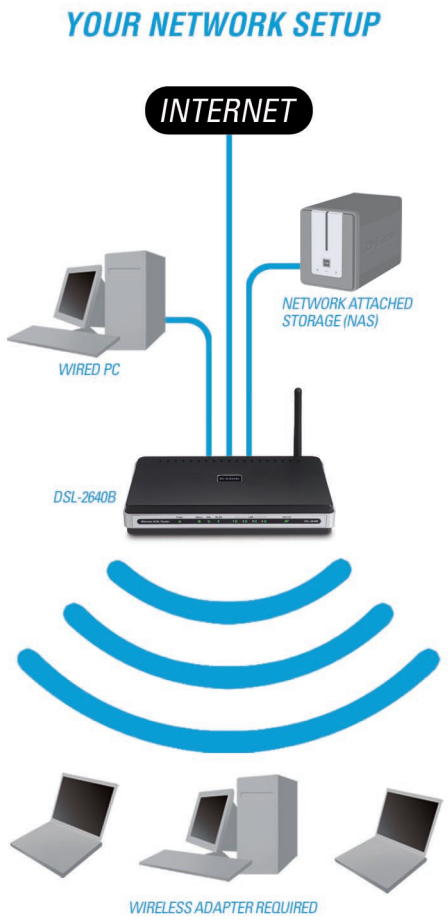
Connect the PC to the Router

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

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

Connect the Power Adapter

- Complete the process by connecting the supplied 12VAC, 1A 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.



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.x (where "x" 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

These are instructions for configuring your Windows® 2000 operating system. If you are using Windows® XP please proceed to page 10.

1. In the Windows taskbar, click on the **Start** button and point to **Settings** > **Control Panel** > **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

These are instructions for configuring your Windows® XP operating system. If you are using Windows® 2000 please proceed to page 9.

1. In the Windows taskbar, click on the **Start** button then go to **Control Panel** 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 on the radio button labeled **Use the following IP address** and type 192.168.1.x (where x is any number between 2 and 254) for the IP address field and 255.255.255.0 for the Subnet Mask field.
5. Click on **OK** twice to save your changes and then close the **Control Panel**.

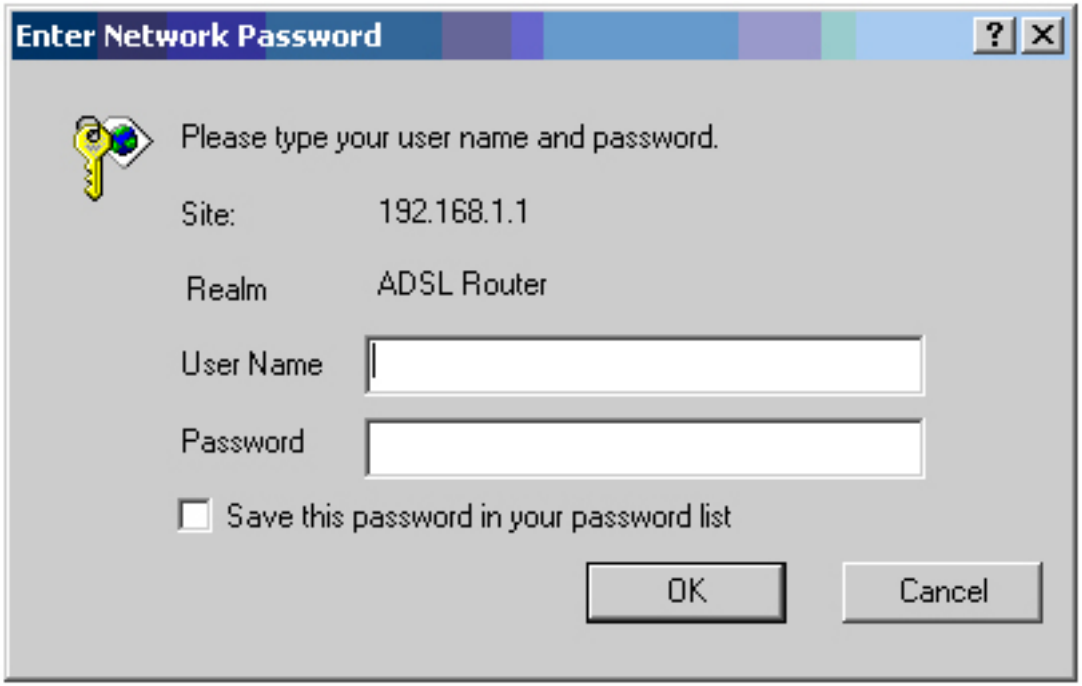
Log in to the Router

This section will explain 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 press **Enter**.

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



Note: *There are three account types, each requiring a different username and password.*

- The user account provides limited access to certain configurations (username / password: **user / user**).
- The admin account can perform all functions (username / password: **admin / admin**).
- The support account is for ISP technicians for maintenance purposes (username / password: **support / support**).

Note: *Passwords can be changed at any time.*

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

Note: *This manual has been prepared using the admin user name.*

Home

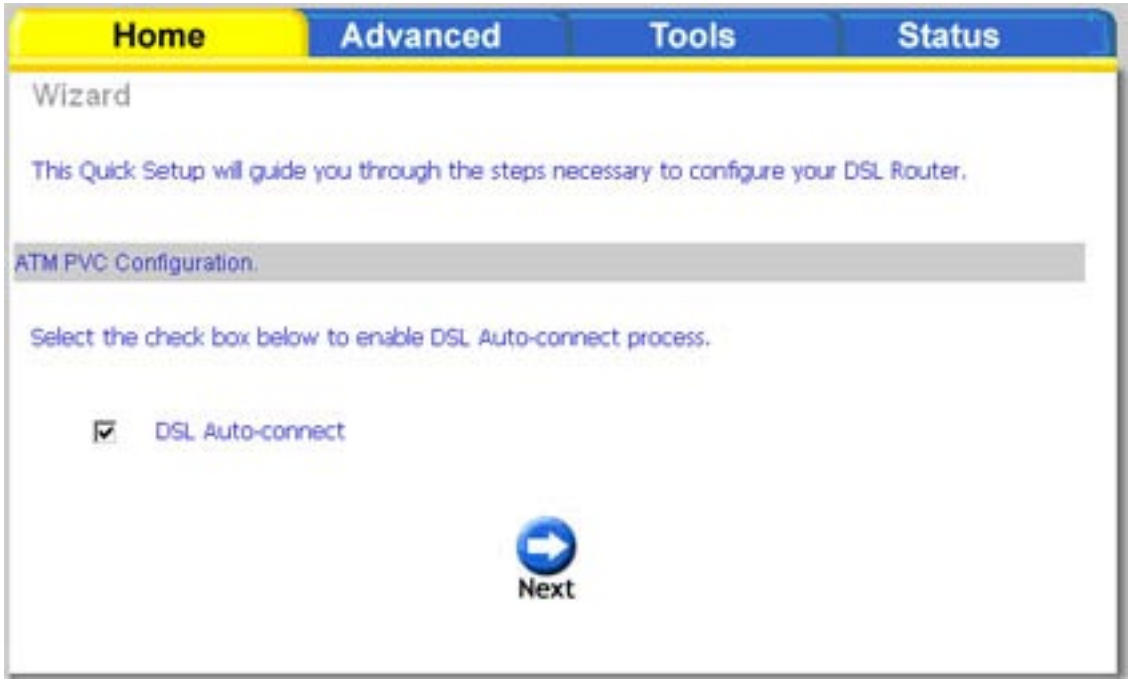
The home section provides configurations for general use, including a Quick Setup Wizard with steps to quickly set up your router for Internet connection. Also included in this section are LAN/WAN setup and DNS configuration. The below sections explain the setup for each.

Wizard

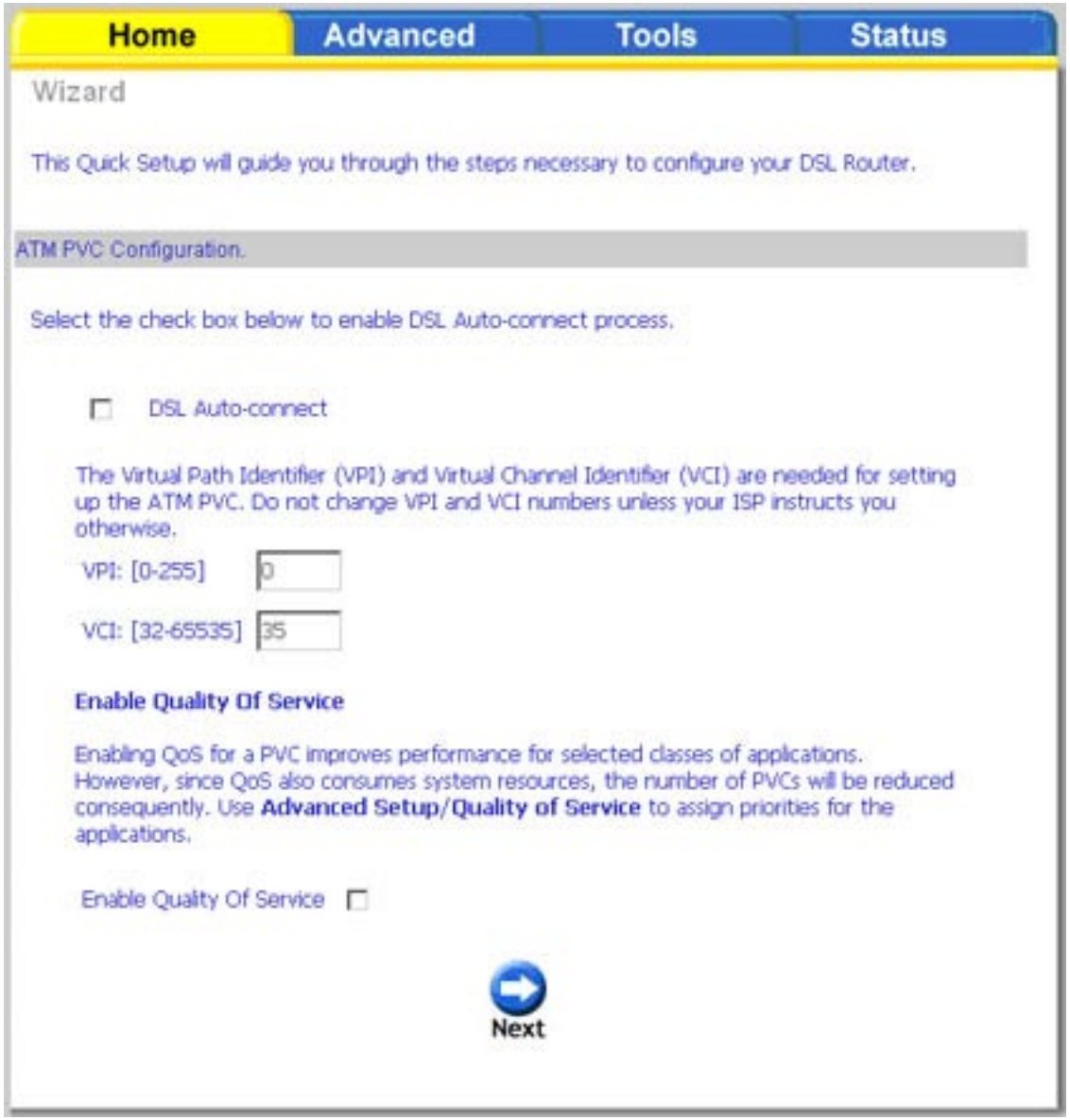
This section will explain how to quickly configure the router if your only intention is to access the Internet.

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.

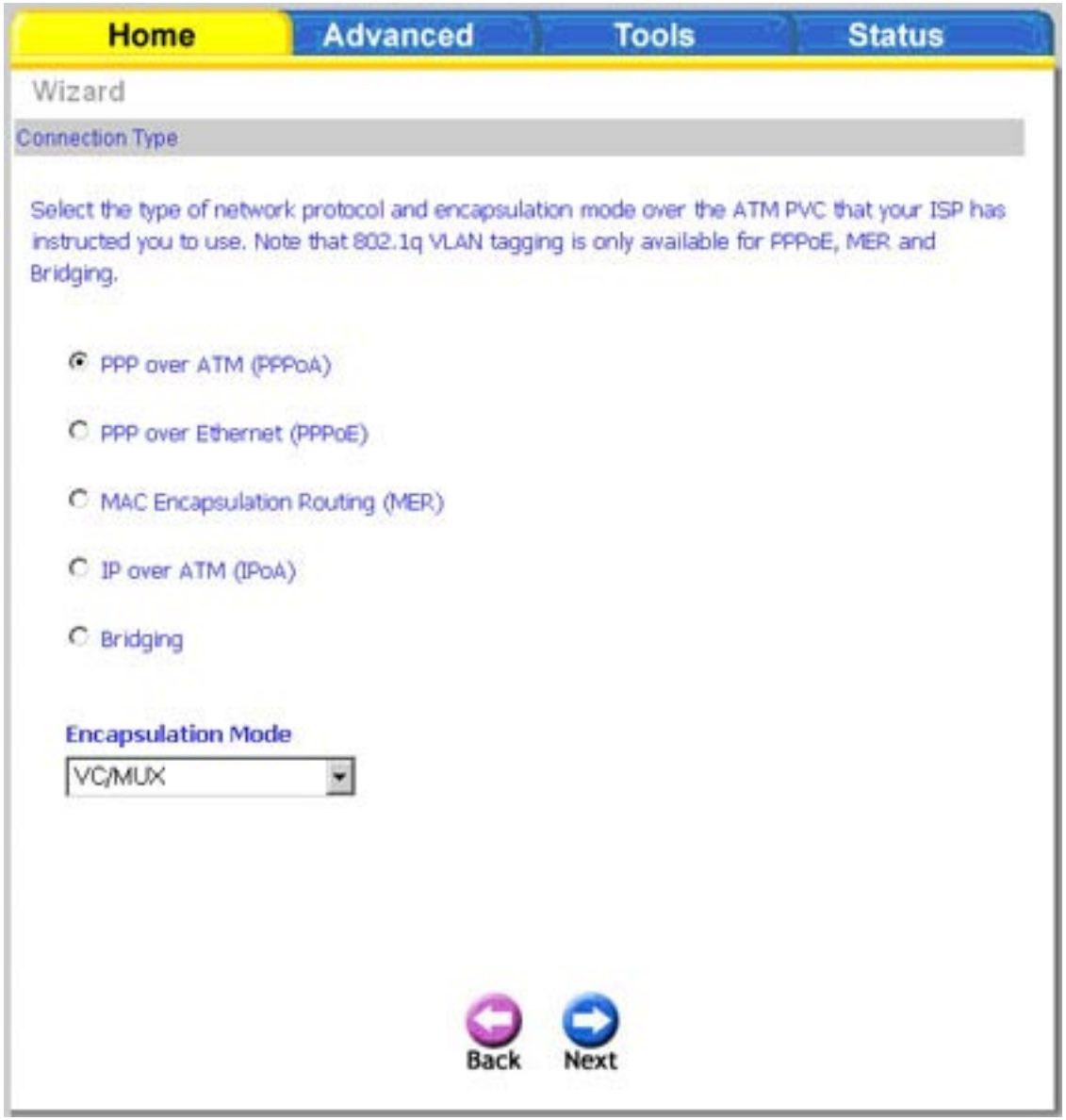


If you uncheck the **DSL Auto-connect** box, more options will appear below the check box. Enter the VPI/VCI values as indicated by your ISP. There is also an option to enable Quality of Service. When you are ready, click **Next** to continue.

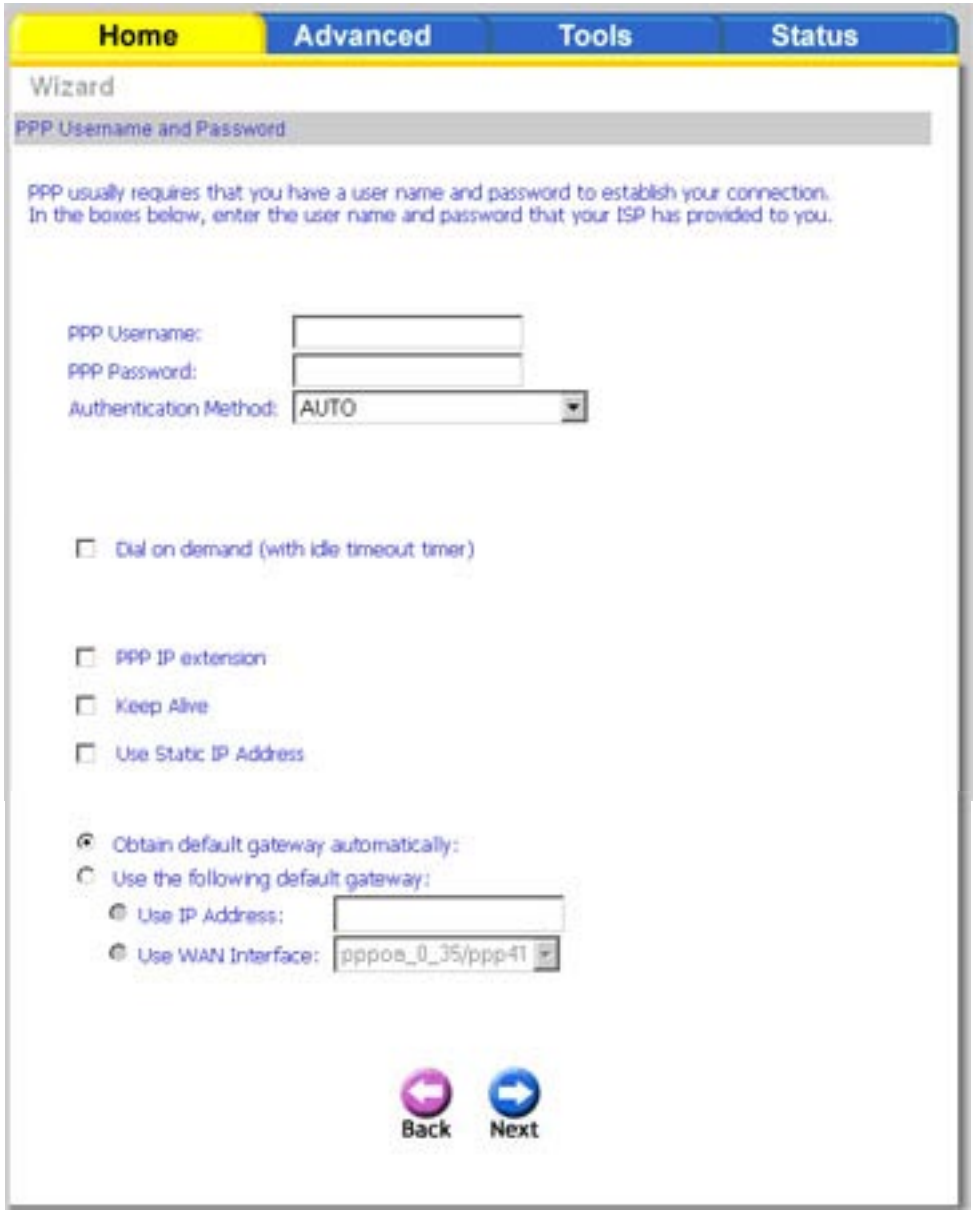


Next is the Connection Type screen where you can select the type of network protocol and encapsulation mode over the ATM PVC that your ISP has instructed you to use. There is also an option to Enable 802.1q (available for all encapsulation modes except PPPoA over ATM and IP over ATM). Select this option if required by your ISP. The following is a PPPoA example. Click **Next** to continue.

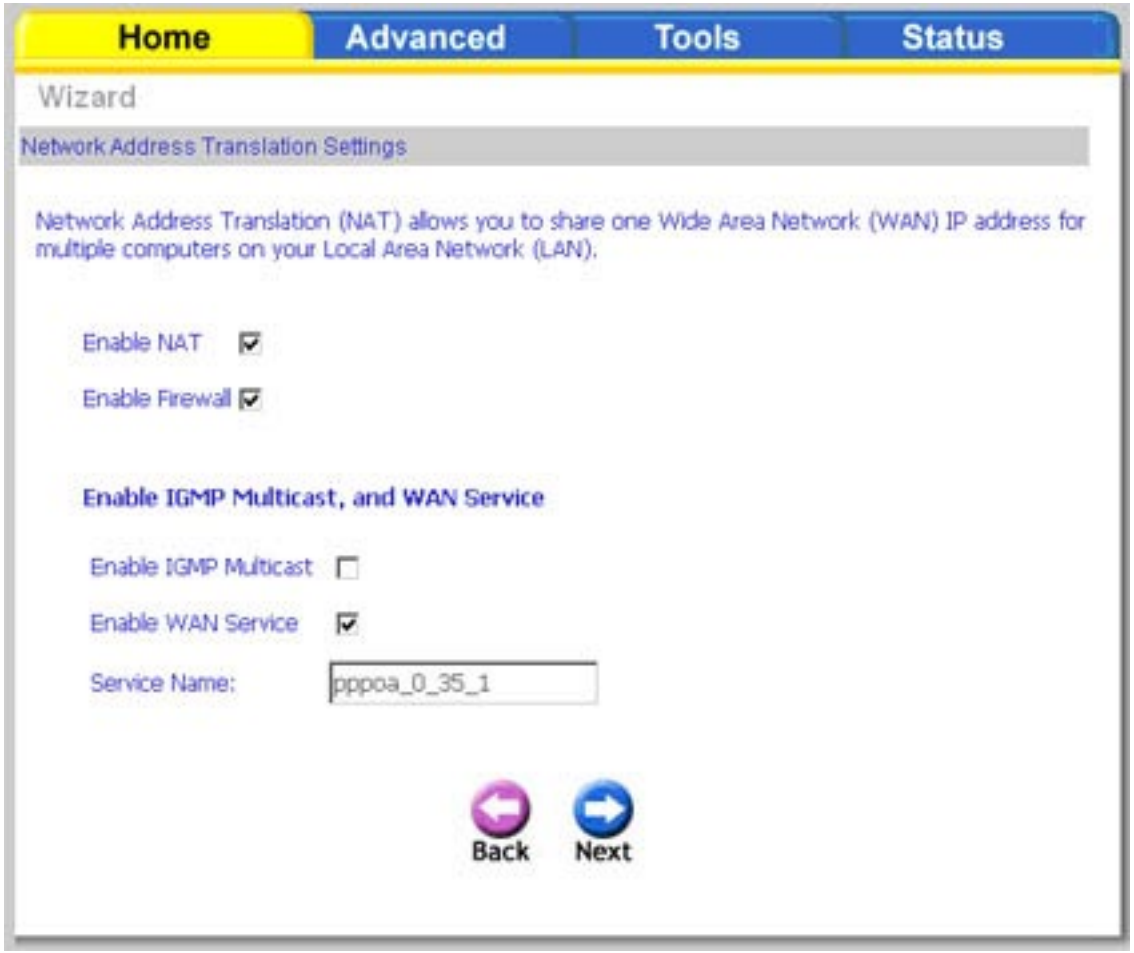
Select an appropriate network protocol and encapsulation mode. Click **Next** to continue.



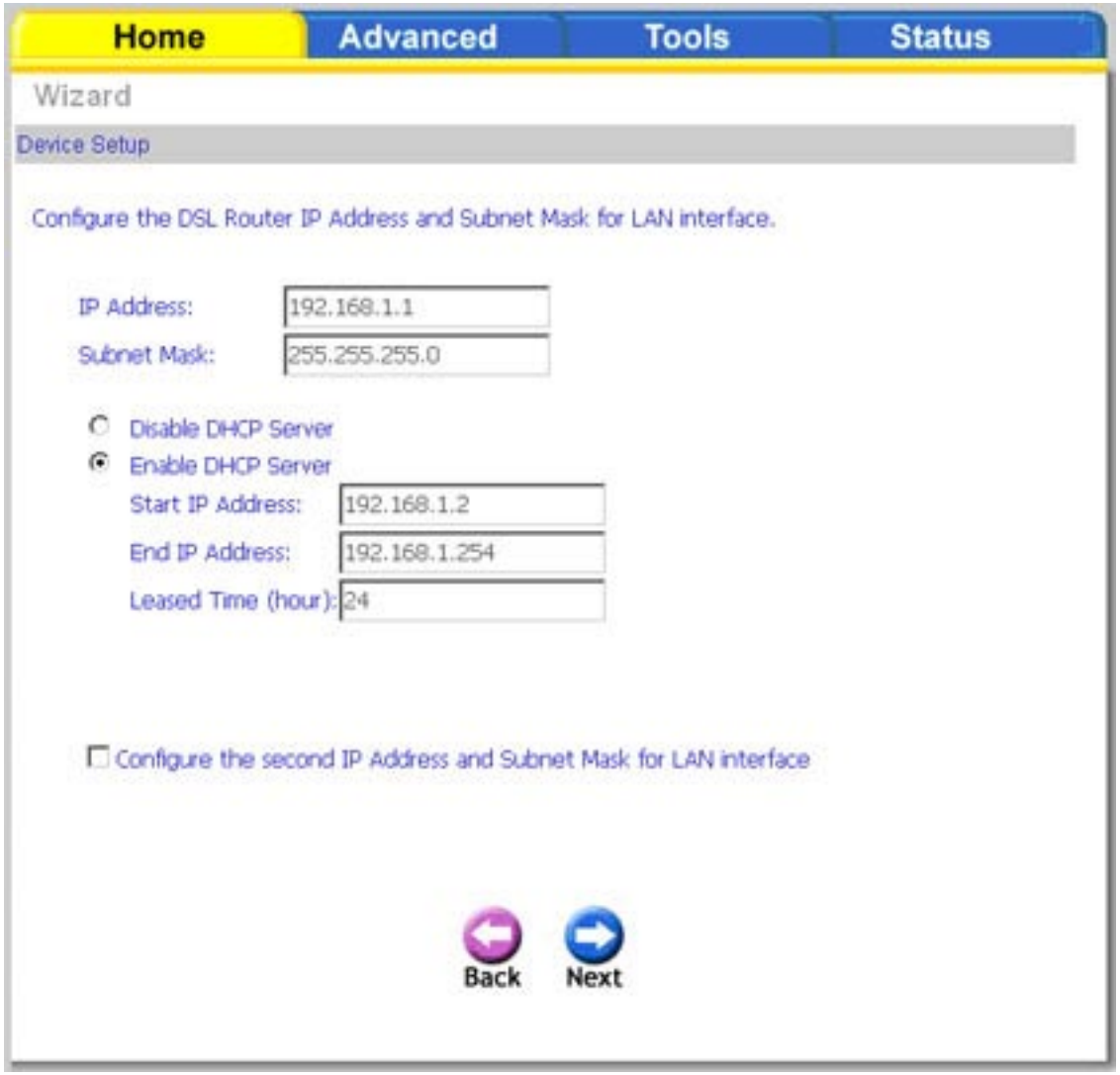
Enter the PPP username and password given to you by your ISP. Then decide if you will be using any features such as dial on demand, PPP IP extension, keep alive and then click **Next**.



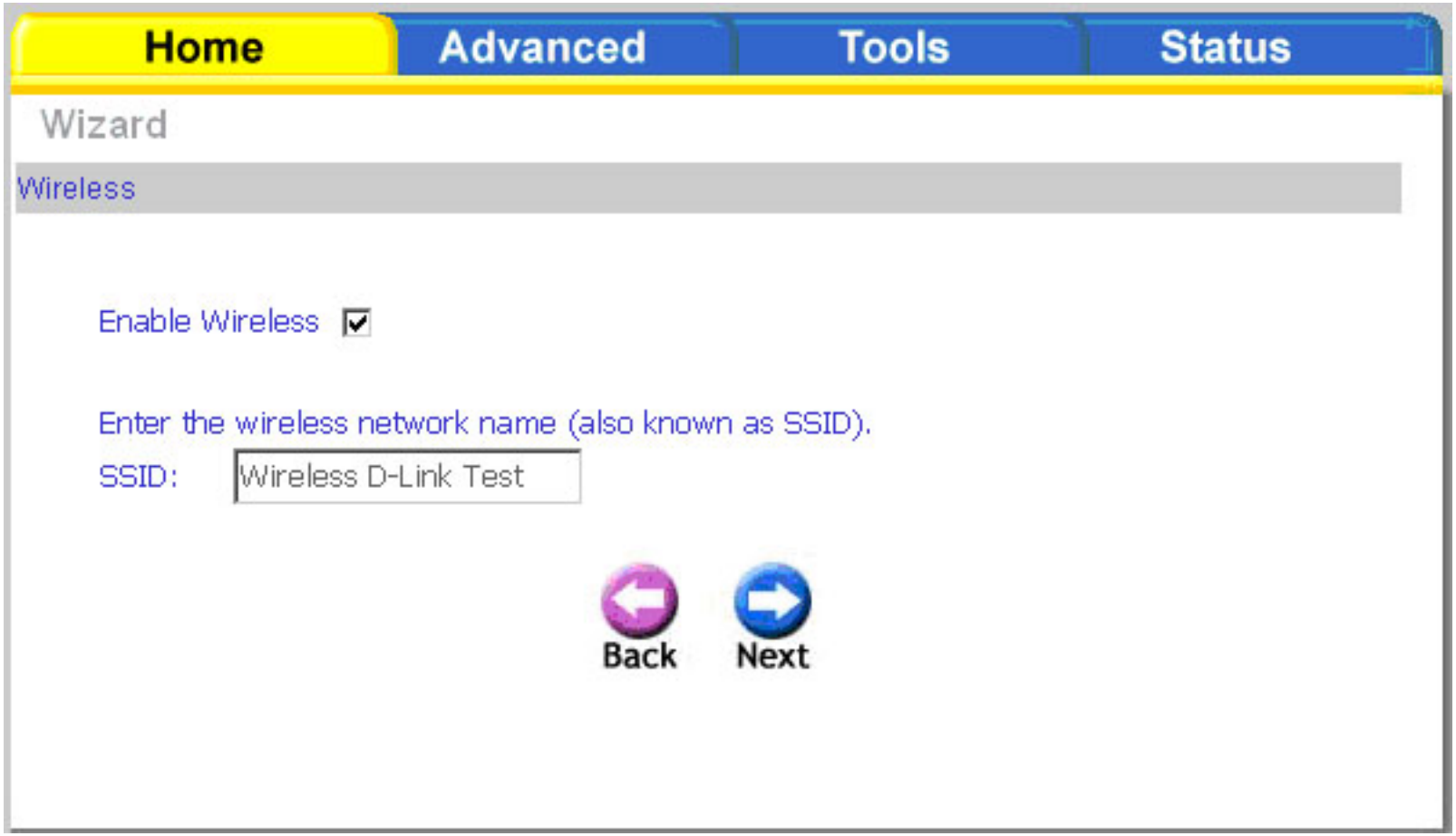
The next step is to configure the Network Address Translation (NAT) settings. For the example, NAT will be enabled. Leave the remaining fields at their defaults and click **Next** to continue.



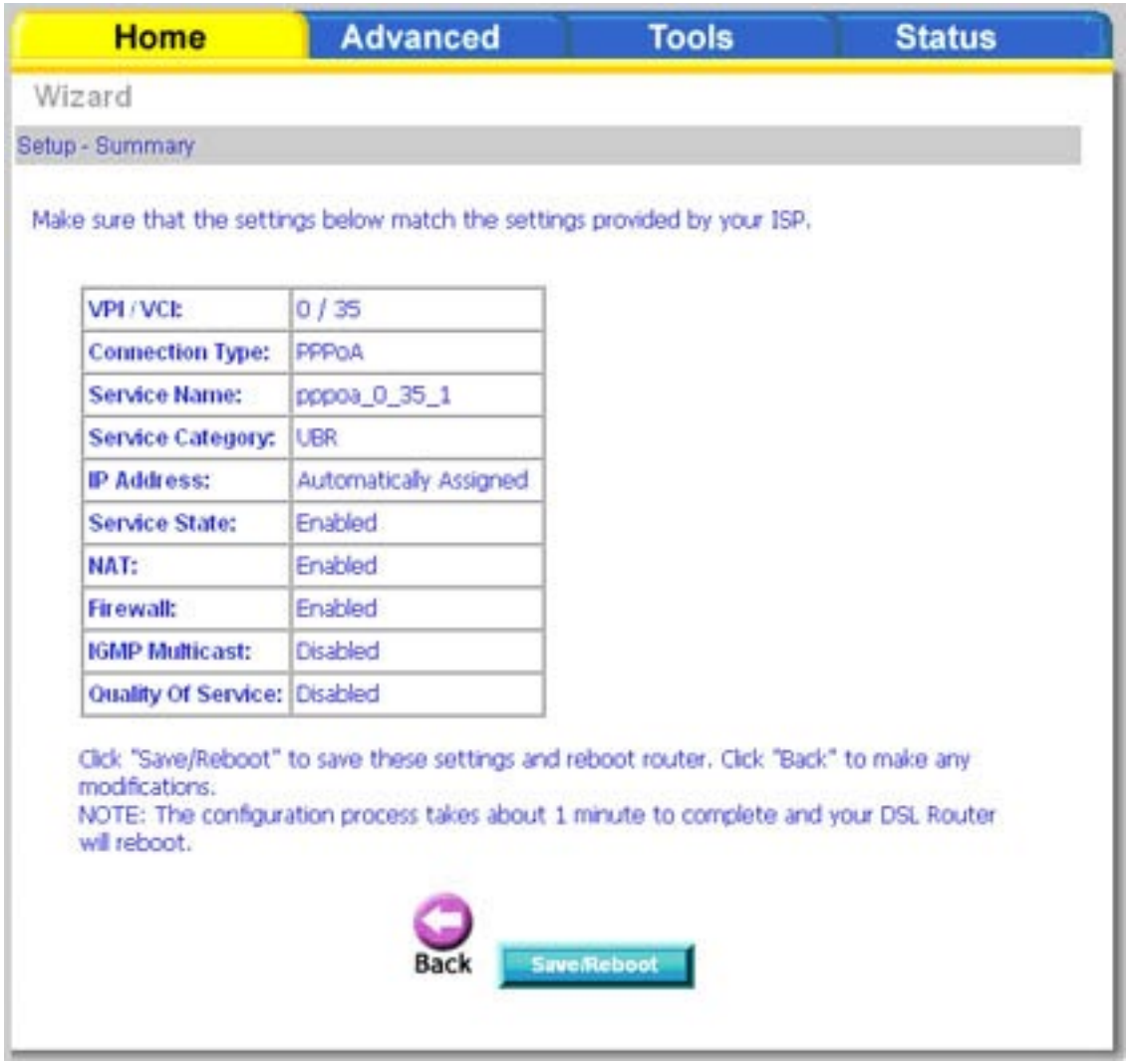
In this section, you can configure the DSL Router IP address and Subnet Mask to make the LAN interface correspond to your LAN's IP Subnet. If you want the DHCP server to automatically assign IP addresses, then enable the DHCP server and enter the range of IP addresses that the DHCP server can assign to your computers. Disable the DHCP server if you would like to manually assign IP addresses. Click **Next** to continue.



This next screen will allow you to enable the wireless function of your router. If you enable wireless, be sure to enter a wireless network name (SSID) to identify your wireless connection. You will need to know the wireless network name (SSID) to connect any wireless computers on your network to your router.



After all WAN configurations are complete, the WAN Setup Summary screen displays all WAN settings that you have made. Check that the settings are correct before clicking on the **Save / Reboot** button. Clicking on **Save / Reboot** will save your settings and restart your router.

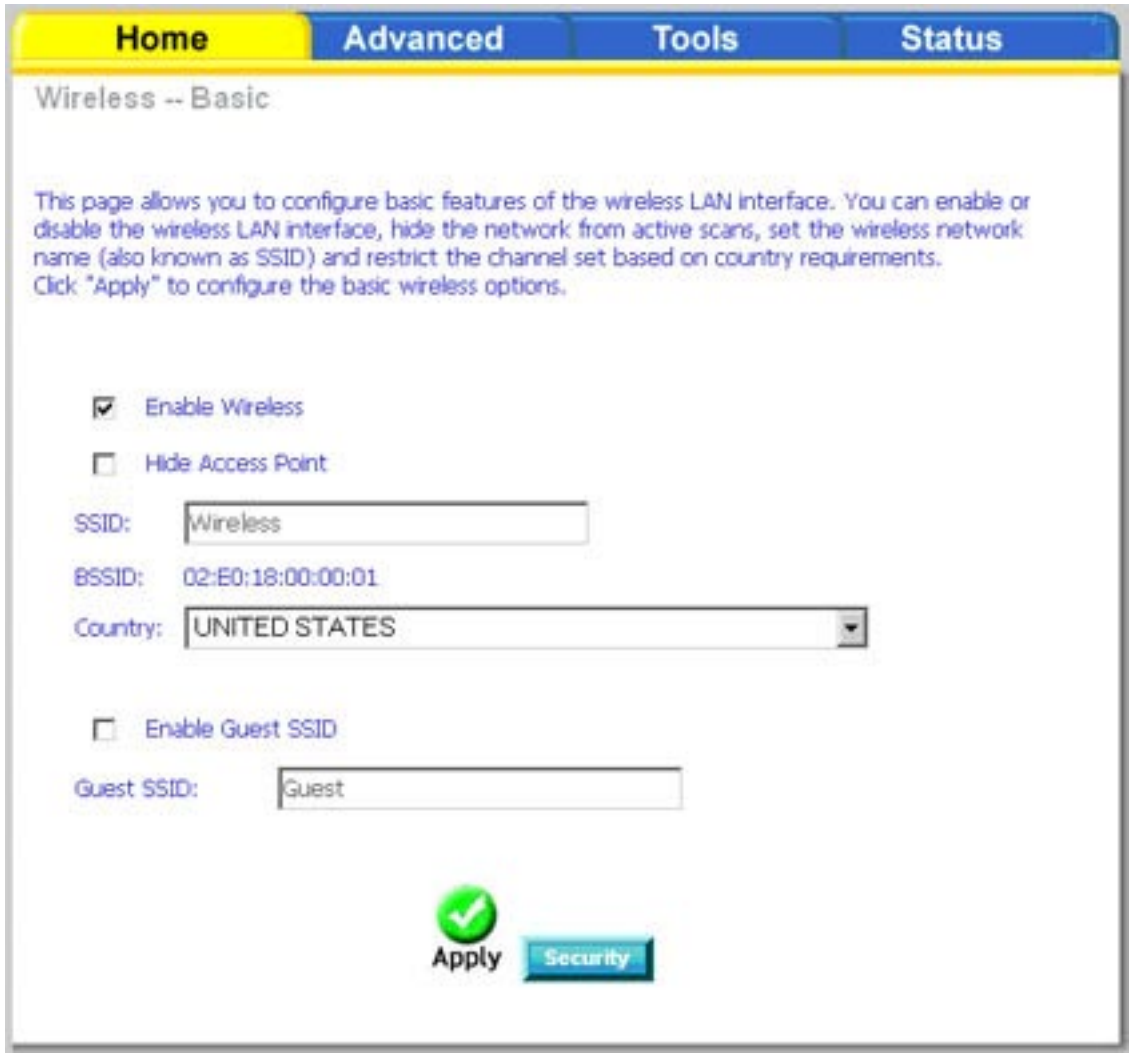


Wireless

The Wireless – Basic screen allows you to configure basic features of the wireless interface. You can enable or disable the wireless, hide the network from active scans, set the wireless network name (SSID), and restrict the channel set based on country requirements.

The default setting for wireless is enabled. If you intend on using the wireless, make sure you have entered a wireless network name in the (SSID) field and have selected your country from the drop-down list.

Click **Apply** to save your changes. Click **Security** to proceed to the wireless security section.



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 selected, the screen will change to reflect the authentication method and additional fields will appear which may require configuration.

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.

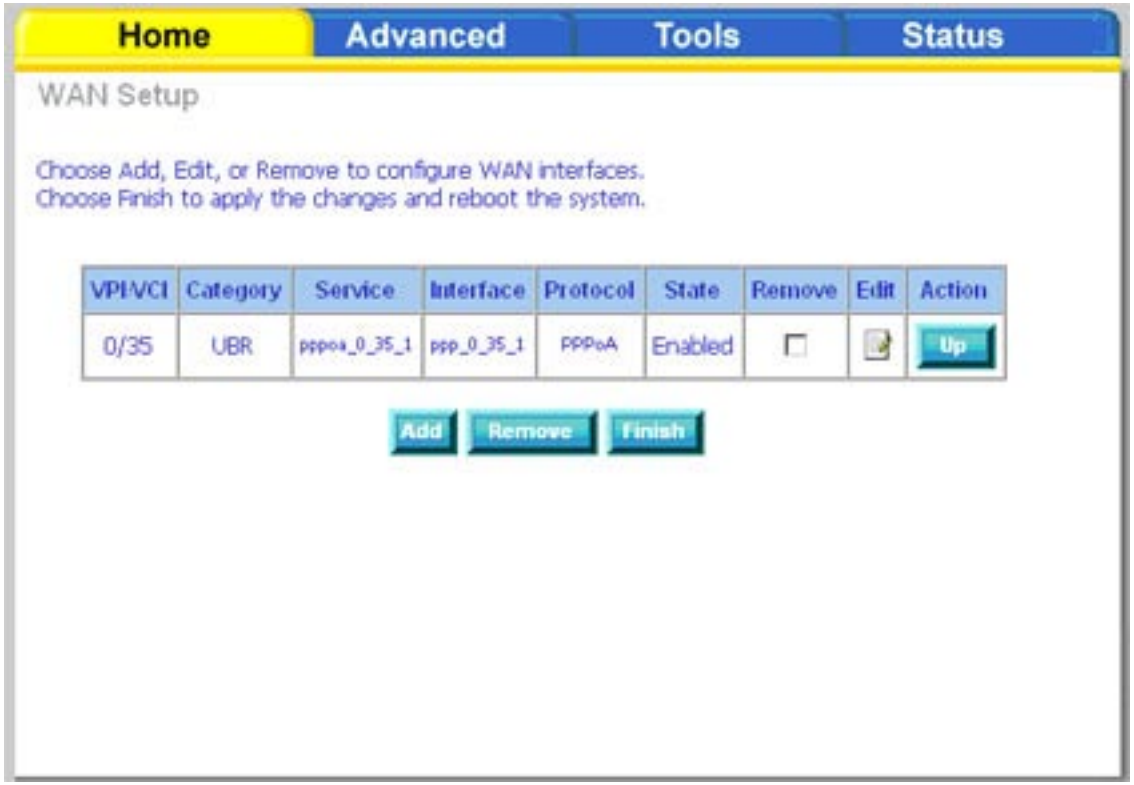
Mixed WPA2/WPA: During transitional times for upgrades in the enterprise environment, this mixed authentication method allows “upgraded” users and users not yet “upgraded” to access the network via the router. RADIUS server information must be entered for WPA and a as well as a group re-key interval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

WAN

Configure the WAN settings as provided by your ISP.

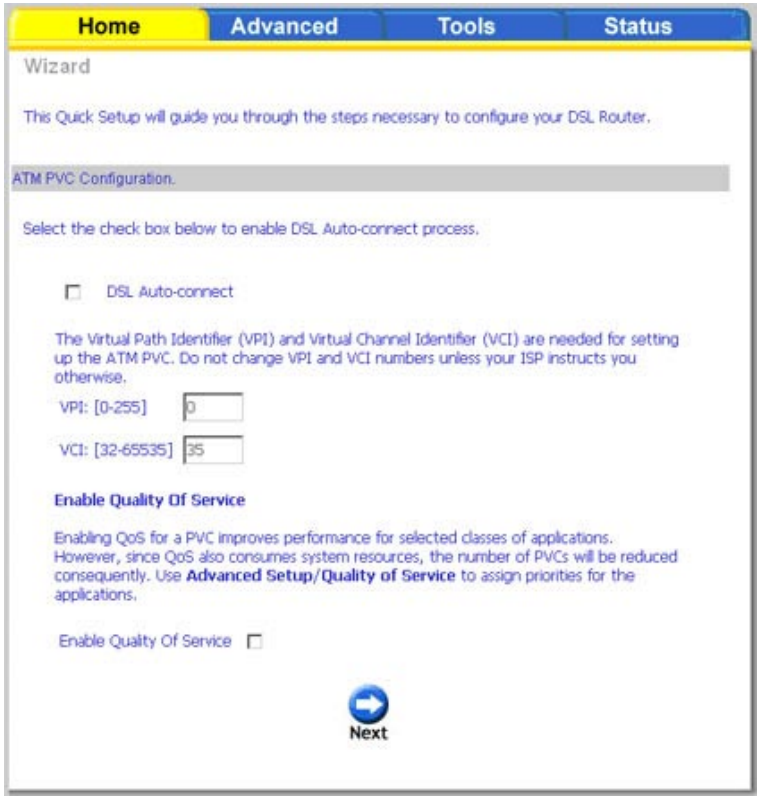
Click on the **Add** button if you want to add a new connection for the WAN interface and to proceed to the ATM PVC Configuration screen as seen on page 25. The ATM PVC Configuration screen allows you to configure an ATM PVC identifier (VPI and VCI) and select a service category.



Note: *The Following settings are ISP dependant. For information regarding proper configuration, contact your ISP.*

VPI: Virtual Path Identifier. The valid range is 0 to 255.

VCI: Virtual Channel Identifier. The valid range is 32 to 65535.



Service Five classes of traffic are listed:

UBR Without PCR (Unspecified Bit Rate without Peak Cell Rate): UBR service is suitable for applications that can tolerate variable delays and some cell losses. Applications suitable for UBR service include text/ data/image transfer, messaging, distribution, and retrieval and also for remote terminal applications such as telecommuting.

UBR With PCR (Unspecified Bit Rate with Peak Cell Rate): UBR service is suitable for applications that can tolerate variable delays and some cell losses. The Peak Cell Rate is a determining factor in how often cells are sent in an effort to minimize lag or jitter caused by traffic inconsistencies.

CBR (Constant Bit Rate): Used by applications that require a fixed data rate that is continuously available during the connection time. It is commonly used for uncompressed audio and video information such as videoconferencing, interactive audio (telephony), audio / video distribution (e.g. television, distance learning, and pay-per-view), and audio / video retrieval (e.g. video-on-demand and audio library).

Non Realtime VBR (Non-Real-time Variable Bit Rate): Can be used for data transfers that have critical response-time requirements such as airline reservations, banking transactions, and process monitoring.

Realtime VBR (Real-time Variable Bit Rate): Used by time-sensitive applications such as real-time video. Rt-VBR service allows the network more flexibility than CBR.

Quality of Service: Can be enabled only for UBR without PCR, UBR with PCR, and Non Realtime VPR.

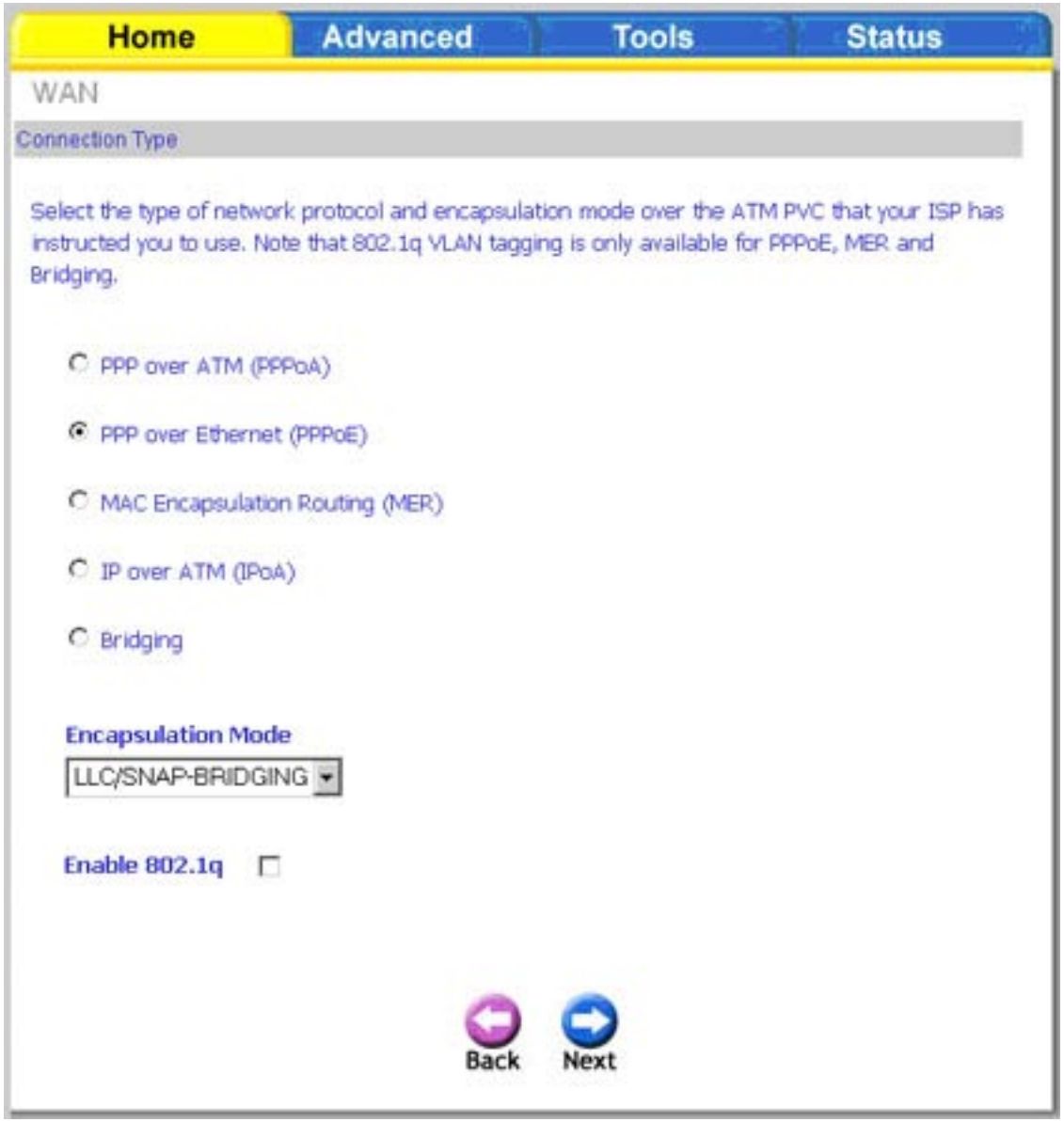
This screen shows the types of network protocols and encapsulation modes that can be configured:

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

Select the type of network protocol and encapsulation over the ATM PVC that your ISP has instructed to use.

If you will be using VLAN tagging, click on the Enable 802.1q checkbox and then enter the VLAN ID number. When finished with your selections, click **Next** to continue.

Note: *These settings are ISP dependant. For information regarding proper configuration, contact your ISP.*



The following screen allows you to enter PPP username and password as well as make any selections regarding your connection.

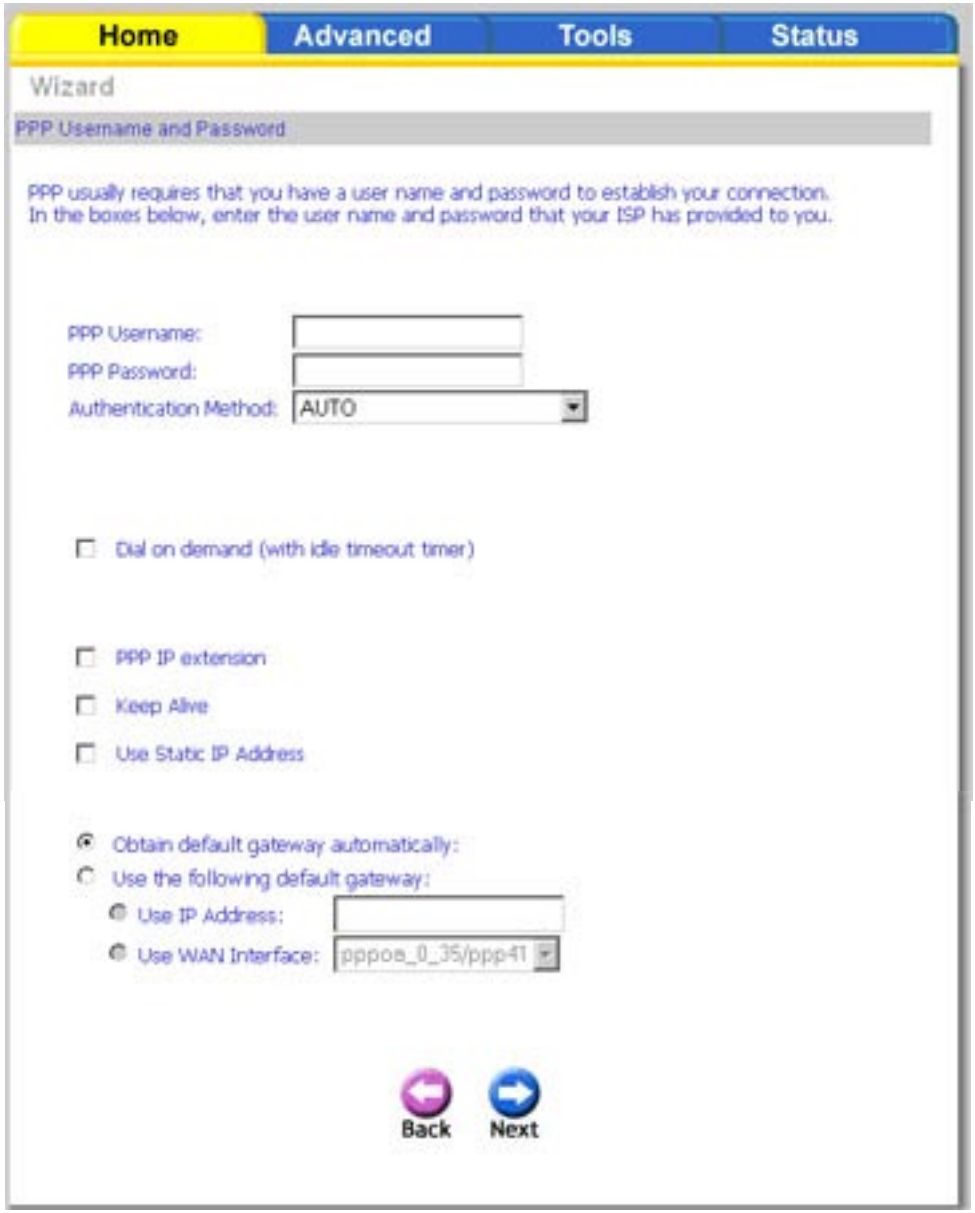
Dial on demand: Allows you to manually connect to the Internet so you are not permanently connected. Idle timeout timer is included.

PPP IP extension: Used by some ISP's. Check with your ISP to see if it is required.

Keep alive: Keeps you connected to your ISP even when no activity is present for a certain period of time.

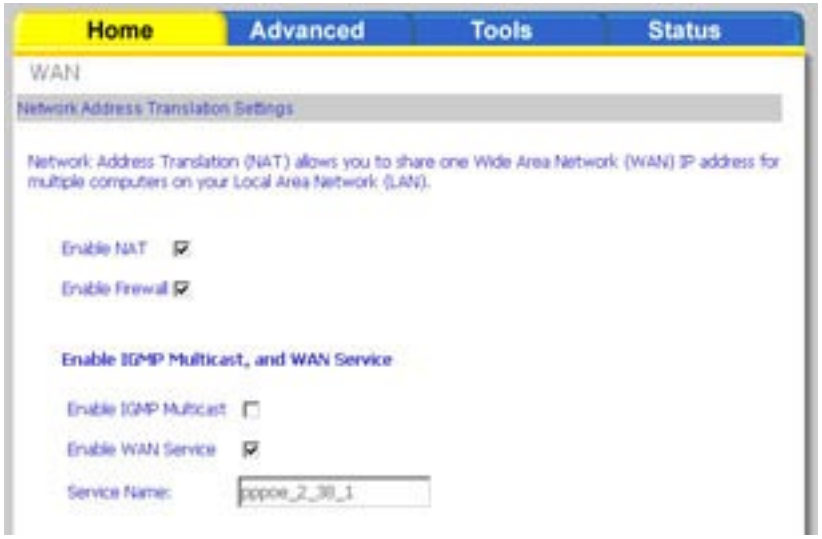
Use static IP address: Select if you want to use a non-DHCP issued IP address to connect to the Internet. If selected, you will be asked to enter the static IP address.

Note: *These settings are ISP dependant. For information regarding proper configuration, contact your ISP.*



When finished, click **Next** to proceed to the NAT Settings screen.

This screen allows you to configure the Network Address Translation settings for the router.



Enable Select enable if you wish to share one WAN IP address for multiple computers on your LAN.

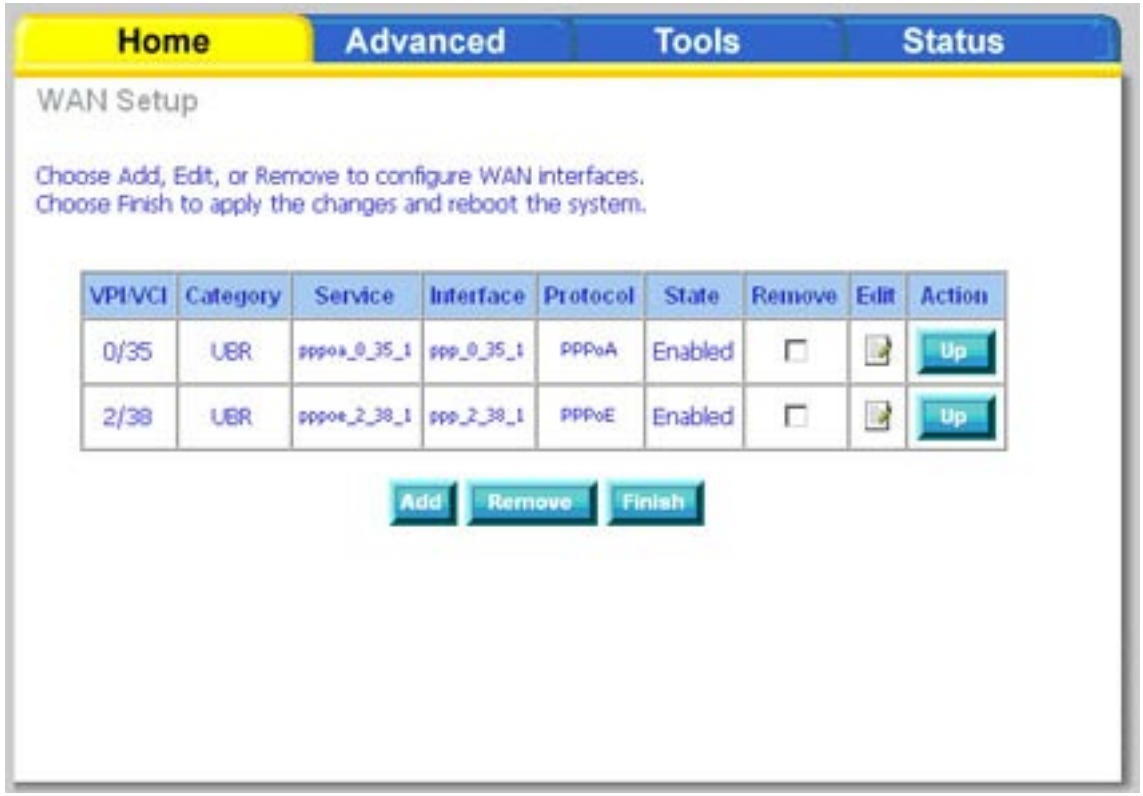
Enable Firewall: Select if you wish to enable the router's firewall for security.

Enable IGMP Multicast: Select enable if you wish to be able to provide multicasts, mostly used in video streaming.

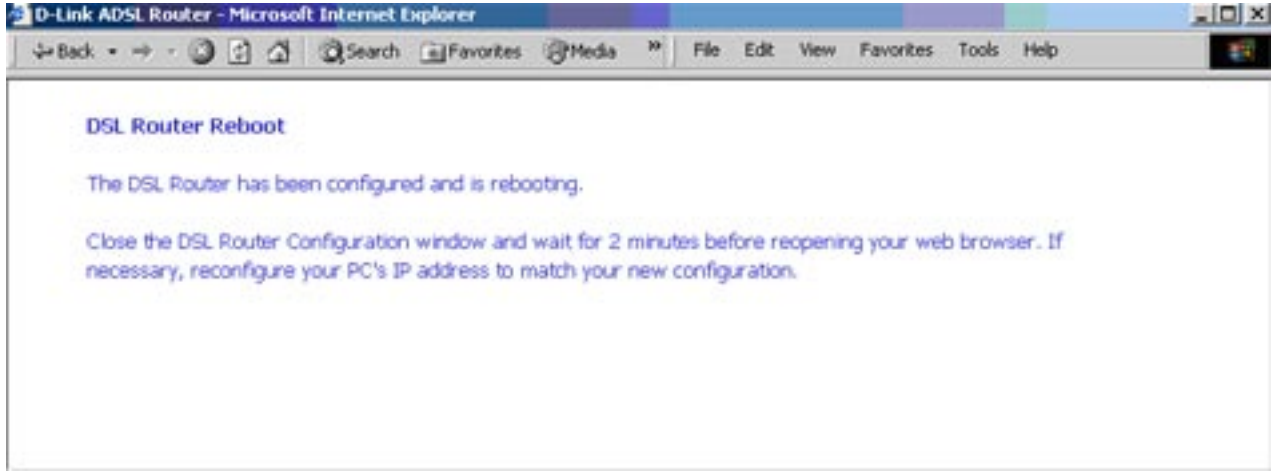
Enable WAN Select if you wish to enable WAN service and then set the Service Name.

When finished, click the **Next** button and the following WAN summary screen will be displayed. This screen will outline all WAN settings for review. When satisfied with the settings click the **Apply** button.

After you apply the configuration, it will return you to the WAN Setup screen showing the new configuration. Select the **Finish** button to save the changes and reboot the router.



When the router restarts the DSL Router Reboot screen will appear during the reboot process. Close the DSL Configuration window and wait at least two minutes before reopening your web browser.

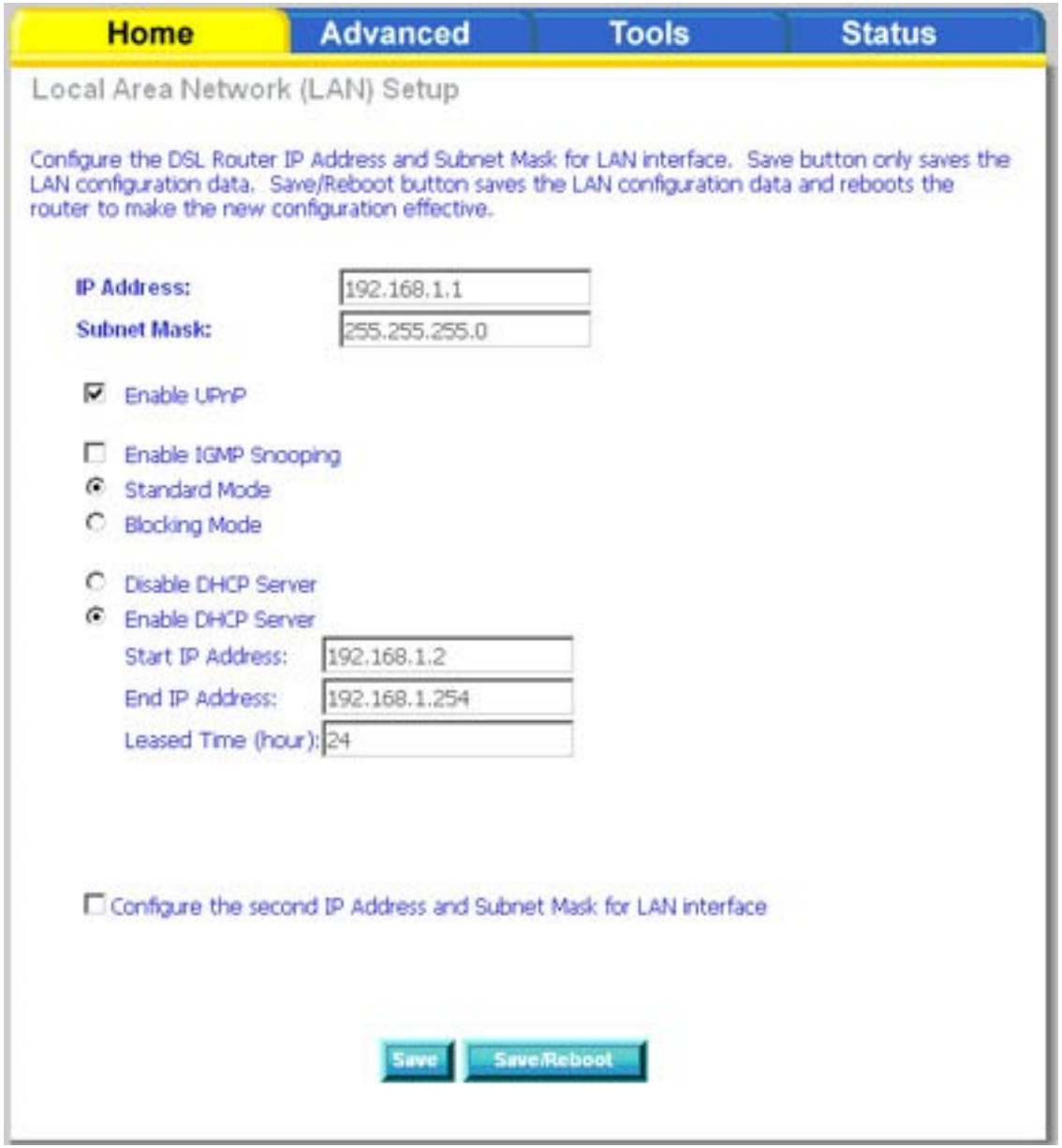


LAN

You can configure the DSL Router IP address and Subnet Mask for the LAN interface.

If you will be multicasting (e.g. video streaming) you can enable IGMP snooping. IGMP snooping allows the router to efficiently determine where the multicast traffic came from and where it is headed. There are two IGMP snooping options: standard or blocking mode.

If you want the DHCP server to automatically assign IP addresses, select enable DHCP server and enter the range of IP addresses that the DHCP server can assign. Select Disable DHCP server if you would like to manually assign IP addresses.



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

DNS

DNS Server Configuration

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

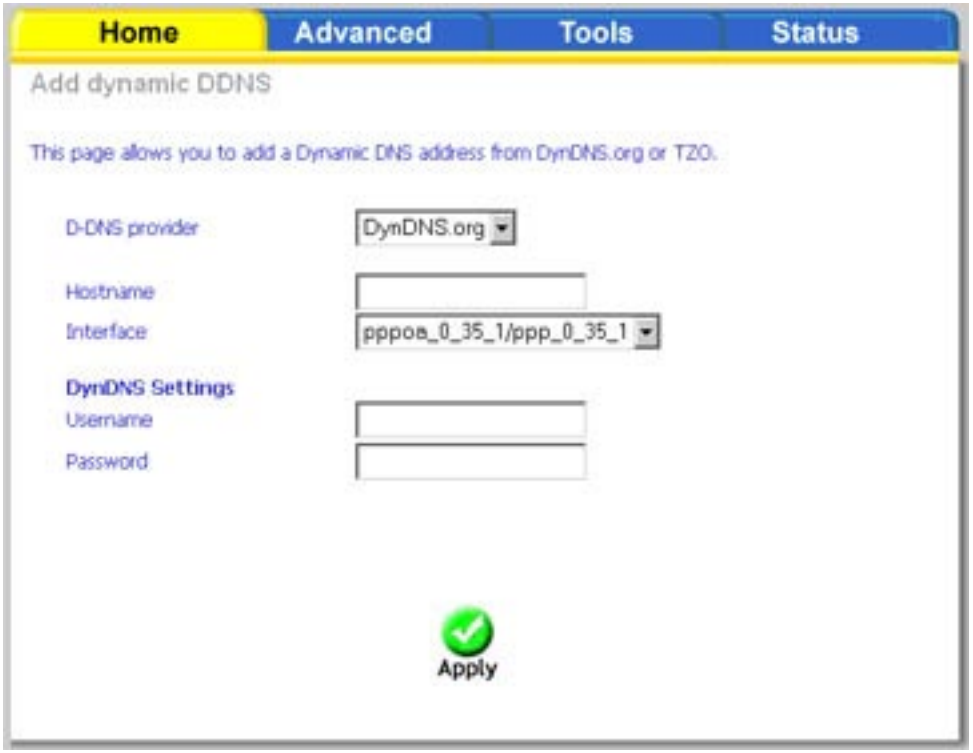
If you uncheck the **Enable Automatic Assigned DNS** checkbox, two additional fields will appear (**primary** and **secondary DNS server)**. Enter one primary and one secondary DNS address in each field. Click **Apply** to save the configuration.

Dynamic DNS

Dynamic DNS is a service for allowing an Internet domain name to be assigned to a changing IP address. This makes it possible for other sites on the Internet to establish connections to you without needing to track the IP address themselves.

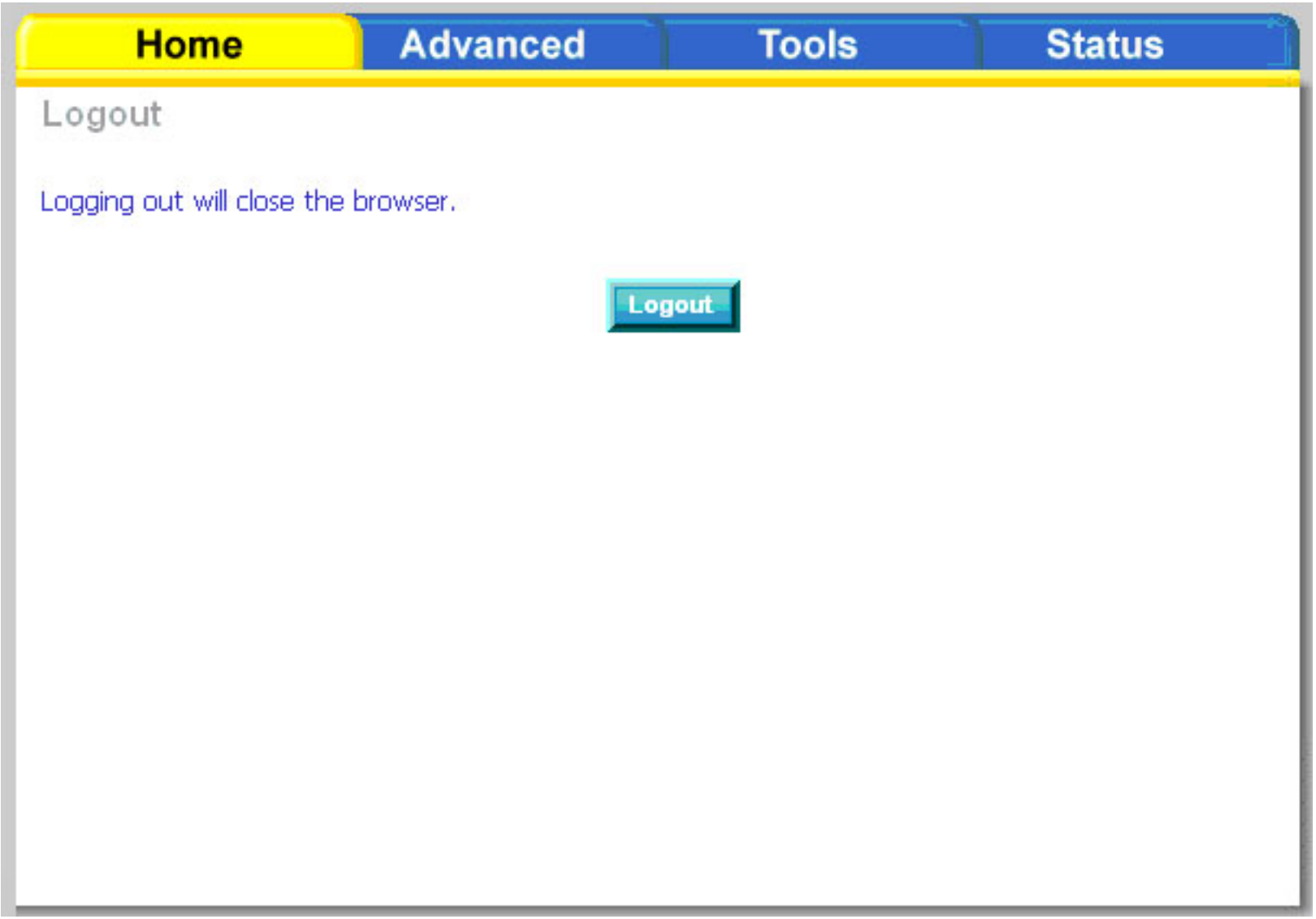
Click on **Add** to set up a dynamic DNS configuration.

This screen allows you to add a dynamic DNS address from DynDNS.org or TZO. First select the DDNS provider (*DynDNS.org or TZO)*, from which you have obtained a dynamic DNS address. Enter the hostname and the interface that you are using. Also enter the username and password assigned by the DNS service. Click on **Apply** to save these configurations.



Logout

To log out of the router's user interface at any time during the setup, click on the **Logout** button. A confirmation screen will appear confirming that you really want to log out.

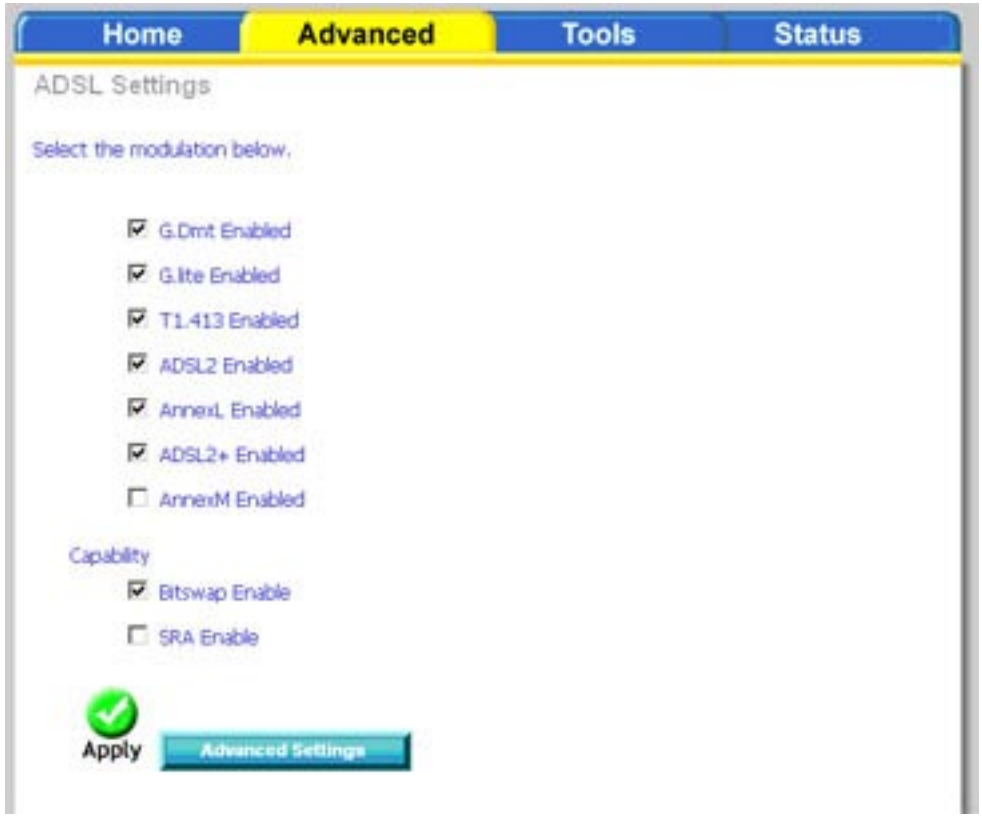


Advanced Setup

This section of the setup is an advanced version of the quick setup. If you want to make specific configurations to your router such as creating a virtual server, DMZ, RIP, Quality of Service (QoS), etc., consider going through this advanced setup for a more comprehensive configuration.

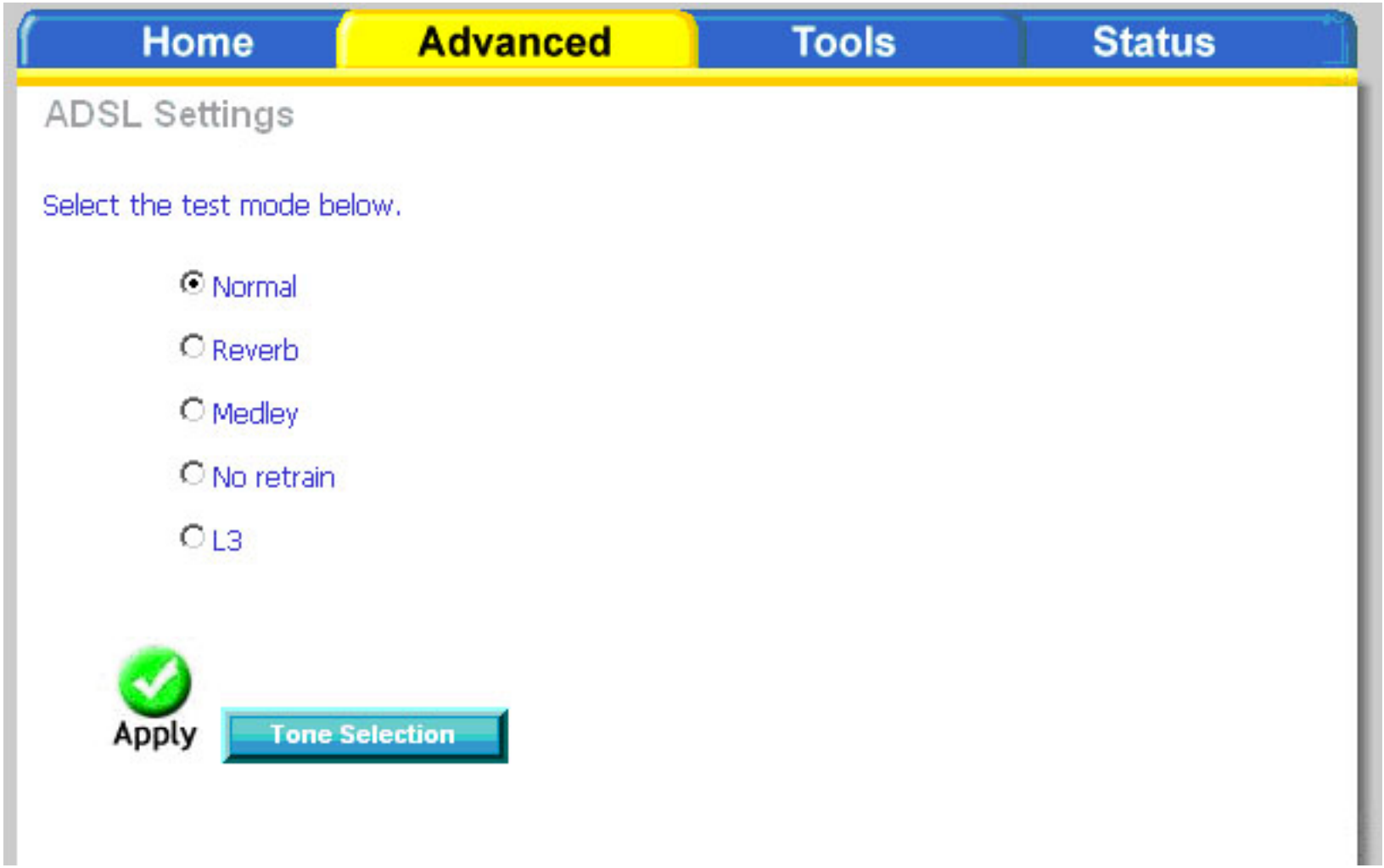
ADSL

The ADSL settings page contains modulation and capability settings. Consult your ISP to determine the correct settings. Click **Apply** if you are finished or click on **Advanced Settings** if you want to configure more advanced settings.



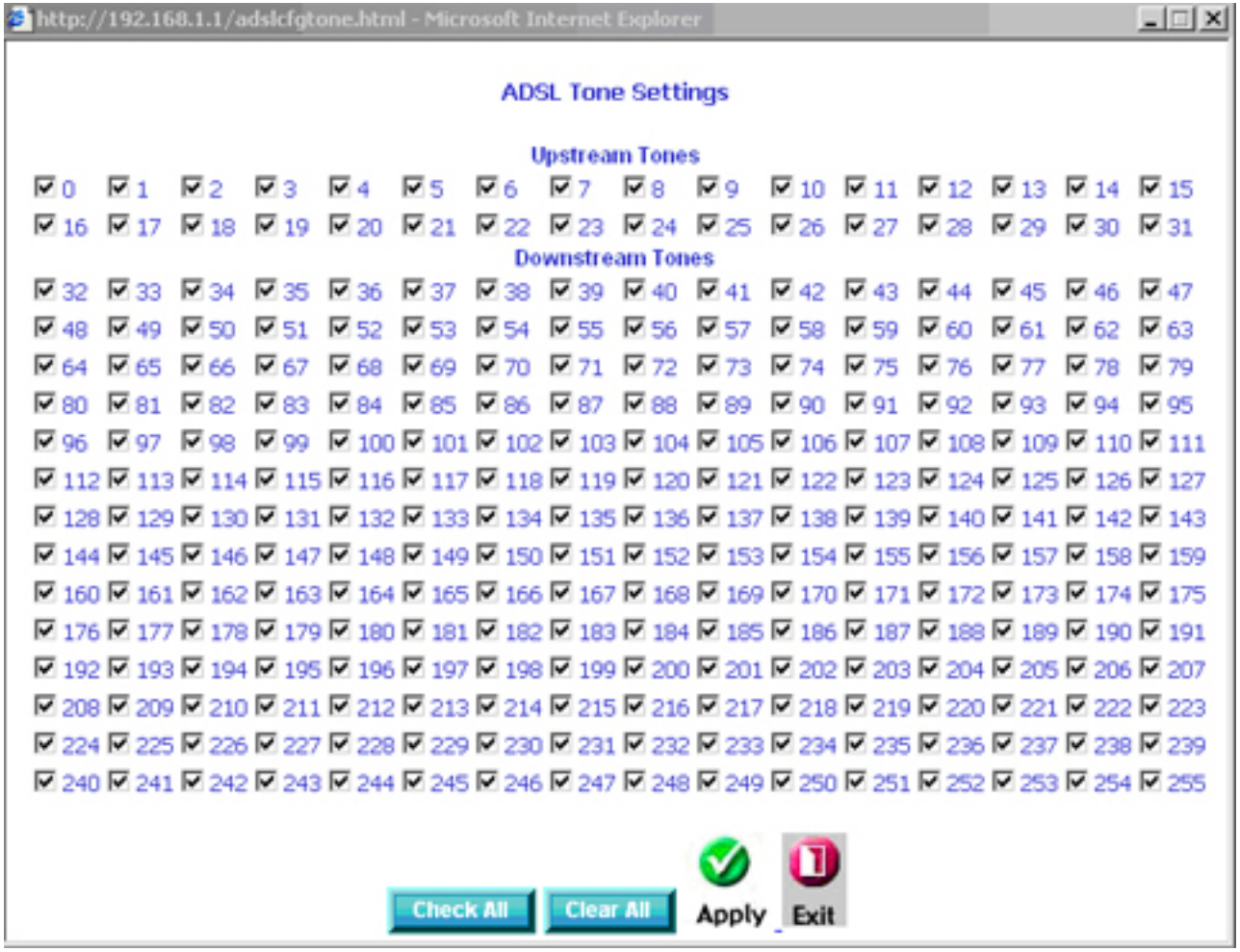
ADSL Settings

The test mode can be selected from the ADSL Advanced Settings page. Test modes include normal, reverb, medley, no retrain, and L3. After you make your selection, click on **Apply** to save these settings first before you go to **Tone Selection**.



ADSL Tone Settings

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



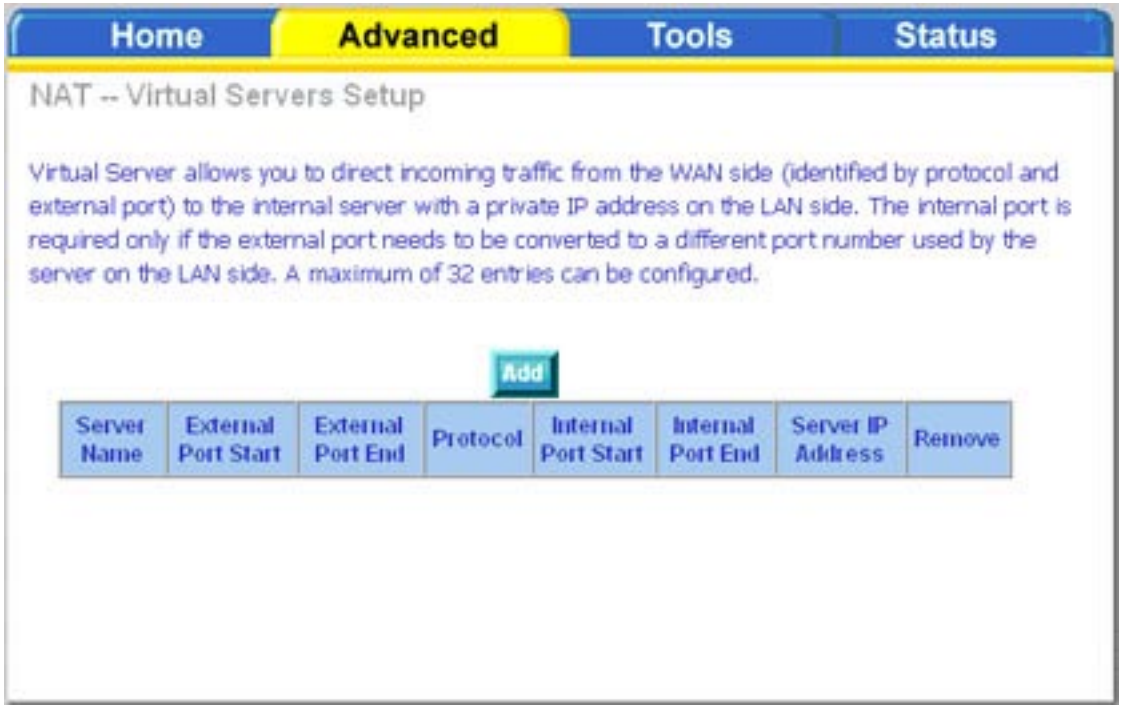
Virtual Server

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

NAT—Virtual Servers Setup

A virtual server allows you to direct incoming traffic from the WAN side to a specific IP address on the LAN side. This is useful if you have software that requires communication with the Internet (e.g. peer-to-peer, games, etc.).

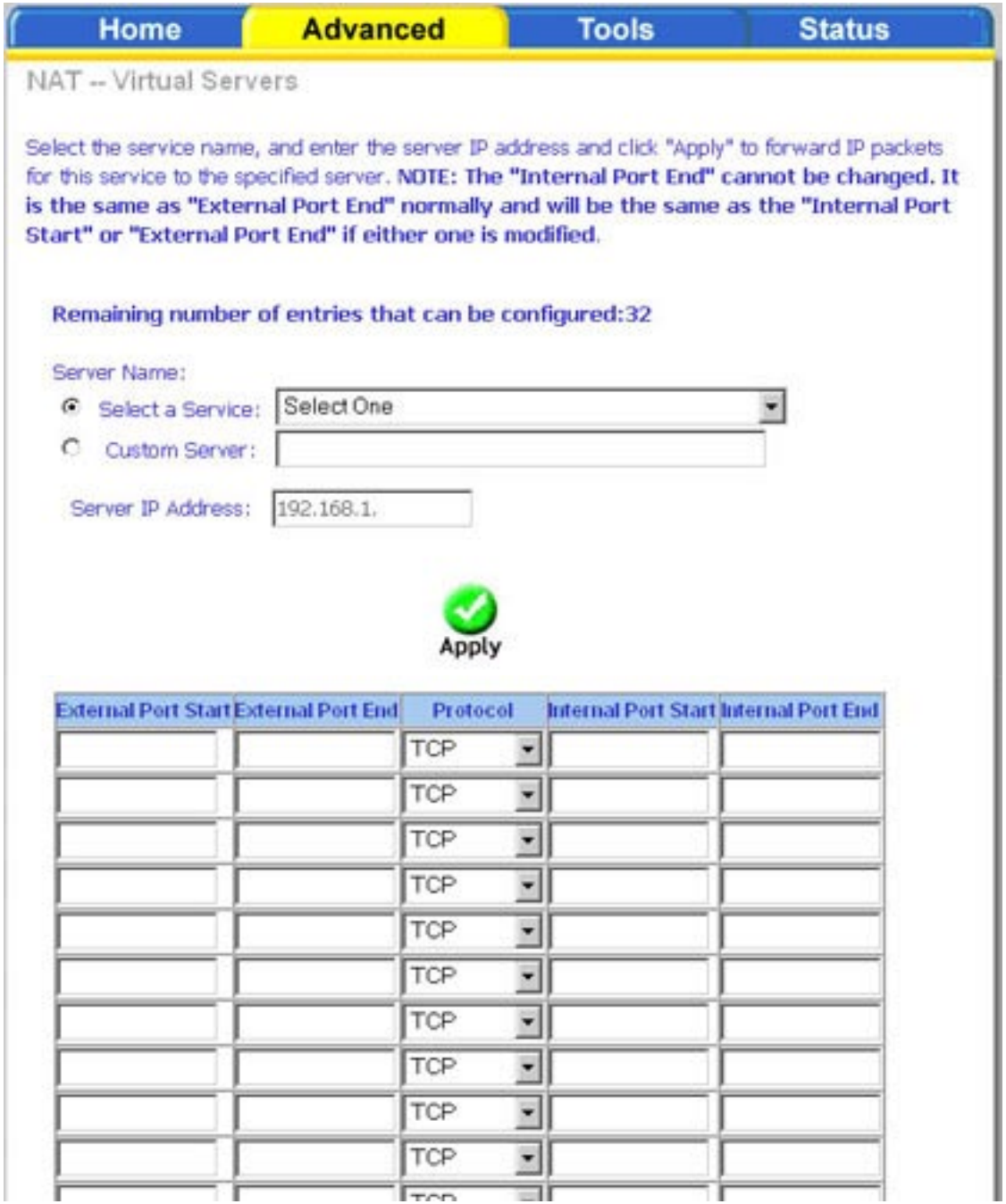
This figure shows the Virtual Servers Setup page that allows you to configure your virtual server(s). Click on the **Add** button to configure a virtual server.



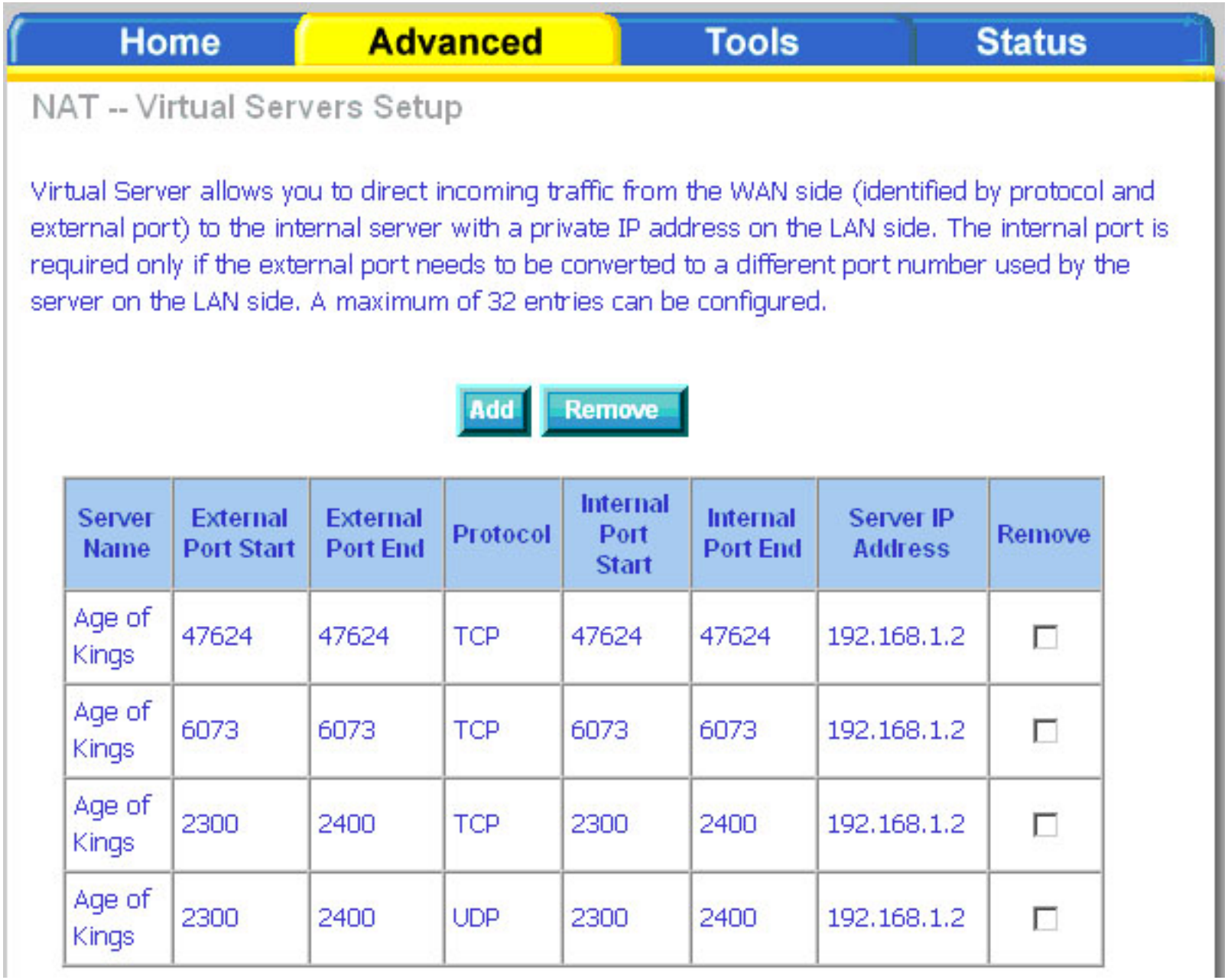
Select a virtual server from the drop-down list and then enter the server IP address. The Server IP Address would normally be the IP address of the computer on your network which is using the application or game.

To determine your IP address see **Networking Basics** in the Appendix section of this manual.

Once you are satisfied with your selection, click **Apply** once.



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 its check box in the Remove column and click on the **Remove** button.



Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Remove
Age of Kings	47624	47624	TCP	47624	47624	192.168.1.2	☐
Age of Kings	6073	6073	TCP	6073	6073	192.168.1.2	☐
Age of Kings	2300	2400	TCP	2300	2400	192.168.1.2	☐
Age of Kings	2300	2400	UDP	2300	2400	192.168.1.2	☐

DMZ

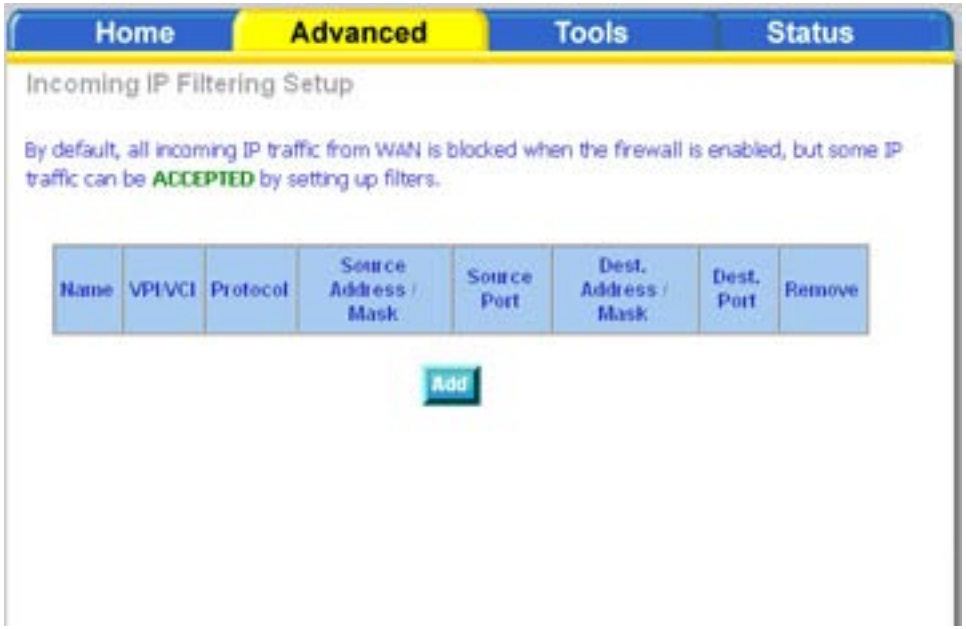
You can define the IP address of the DMZ Host on this screen. The DMZ is used to forward all IP packets coming into the router to a specified IP address. Enter the IP address and click **Apply**.

IP Filter

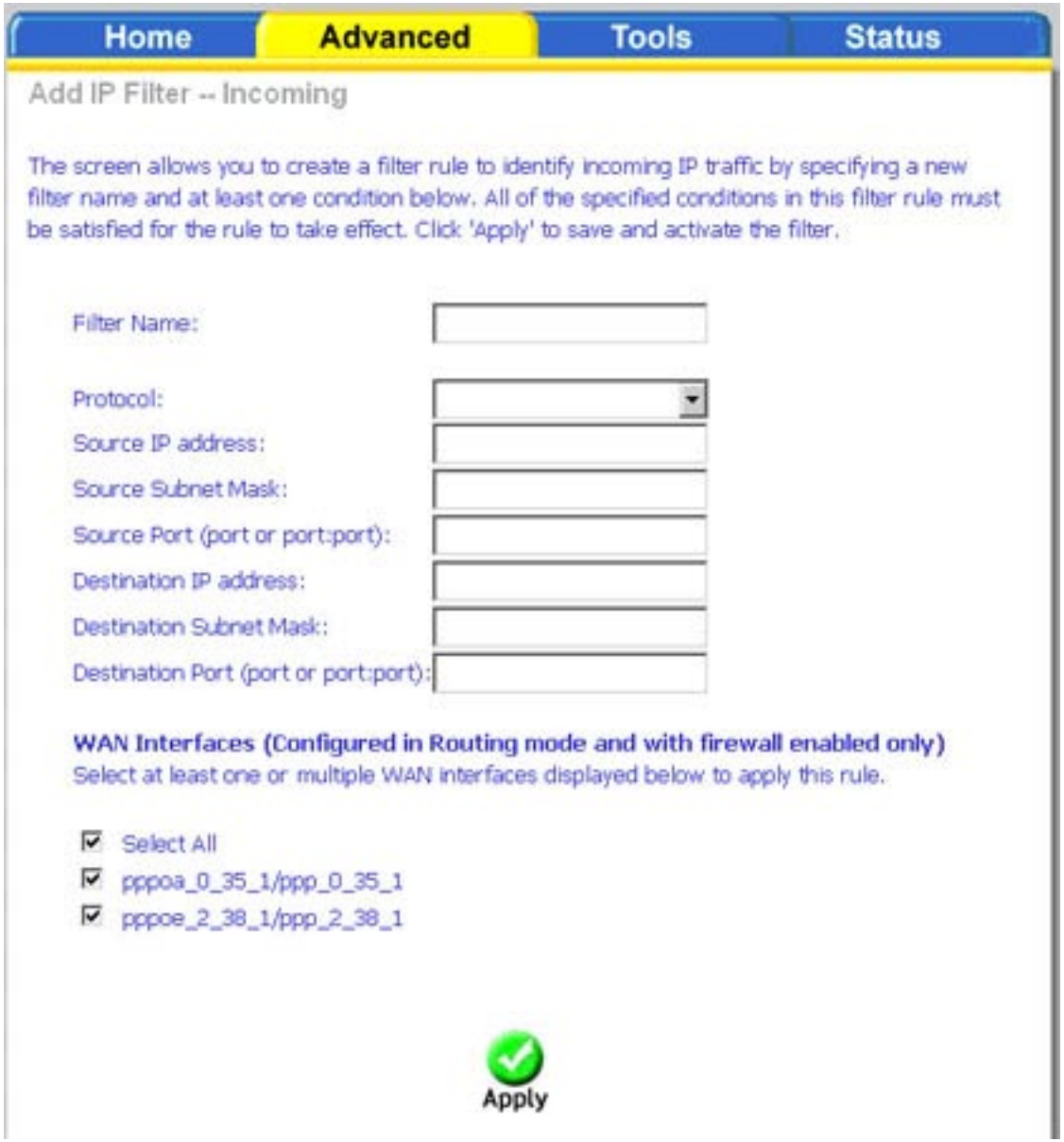
IP filters can be configured to manage your incoming and outgoing traffic. This is useful to allow or block certain traffic through the router. Click on the **Inbound** or **Outbound** buttons to configure the inbound and outbound filters.

Incoming IP Filtering Setup

An Incoming IP filter allows you to specify which WAN traffic is allowed to pass through the firewall. Click on the **Add** button to add incoming filter settings.



This next screen will appear when you click **Add**. Enter the filter name, select the Protocol, enter source information (from the WAN side), and destination information (to the LAN side). Make sure at least one or multiple WAN interfaces are selected to apply the rule. Click **Apply** to save.

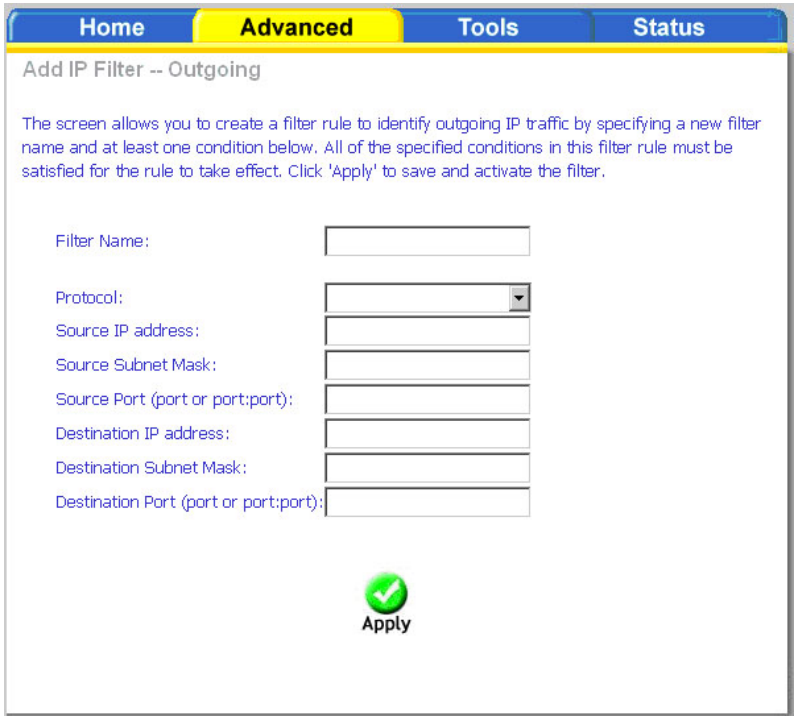


The following screen appears when you apply the IP filter. The screen lists the IP filters that were added from the previous screen. To add another filter click **Add.** To remove any previously created filter, place a checkmark next to the filter in the “Remove” column and click **Remove**.

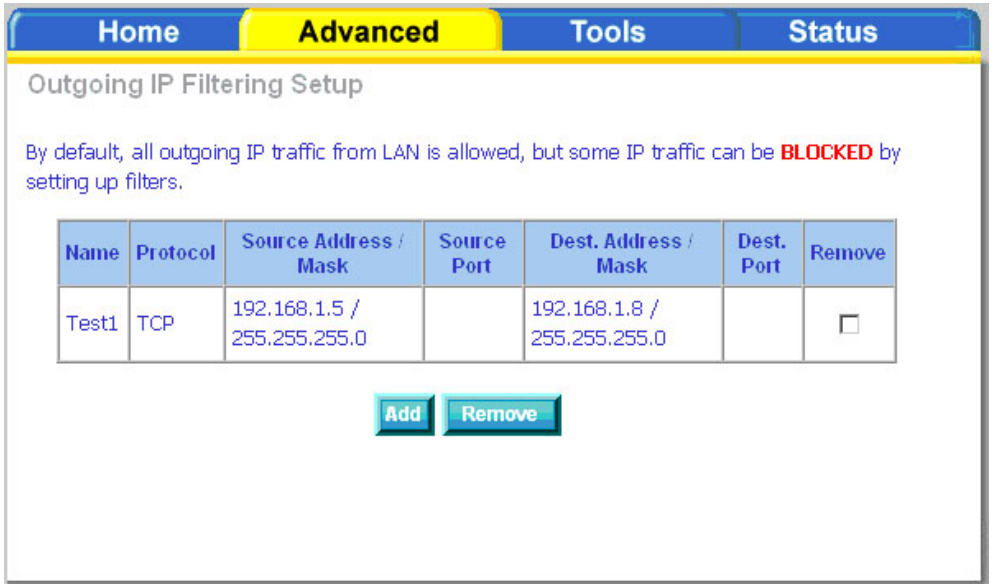
Outgoing IP Filtering Setup

An Outgoing IP filter allows you to specify which LAN traffic is blocked from passing through to the WAN side (Internet). Click on the **Add** button to add outgoing filter settings.

This next screen will appear when you click **Add**. Enter the filter name, select the Protocol, enter source information (from the LAN side), and destination information (to the WAN side). Click **Apply** to save the filter.



The following screen appears when you apply the IP filter. The screen lists the IP filters that were added from the previous screen. To add another filter click **Add.** To remove any previously created filter, place a checkmark next to the filter in the "Remove" column and click **Remove**.

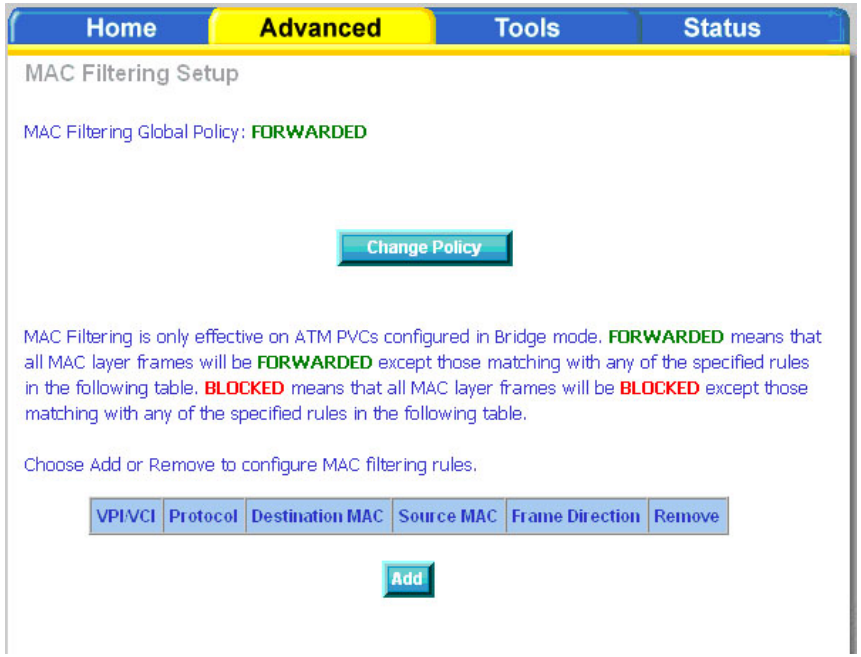


Bridge Filters

MAC Filtering Setup

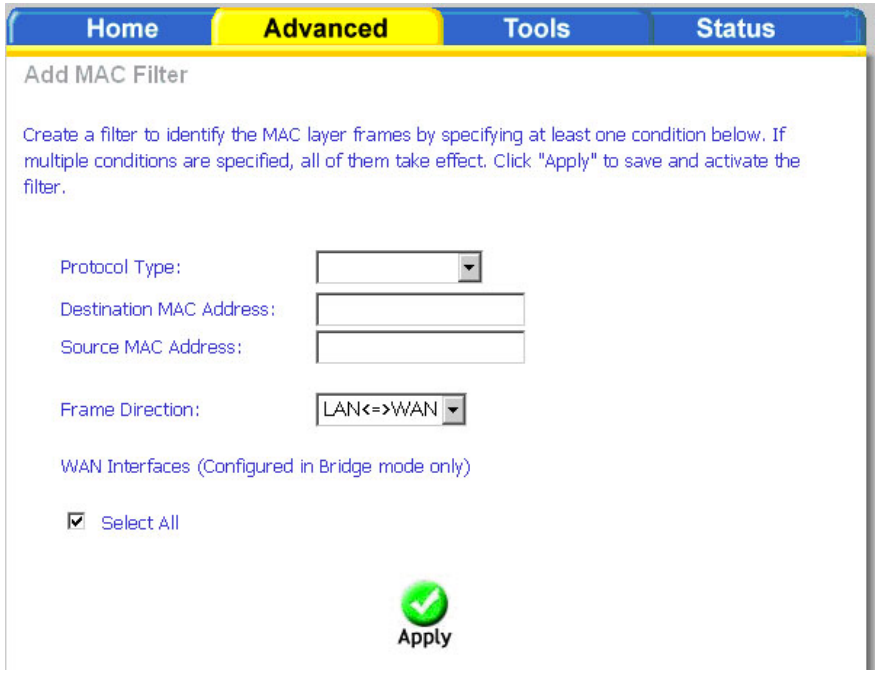
MAC filtering can forward or block traffic by MAC address. You can change the policy or add settings to the MAC filtering table using the MAC Filtering Setup screen.

Forwarded means that all MAC layer frames will be forwarded except those matching any specified rules. **Blocked** means all MAC layer frames will be blocked except those matching any specified rules.



If you click **Change Policy**, a confirmation dialog allows you to verify your change. Select **Yes** to continue, or **No** to to cancel.

If you want to add an entry to the MAC filtering table, Select **Add** from the MAC Filtering Setup screen. The Add MAC Filter screen should then appear. Select a Protocol Type, enter the Destination and Source MAC address, the necessary Frame Direction, and WAN interface (bridge mode only). Click **Apply** to save.



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

Parental Control

Time of Day Restrictions

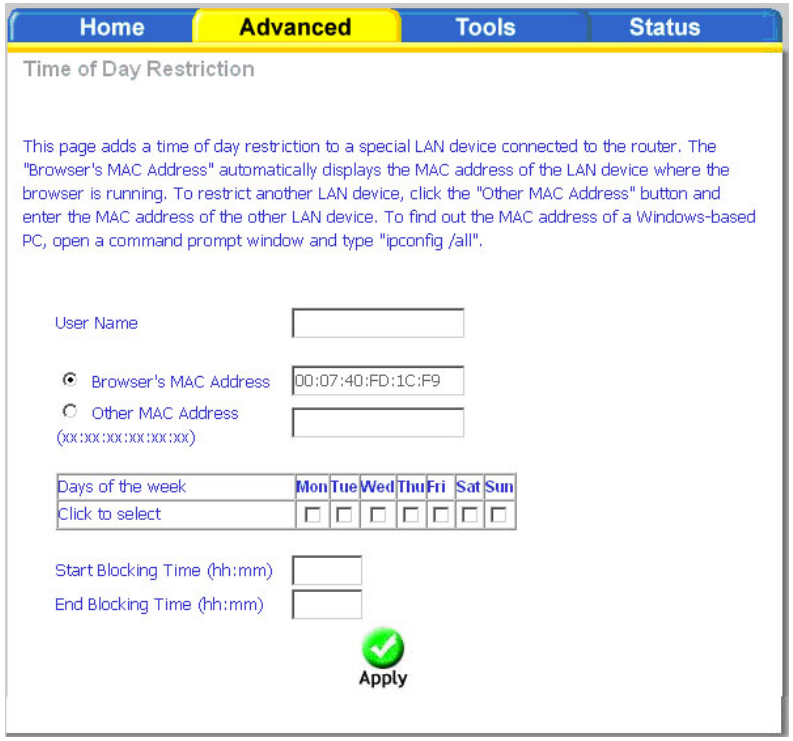
In a home setting, parents can disallow access to the router (and the Internet) by creating special rules called **Time of Day Restrictions.** Using these restrictions, parents can define the time and days computers on the network are allowed to access the Internet.

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

After you click you **Add**, you will see the Time of Day Restriction Add screen. Enter the MAC address of the computer you wish to place on a time of day restriction, select which days you would like the restriction to be in place, and Enter a start and end blocking time.

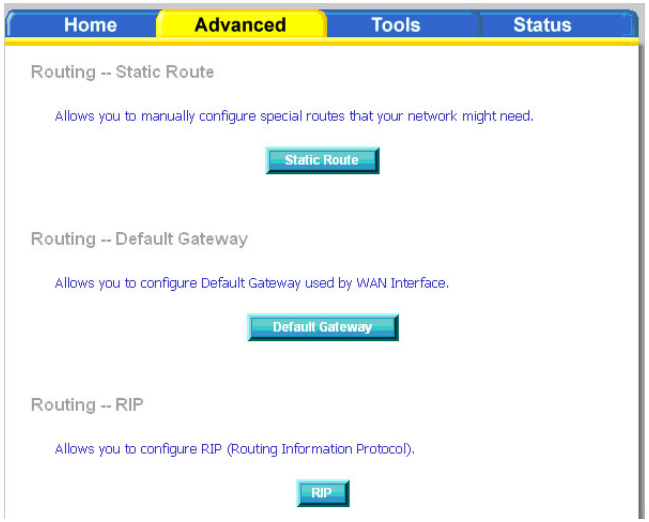
To determine the MAC address of a computer see “Networking Basics” in the Appendix section of this manual.

Click **Apply** to save the settings and continue.



Routing

There are three sections under the Routing Page in Advanced Settings. The Static Route section allows you to manually configure any specific routes that may be needed. The Default Gateway section allows you to configure the default gateway used by the WAN interface. The RIP function allows you to configure RIP (routing information protocol).

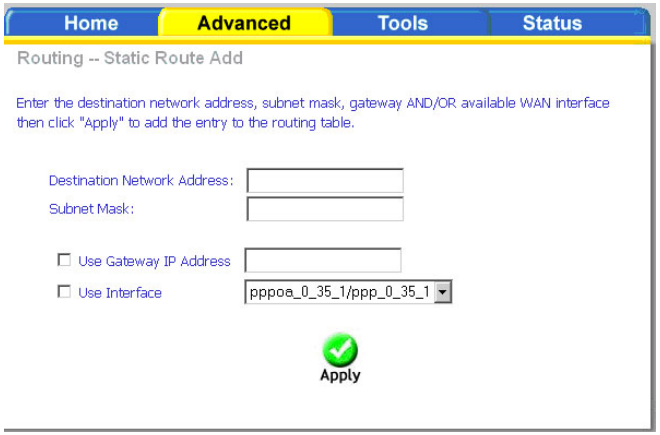


Clicking on any of the three buttons(**Static Route**, **Default Gateway**, or **RIP)**, will bring you to its associated page.

Routing--Static Route

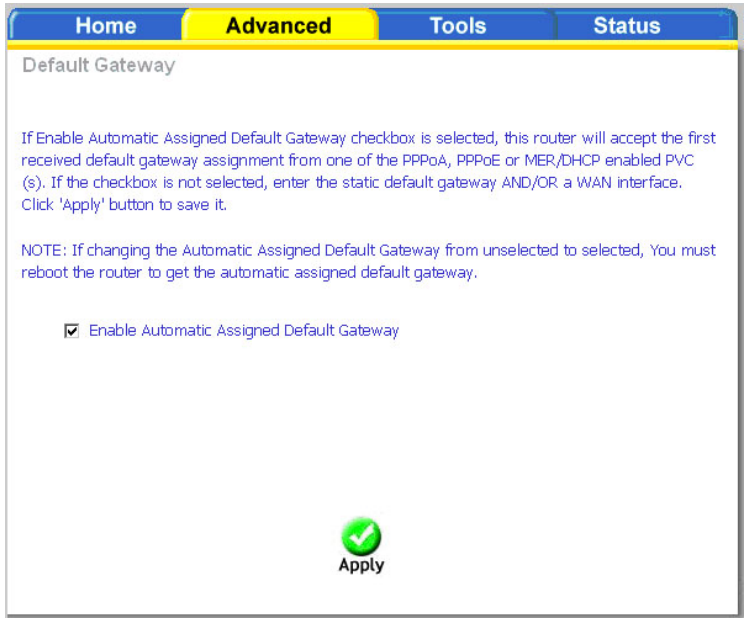
The Static Route page can be used to add a routing table (a maximum of 32 entries can be configured). To proceed, click on **Add**.

On the Static Route Add page, enter the destination network address, subnet mask, gateway IP address, and select an available WAN interface. When complete, click **Apply**.



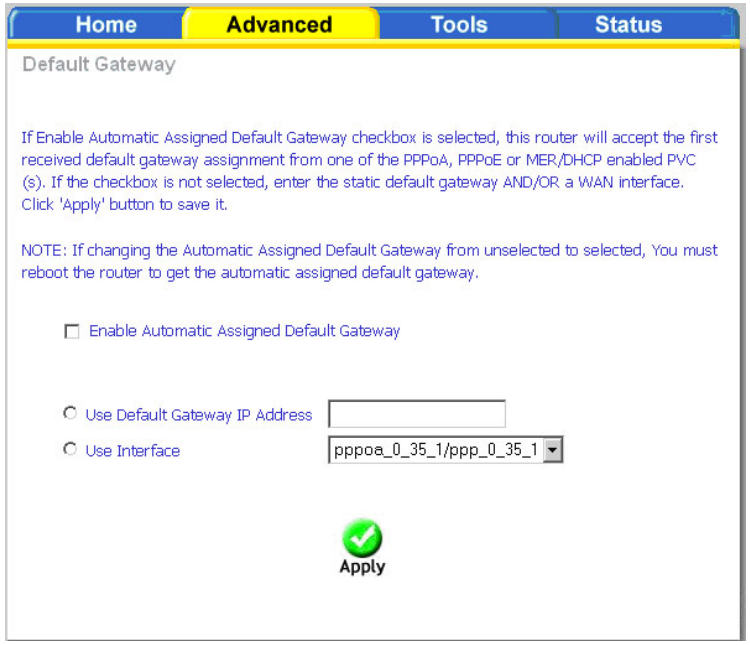
Routing--Default Gateway

If the Automatic Assigned Gateway checkbox is selected the router will automatically attempt to obtain a gateway IP address from your ISP. If you uncheck the Enable Automatic Assigned Default Gateway, you can manually assign a gateway address.



This shows the Default Gateway screen when the Enable Automatic Assigned Default Gateway is unchecked. Enter a gateway IP in the Use Default Gateway IP Address field and/or select a WAN Interface.

When ready, click **Apply**.

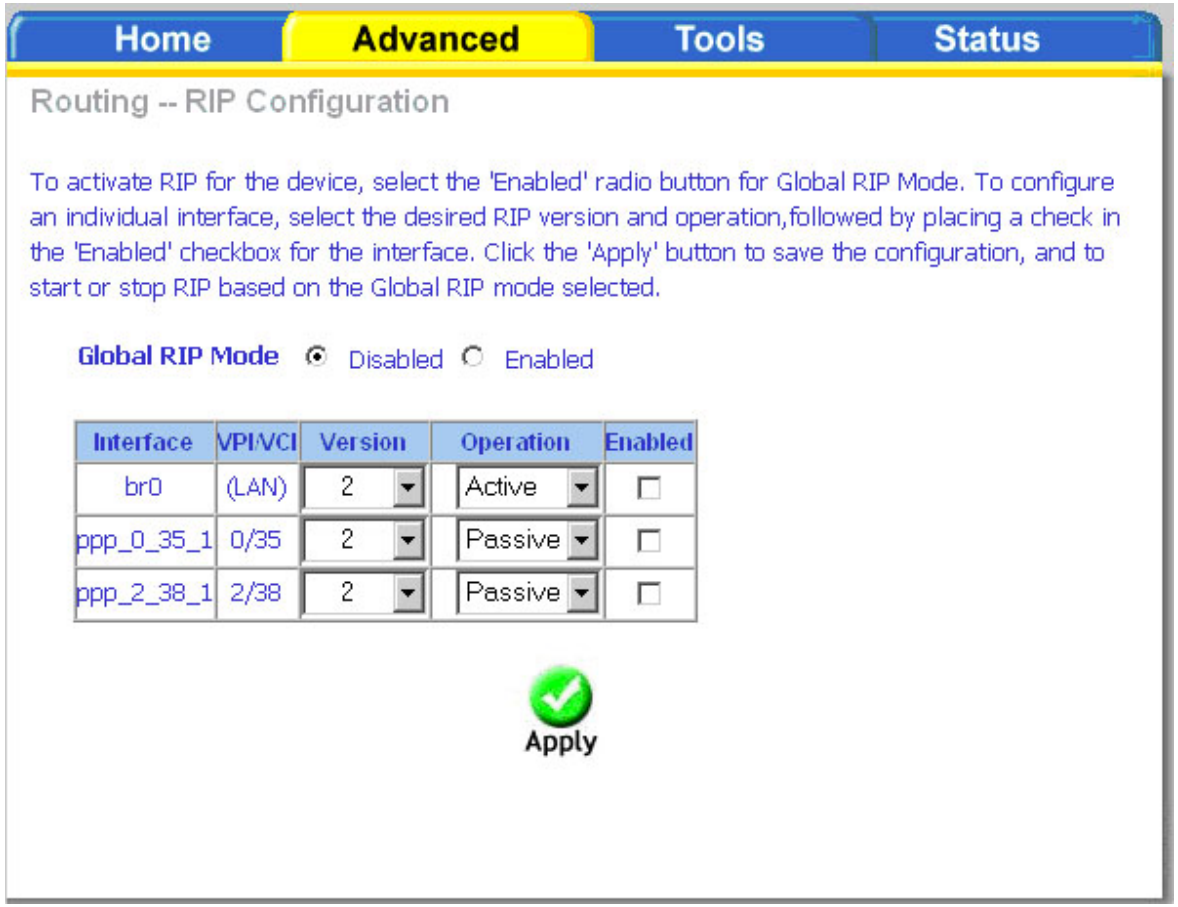


RIP

RIP (Routing Information Protocol) is a process of moving a packet from one node to another by forwarding the packet to the next router. It determines a route based on the smallest hop count between source and destination routers.

If RIP is enabled, the router operation can be configured as active or passive. Click **Apply** to save any changes.

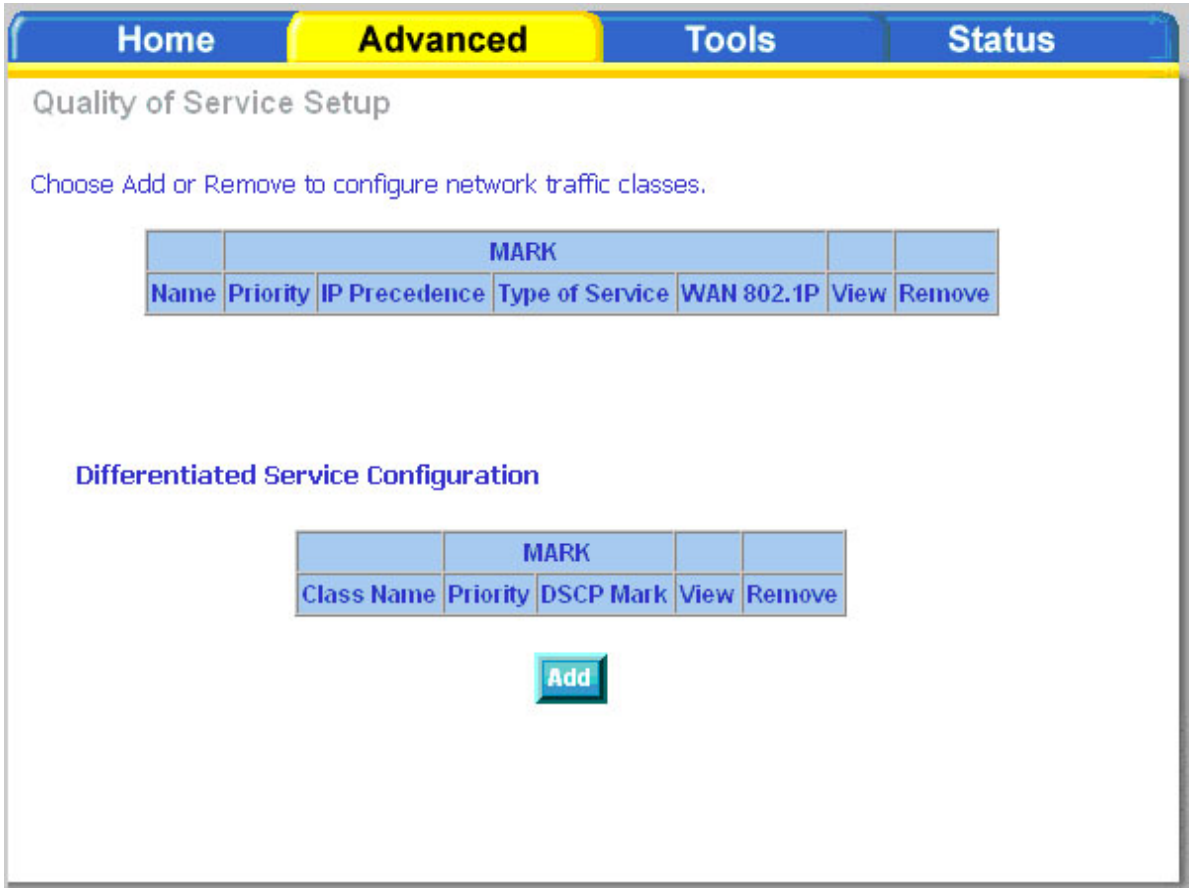
If RIP is set to active, the router will advertise its routes (reachability information) to others; if RIP is set to passive, the router will not advertise its routes, but will listen and update its routes based on other routers' advertisements.



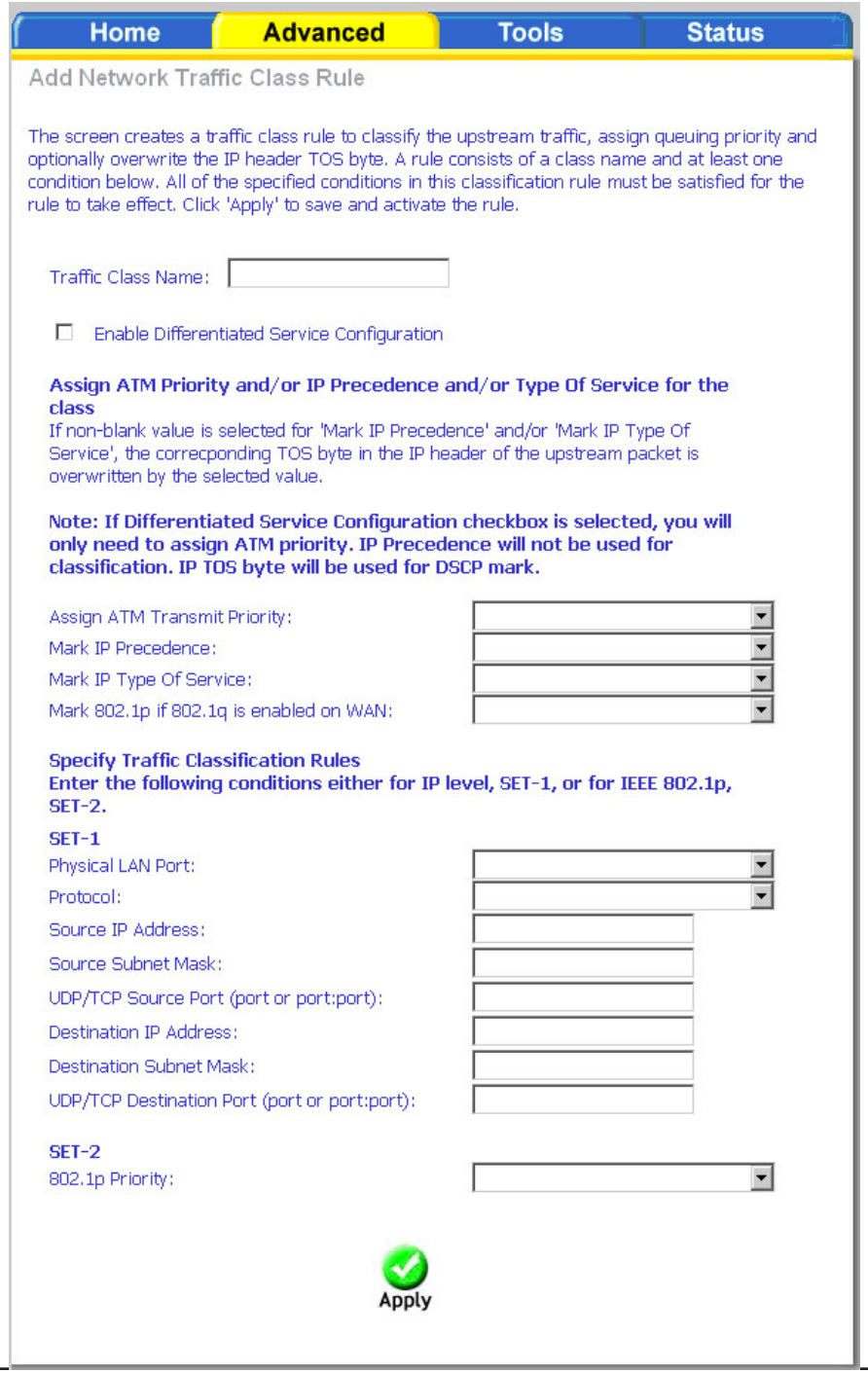
Quality of Service

QoS (Quality of Service) is a method of identifying, classifying and assigning priorities to traffic that passes through the router. This ensures that time sensitive data (e.g. video streaming) is given priority over other non-essential data.

You can configure the Quality of Service to apply different priorities to traffic on the router. Click **Add** to view the Add Network Traffic Class Rule screen.



This screen allows you to add a network traffic class rule. A rule consists of a traffic class name and at least one condition. All configured conditions must first be met before the rule takes effect. Click **Apply** to save any changes.

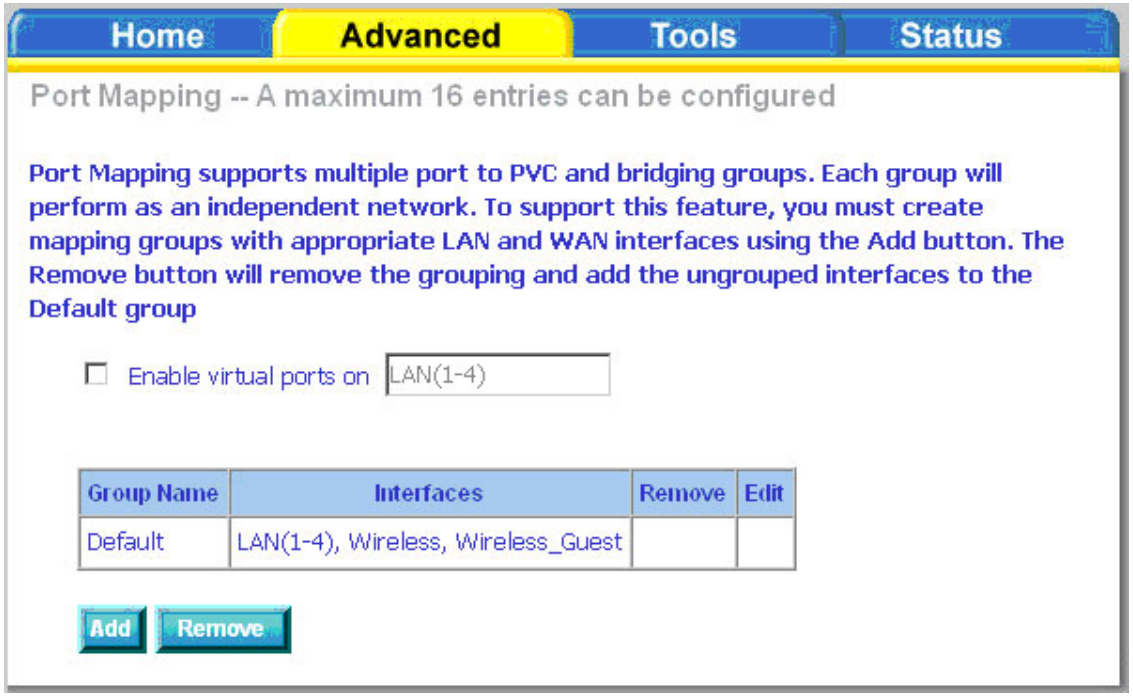


Port Mapping

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 should be created.

Click on the **Add** button to create a mapping group.

If you need to remove an entry, select the checkbox in the remove column next to the desired group and click the **Remove** button.



After clicking the **Add** button, the Port Mapping Configuration screen appears, allowing you to create mapping groups.

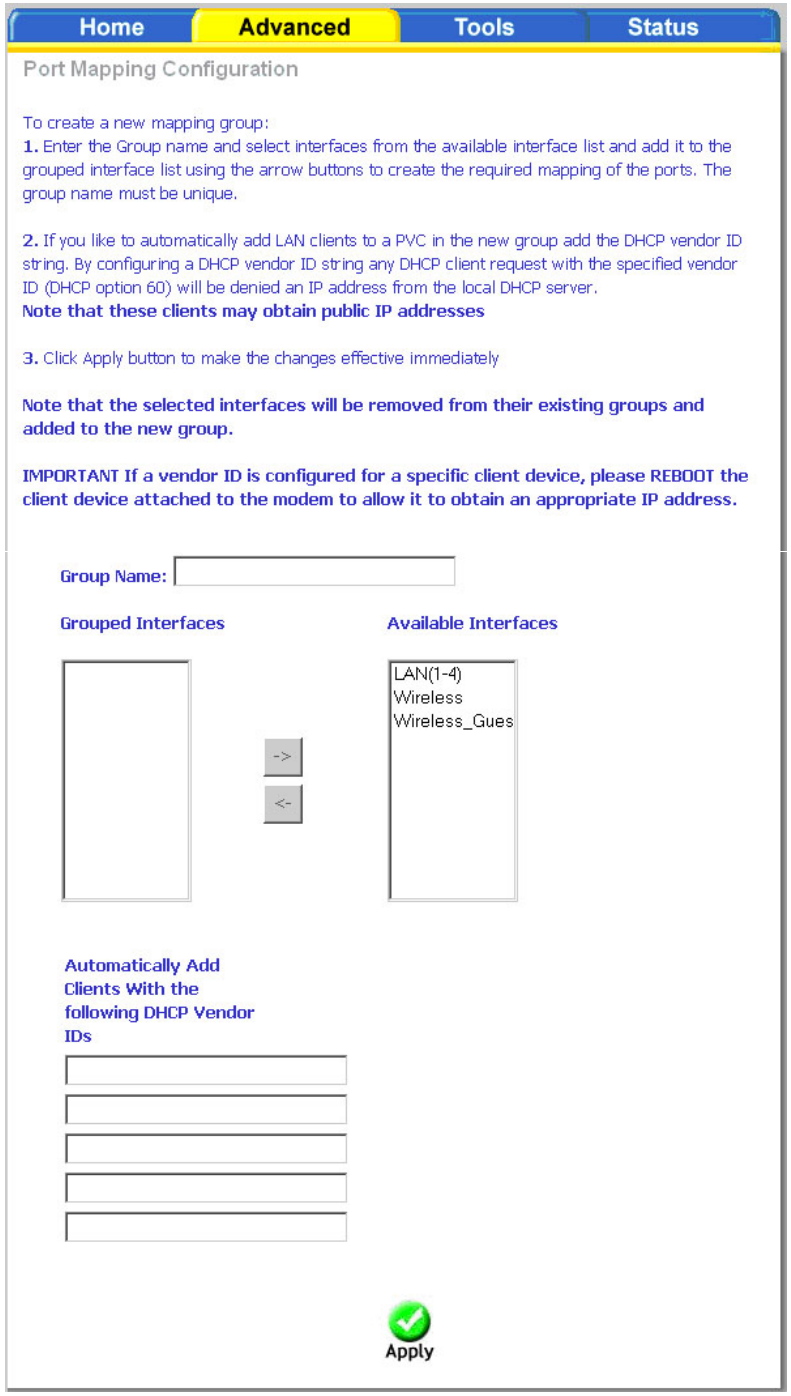
To create a mapping group, enter a group name in the Group Name field.

Then select interfaces from the Available Interface List and add them to the Grouped Interfaces List by using the arrow buttons.

If you want certain LAN clients to be automatically added to a PVC in the group when they connect, enter the clients' DHCP vendor ID in the Automatically Add Clients with the Following DHCP Vendor IDs field.

Note: *Any DHCP client request with the specified DHCP vendor ID will be denied an IP address from the local DHCP server. These clients may obtain public IP addresses from your ISP.*

Click **Apply** when finished.



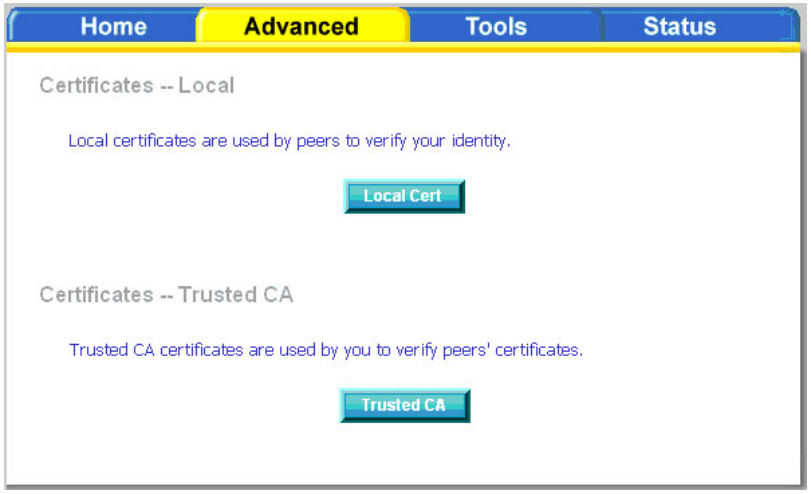
Certificate

Certificates are used to verify your router's identity by clients and other network devices (e.g. switches, other routers) and for your router to verify others identities. There are two types of certificates, Local Certificates and Trusted CA.

Local Certificates are used by your peers to verify your routers' identity. Trused CA Certificates are used by your router to verify your peers' certificates.

Click the **Local Cert.** button to configure your Local Certificates.

Click the **Trused CA** button to configure your Trusted CA Certificates.



Local

A local certificate identifies your router over the network. This page allows you to add, view or remove certificates. A maximum of four certificates can be saved on the router.

To apply for a certificate, click on **Create Certificate Request.**

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

If you selected **Create Certificate Request** the Create New Certificate Request screen will appear. Enter the following information in its appropriate field:

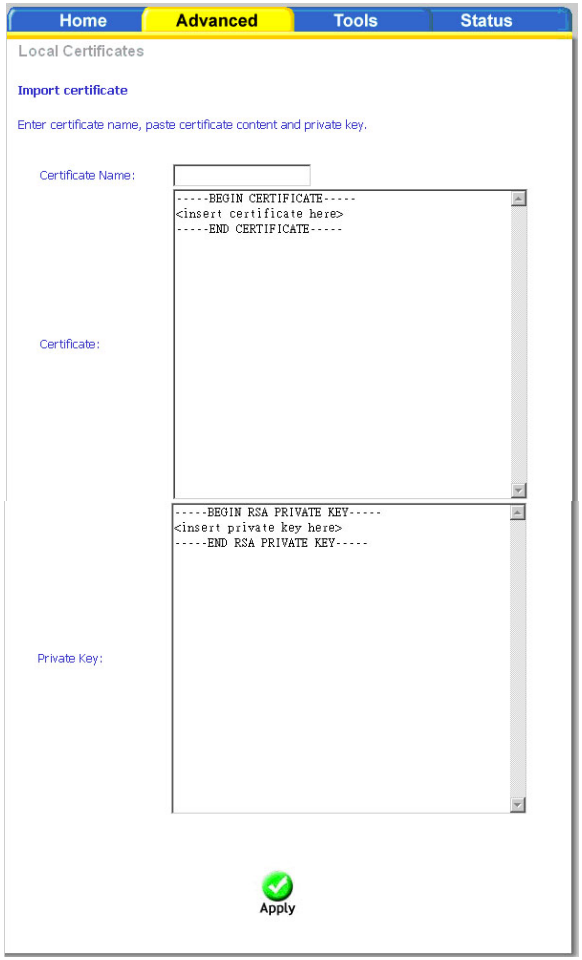
- Certificate name
- Common name
- Organization name
- State/province name
- Country/region name

Click **Apply** to continue.

If you selected **Import Certificate** the Import Certificates screen will appear.

Enter the Certificate Name in the field provided.

Import your existing certificate by pasting the certificate content into the Certificate field and paste the private key into the Private Key field.



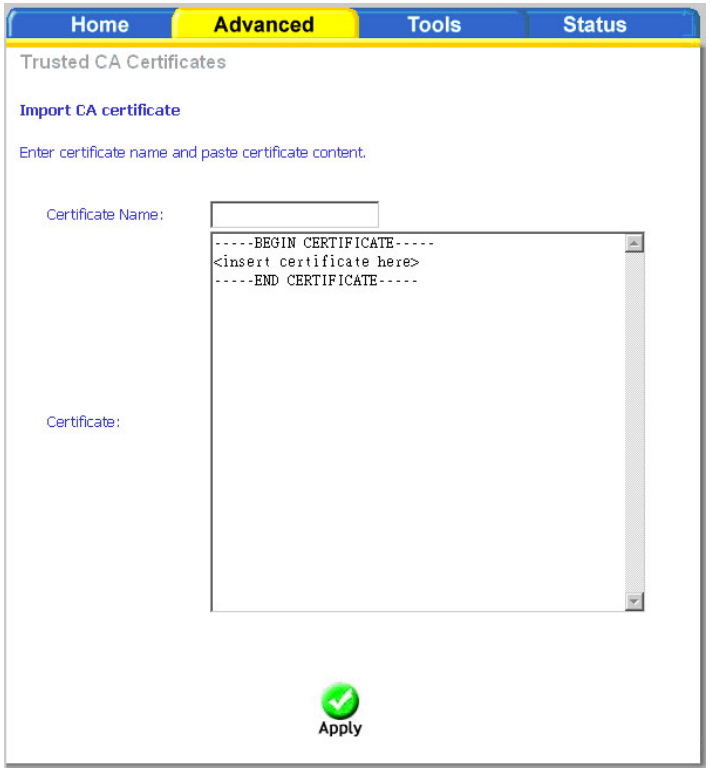
Click **Apply** to submit the request to import the certificate.

Trusted CA

The trusted certificate authority (CA) allows you to verify the certificates of your peers. Note that you can store up to 4 certificates. This screen also allows you to view the CA's that you may have already added and can be removed.

Click **Import Certificate** to continue to the next screen.

Enter the certificate name in the Certificate Name field.

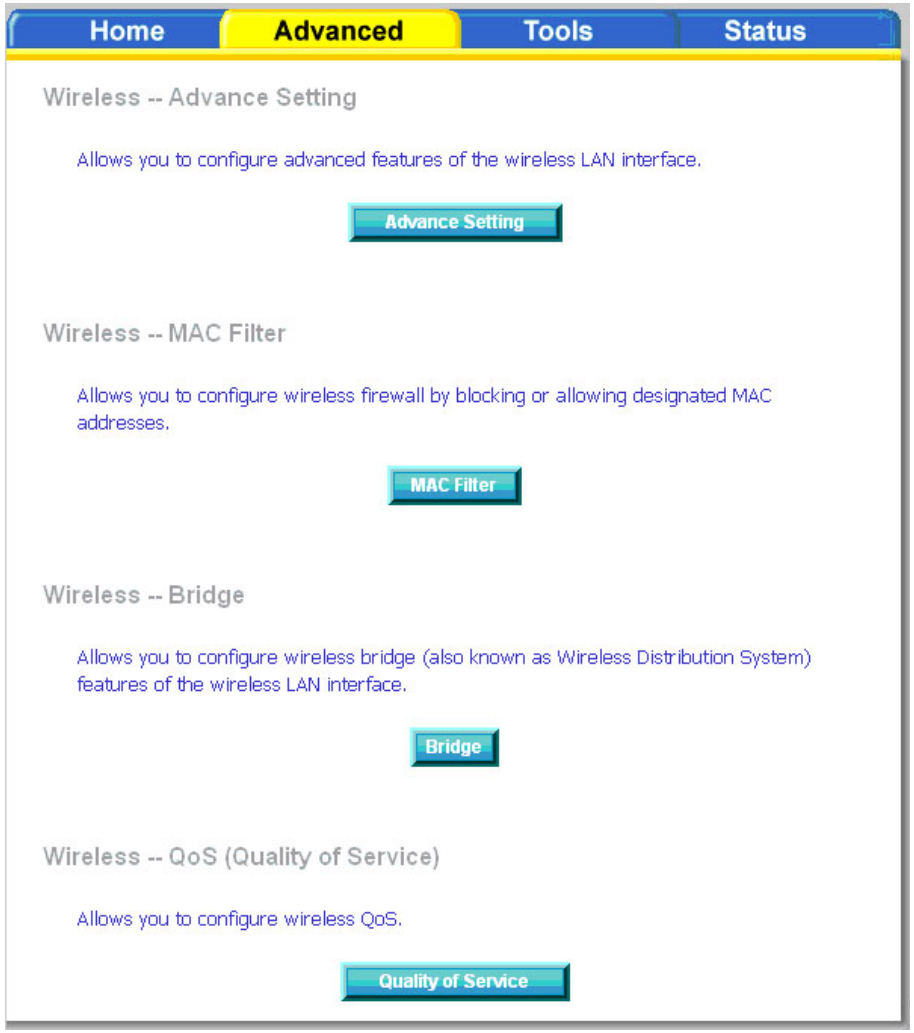


Paste the content of the certificate that you wish to add in the Certificate field and click **Apply**.

Wireless

The Wireless section under Advanced contains four sections for further configurations. Sections include:

- Advanced Settings
- MAC Filter
- Bridge
- QoS (Quality of Service)



The **Wireless -- Advance Setting** section allows you to configure advanced wireless settings such as the channel, data rate, frequency band, etc.

The **Wireless -- MAC Filter** section allows you to configure the wireless firewall by allowing or blocking designated MAC addresses.

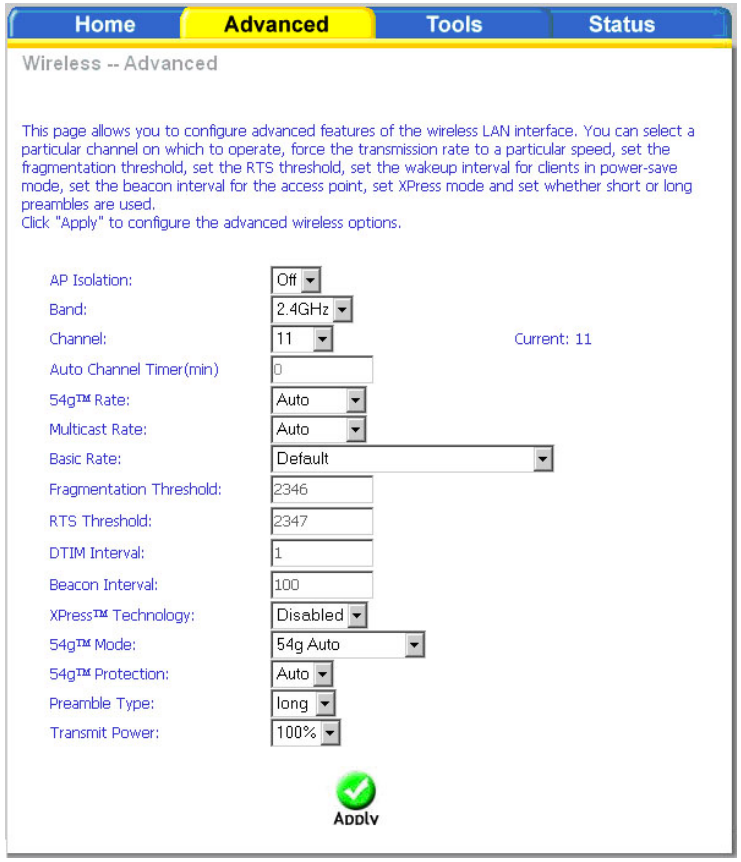
The **Wireless -- Bridge** section allows you to configure a WDS (Wireless distribution System). WDS allows your wireless network to be expanded using multiple access points without the need for wired connections between the APs.

The **Wireless -- QoS** section allows you to configure the wireless quality of service for the router.

Wireless--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.

54g™ Rate: The wireless link rate at which information will be received and transmitted on your wireless network.

Multicast Rate: The rate at which a message is sent to a specified group of recipients.

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

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

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

DTIM Interval: Sets the Wake-up interval for clients in power-saving mode.

Beacon Interval: A Beacon is 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 frameburstingto 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 device.

54g™ Mode: 54g is a Broadcom Wi-Fi technology.

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

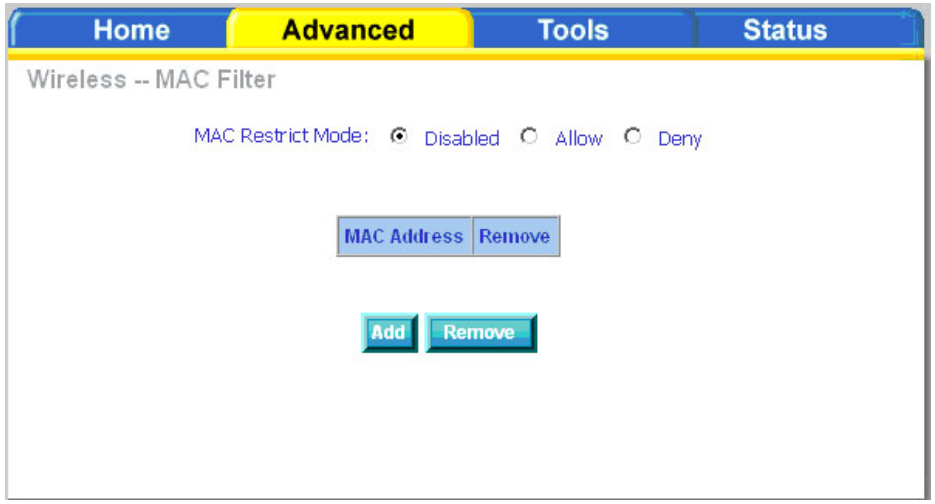
Preamble Type: This is the length of the CRC (Cyclic Redundancy Check) block for communication between the router and wireless clients. High network traffic areas should select Short preamble type.

Transmit Power: This is the percentage of power that should be transmitted from your wireless router. Select from 20%, 40%, 60%, 80%, and 100%.

Wireless--MAC Filter

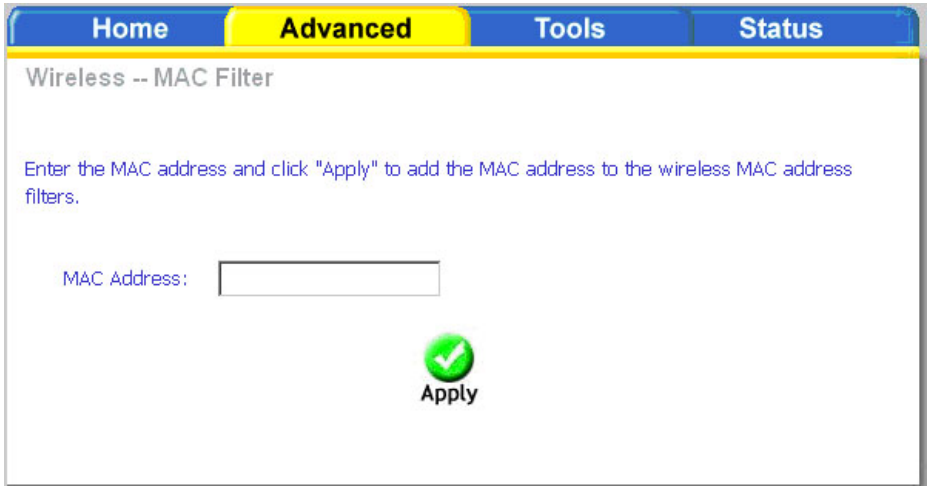
The MAC Filter feature allows you to disable, allow or deny users access to the wireless router based on their MAC address. To add MAC addresses, click on **Add** to continue. Click on **Remove** if you want to take out a MAC address from the MAC filter list.

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. Using the MAC Restrict Mode, you can disable MAC filtering, allow access based on MAC address, or deny access based on MAC address.



When you click **Add** from the MAC filter screen, a MAC address add screen will appear. Enter a MAC address of a computer on your network and click **Apply**.

To determine the MAC address of a computer see “Networking Basics” in the Appendix section of this manual.



Wireless--Bridge

This section allows you to configure WDS (Wireless distribution System). WDS allows your wireless network to be expanded using multiple access points without the need for wired connections between the APs.

AP Mode: Select Access Point to allow the router to connect wirelessly to other WDS enabled routers and allow wireless clients to connect. Wireless Bridge will only allow the router to connect to other WDS enabled routers.

Bridge Restrict: Select Disabled to disable wireless bridge restriction. This will allow any wireless bridge to connect to the router. Select Enabled or Enabled(Scan) to restrict the router from connecting to wireless bridges that are not authorized.

Remote Bridges MAC Address: If Bridge Restrict is set to Enabled or Enabled(scan) only those bridges whose MAC addresses appear in these fields will be granted access.

Click **Refresh** to update the Remote Bridges MAC Address fields. Click **Save/Apply** to save the wireless bridge options.

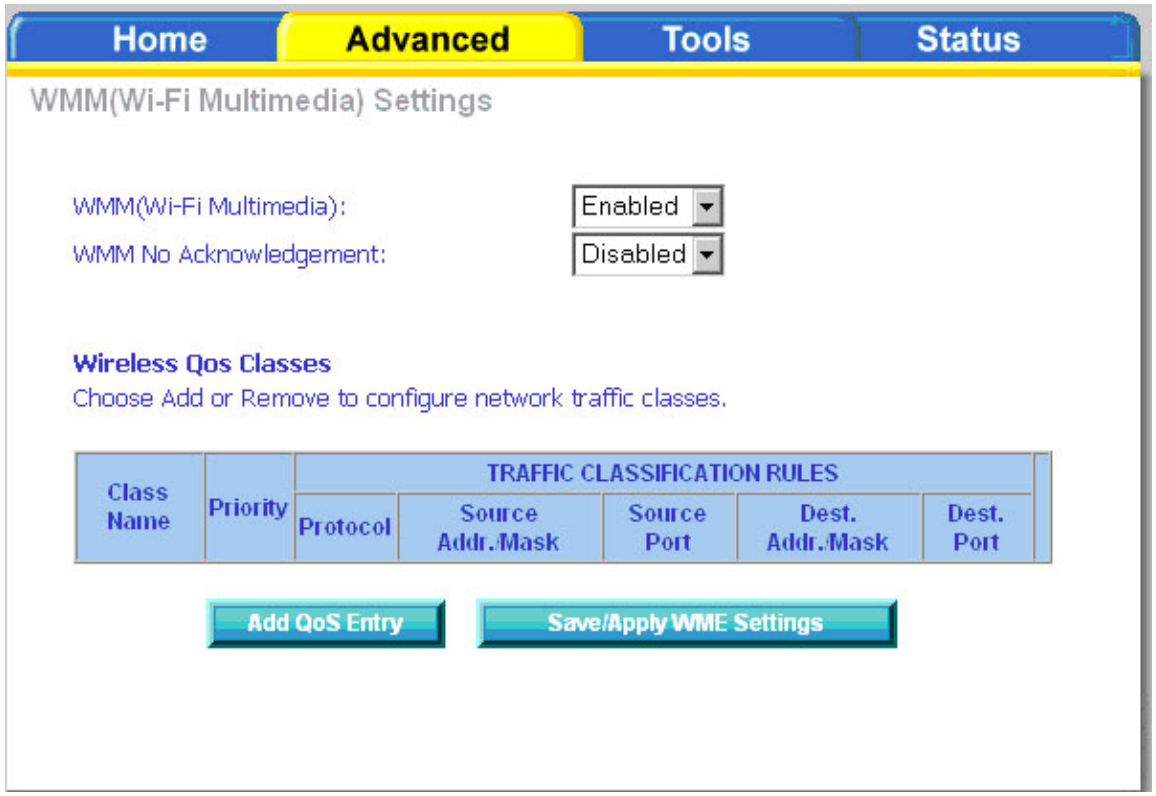
Wireless--QoS

WMM (Wi-Fi Multimedia) technology is available on the wireless router, allowing you to give multimedia applications a higher quality of service and priority in a wireless network so applications such as videos will be of higher quality. Enabling WMM may delay the network traffic of other lower assigned quality applications.

WMM No Acknowledgement can only be enabled if you enable WMM. WMM No Acknowledgement refers to the acknowledgement policy used at the MAC level.

To create a QoS entry, click the **Add QoS Entry** button to proceed to add or remove traffic class rules for your network. Click on Save/Apply WME Settings.

See the “QoS” section on page 51 for more information.



Tools

The tools section contains various administrator functions to maintain your router. Sections include the following; Admin, Time, Remote Log, System, Firmware, and Test.

- **Admin:** Allows you to change the password for the various user names available
- **Time:** Allows you to set the router's time
- **Remote Log:** Allows you to view logs of the router's activities
- **System:** Allows you to perform functions such as save / reboot, backup, update settings, and restore default settings
- **Firmware:** Allows you to upgrade your router with new available firmware versions
- **Test:** Allows you to view test information for your Internet connection

Access Control

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

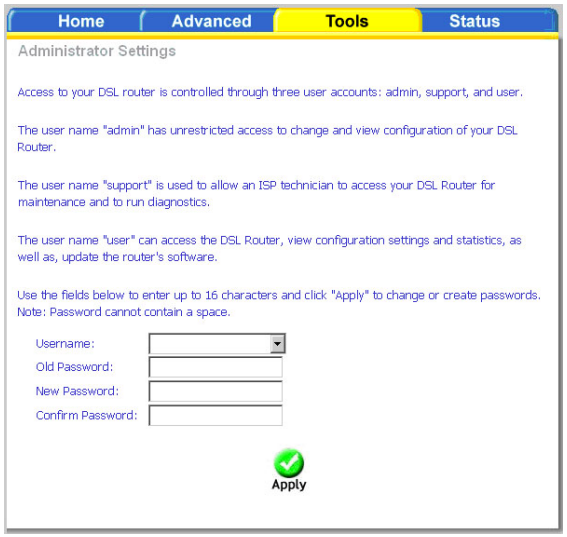
Click the **Admin** button to change the routers account passwords.

Click the **Services** button to configure what services are allowed to pass through the router.

Click the **IP Address** button to define who is permitted access to local management features.

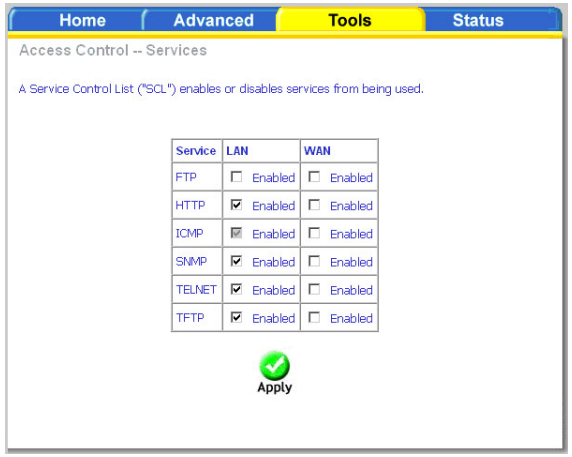
Access Control—Admin

There are three usernames and passwords (**admin, support**, and **user**) that can be used to control your router. The passwords for these usernames can be changed on the Admin screen. Select the Username, enter the Old Password, enter a New Password, and then confirm the new password. When you are ready, click **Apply** at the bottom of the page.



Access Control—Services

From this page you can enable/disable certain services from passing through your router. Services that can be enabled/disabled on the LAN/WAN are FTP, HTTP, ICMP, SNMP, Telnet, and TFTP.



FTP: (File Transfer Protocol) Used for file transfer.

HTTP: (Hyper Text Transfer Protocol) A communications protocol that enables Web browsing.

ICMP: (Internet Control Message Protocol) supports packets containing error, control, and informational messages.

SNMP: (Simple Network Management Protocol) A protocol used for network management and monitoring network devices.

Telnet: A standard Internet protocol for accessing remote systems.

TFTP: (Trivial File Transfer Protocol) A very simple form of the File Transfer Protocol (FTP).

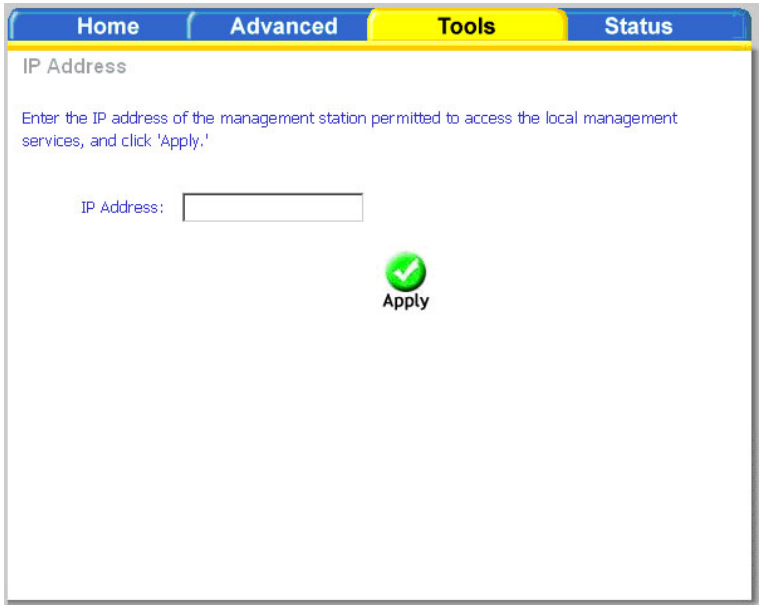
Access Control—IP Address

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

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

If Access Control Mode is disabled, any workstation connected locally to your router can access the web interface provided the correct username and password is supplied at log on.

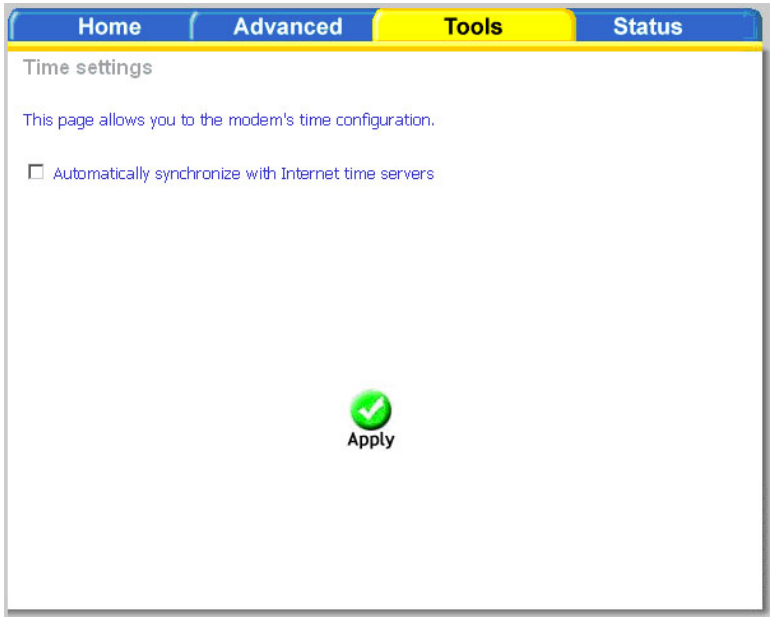
Enter the IP address of the management station permitted to access the local configuration and click **Apply**. This will return you to the previous screen where you can enable access control.



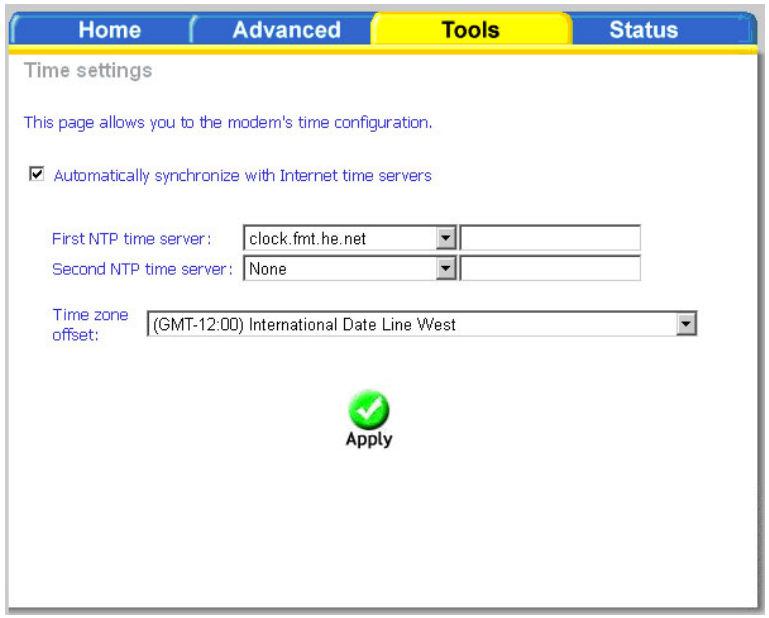
Time

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

To set the router's time, click on the **automatically synchronize with Internet time servers** checkbox. Addional time settings will appear below the checkbox.



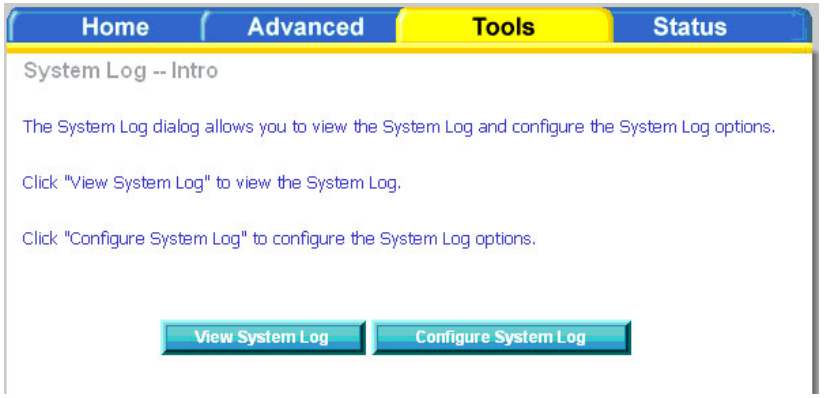
Select from the list of NTP (Network Time Protocol) time servers. Then select the time zone that you are in and click **Apply** to save.



Remote Log

The System Log screen 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.

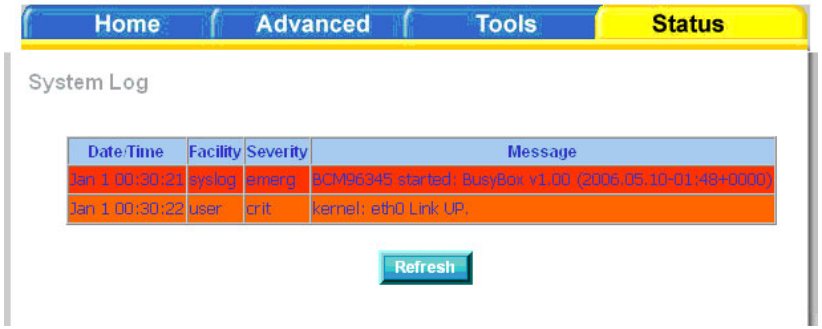


Note: *When you click on the View System Log button, the System Log screen is located under the Status section (see screen on right). To return to the previous screen to configure system log, remember to click on the Tools tab (located on top row) first and then click on Remotelog.*

The System Log screen shows the date/time of the log, the facility that was logged, the severity level and the log message. Click on **Refresh** to view any new information that has been logged.

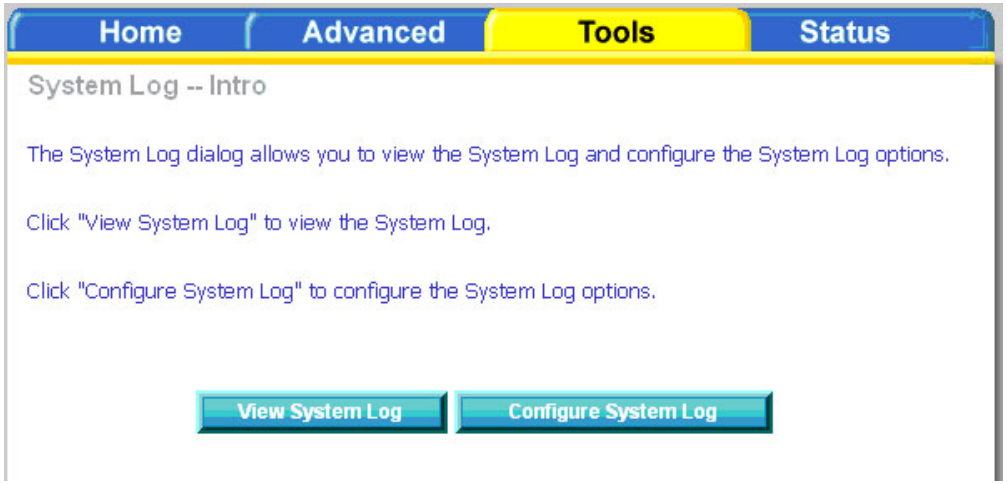
System log when log is disabled.

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

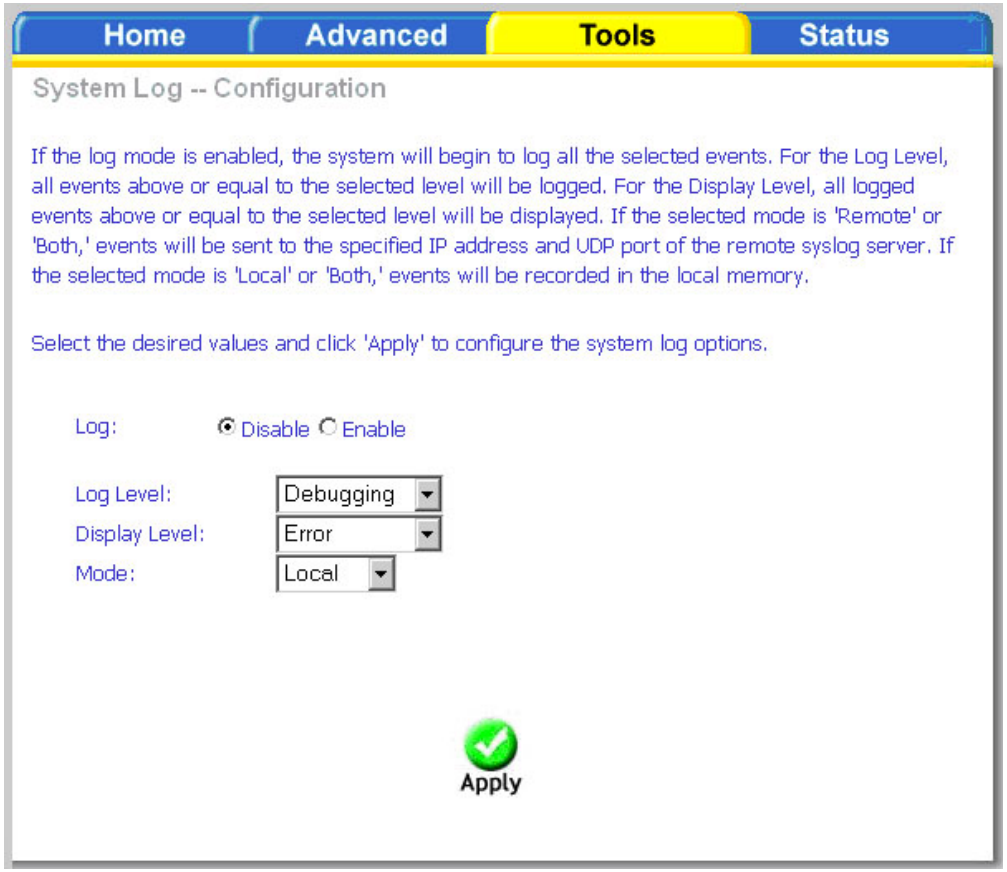


System log when log is enabled.

To configure the system log, click the **Configure System Log** button.



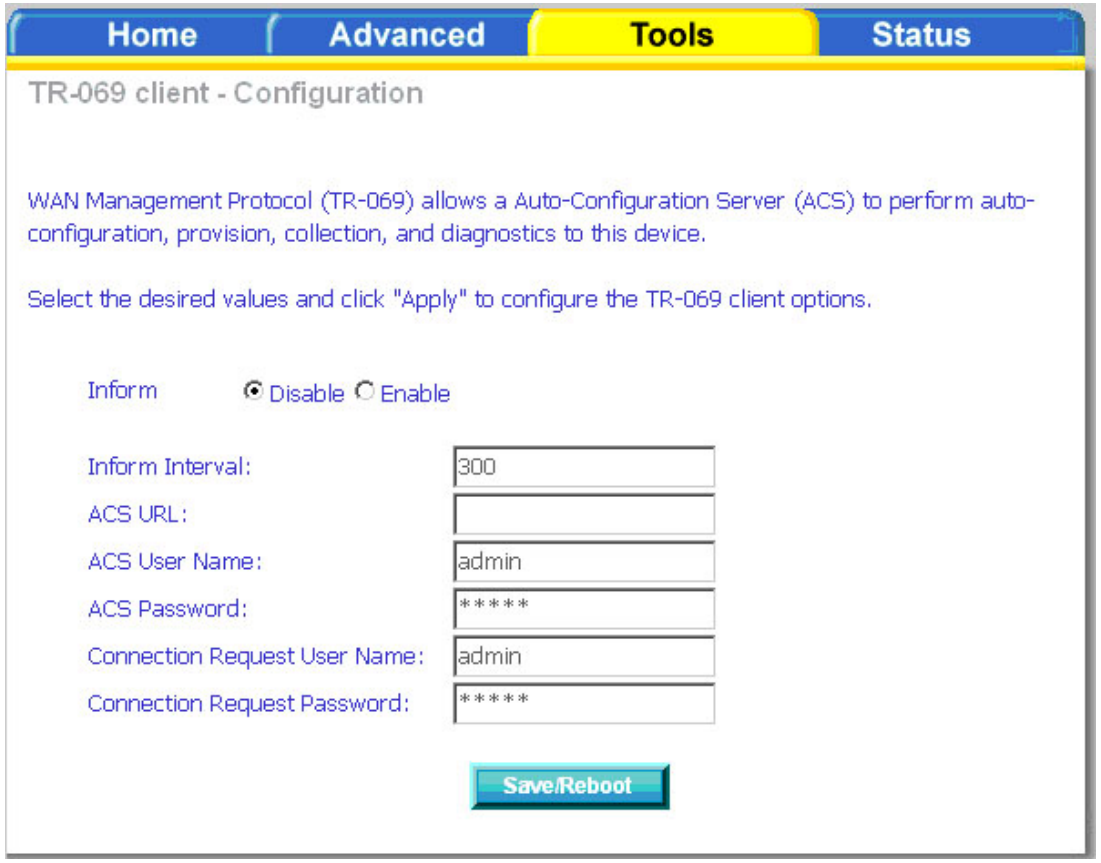
From the configuration screen, set the log to Enable, select the Log Level, Display Level and Mode. If the selected mode is “Remote” or “Both”, events will be sent to a specified IP address and UDP port of a remote system log server. If the selected mode is “Local” or “Both”, events will be recorded and viewed locally. Select the desired values and click **Apply** to save the system log options.



TR-069 Client

The router includes a TR-069 client, a WAN management protocol. TR-069 provides standardized remote device management for residential gateways. This client allows your router to be configured remotely by your ISP (if supported), or any service providing Auto-Configuration Servers (ACS)

If you wish to enable this protocol, then select **enable**. Contact your ISP to determine the ACS URL, ACS User Name, and ACS Password. You must click on the **Save/Reboot** button for the change to take place.



System

The system section includes several tools on one page, including save and reboot, backup settings, update settings, and restore default settings.

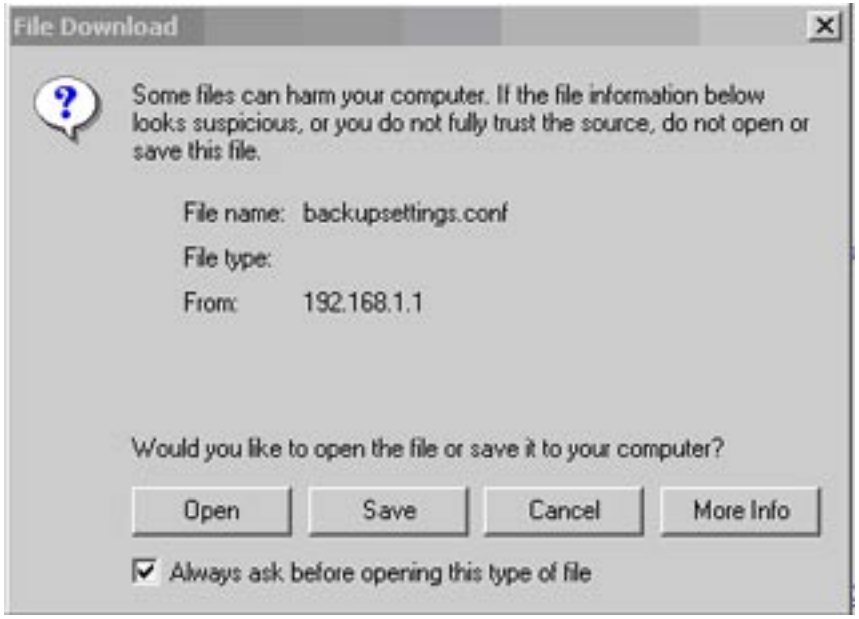
Save and Reboot

The Save/Reboot button, when clicked, will save all configuration changes made on the router and restart the device. All new configuration settings will take effect when the router starts up again.

Backup Settings

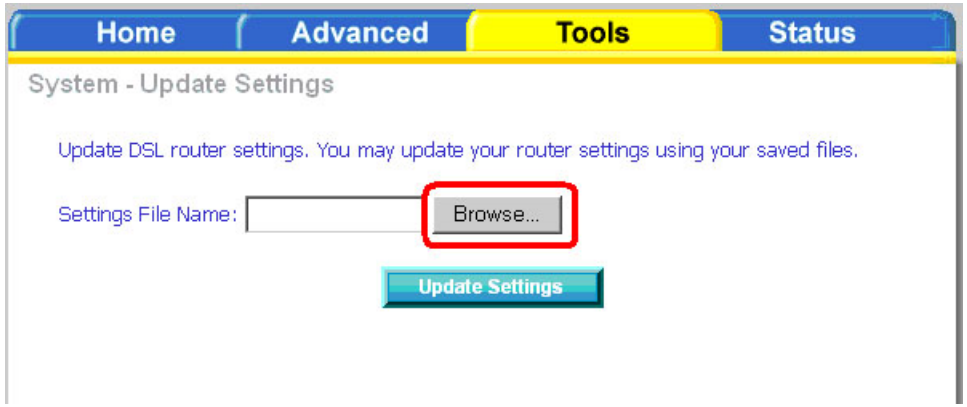
The Backup Settings button allows you to save your router configuration to a file on your computer so that it may be accessed again later. This feature is useful if you have changed the configuration on the router, but would like to revert to a previous configuration.

To save your current configuration, click the **Backup Settings** button. The following pop-up screen will appear with a prompt to open or save the file to your computer.



Update Settings

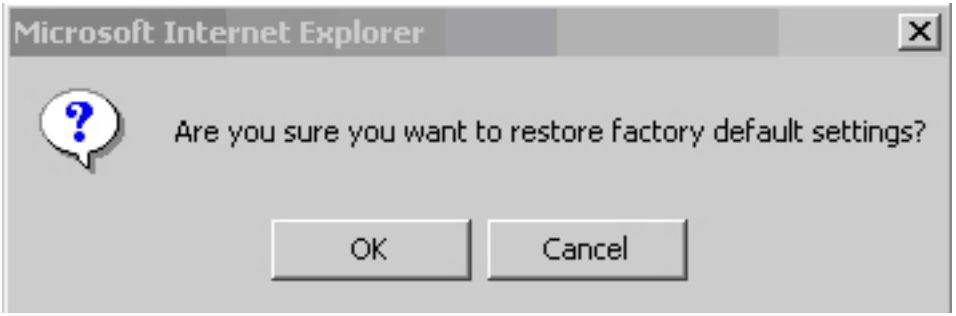
To load a previously saved configuration file onto your router, click **Browse**, select the file on your computer and then click on Update Settings.



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

Restore Default Settings

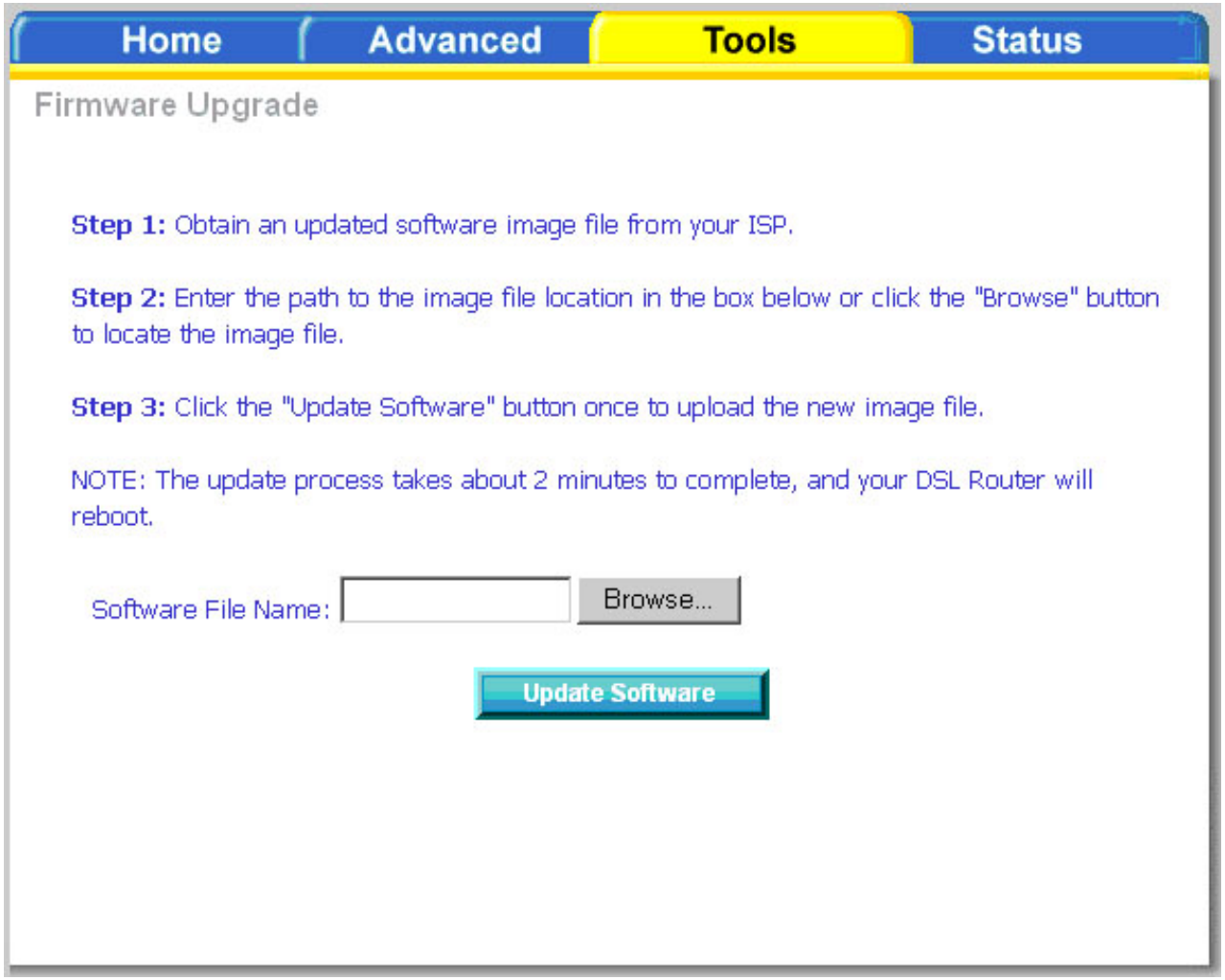
Restore Default Settings will delete all current settings and restore the router to factory default settings. Click on the **Restore Default Settings** button to proceed. The following confirmation dialog will appear confirming your decision to restore default settings. Click on **OK** to continue.



Firmware

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

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

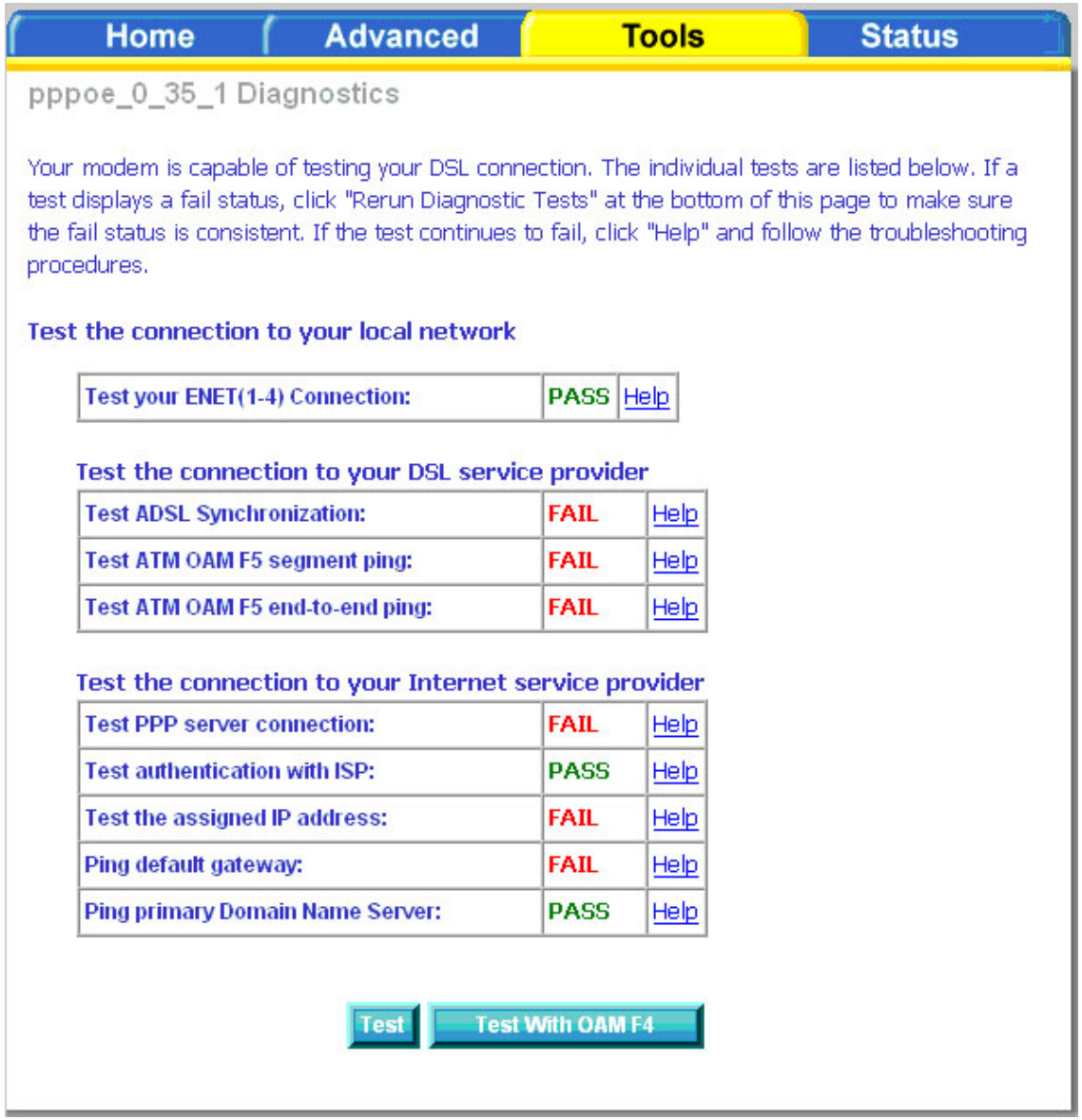


Test

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

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

There are three buttons at the bottom of the page; **Next Connection** (appears only if you have created more than one connection), **Test** and **Test with OAM F4** (which will allow you to retest if necessary).

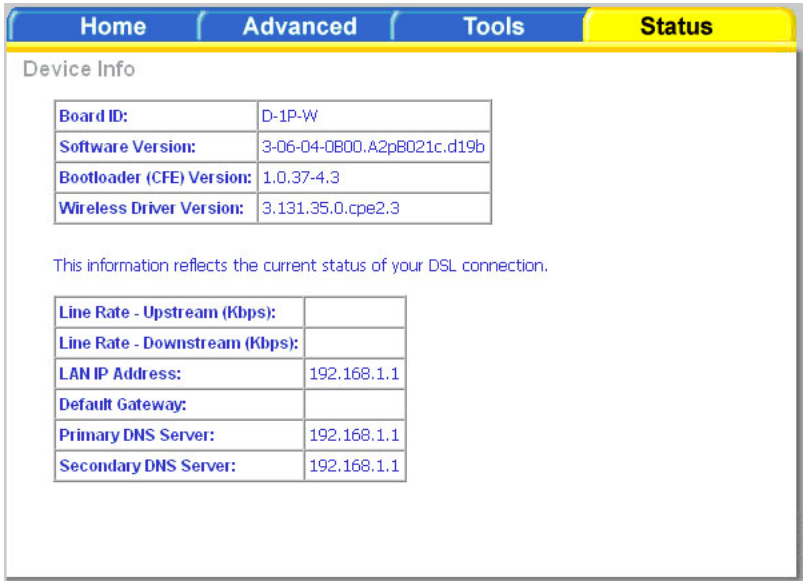


Status

The status section allows you to view general and status information for your router's connection.

Device Info

The Device Info page shows details of the router such as the version of the software, bootloader, LAN IP address, etc. It also displays the current status of your DSL connection.

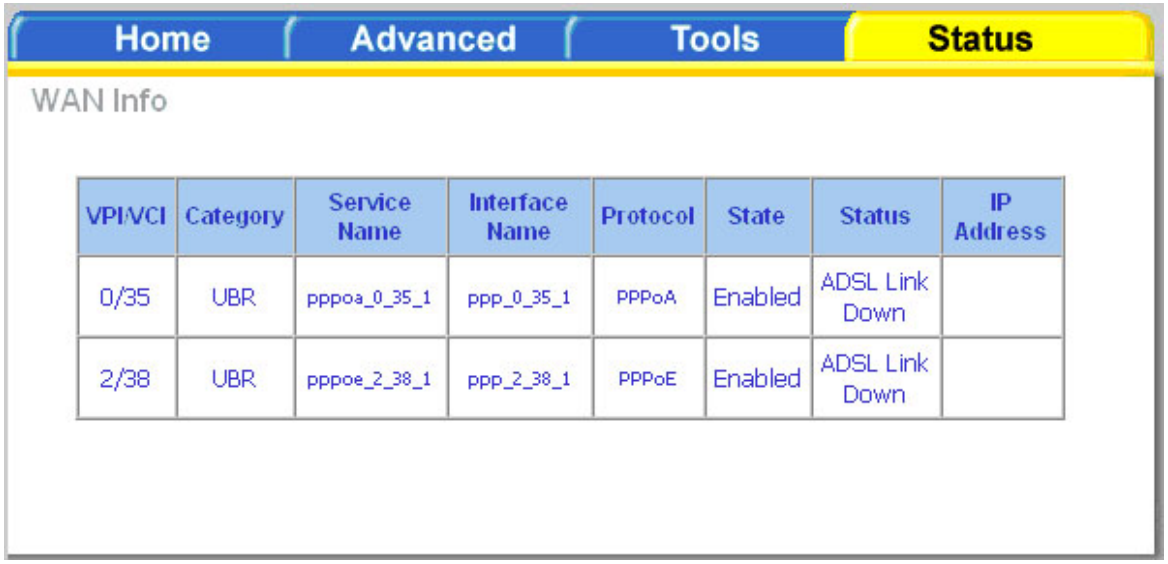


DHCP Clients

Access the DHCP Leases screen by clicking **DHCP** under **Status**. This shows the computers, identified by the hostname and MAC address, that have acquired IP addresses by the DHCP server. The table will also show the time the DHCP lease will expire.

WAN Info

The WAN Info screen displays WAN connections previously set up in the Home section. There is an extra “Status” column used for connection status information, displaying either ADSL Link Down or ADSL Link Up.



VPI/VCI	Category	Service Name	Interface Name	Protocol	State	Status	IP Address
0/35	UBR	pppoa_0_35_1	ppp_0_35_1	PPPoA	Enabled	ADSL Link Down	
2/38	UBR	pppoe_2_38_1	ppp_2_38_1	PPPoE	Enabled	ADSL Link Down	

Route Info

The Route Info section displays route information showing the IP addresses of the destination, gateway, and subnet mask as well as other route information.

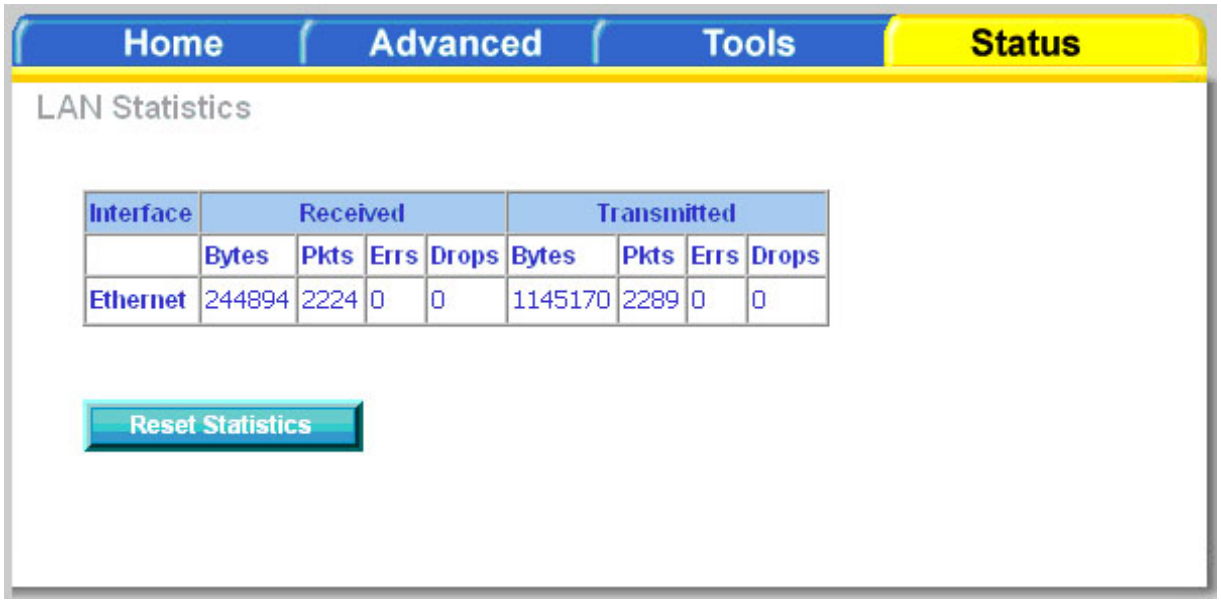
Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0

Log

This is the same screen as seen in the Remotelog section under tools.

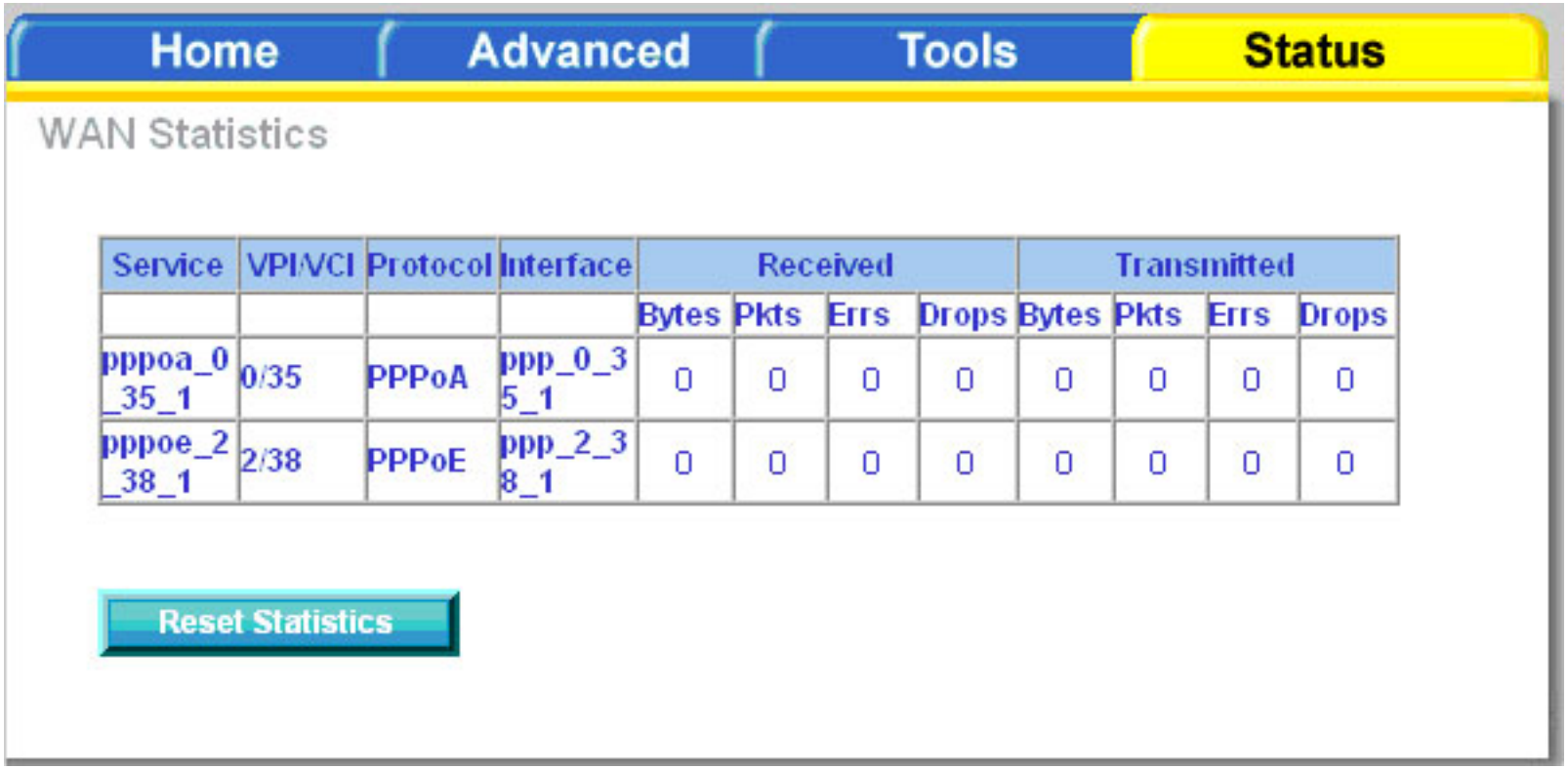
LAN

The LAN section shows received and transmitted packet information for the Ethernet interface. Click on Reset Statistics to renew the information.



WAN

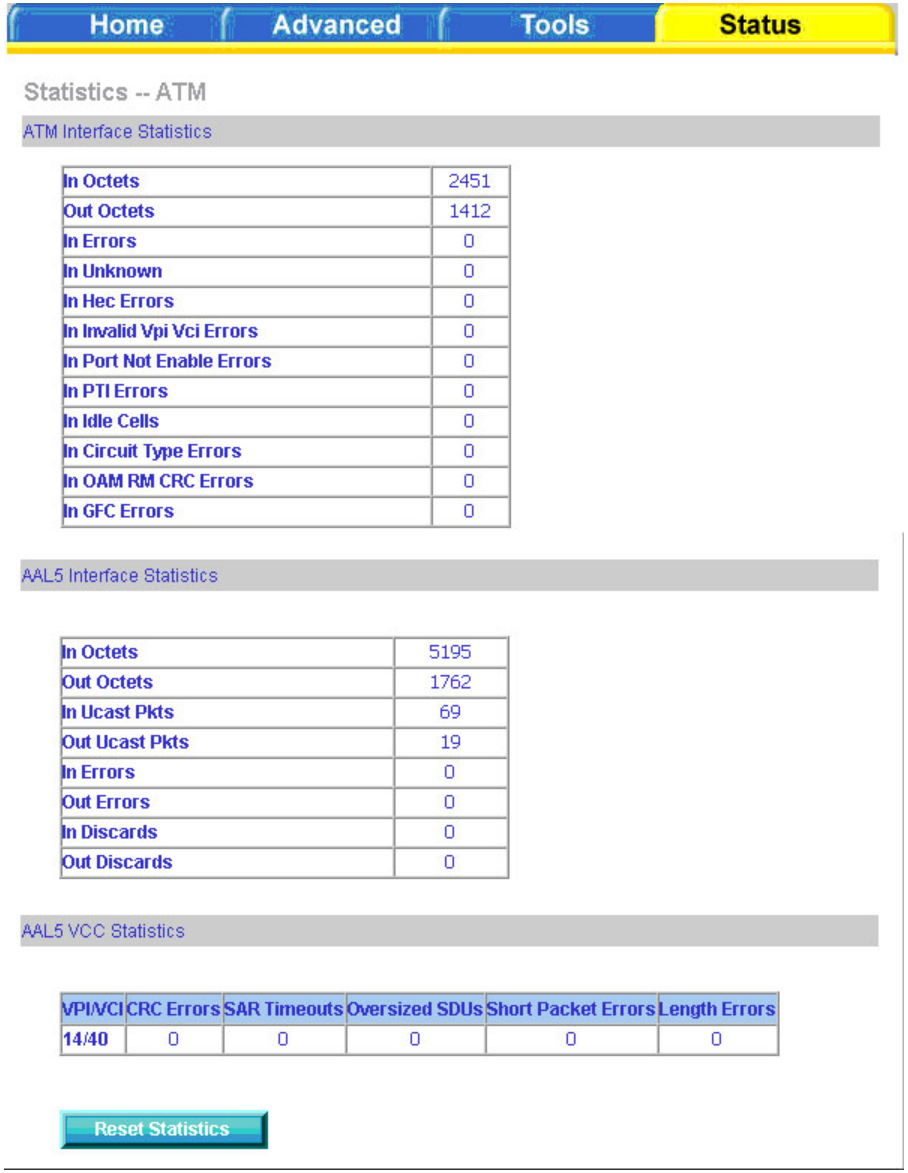
The WAN section shows received and transmitted packet information for the WAN connections that you have set up. Click on **Reset Statistics** to renew the information.



Service	VPI/VCI	Protocol	Interface	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
pppoa_0_35_1	0/35	PPPoA	ppp_0_35_1	0	0	0	0	0	0	0	0
pppoe_2_38_1	2/38	PPPoE	ppp_2_38_1	0	0	0	0	0	0	0	0

ATM

The ATM section displays statistical values for your ATM interface as well as for AAL5 and AAL5 VCC. Click on **Reset Statistics** to reset the values.



ADSL

Information contained in the ADSL screen is useful for troubleshooting and diagnosing connection problems.

Home | Advanced | Tools | Status

ADSL Statistics

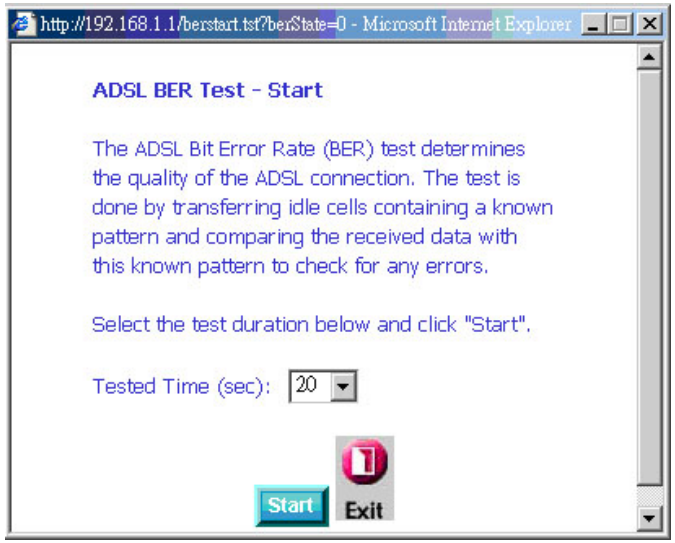
Mode:		G.DMT
Type:		Fast
Line Coding:		Trellis On
Status:		No Defect
Link Power State:		L0
	Downstream	Upstream
SNR Margin (dB):	11.9	12.0
Attenuation (dB):	0.0	1.0
Output Power (dBm):	7.8	12.5
Attainable Rate (Kbps):	9568	1056
Rate (Kbps):	8000	800
K (number of bytes in DMT frame):	251	26
R (number of check bytes in RS code word):	0	0
S (RS code word size in DMT frame):	1	1
D (interleaver depth):	1	1
Delay (msec):	0	0
Super Frames:	18171	18169
Super Frame Errors:	1	200
RS Words:	0	0
RS Correctable Errors:	0	0
RS Uncorrectable Errors:	0	N/A
HEC Errors:	1	86
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	5829071	0
Data Cells:	1040	0
Bit Errors:	0	0
Total ES:	2	0
Total SES:	1	0
Total UAS:	205	0

ADSL BER Test | Reset Statistics

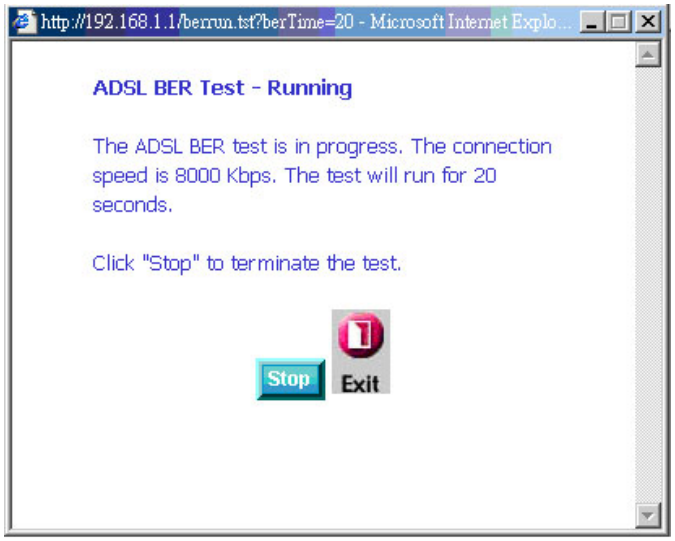
ADSL BER Test

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

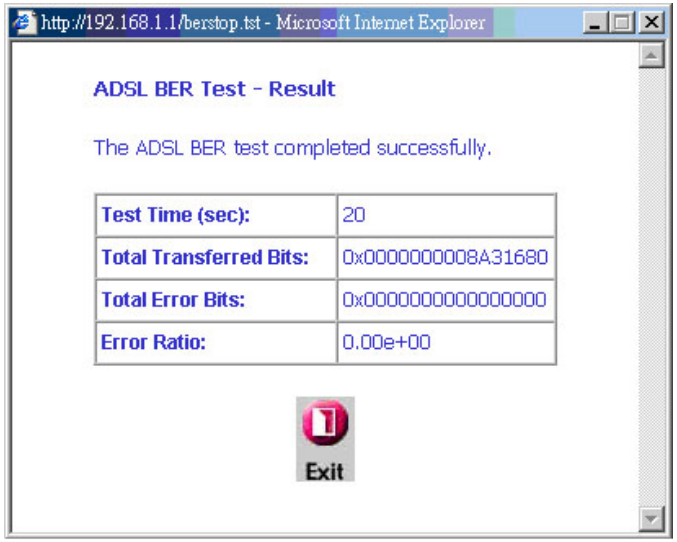
If you click on the **ADSL BER Test** button at the bottom of the ADSL Statistics page, the following pop-up screen will appear allowing you to set the tested time and to begin the test. Click **Start** to begin the test.



When you start the ADSL BER Test, the following progress window will display the connection speed as well as the length of time that the test will run for. At any time during the test, click on the **Stop** button to terminate the test.

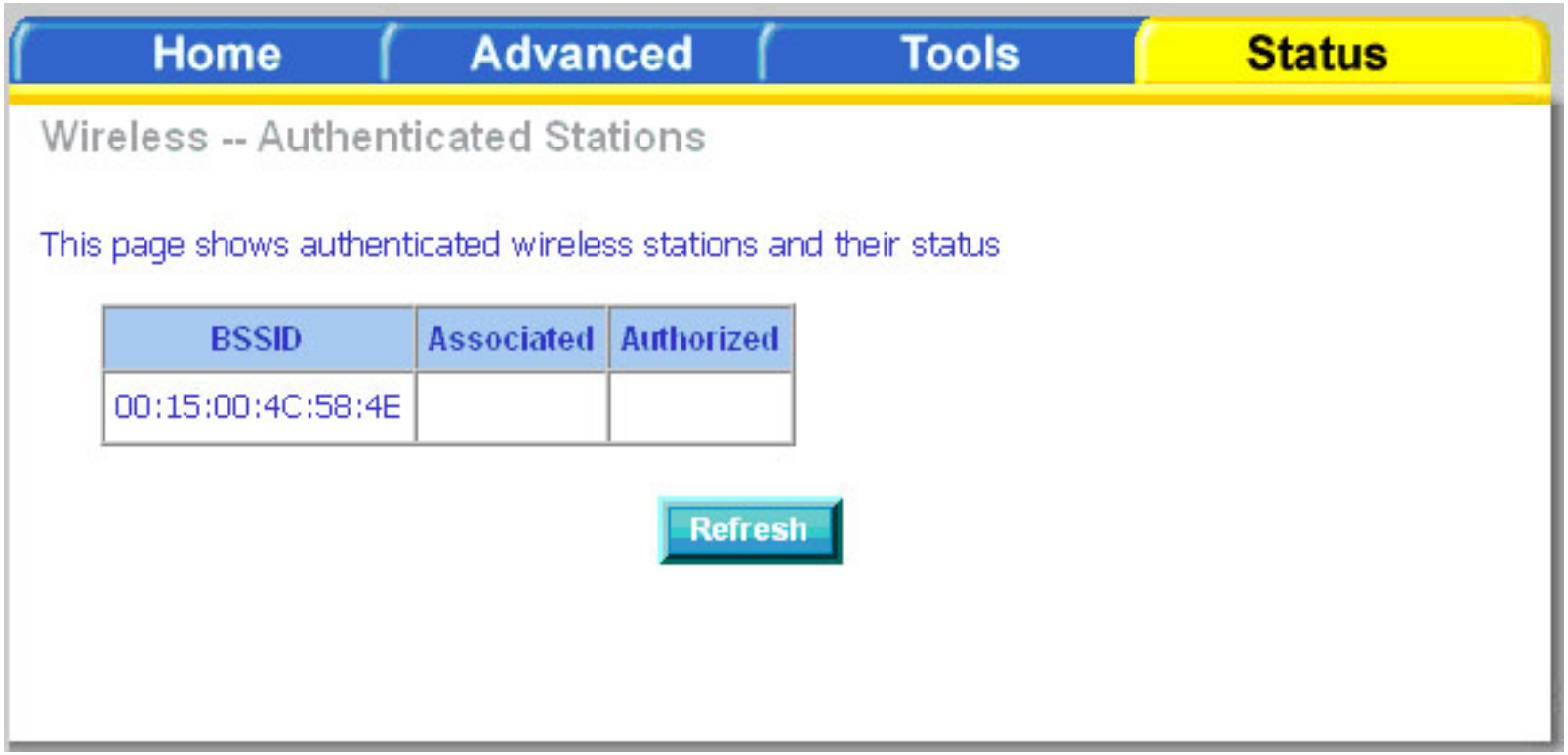


When the test is complete, the following window will display the test results showing the test time, total transferred bits, total error bits and error ratio. Click **Exit** to close the window.



Wireless Station Info

This page displays the stations (identified by their BSSID) that are associated with your wireless router. Click on **Refresh** to renew the page for new wireless stations.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-2640B. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

1. Why can't I access the web-based configuration utility?

When entering the IP address of the D-Link router (192.168.1.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:

    - Internet Explorer 6.0 or higher
    - Netscape 8 or higher
    - Mozilla 1.7.12 (5.0) or higher
    - Opera 8.5 or higher
    - Safari 1.2 or higher (with Java 1.3.1 or higher)
    - Camino 0.8.4 or higher
    - Firefox 1.5 or higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:

  - Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.

  - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.

  - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.

  - Close your web browser (if open) and open it.

- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the web management.

- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

2. What can I do if I forgot my password?

If you forgot your password, you must reset your router. Unfortunately this process will change all your settings back to the factory defaults.

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. For information about logging into the router see page 11.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology as become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, and etc
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as far away as possible from the router/access point. This would significantly reduce any interference that the appliances might cause since they operate on same frequency.

Security

Don’t let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to the Wireless section of this manual for detailed information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

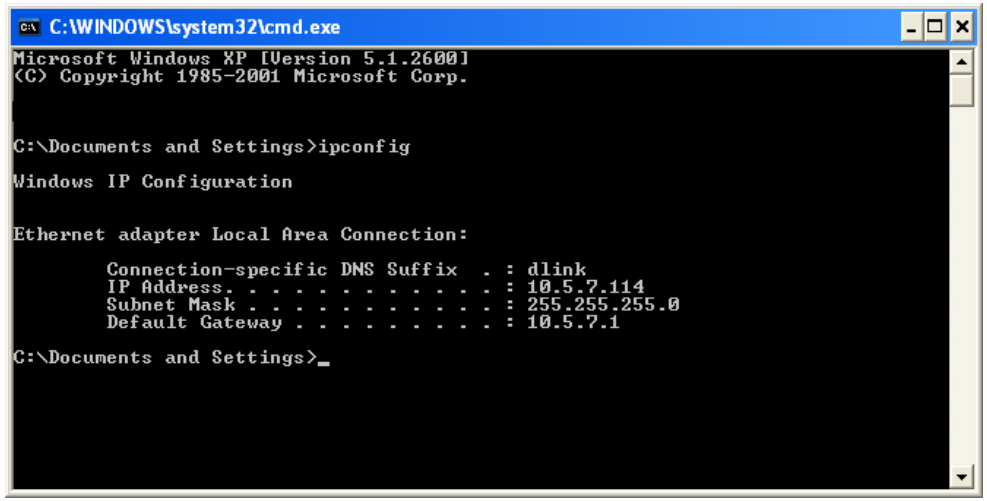
Networking Basics

Check your IP address

After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK**.

At the prompt, type ***ipconfig*** and press **Enter**.



This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.

Check your MAC

Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK**.

At the prompt, type ***ipconfig /all*** and press **Enter**.

This will display information about all installed adapters on your computer. Your MAC address is listed as the “Physical Address” and should look like xx-xx-xx-xx-xx-xx or xx:xx:xx:xx:xx:xx

Statically Assign an IP address

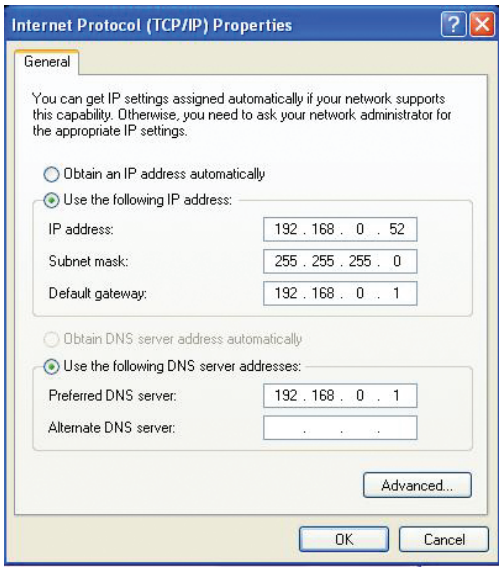
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1
Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2
Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.

Step 3
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.



Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5
Click OK twice to save your settings.

Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DSL-2640B)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the router).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

For customers within the United States:

Phone Support:
(877) 453-5465

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(800) 361-5265

Internet Support:
http://support.dlink.ca

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Software Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for Hardware and Software portions of D-Link’s products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold “As-Is” without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization (“RMA”) number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: The Limited Warranty provided herein by D-Link does not cover: Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

CE Mark Warning: This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC 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 harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures**:**

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

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Registration

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0
September 26, 2006