USER MANUAL

DSL-2740B

VERSION 1.01

D-Link®

BROADBAND

Table of Contents

Product Overview 4
Package Contents 4
System Requirements 4
Introduction 5
Features 6
Hardware Overview 7
Connections 7
LEDs 8
Installation 9
Before you Begin 9
Installation Notes 10
Information you will need from your ADSL service provider 12
Information you will need about DSL-2740B 14
Wireless Installation Considerations 16
Device Installation 17
Power on Router 17
Network Connections 18
Configuration 20
Web-based Configuration Utility 20
SETUP 21
WIZARD 21
ADSL 27
WLAN 28
LAN 29
DNS 30
ADVANCED 31
ADVANCED ADSL 31
ADVANCED WLAN 32
WLAN SECURITY 33
WLAN Filter 36
WLAN BRIDGE 37
WLAN QOS 38
FIREWALL 39
VIRTUAL SERVER 40
PORT TRIGGERING 41
DMZ 42
OUTGOING IP FILTER 43
INCOMING IP FILTER 44
BRIDGE FILTER 45
PARENT CONTROL 46
URL FILTER 47
QUALITY OF SERVICE 48
ROUTING 49
RIP 50
PORT MAPPING 51
TOOLS 53
Diagnostics 53
BACKUP SETTINGS 54
UPDATE SETTINGS 54
RESTORE DEFAULT 55
TR069 CLIENT 55

SNMP CONFIGURATION 56
DDNS 57
TIME 58
ACCESS SERVICE 59
ACCESS IP 60
PASSWORD 60
UPDATE FIRMWARE 61
SAVE / REBOOT 61
STATUS 62
DEVICE INFO 62
ADSL 63
LAN 64
WAN 64
ATM 65
ROUTE 65
ARP 66
DHCP CLIENTS 66
WLAN STATION 67
SYSTEM LOG 68
Troubleshooting 69
Wireless Basics 71
Networking Basics 74
Check your IP address 74
Statically Assign an IP address 75
Technical Specifications 76

Package Contents

- DSL-2740B Wireless ADSL Router
- 3 Detachable Antennas
- Power Adapter
- CD-ROM with Installation Wizard, User Manual, and Special Offers
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- One Quick Installation Guide

Note: Using a power supply with a different voltage rating than the one included with the DIR-635 will cause damage and void the warranty for this product.

System Requirements

- ADSL Internet service
- Computer with:
  - 200MHz Processor
  - 64MB Memory
  - CD-ROM Drive
  - Ethernet Adapter with TCP/IP Protocol Installed
  - Windows XP/20004
  - Internet Explorer v6 or later, FireFox v1.5
- D-Link Click'n Connect Utility
  - Computer with Windows 2000/XP

Introduction

HIGH-SPEED ADSL2/2+ INTERNET CONNECTION
Latest ADSL2/2+ standards provide Internet transmission of up to 24Mbps downstream, 1Mbps upstream.

HIGH-PERFORMANCE WIRELESS
Embedded latest draft 802.11n technology for highspeed wireless connection, complete compatibility with 802.11b/g wireless devices

TOTAL SECURITY & QoS
Firewall protection from Internet attacks, user access control, WPA/WPA2 wireless security and priority queues for smooth VoIP traffic/streaming multimedia

ULTIMATE INTERNET CONNECTION
The DSL-2740B RangeBooster N ADSL2+ router is a versatile, high-performance remote router for home and the small office. With integrated ADSL2/2+ supporting up to 24Mbps download speed, firewall protection, Quality of Service (QoS), draft 802.11n wireless LAN and 4 Ethernet switch ports, this router provides all the functions that a home or small office needs to establish a secure and high-speed remote link to the outside world.

ULTIMATE WIRELESS CONNECTION WITH MAXIMAL SECURITY
Powered by RangeBooster N technology, this router provides wireless speeds that are up to 4 times faster than 802.11g 1. Maximize wireless performance by connecting this router to computers equipped with RangeBooster N wireless interfaces and stay connected from virtually anywhere at home and in the office. The router can also be used with 802.11g and 802.11b wireless networks to enable significantly improved reception. It supports WPA/WPA2 and WEP for flexible user access security and data encryption methods.

FIREWALL PROTECTION & QoS
Security features prevents unauthorized access to the home and office network, be it from the wireless devices or from the Internet. The router provides firewall security using Stateful Packet Inspection (SPI) and hacker attack logging for Denial of Service (DoS) attack protection. SPI inspects the contents of all incoming packet headers before deciding what packets are allowed to pass through. Router access control is provided with packet filtering based on port and source/destination MAC/IP addresses. For Quality of Service (QoS), the router supports multiple priority queues to enable a group of home or office users to experience the benefit of smooth network connection of inbound and outbound data without concern of traffic congestion. This QoS support allows users to enjoy high ADSL transmission for applications such as VoIP and streaming multimedia over the Internet.

*Maximum wireless signal rate derived from IEEE standard 802.11g and draft 802.11n specifications. 802.11n speeds obtainable when operating among RangeBooster N products. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Features

- **Faster Wireless Networking** - The DSL-2740B provides up to 270Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Compatible with 802.11b and 802.11g Devices** - The DSL-2740B is still fully compatible with the IEEE 802.11b standard, so it can connect with existing 802.11b PCI, USB and Cardbus adapters.

- **DHCP Support** - Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.

- **Network Address Translation (NAT)** - For small office environments, the DSL-2740B allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user. NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.

- **Precise ATM Traffic Shaping** - Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.

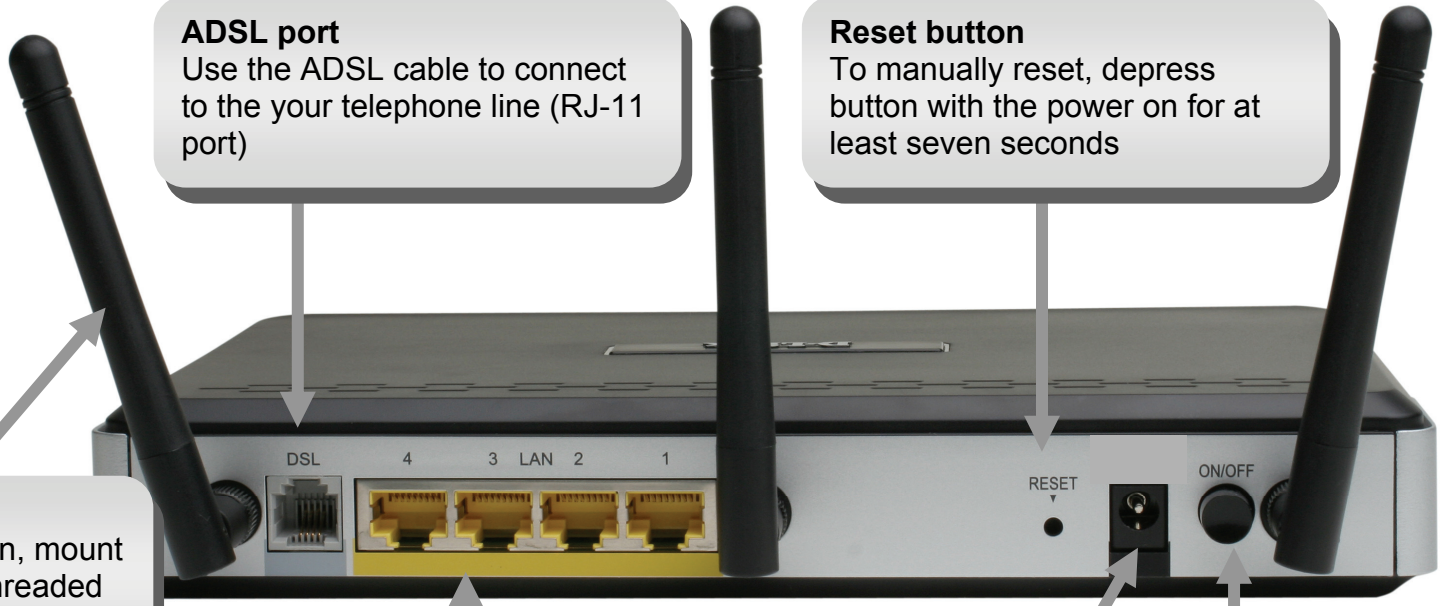
- **High Performance** - Very high rates of data transfer are possible with the Router. Up to 24Mbps downstream bit rate using the G.dmt standard. (For ADSL2+)

- **Full Network Management** - The DSL-2740B incorporates TR-069 & SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via Telnet connection.

- **Easy Installation** - The DSL-2740B uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.

*Maximum wireless signal rate derived from IEEE standard 802.11g and draft 802.11n specifications. 802.11n speeds obtainable when operating among RangeBooster N products. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Hardware Overview
Connections



ADSL port
Use the ADSL cable to connect to the your telephone line (RJ-11 port)

Reset button
To manually reset, depress button with the power on for at least seven seconds

Antenna
For wireless operation, mount the antenna on the threaded antenna post.

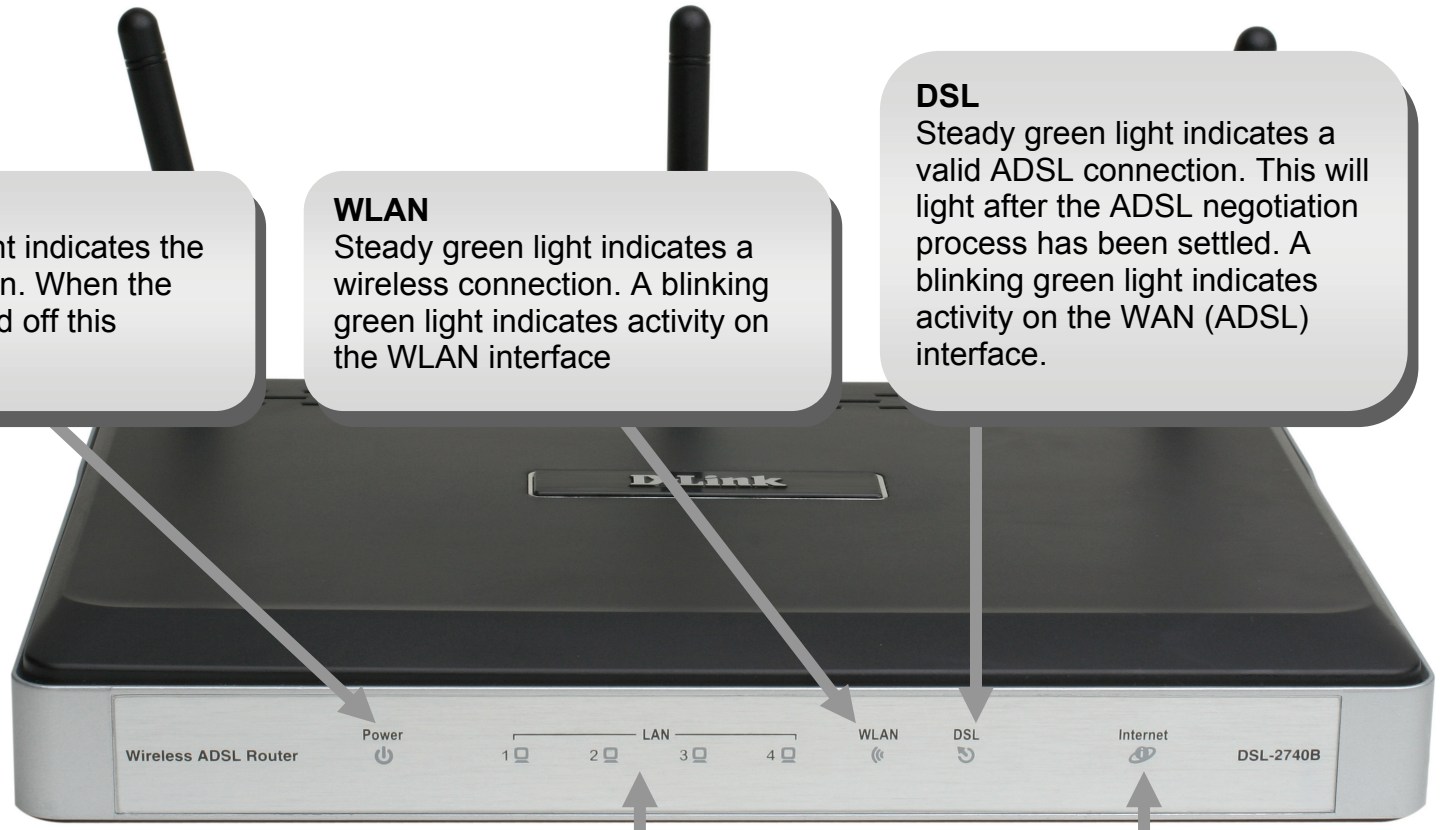
Ethernet ports
Use the Ethernet ports to connect the Router to your Ethernet LAN or Ethernet devices

Power insert
Use the adapter shipped with the Router to connect to power source

Power button
Push in to power-on the Router. Push again to power-off the Router

Hardware Overview

LEDs



Power
Steady green light indicates the unit is powered on. When the device is powered off this remains dark.

WLAN
Steady green light indicates a wireless connection. A blinking green light indicates activity on the WLAN interface

DSL
Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates activity on the WAN (ADSL) interface.

LAN
A solid green light indicates a valid link on startup. These lights blink when there is activity currently passing through the Ethernet port.

Internet
Steady green light indicates a successful Internet connection. Steady red light indicates failed Internet connection. Dark if no WAN protocol is configured.

Installation

This section will walk you through the installation process. Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, or in the attic or garage.

Before you Begin

Please read and make sure you understand all the prerequisites for proper installation of your new Router. Have all the necessary information and equipment on hand before beginning the installation.

Installation Notes

In order to establish a connection to the Internet it will be necessary to provide information to the Router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the Router. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

Low Pass Filters
Since ADSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the ADSL line. These filters are easy to install passive devices that connect to the ADSL device and/or telephone using standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems
The DSL-2740B uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, and Windows XP.

Web Browser
Any common web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Opera, Microsoft Internet Explorer® version 6.0, Netscape Navigator® version 6.2.3, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)
Any computer that uses the Router must be able to connect to it through the Ethernet port on the Router. This connection is an Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet NIC adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the Router. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

802.11 Wireless LAN Configuration

All the 802.11 wireless LAN settings may be configured on a single page using the web-based manager. For basic wireless communication you need to decide what channel to use and what SSID to assign. These two settings must be the same for any wireless workstations or other wireless access point that communicate with the DSL-2740B through the wireless interface.

Security for wireless communication can be accomplished in a number of ways. The DSL-2740B supports WPA (Wi-Fi Protected Access), WPA2, and mixed WPA/WPA2. Wireless access can also be controlled by selecting MAC addresses that are allowed to associate with the device. Please read the section on Wireless Configuration.

Additional Software

It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using the device a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the Router itself.

If your ADSL service is delivered through a PPPoE or PPPoA connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a PC, a server, a gateway device such as a router or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

Information you will need from your ADSL service provider

Username
This is the Username used to log on to your ADSL service provider's network. It is commonly in the form˜ user@isp.co.uk Your ADSL service provider uses this to identify your account.

Password
This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.

WAN Setting / Connection Type
These settings describe the method your ADSL service provider uses to transport data between the Internet and your computer. Most users will use the default settings. You may need to specify one of the following WAN Setting and Connection Type configurations (Connection Type settings listed in parenthesis):

- PPPoE/PPoA (PPPoE LLC, PPPoA LLC or PPPoA VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)
- IPoA/MER (Static IP Address) (Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux or IPoA)
- MER (Dynamic IP Address) (1483 Bridged IP LLC or 1483 Bridged IP VC-Mux)

Modulation Type
ADSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (ADSL2+ Multi-Mode) used for the Router automatically detects all types of ADSL, ADSL2, and ADSL2+ modulation. However, if you are instructed to specify the modulation type used for the Router, you may choose among the numerous options available on the Modulation Type drop-down menu on the ADSL Configuration window (Advanced > ADSL)

Security Protocol
This is the method your ADSL service provider will use to verify your Username and Password when you log on to their network. Your Router supports the PAP and CHAP protocols.

VPI
Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

VCI
Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN Settings window of the web management interface.

Information you will need about DSL-2740B

Username
This is the Username needed access the Router's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is "admin." The user cannot change this.

Password
This is the Password you will be prompted to enter when you access the Router's management interface. The default Password is "admin." The user may change this.

LAN IP addresses for the DSL-2740B
This is the IP address you will enter into the Address field of your web browser to access the Router's configuration graphical user interface (GUI) using a web browser. The default IP address is 192.168.1.1. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.

LAN Subnet Mask for the DSL-2740B
This is the subnet mask used by the DSL-2740B, and will be used throughout your LAN. The default subnet mask is 255.255.255.0. This can be changed later.

Information you will need about your LAN or computer:

Ethernet NIC

If your computer has an Ethernet NIC, you can connect the DSL-2740B to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2740B to connect to other computer or Ethernet devices.

DHCP Client status

Your DSL-2740B ADSL Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-2740B will assign are from 192.168.1.2 to 192.168.1.254. Your computer (or computers) needs to be configured to Obtain an IP address automatically (that is, they need to be configured as DHCP clients.)

It is recommended that your collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your DSL-2740B Wireless ADSL Router.

Wireless Installation Considerations

DSL-2740B lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

Device Installation

The DSL-2740B Wireless ADSL Router maintains three separate interfaces, an Ethernet LAN, a wireless LAN and an ADSL Internet (WAN) connection. Carefully consider the Router's location suitable for connectivity for your Ethernet and wireless devices. You must have a functioning broadband connection via a bridge device such as a Cable or ADSL modem in order to use the Router's WAN function.

Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture, direct sunlight or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.
The Router can be placed on a shelf, desktop, or other stable platform. If possible, you should be able to see the LED indicators on the front if you need to view them for troubleshooting.

Power on Router

The Router must be used with the power adapter included with the device.

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a suitable nearby power source.
2. Push down the Power button, and you should see the Power LED indicator light up and remain lit.
3. If the Ethernet port is connected to a working device, check the Ethernet Link/Act LED indicators to make sure the connection is valid. The Router will attempt to establish the ADSL connection, if the ADSL line is connected and the Router is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Router can establish a connection.

Factory Reset Button

The Router may be reset to the original factory default settings by using a ballpoint or paperclip to gently push down the reset button in the following sequence:

1. Press and hold the reset button while the device is powered off.
2. Turn on the power.
3. Wait for 5~8 seconds and then release the reset button.

Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address **192.168.1.1** and the subnet mask is **255.255.255.0**, the default management Username is “admin” and the default Password is “admin.”

Network Connections

Connect ADSL Line

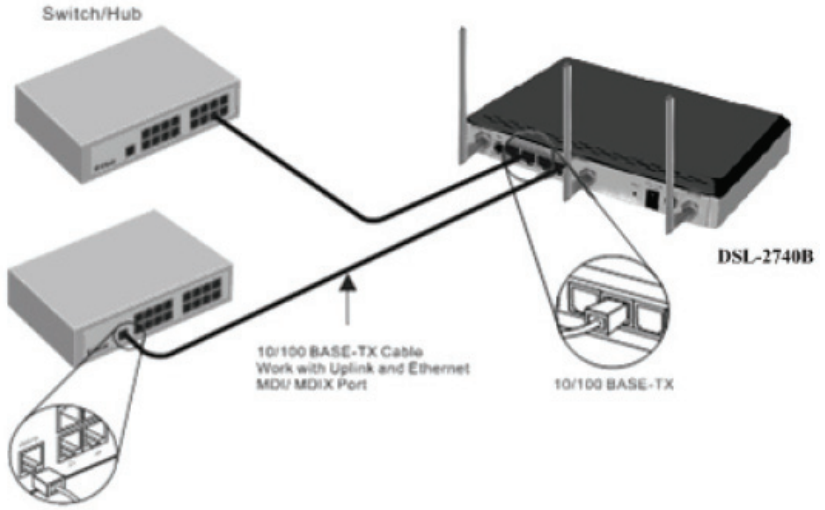
Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider’s network backbone and ultimately to the Internet.

Connect Router to Ethernet

The Router may be connected to a single computer or Ethernet device through the 10BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

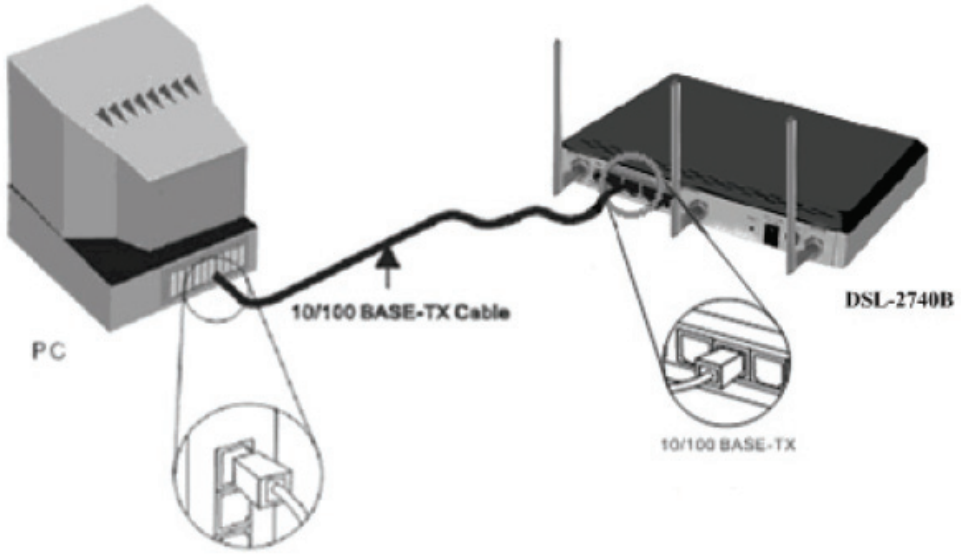
Hub or Switch to Router Connection

Connect the Router to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable as shown in this diagram. If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.



Computer to Router Connection

You can connect the Router directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided as shown in this diagram.



Configuration

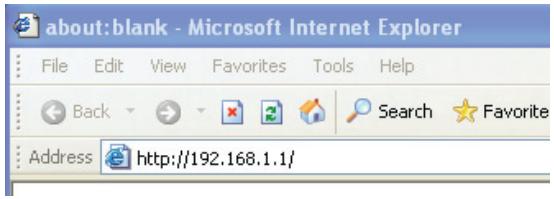
This section will show you how to configure your new D-Link wireless router using the web-based configuration utility.

Web-based Configuration Utility

Connect to the Router

To configure the WAN connection used by the Router it is first necessary to communicate with the Router through its management interface, which is HTML-based and can be accessed using a web browser. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the Router. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client.

To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.1.1).



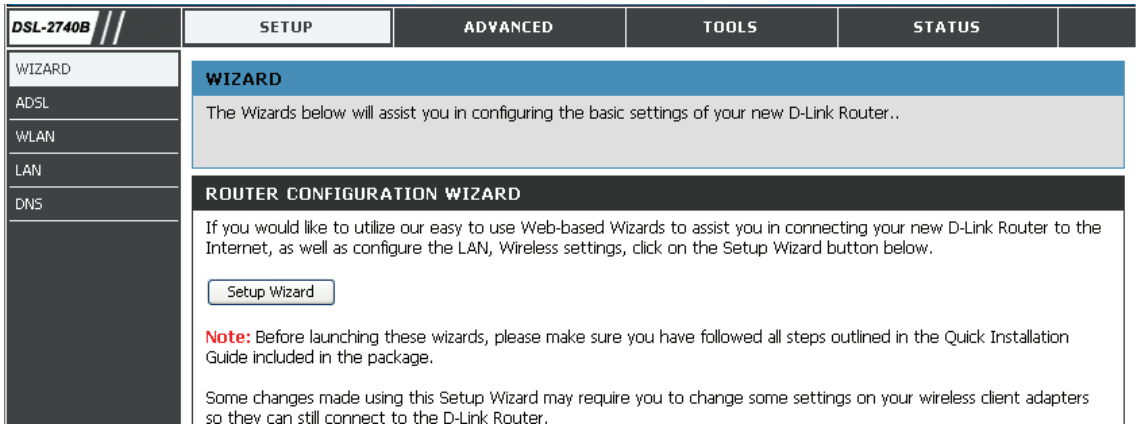
Type **"admin**" for the User Name and "**admin**" in the Password field. If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.

SETUP

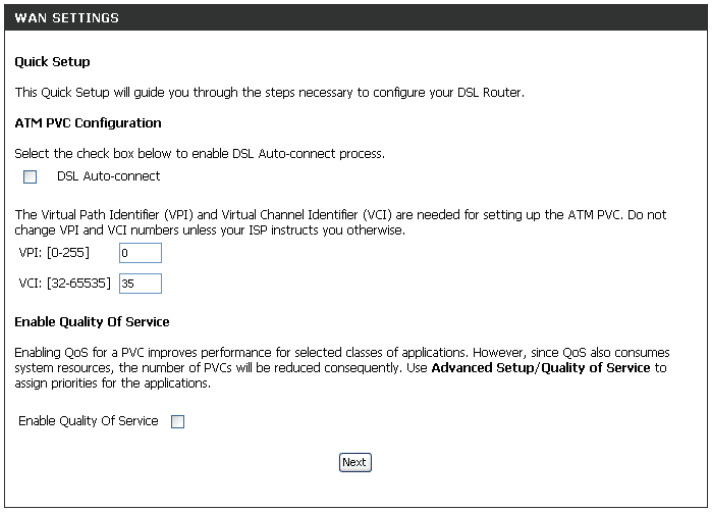
This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various windows used to configure and monitor the Router including how to change IP settings and DHCP server setup.

WIZARD

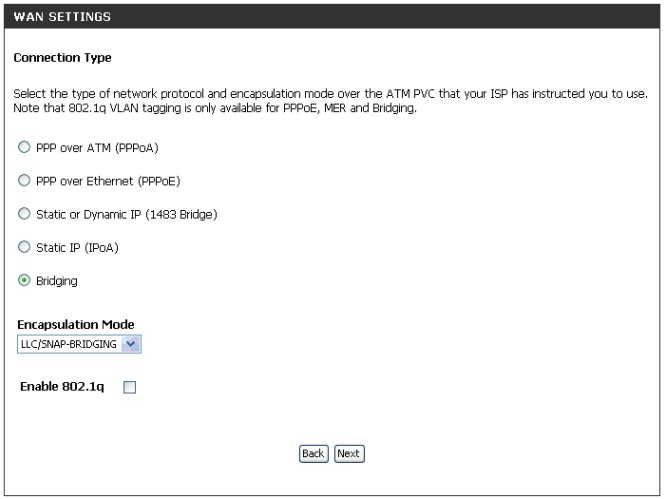
Click the **Setup Wizard** button to launch the **Setup Wizard.**



First configure **VPI** and **VCI** for your ADSL connection. Your ISP has given this information to you. Or select **DSL Auto-connect** and allow router to detect the available VPI/VCI for you. You can also enable QoS (Quality of Service) by checking **Enable Quality Of Service.**



Now select the Connection Type used for the Internet connection. Your ISP has given this information to you. The connection types available are **PPPoA, PPPoE, MER, IPoA** and **Bridge Mode**. The Encapsulation Mode includes **LLC/SNAP-BRIDGING** and **VC/MUX**. Each connection type has different settings that are configured in the next **Setup Wizard** window.

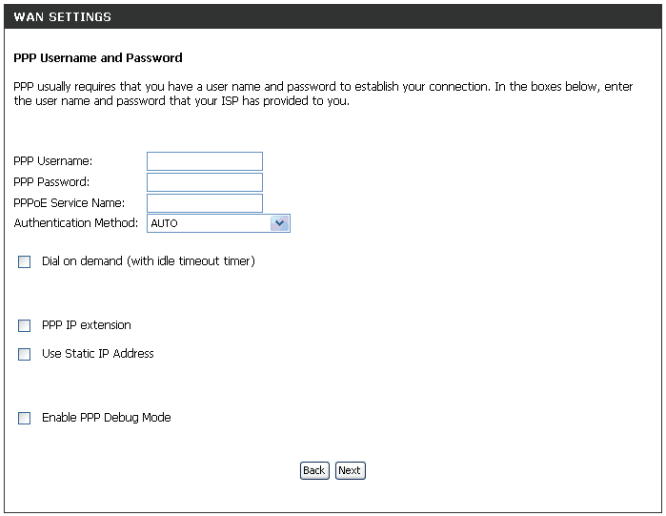


Using the Setup Wizard - For Bridge Mode connections

Click **Next** to go to the next **Setup Wizard** window.

Skip to Page 25: **Using the Setup Wizard - For WAN Connection Settings**

Using the Setup Wizard - For PPPoE/PPPoA connection



Type in the **Username** and **Password** (and PPPoE Service Name, if required by your ISP).

Select the specific **Authentication Method** from the drop-down menu (PAP or CHAP). Or user default AUTO to allow Router to negotiate with PPP server automatically.

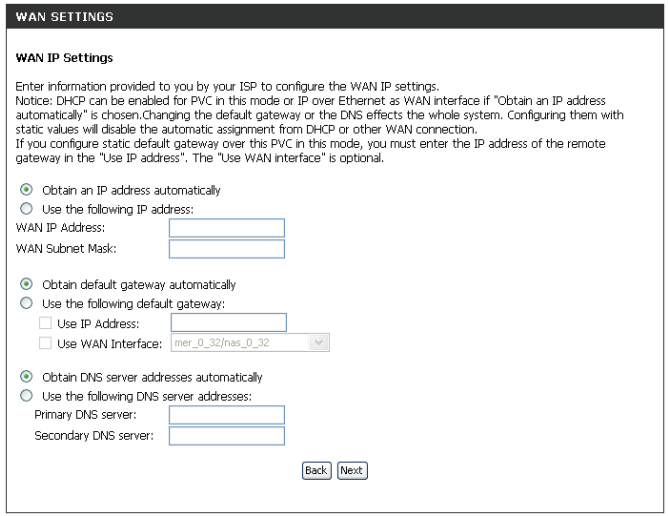
Click **Next** to go to the next **Setup Wizard** window.

Dial on demand
If checked, will tear down the PPP link automatically when there is no incoming/outgoing packet via WAN interface for the programmed period of time that is set below (in minutes). Router activates PPPoE connection automatically when user wants to access Internet.
PPP IP extension
Router passes the obtained IP address to the local PC and acts as a bridge only modem.
Use Static IP Address
Type in the IP address given by your ISP in this field if your Router's IP address is not dynamically assigned.
Enable PPP Debug Mode
Enable PPP debug mode so you can see the PPP authentication process from Status Log.

Using the Setup Wizard - For Dynamic IP (1483 Bridge) connection

Select **Obtain an IP address/Default gateway/DNS server automatically**.

Click **Next** to go to the next **Setup Wizard** window.

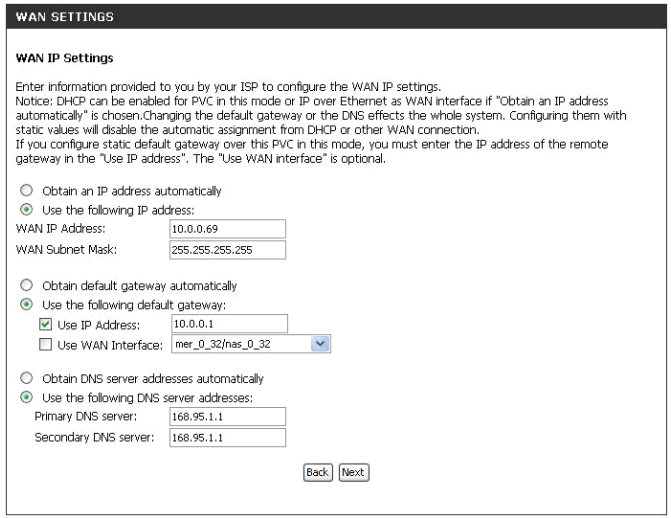


Using the Setup Wizard - For Static IP Address (1483 Bridge) connection

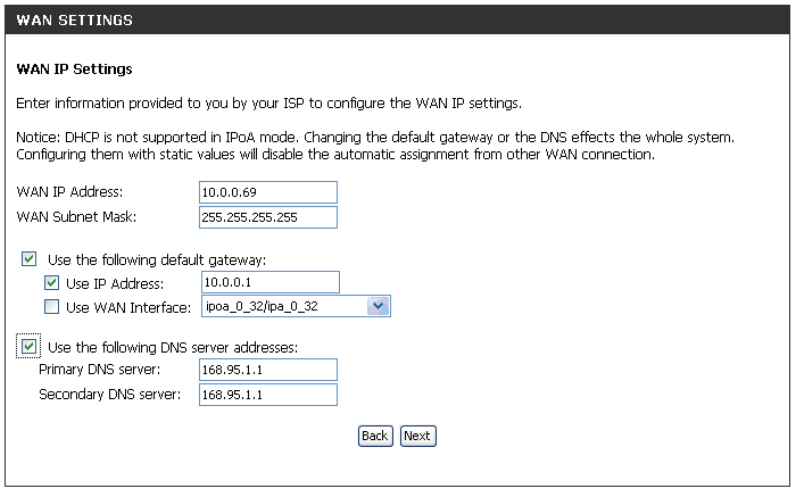
Enter the **WAN IP Address**, **WAN Subnet Mask** provided by your ISP.

Select **Use the following default gateway/DNS server addresses** and enter the **ISP Gateway Address**, **Primary DNS Address**, and **Secondary DNS** Server IP **Address** as instructed by your ISP.

Click **Next** to go to the next **Setup Wizard** window.



Using the Setup Wizard - For Static IP Address (IPoA) connection

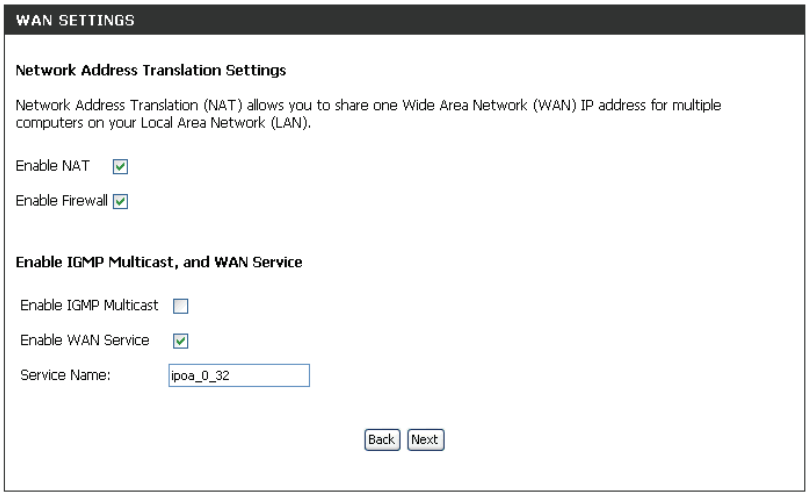


Enter the **WAN IP Address**, **WAN Subnet Mask** provided by your ISP.

Select **Use the following default gateway/DNS server addresses** and enter the **ISP Gateway Address**, **Primary** and **Secondary DNS Server** IP Address as instructed by your ISP.

Click **Next** to go to the next **Setup Wizard** window.

Using the Setup Wizard - For WAN Connection Settings



NAT

Network Address Translation may be enabled or disabled with the pull-down menu. Keep in mind that disabling NAT allows only a single computer to be used for Internet access through the Router. NAT is enabled and disabled for the Router on all connections (i.e. Pvc0 – Pvc7) if your Router is set up for multiple virtual connections.

Firewall

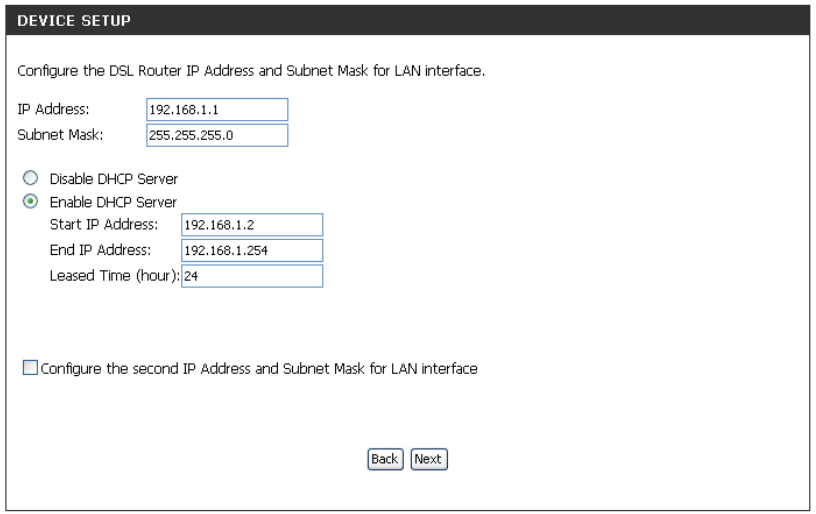
Use this to universally enable or disable the Firewall and Filter features available in the Router. If you disable this you will not be able to configure settings in the **Firewall Configuration** window or **Filters** window in the **Advanced** directory.

Select the specific functions to be enabled.

Click **Next** to go to the next **Setup Wizard** window.

Using the Setup Wizard - For LAN Settings

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router.

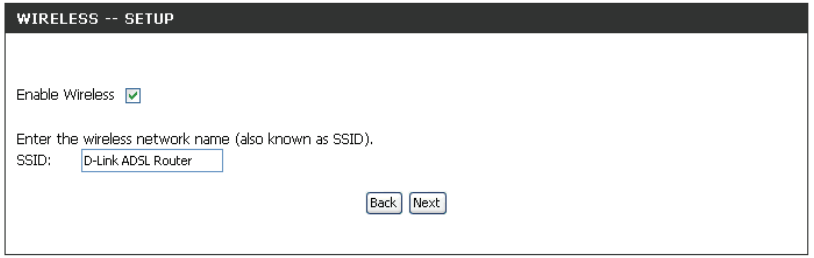


Enter the desired **IP address** and **Subnet Mask**.

Enter the **Start** and **Stop IP Address** for the **DHCP Server**, or disable **DHCP Server**.

Click **Next** to go to the next **Setup Wizard** window.

Using the Setup Wizard - For Wireless LAN Settings



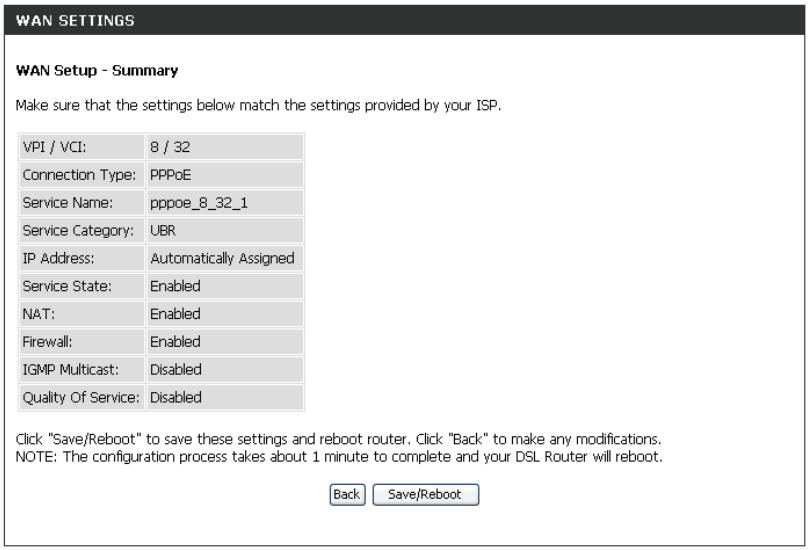
Click the **Enable Wireless** box to allow the router to operate in the wireless environment.

The **SSID** identifies members of the Service Set. Accept the default name or change it to something else. If the default SSID is changed, all other devices on the wireless network must use the same SSID.

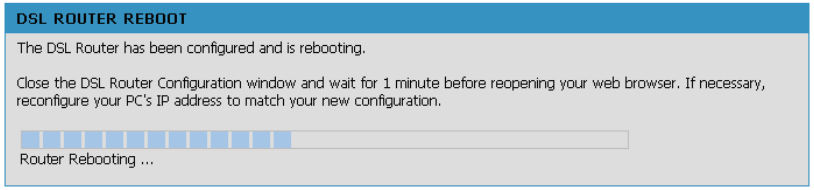
Click **Next** to go to the next window and complete the Setup Wizard.

Using the Setup Wizard - Finish and Restart

Finally you can confirm that the setup process is completed. If you are satisfied that you have entered all the necessary information correctly, click the **Save/Reboot** button to save the new configuration settings and restart the Router. If you need to change settings from a previous window, click the **Back** button.

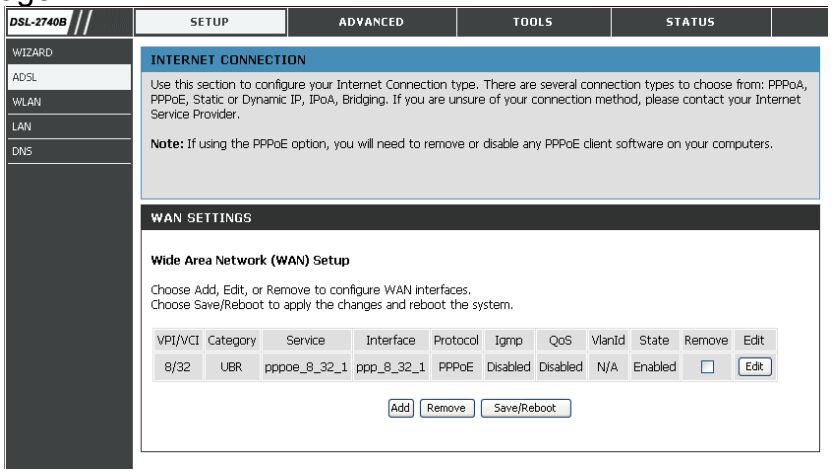


Do not turn the Router off while it is restarting. After the Router is finished restarting, you are now ready to continue to configure the Router as desired. You may want to test the WAN connection by accessing the Internet with your browser.



ADSL

To access the ADSL (WAN) Settings window, click on the **ADSL** link button on the left side of the first window that appears when you successfully access the web manager. You can add, remove and edit the WAN interface from this page:



To add a WAN connection, click the **Add** button and follow the step-by-step instruction as in **WIZARD**.

To delete a WAN connection, select the specific **Remove** box and then click **Remove** button.

To edit a WAN connection, click the specific WAN interface **Edit** button and follow the step-by-step instruction as in **WIZARD**.

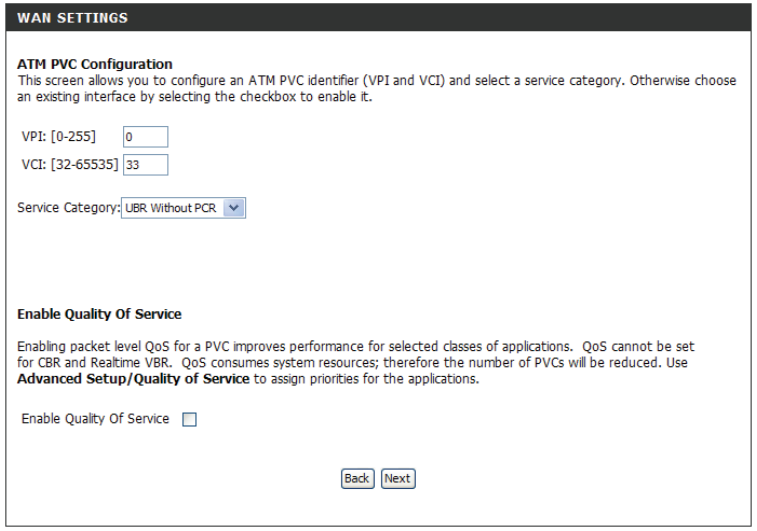
Click the **Save/Reboot** button to apply your settings.

Service Category

The ATM settings allow the user to adjust ATM Quality of Service (QoS) or traffic parameters to suit specific traffic requirements. For applications or circumstances where packet loss or packet delay is a concern, ATM QoS can be adjusted to minimize problems. For most accounts, it will not be necessary to change these settings. Altering QoS settings can adversely affect performance of some commonly used Internet applications.

If you plan to change QoS or traffic parameters, contact your ISP or network services provider for information on what types of adjustment are available or possible for your account. Your ISP may not support the class of service you want to use.

To adjust ATM QoS parameters, select one of the Service Categories listed here and type in the PCR value in the entry field below. For the VBR service category, an additional parameter (SCR) must also be defined.



WLAN

To access the **WLAN Settings** window, click on the **WLAN** link button on the left side of the first window that appears when you successfully access the web manager.

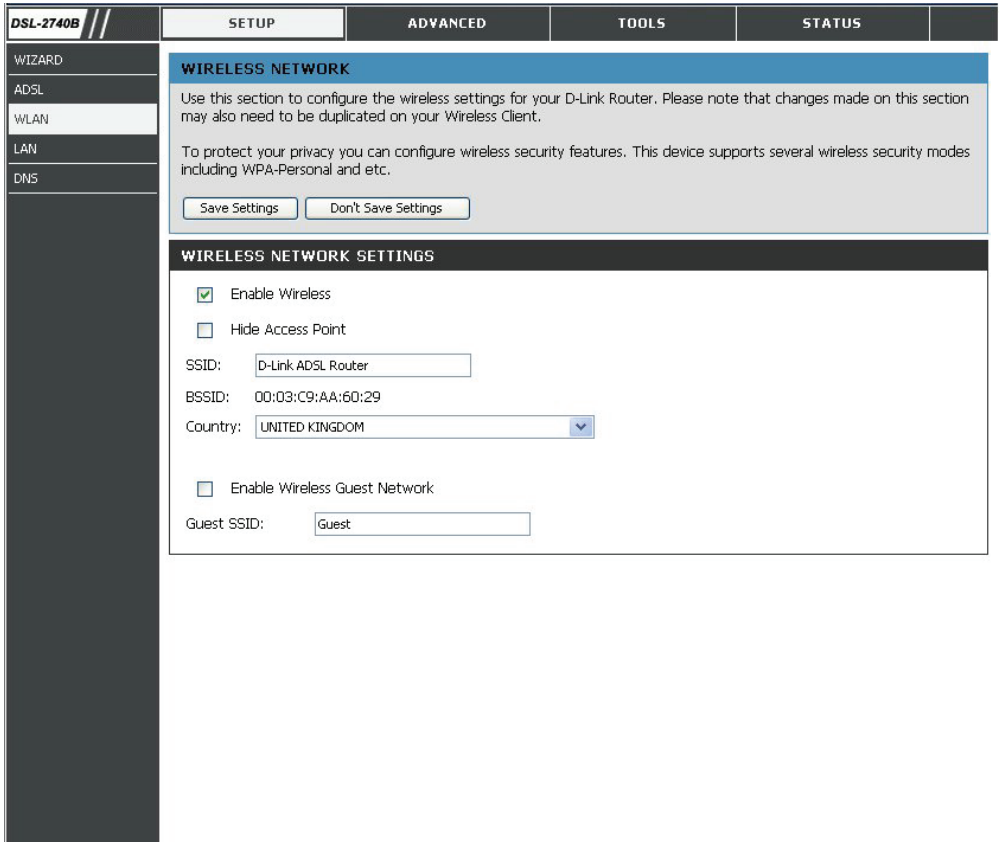
Click the **Enable Wireless** box to allow the router to operate in the wireless environment.

Click the **Hide Access Point** box to allow the router to stop broadcasting its SSID.

The **SSID** identifies members of the Service Set. Accept the default name or change it to something else. If the default SSID is changed, all other devices on the wireless network must use the same SSID.

Select your region form the **Country** drop down list. Operating channels are different for different country/region based on regulation.

Please go to **Advanced** section for more wireless settings.



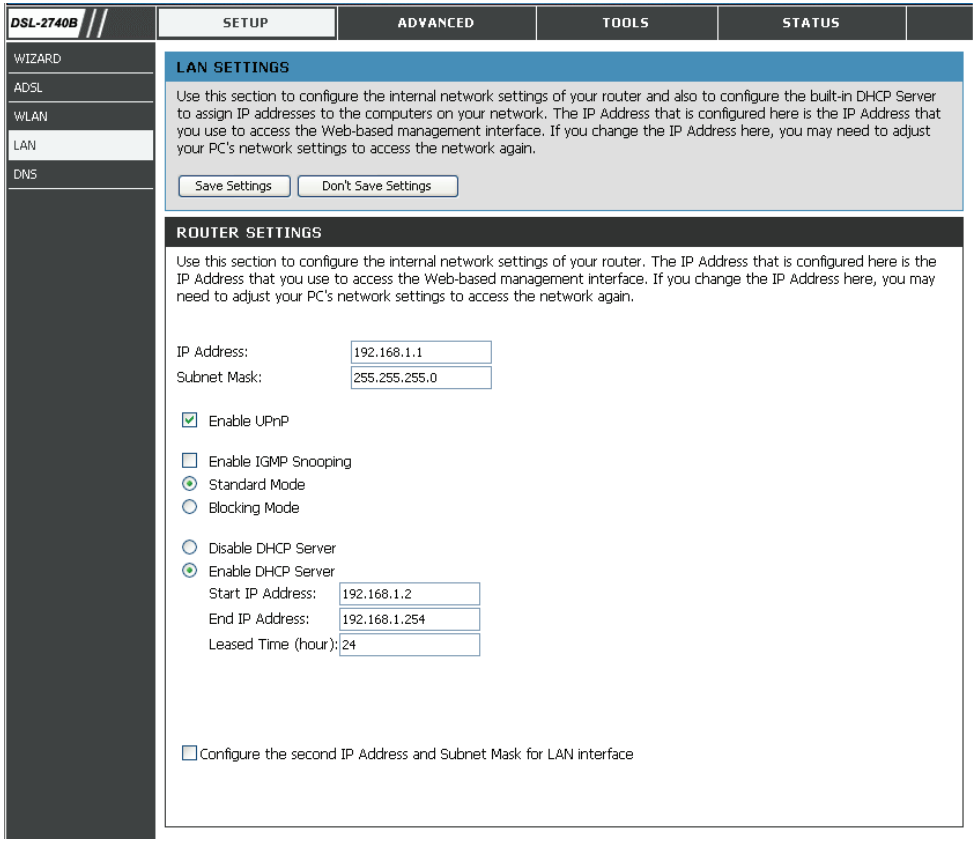
LAN

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router.

To access the LAN setting window, click the **LAN** button in the **Setup** directory.

To change the LAN **IP Address** or **Subnet Mask**, type in the desired values and click the **Save Settings** button. You will be asked to reboot by a pop-up window. Click **OK** to reboot the router.

You might need to re-configure your PC NIC seetings to enter the Router's web manager after reboot.



UPnP: When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices.

IGMP Snooping: IGMP snooping is a feature that allows the layer-2 device (switch) to "listen in" on the IGMP conversation between hosts and routers.

Standard Mode: Listen and forward

Blocking Mode: Listen and block

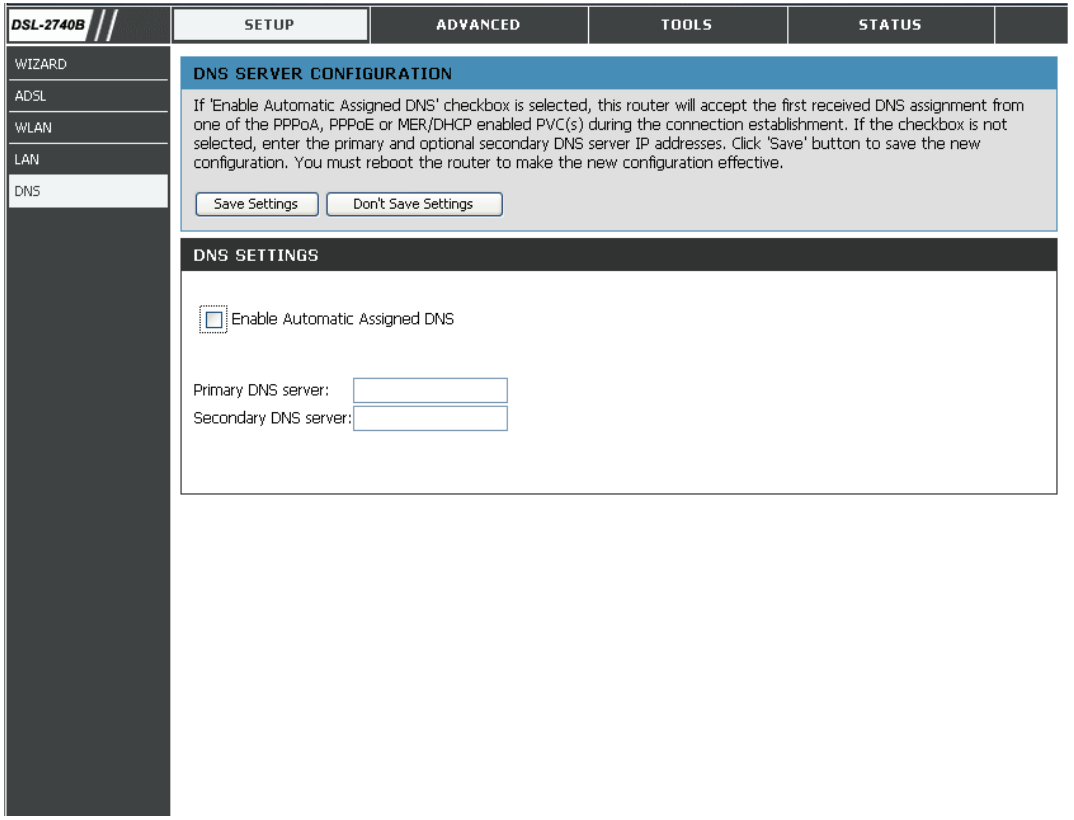
DHCP: The DHCP server is enabled by default for the Router's Ethernet LAN interface. DHCP service will supply IP settings to workstations configured to automatically obtain IP settings that are connected to the Router though the Ethernet port. When the Router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the Router the range of IP addresses in the pool used for DHCP on the LAN will also be changed. The IP address pool can be up to 253 IP addresses.

DNS

The Router can be configured to relay DNS settings from your ISP or another available service to workstations on your LAN. When using DNS relay, the Router will accept DNS requests from hosts on the LAN and forward them to the ISP's, or alternative DNS servers. DNS relay can use auto discovery or the DNS IP address can be manually entered by the user. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most users who are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, should check **Enable Automatic Assigned DNS** box.

If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the **Primary DNS Server** and the **Secondary DNS Server**.

When you have configured the DNS settings as desired, click the **Save Settings** button.

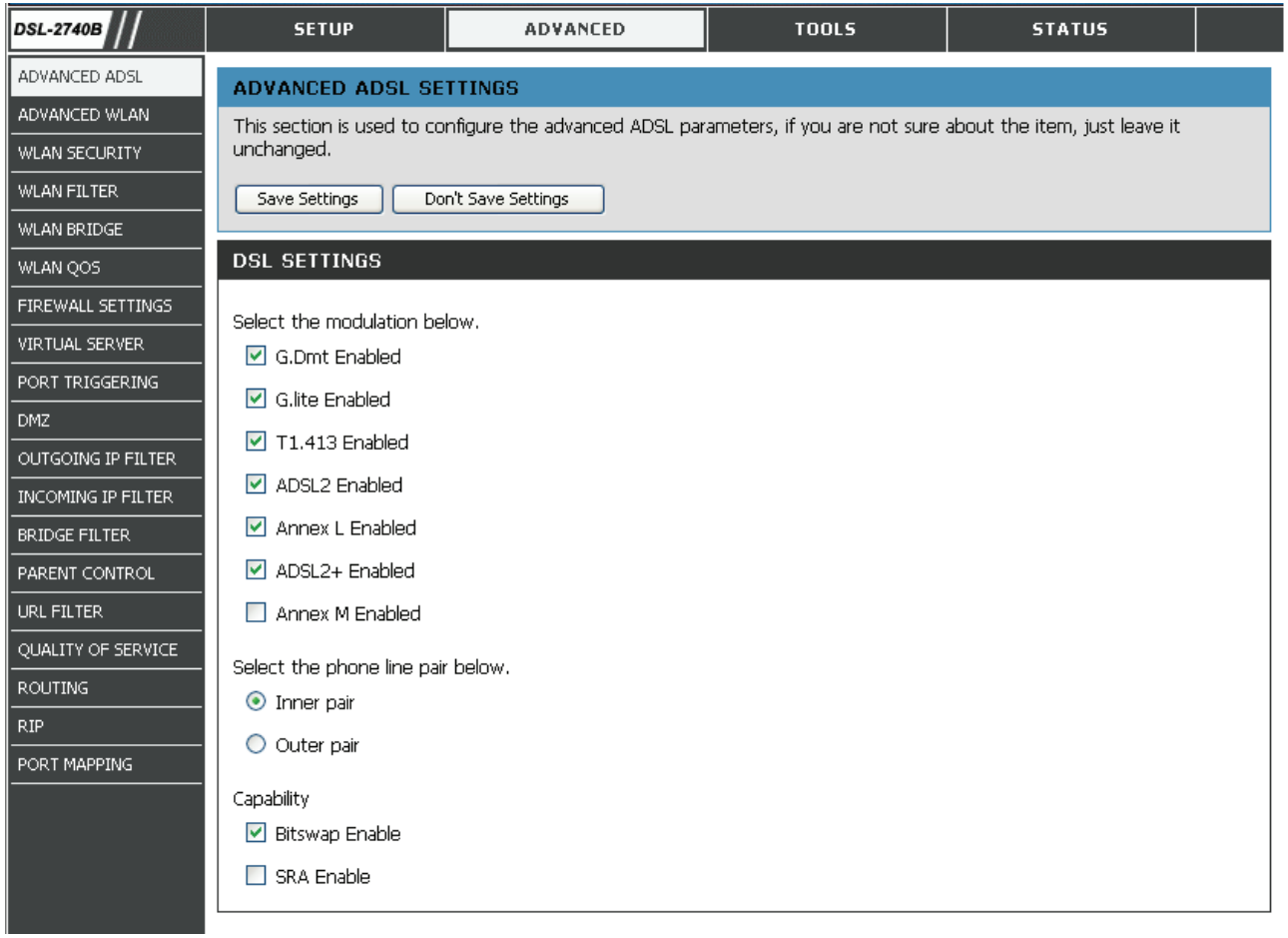


ADVANCED

These include the more advanced features used for network management and security as well as administrative tools to manage the Router, view statistics and other information used to examine performance and for troubleshooting.

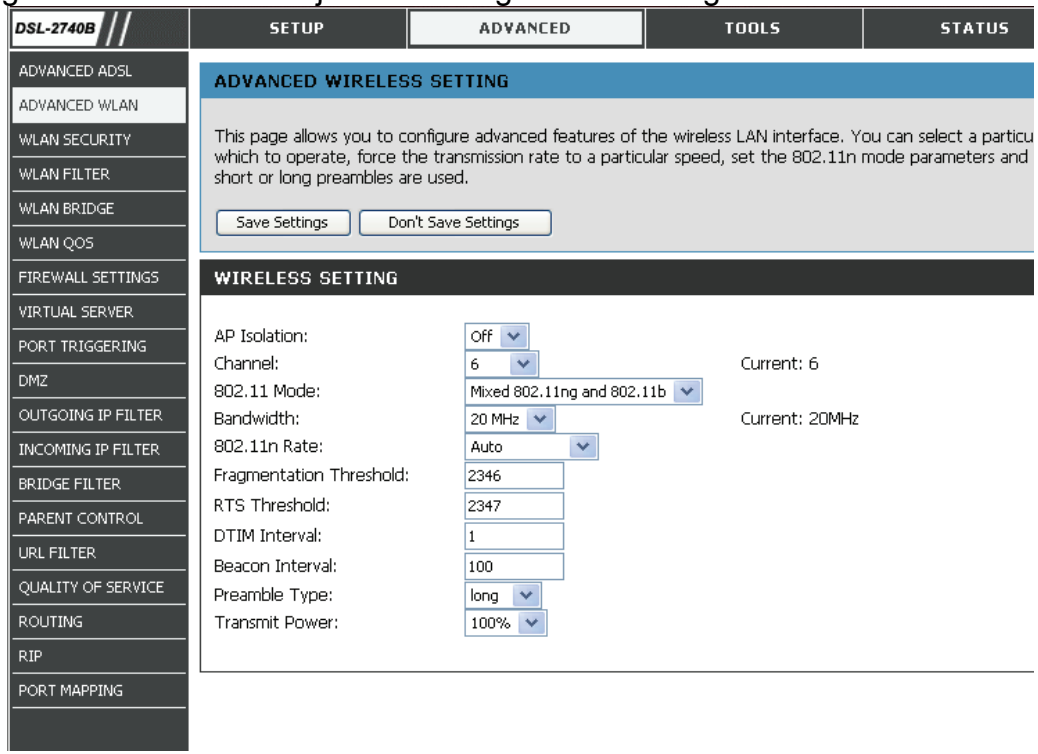
ADVANCED ADSL

The **ADSL Configuration** window allows the user to set the configuration for ADSL protocols. For most ADSL accounts the default settings ***(ADSL2+)*** will work. This configuration works with all ADSL implementations. Do not change any settings unless you have been instructed. To make ADSL settings, select the desired items and click the **Save Settings** button.



ADVANCED WLAN

ADVANCED WLAN page allows you to do more advanced wireless settings. Most users will do just fine using default settings.



AP Isolation: This is used to islolate wireless clients which connect to different APs.

Channel: Operation channel of your access point. Channel availability is different for different countries due to their regulation.

802.11 Mode: Select **Mixed 802.11ng and 802.11b** to operate in b/g/n mode. Or select specified mode to use.

Bandwidth: Channel bandwidth. Maximum rate for **20 MHz** is 130 Mbps. Maximum rate for **40 MHz** is 270 Mbps.

802.11n Rate: Select **Auto** to operate in all available transmission rates. Or select specified rate to use.

Fragmentation Threshold: Maximum frame size. Frame larger than the threshold are fragmented into multiple packets and transmitted. The range is **256~2346** bytes.

RTS Threshold: If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.The range is **0~2347** bytes.

DTIM Interval: Interval of the Delivery Traffic Indication Message (DTIM). A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the router has buffered broadcast or multicast for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast message. The range is **1~255** milliseconds,

Beacon Interval: The **Beacon Interval** value indicates the frequency interval of the beacon. A beacon is a packet broadcast by the router to synchronize the wireless network. The value is **1~65535** milliseconds.

Preamble Type: The **preamble** is used to synchronize the transmitter and receiver and derives common timing relationship. The **Short** preamble improves throughput but not all wireless clients support short preamble type.

Transmit Power: 5-level of transmit power are available: **20%**, **40%**, **60%**, **80%**, and **100%**.

WLAN SECURITY

In the **WLAN Security** window, select the type of security you want to configure. The window will change to present the settings specific to the method being configured. The Router's wireless security options include WEP, 802.1x, WPA, WPA-PSK (Pre- Shared Key), WPA2, WPA2-PSK, Mixed WPA/WPA2, Mixed WPA/WPA2-PSK.

WEP

WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. The router offers 64-, or 128-bit encryption with four keys available.

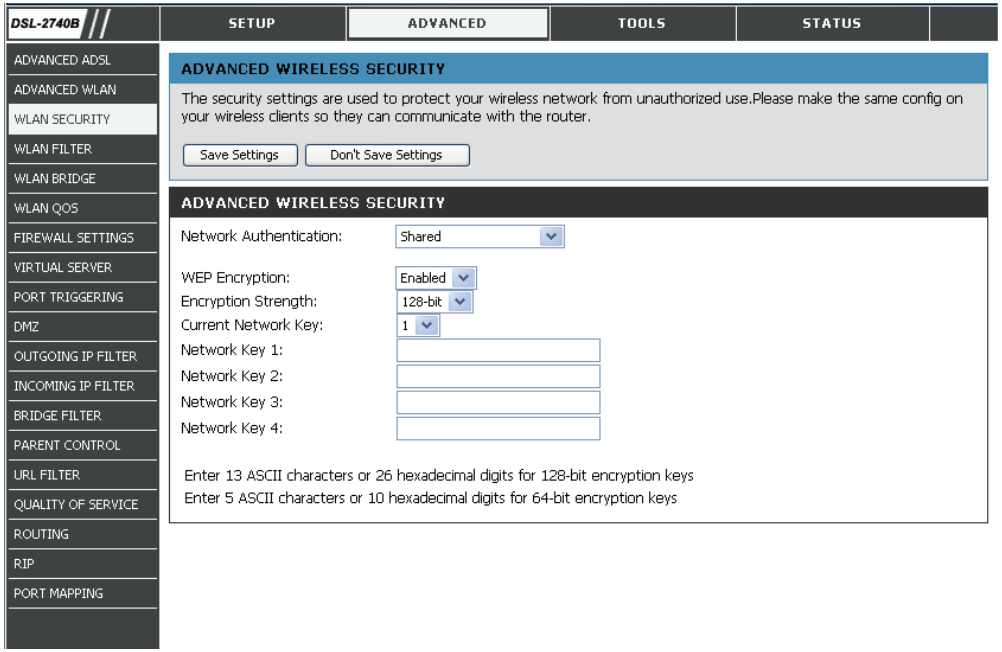
Select **Network Authentication** type from the drop-down list. (**Shared** is bettern than **Open**)

Select **Encryption Strength** from the drop-down list. (**128-bit** is stronger than **64-bit**)

Specify the encryption key from the **Current Network Key** drop-down list.

Enter the key into the **Network Key** field 1~4. (Key length is outlined at the bottom of the window.)

Click the **Save Settings** button to apply settings.



802.1x

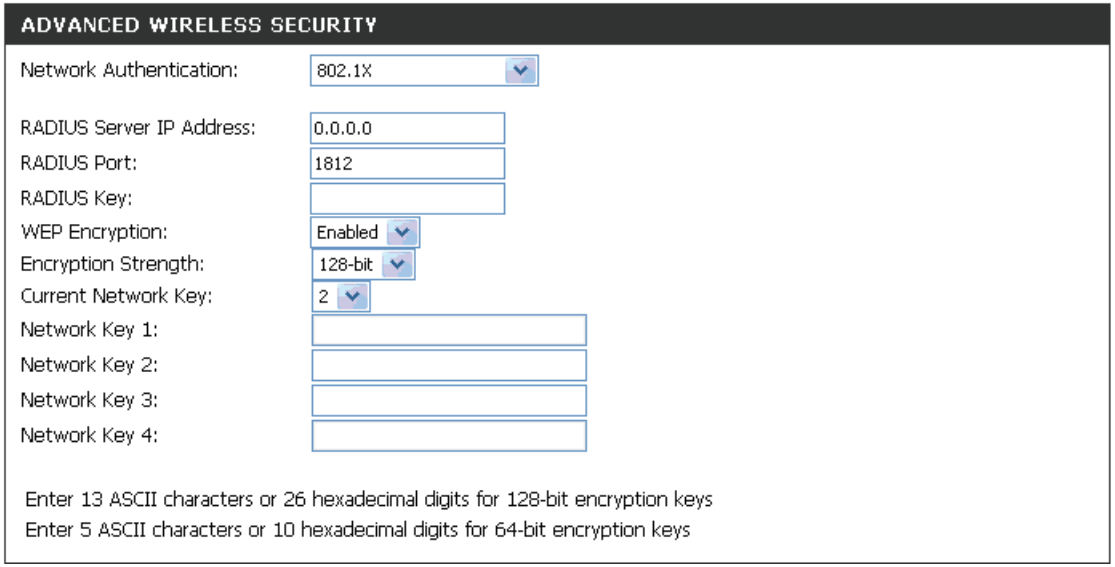
Some network-security experts now recommend that wireless networks use 802.1X security measures to overcome some weaknesses in standard WEP applications. A RADIUS server is used to authenticate all potential users.

Select 802.1x from the **Network Authentication** drop-down list.

Enter your RADIUS server data: **IP Address, Port, and Key**.

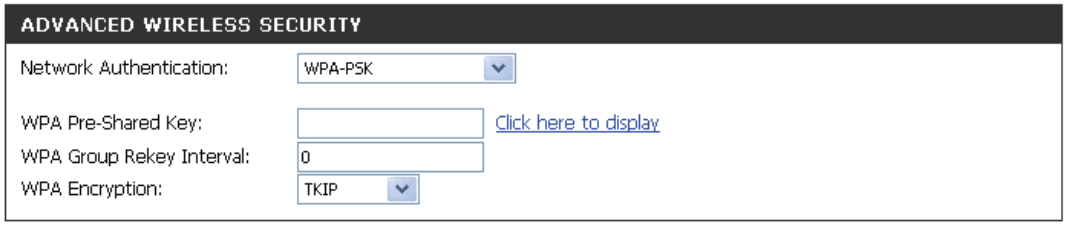
Configure WEP Encryption. (See above section for detail.)

Click the **Save Settings** button to apply settings.



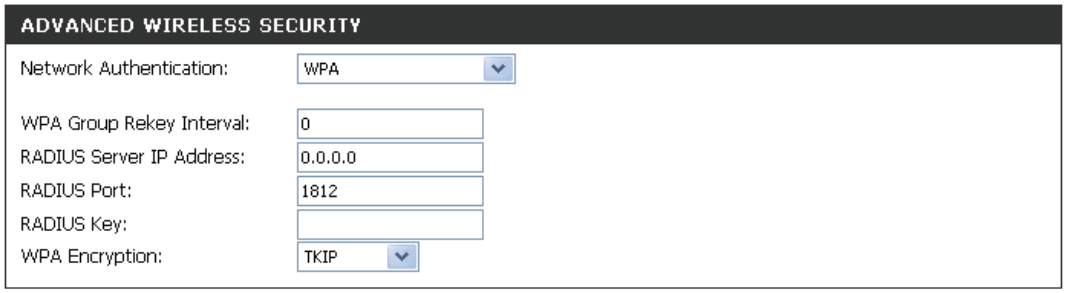
WPA-PSK

WPA-PSK configuration is similar to WEP. The key length is between 8 to 63 ASCII codes.



WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP.
To take full advantage of WPA, a RADIUS server is needed in your network to authenticate users. For most home or SOHO users, WPA-PSK is the easiest way to implement and provides adequate protection for your wireless network.



Select your wireless security method from the **Network Authentication** drop-down list.

Enter the **RADIUS Server IP Address**, **Port**, and **Key**.

Select the encryption method from **WPA Encryption** drop-down list.

Click **Save Settings** to apply your settings.

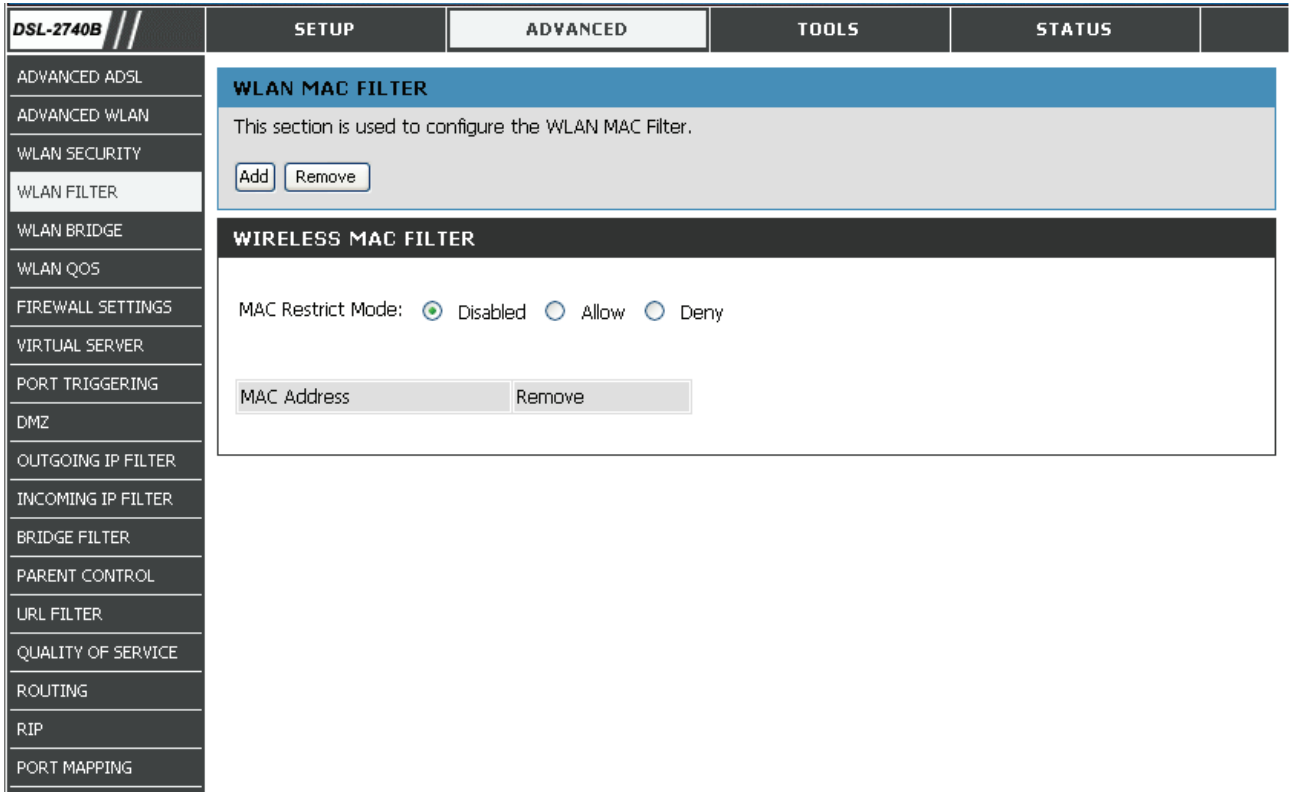
WLAN Filter

The **WLAN Filter** is used to control wireless client devices access based on their MAC addresses. You can choose to allow or deny the specific MAC addresses.

Click the **Add** button to enter WLAN Filter configuration window.

Enter the specific MAC address and click the **Save Settings** button to apply.

Click the **MAC Restrict Mode** radio button to select filter rule (**Allow** or **Deny**) and enable the WLAN filter.



WLAN BRIDGE

Wireless bridge is used to bridge AP traffic between other APs. You can select Wireless Bridge (also known as Wireless Distribution System) to disables access point functionality. Selecting Access Point enables access point functionality. Wireless bridge functionality will still be available and wireless stations will be able to associate to the AP. Select Disabled in Bridge Restrict which disables wireless bridge restriction. Any wireless bridge will be granted access. Selecting Enabled or Enabled (Scan) enables wireless bridge restriction. Only those bridges selected in Remote Bridges will be granted access. Only APs operating in the same channel can be bridged together.

Notice Wlreless Bridge function is available only when 802.11n is disabled. Please go to **ADVANCED WLAN** page to disable 802.11n before configuring Wireless Bridge.

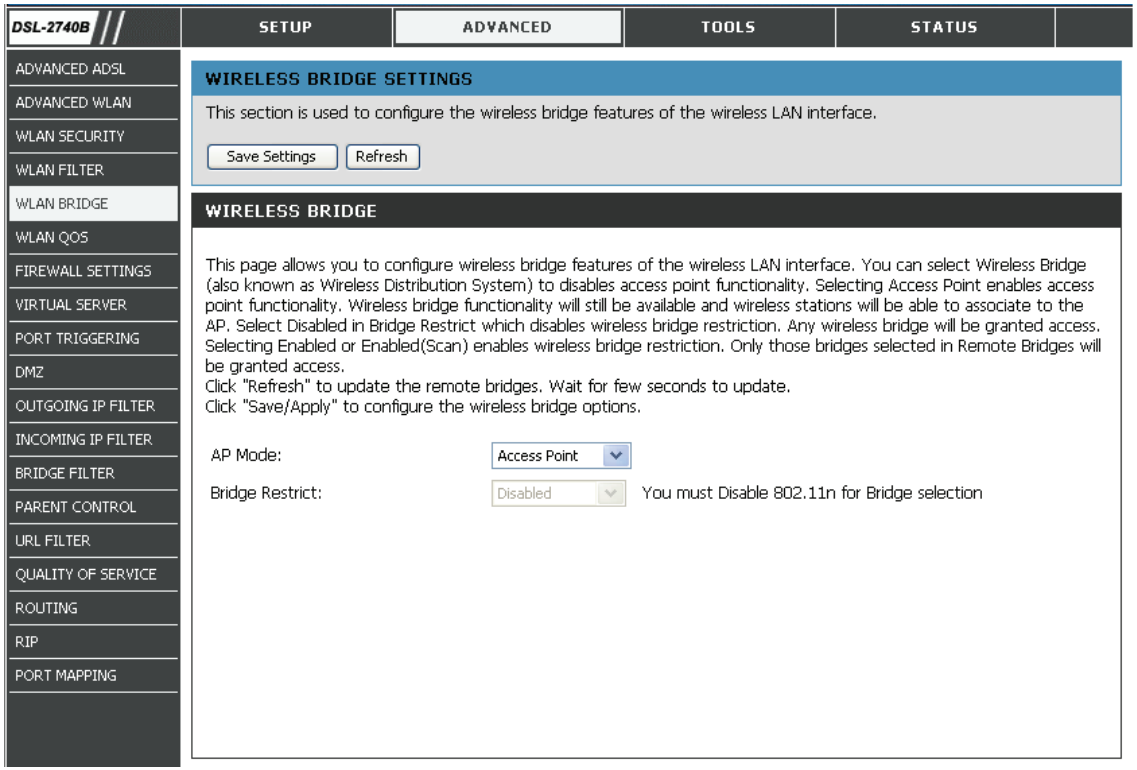
Select **AP Mode** from the drop-down list.

Select **Enabled** in **Bridge Restrict** drop-down list and enter the MAC address of the AP which to be bridged. Or,

Select **Enabled(Scan)** in **Bridge Restrict** drop-down list and the Router starts to search and displays available APs.

Click the specific AP check box.

Click the **Save Settings** button to apply settings.



WLAN QOS

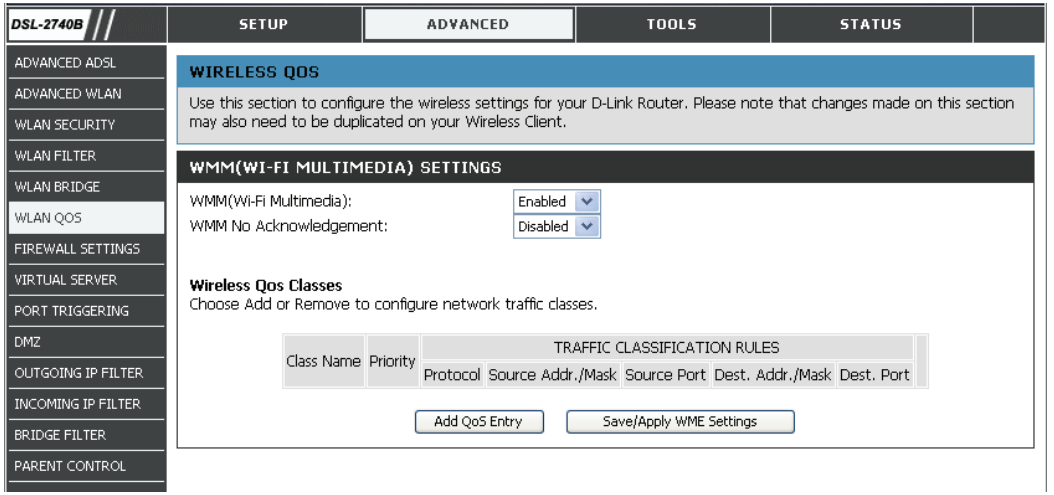
WLAN QoS (Quality of Service), also called WMM (Wi-Fi Multi-media), is used to prioritize the wireless packets when you are using wireles device transmitting delay-sensitive packets (voice, video,..etc).

Notice WMM is not supported by IEEE 802.11n yet. You must trun off 802.11n in **ADVANCED WLAN** section before configuring any WMM settings.

Select **Enabled** from the **WMM (Wi-Fi Multimedia)** drop-down list.

Select **Disabled** from the **WMM No Acknowledgement** drop-down list if your wireless link quality is good. It can increase more bandwidth. Or select **Disable** if your link quality is an issue.

Click the **Add QoS Entry** button to enter QoS configuration window.



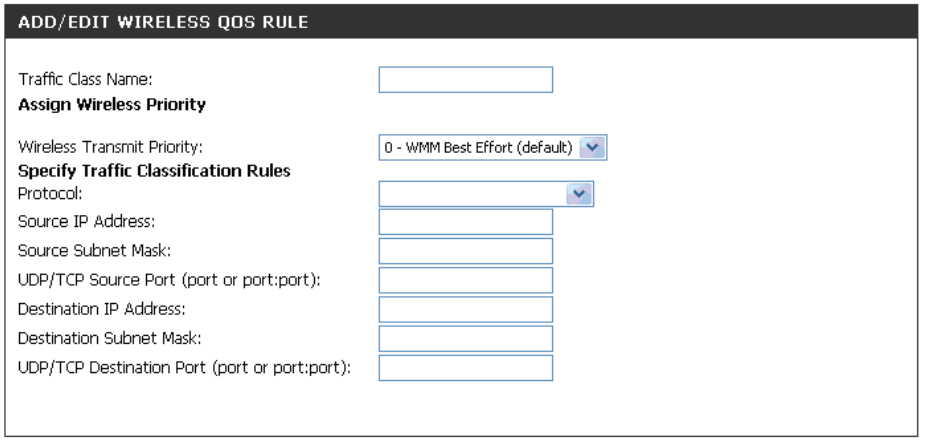
Enter the name of the rule.

Select priority from the **Wireless Transmit Priority** drop-down list (**1~4**, higher number has higher priority).

Specify traffic classification rules. The classification can be de fined in the following parameters: **Protocol**, **Source/Destination IP Address**, **and Source/Destination Port**.

Click the **Save Settings** button to apply this rule.

Click the **Save/Apply WME Settings** button to apply settings.



FIREWALL

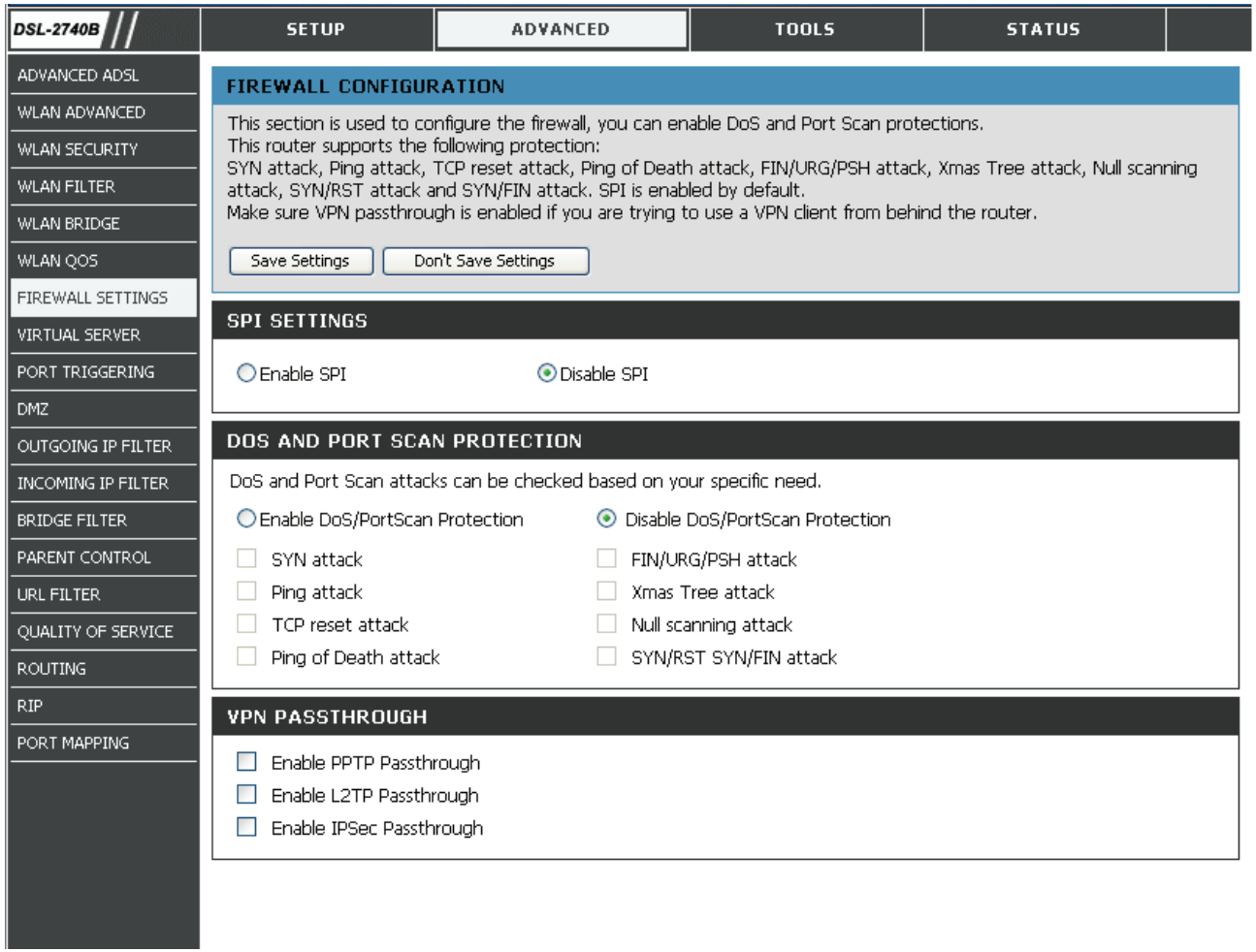
The **Firewall Configuration** window allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. There are two general types of protection (DoS, Port Scan) that can be enabled on the Router, as well as filtering for specific packet types sometimes used by hackers.

SPI: SPI (Stateful Packet Inspection) is a firewall feature that checks the state of network connections. Only legitimate packets are allowed to passthrough.

DoS and Port Scan Protection: A DoS (denial-of-service) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

VPN Passthrough: Select specific VPN type from the VPN **Passthrough** check-box if a VPN client is used behind the Router.



VIRTUAL SERVER

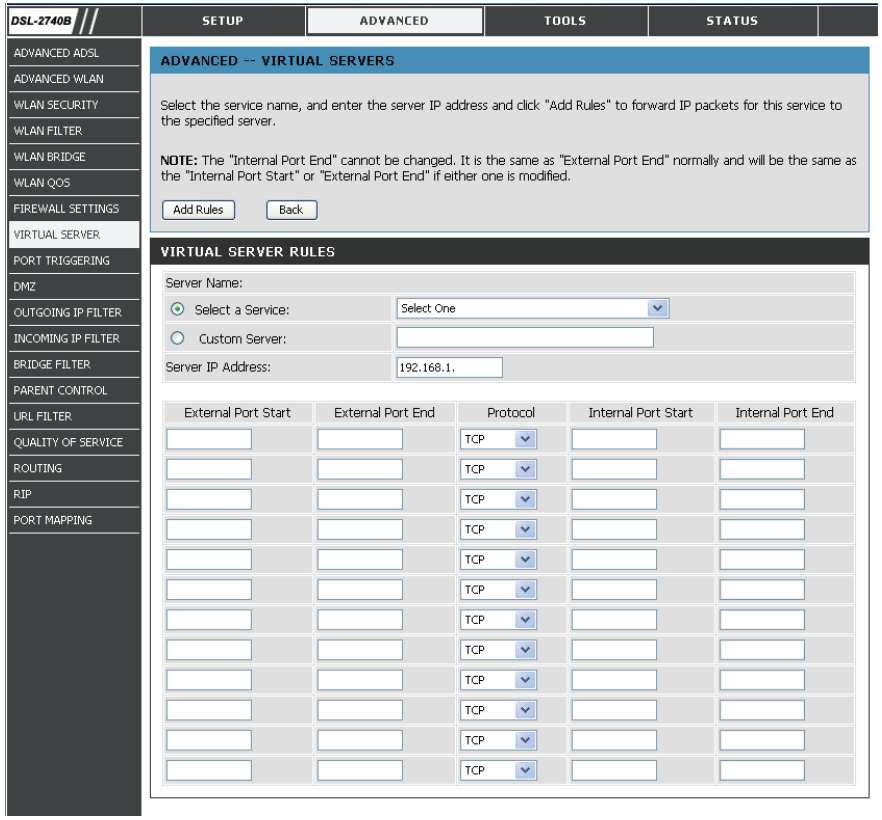
Use the **Virtual Server** window to set up single-port or static-port range forwarding rules applied to inbound (WAN-to-LAN) traffic. The Virtual Server function allows remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DSL-2740B will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the LAN IP address you specify. Remember that the specified Private IP Address must be within the useable range of the subnet occupied by the Router.

Click the **Add A Rule** button to enter your virtual server configuration window.

Select a service from the drop down list for pre-configured server or select **Custom Server** to define your own server.

Enter your server IP address, protocol and port number.

Click **Add Rules** button to apply settings.



Server IP Address: IP address of your server

External Port Start/End: Starting and Ending port number for remote users

Protocol: Protocol used by your server

Internal Port Start/End: Starting and Ending port number that the router will forward to (In most cases, they are the same as External port numbers)

Notice There are many different pre-configured rules available for specific functions such as Internet gaming, VPN, streaming and interactive multi-media, standard TCP/IP protocols, reserved ports, p2p, network management applications, and so on.

PORT TRIGGERING

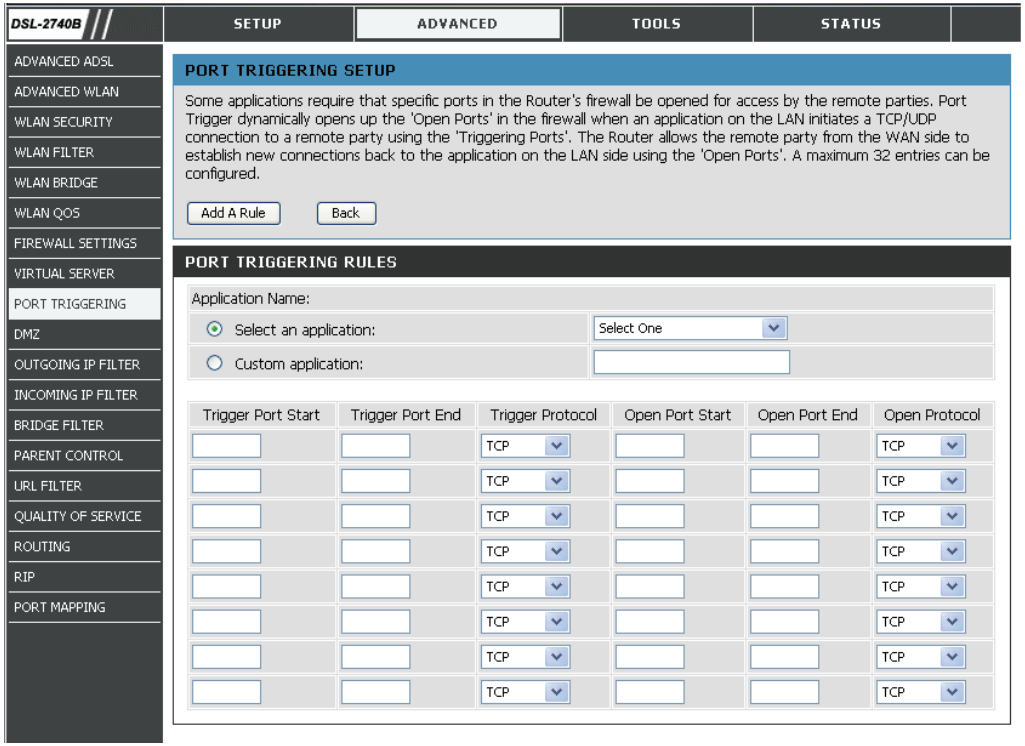
Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Trigger dynamically opens up the 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.

Click the **Add Rule** button to enter your port triggering configuration window.

Select an application from the drop down list for pre-configured applicationr or select **Custom Application** to define your own rules.

Enter your trigger/open port number(s), and trigger/open protocol.

Click **Add A Rule** button to apply settings.



Trigger Port Start/End: Triggered port number initiated by local host

Trigger Protocol: Triggered protocol initiated by local host

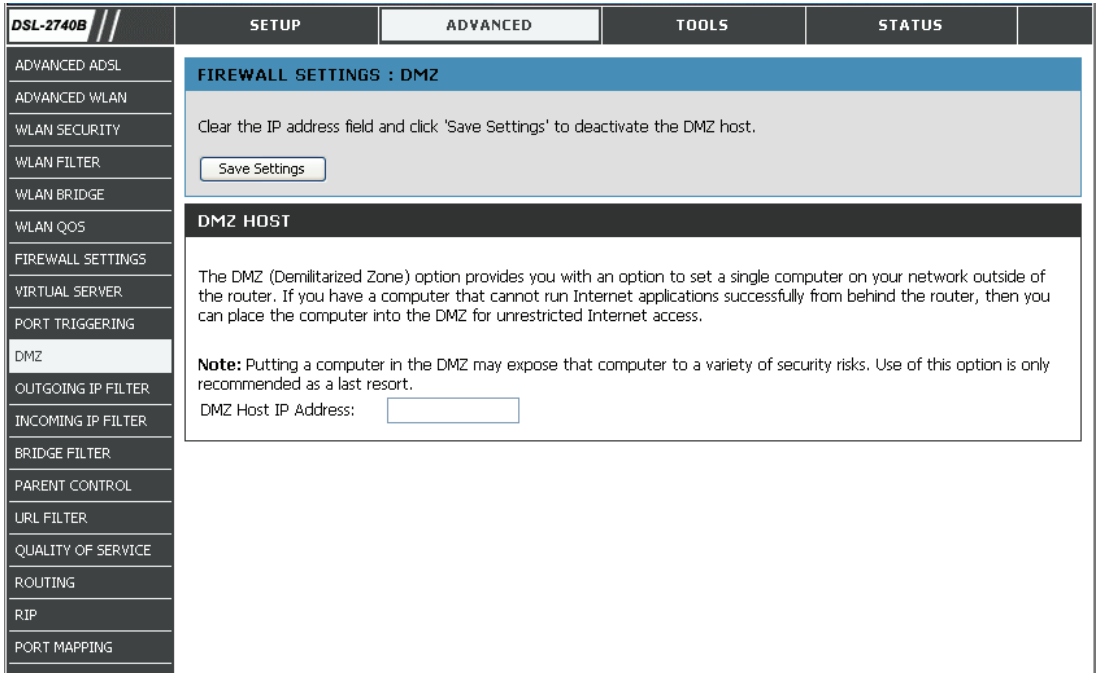
Open Port Start/End: Opened port number(s) for remote users

Open Protocol: Opened protocol for remote users

DMZ

Since some applications are not compatible with NAT, the Router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.

To designate a DMZ IP address, type in the IP Address of the server or device on your LAN in the **DMZ Host IP Address** box, and click the **Save Settings** button. To remove DMZ status from the designated IP address, clear the IP address in the box and click the **Save Settings** button.



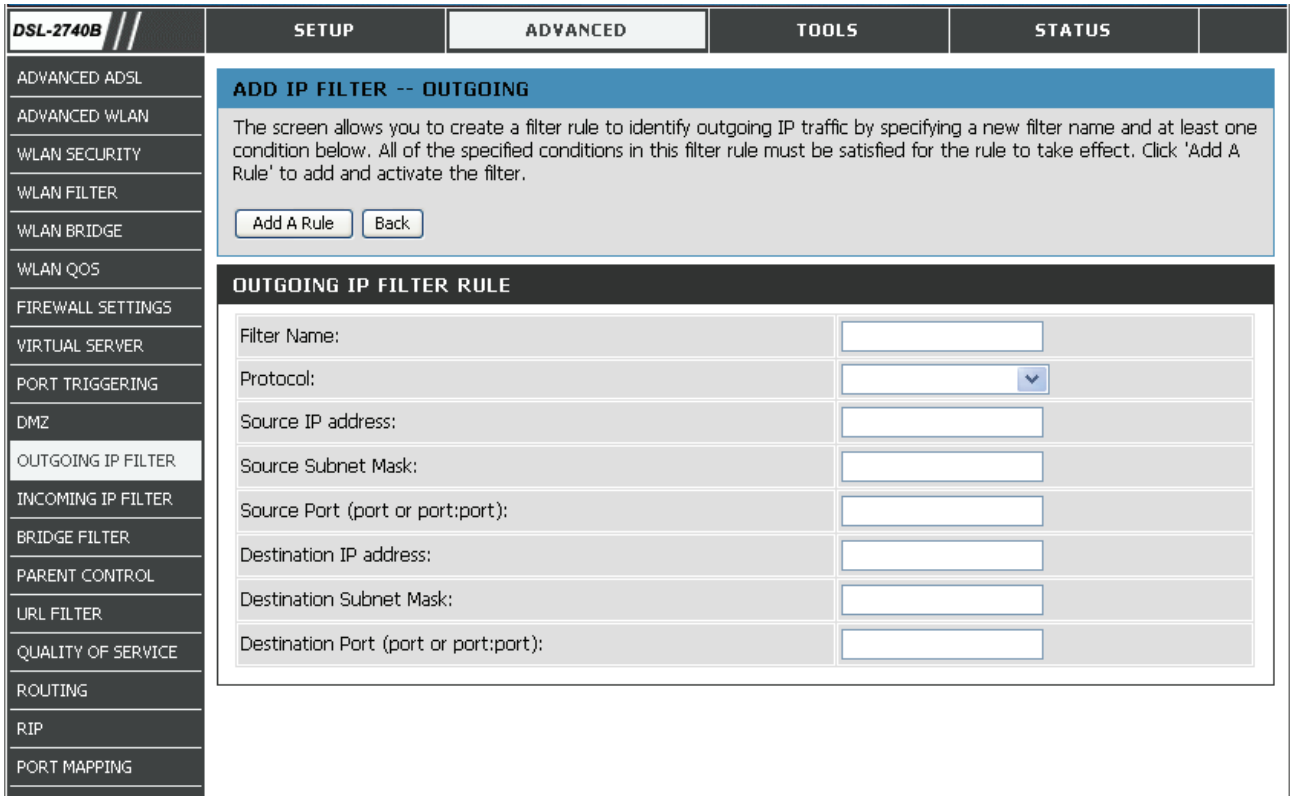
OUTGOING IP FILTER

By default, all outgoing packets are allowed. But you can block specific type of packets from local hosts to Internet by setting up outgoing IP filter.

Click the **Add A Rule** button to enter your outgoing IP filter configuration window.

Enter the filter name and at least one of the following criteria: Protocol, Source/Destination IP Address, and Source/Destination Port.

Click **Add A Rules** button to apply settings.



INCOMING IP FILTER

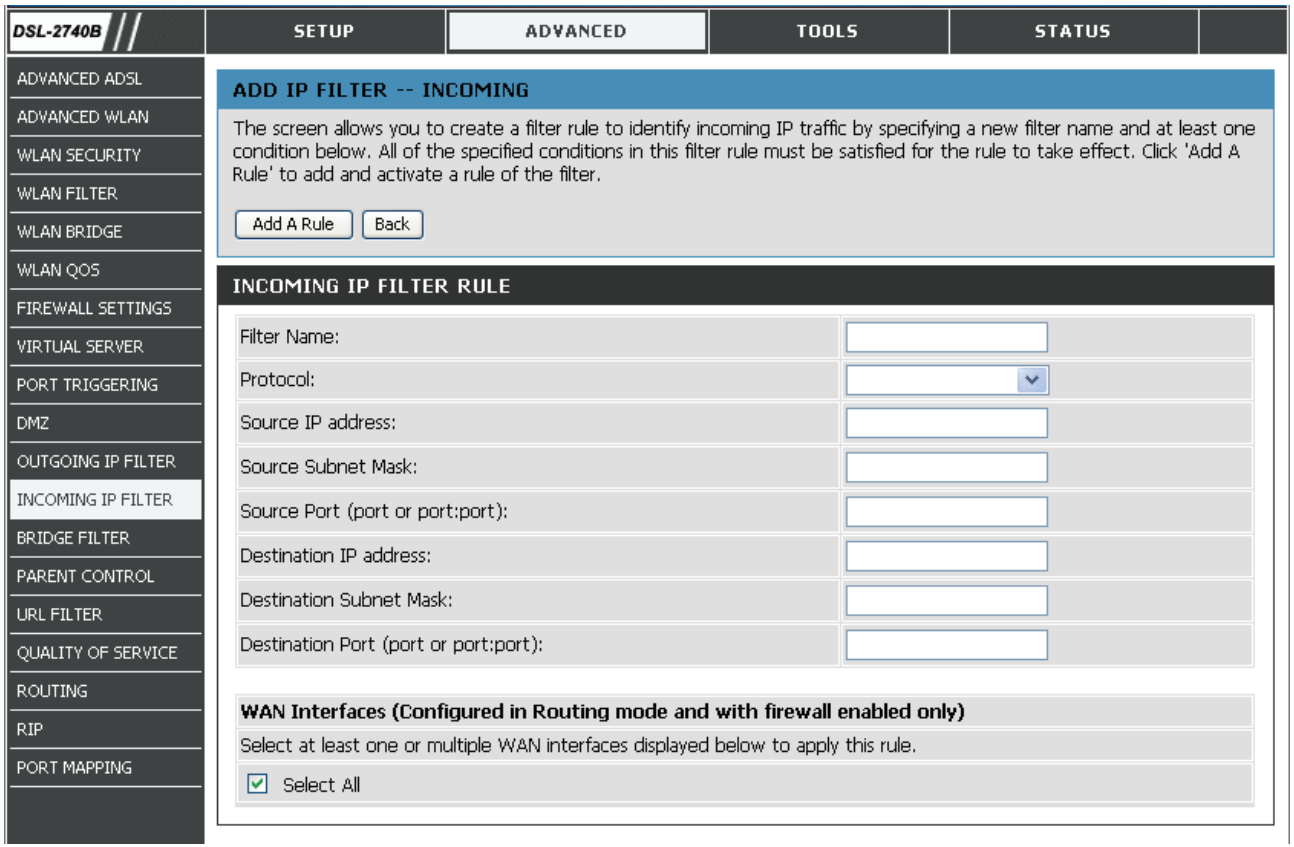
By default, all incoming packets are blocked if Firewall is enabled. But you can allow specific type of packets to be accepted by setting up incoming IP filter.

Click the **Add A Rule** button to enter your incoming IP filter configuration window.

Enter the filter name and at least one of the following criteria: Protocol, Source/Destination IP Address, and Source/Destination Port.

Select WAN interface(s) to apply this rule.

Click **Add A Rules** button to apply settings.



BRIDGE FILTER

Bridge filters are used to block or allow various types of packets through the WAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. Bridge Filter is only effective on ATM PVCs configured in **Bridge** mode. The Global Policy **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching with any of the specified rules in the following table. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching with any of the specified rules in the following table.

Click **Change Policy** button to change bridge filter policy between **Forwarded** and **Blocked**.

Click the **Add A Rule** button to enter your bridge filter configuration window.

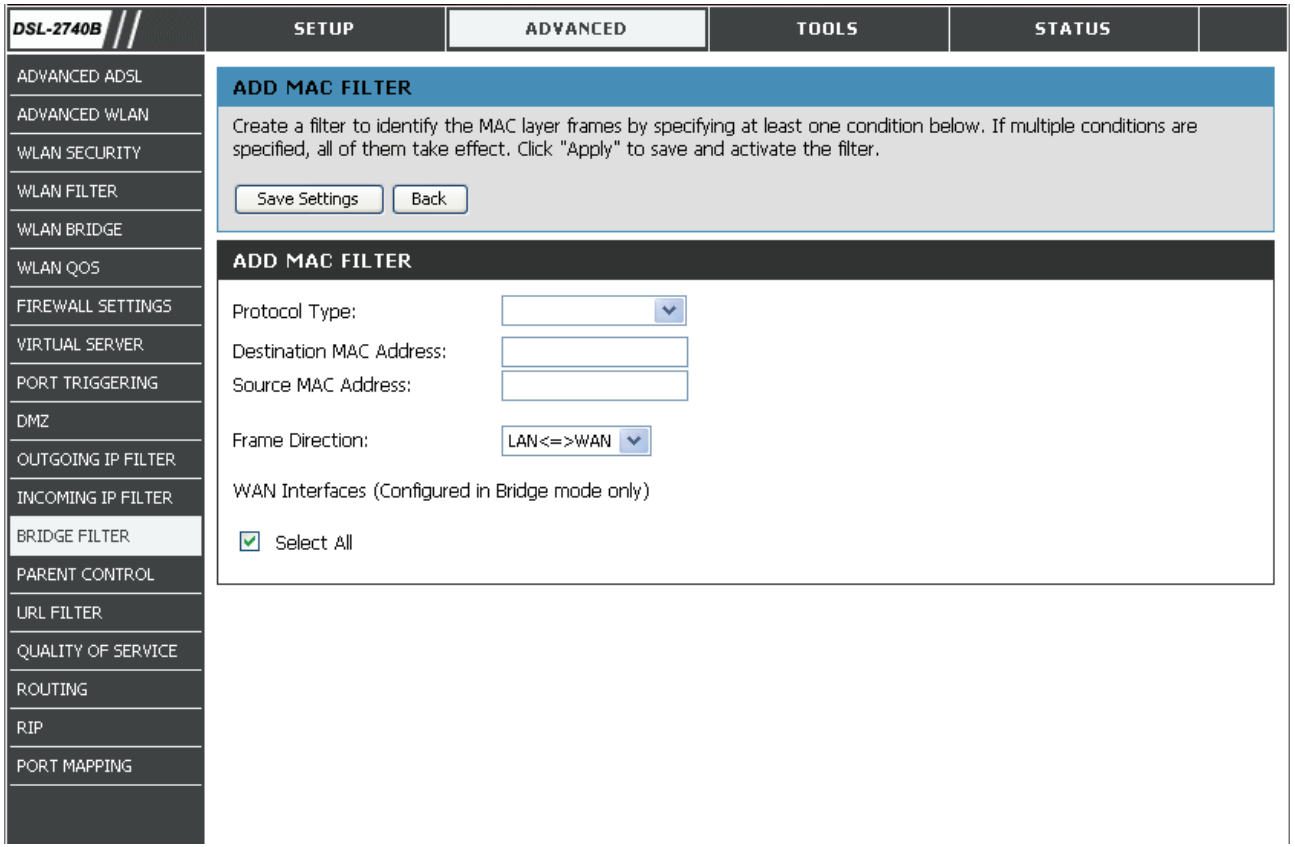
Select **Protocol Type** from the drop-down list, or leave it blank for all protocols.

Enter the Destination/Source MAC address of the specific devices.

Select **Frame Direction** from the drop-down list. **LAN<=>WAN**: Both directions. **WAN=>LAN**: From WAN to LAN only. **LAN=>WAN**: From LAN to WAN only.

Select the WAN interfaces (Bridge only).

Click **Save Settings** button to apply filter rule.



PARENT CONTROL

Parent control is used to prevent specific local hosts from accessing Internet based on their MAC address.

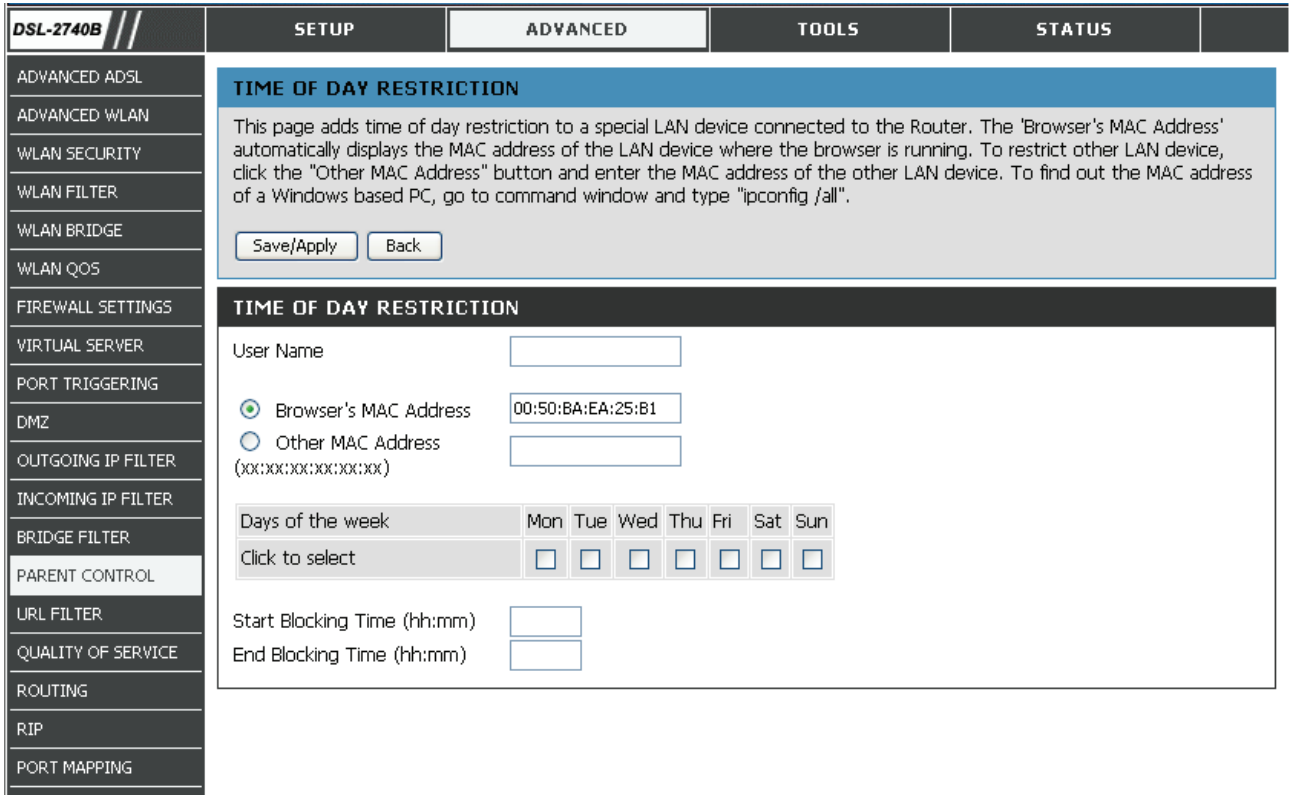
Click the **Add A Rule** button to enter your parent control configuration window.

Enter the user name and MAC address of the restricted PC.

Select days and enter time frame to apply this rule.

Click **Save/Apply** button to apply settings.

Notice Local host's MAC address will be displayed automatically when enter this configuration page. To find out other PC's MAC address. Open the specific PC's command prompt window, type command **ipconfig /all** and check **Physical Address** row.



URL FILTER

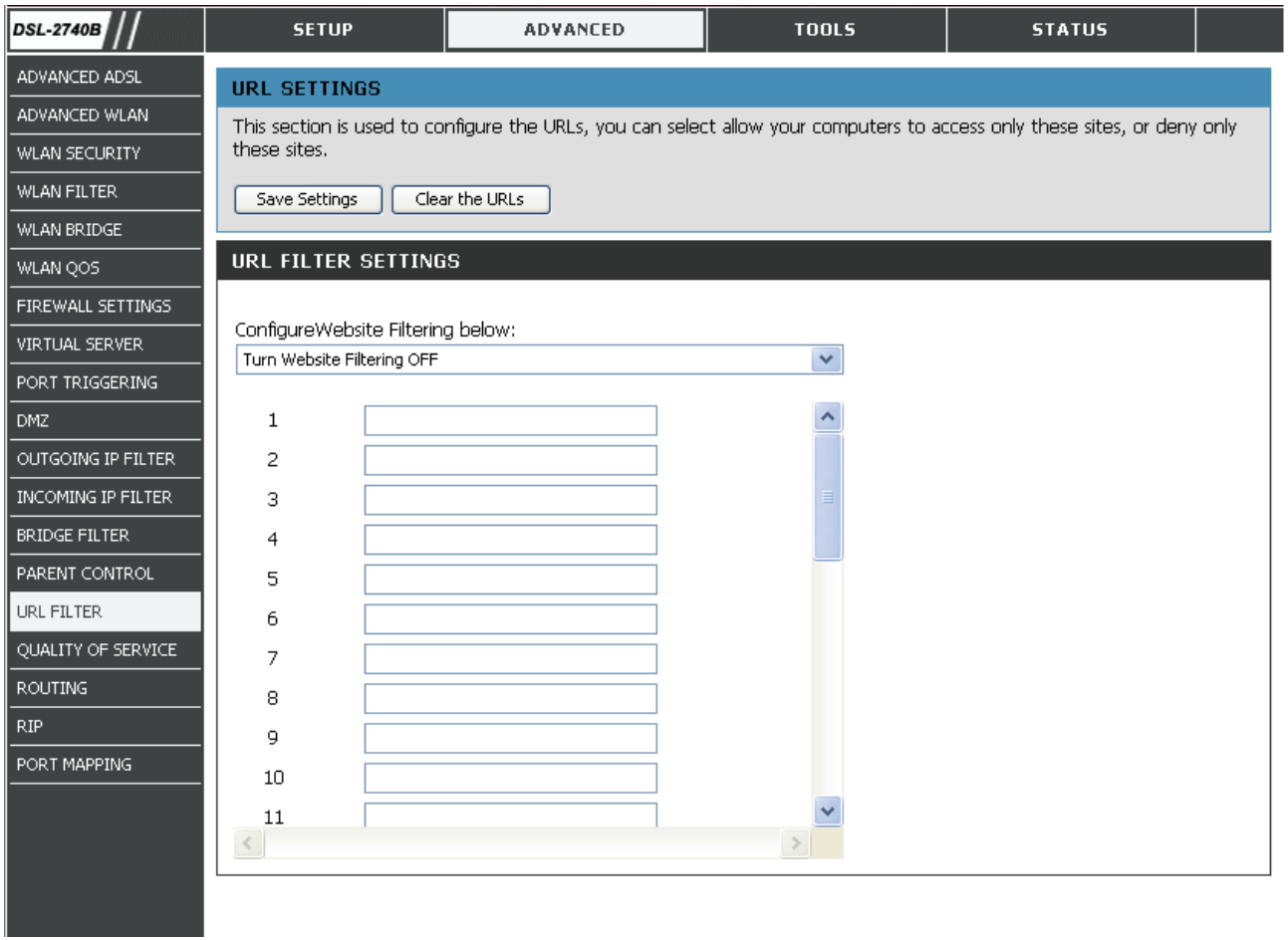
URL filter is used to control Internet website access. You can decide that your local hosts can access these specific websites only, or can not access these websites only.

Select from the drop-down list **Turn on Website Filtering** (**Allow** or **Deny**).

Enter the website URLs or keywords.

Click **Save Settings** to apply this rule

To turn off URL filter, select **Turn Website Filtering OFF** from drop-down list and click **Save Settings**.



QUALITY OF SERVICE

QoS (Quality of Service) is a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header TOS byte. This is to ensure that the delay-sensitive traffic has higher priority to go to Internet. IP Precedence and IP TOS (Type of Service) marking, once enabled, will overwrite the correspondent TOS byte in the IP header. These features, along with Differentiated Service Configuration, are valid only when your ISP has implement these services.

Click the **Add** button to enter your QoS configuration window.

Enter the name of the rule.

Assign ATM priority from the **Assign ATM Transmit Priority** drop-down list.

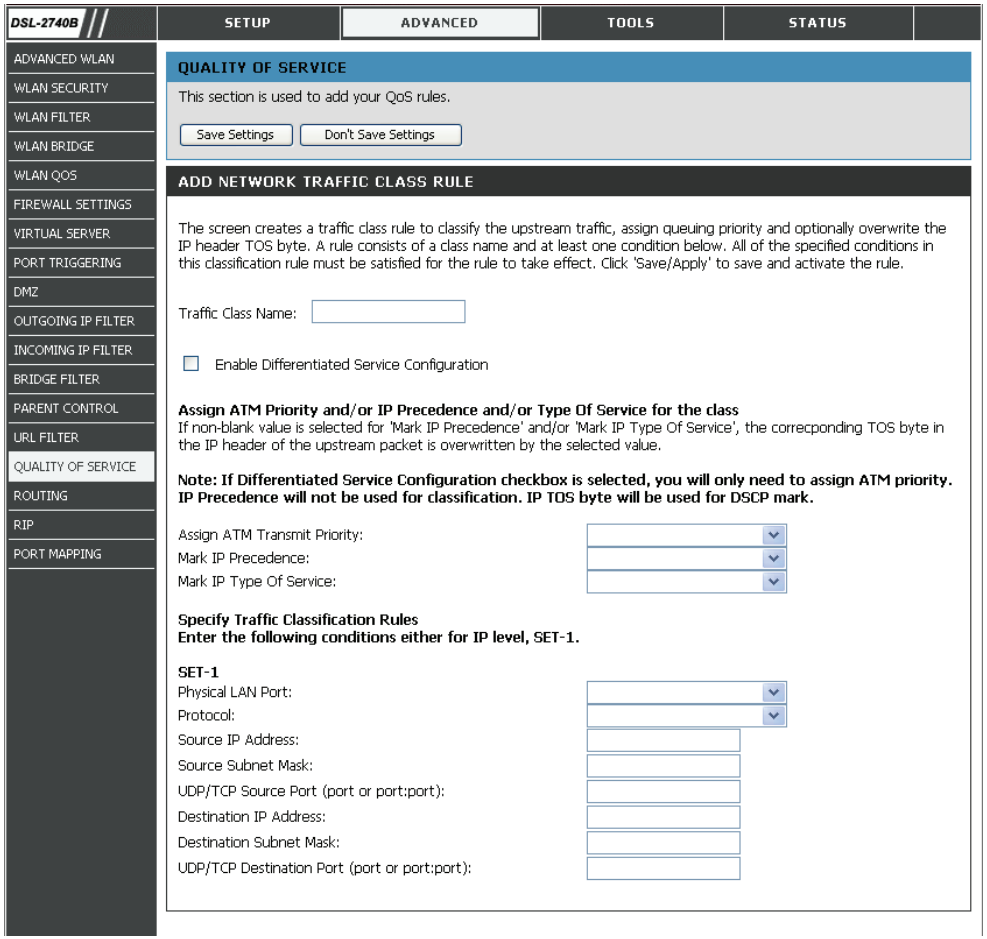
Check **Enable Differentiated Service Configuration** box if it is supported by your ISP.

Select the optional marking on IP Precedence and TOS from the **Mark IP Precedence** and **Mark IP Type Of Service** drop-down lists.

Specify traffic classification rules from **SET-1**. The classification can be de fined in the following parameters: **Physical LAN port**, **Protocol**, **Source/Destination IP Address**, **and Source/Destination Port**.

Click **Save Settings** to apply this rule.

Notice All of the specified conditions in this classification rule must be satisfied for the rule to take effect.
To delete the configured QoS rule, check the box in **Remove** field and click **Remove** button on top.



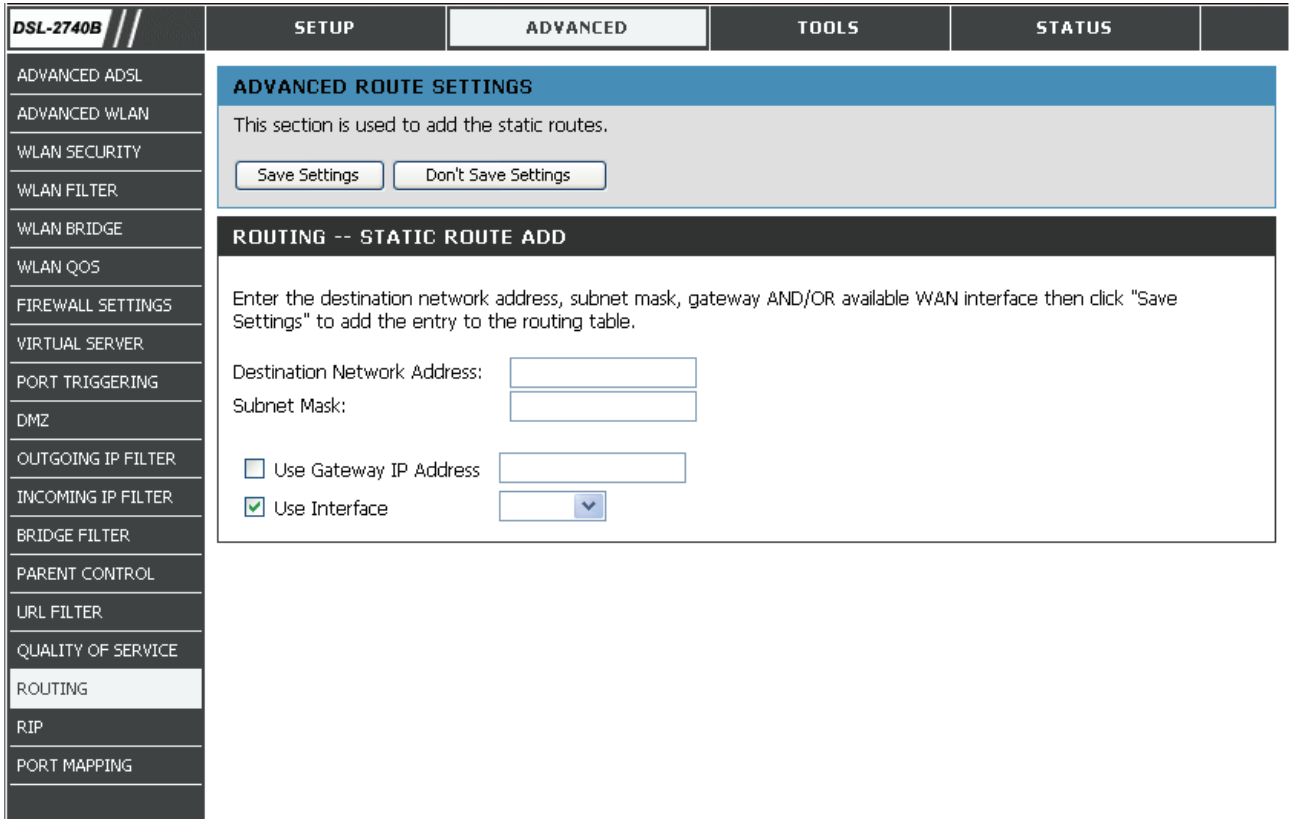
ROUTING

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway.

Click the **Add** button to enter your routing configuration window.

Enter the **Destination Network Address**, **Subnet Mask**, **Gateway IP Address**, and/or available **WAN Interface**.

Click **Save Settings** to apply this rule.



RIP

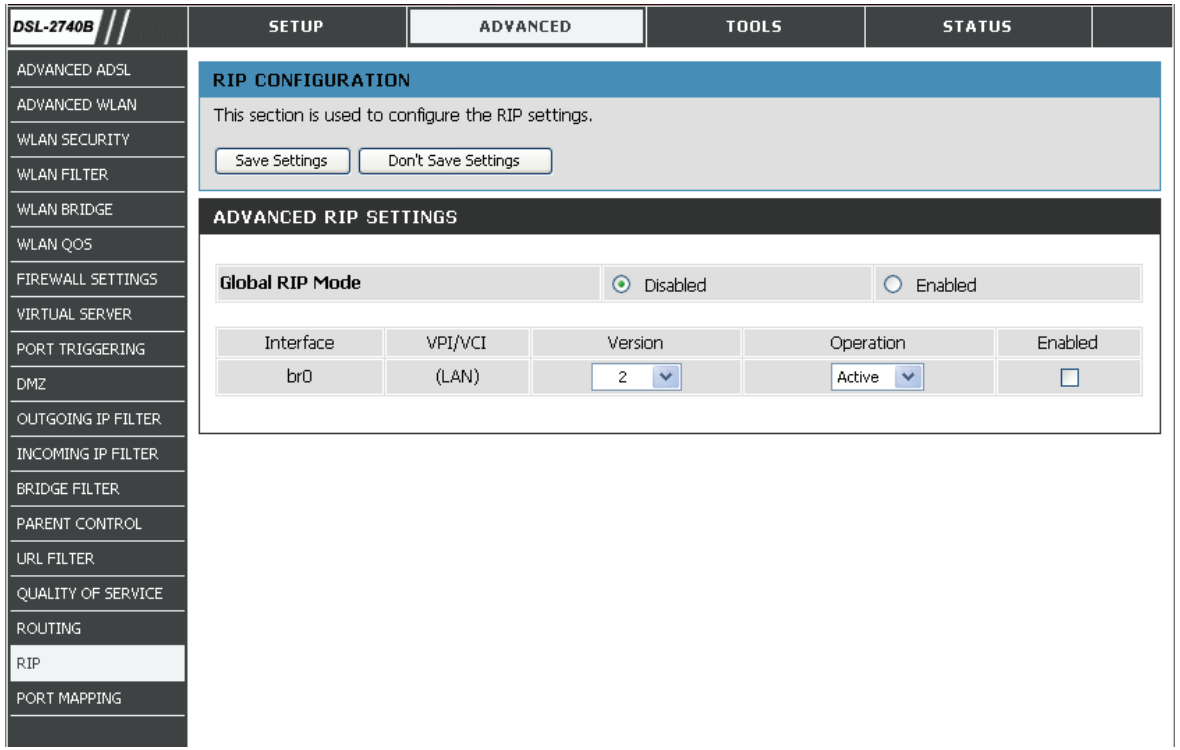
The Router supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN.

Click the **Enabled** radio button to enable the router RIP function.

Select RIP **Version** and **Operation** mode from the drop-down list.

Check **Enabled** box and click **Save Settings** to apply your settings.

To disable RIP, click **Disabled** radio button and click **Save Settings**.



Interface: The interface which RIP function is applied.

Version: RIP has two versions available: RIP 1 and RIP 2. RIP 1 uses classed routing table and RIP 2 uses classless routing table.

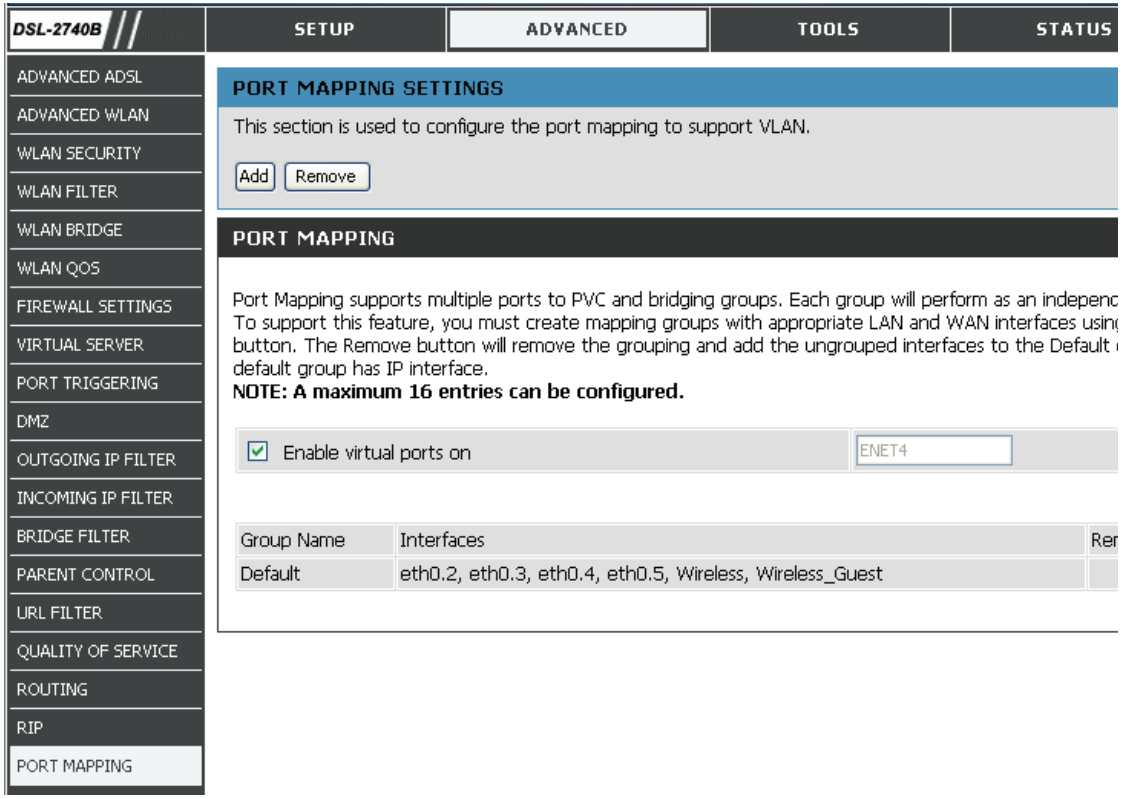
Operation: Two operation modes are available: Active and Passive.
Active mode: Router listens and shares routing table with other devices.
Passive mode: Router only listens and updates its own routing tables.

PORT MAPPING

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces.

By default, all interfaces are included in the **Default** group. And only the **Default** group has IP interface to access Router's configuration window. The interfaces which have been selected to form a mapping group will no longer have the ability to access the router configuration window.

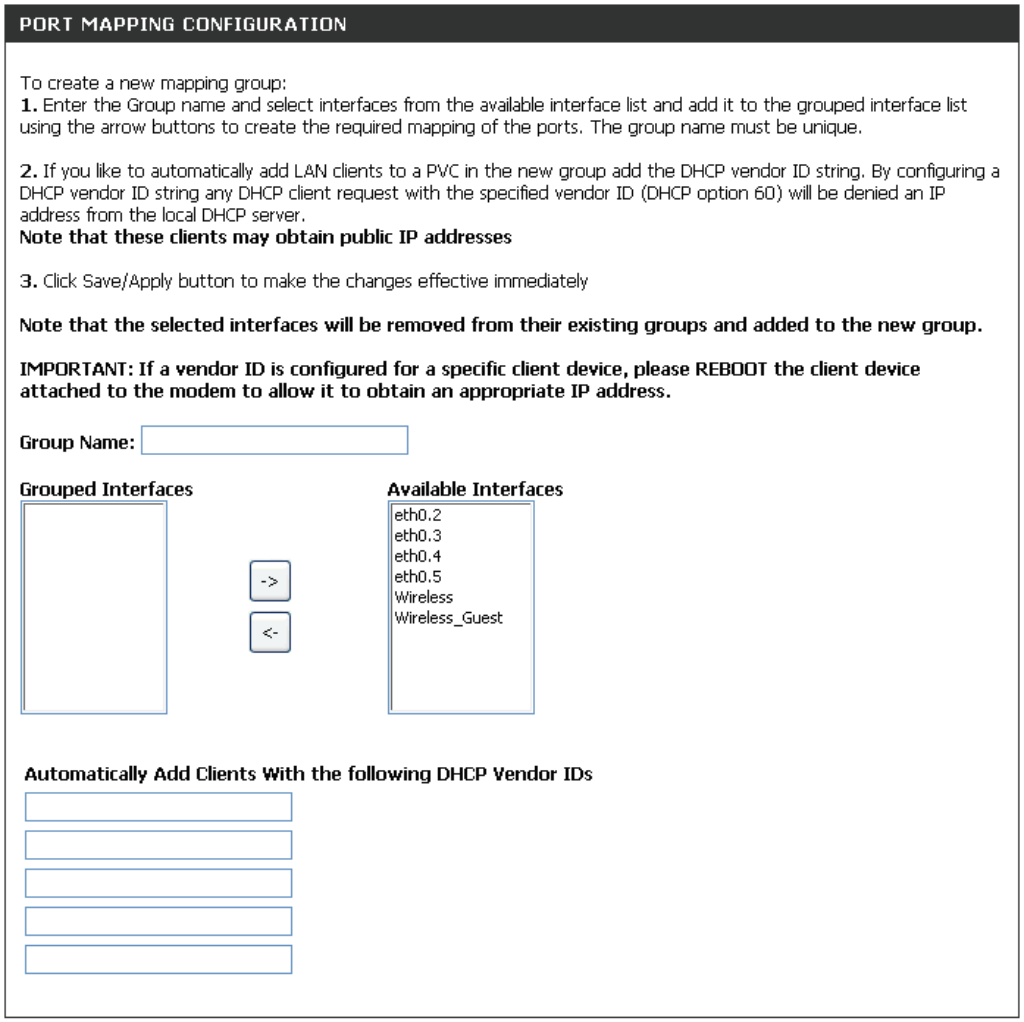
First, select **Enable virtual ports on** box to enable port mapping.



Click **Add** button to enter port mapping configuration window.

Enter the group name and select the specific interfaces from **Available Interfaces** (Default group) to **Grouped Interfaces**.

Click **Save Settings** to apply your settings.

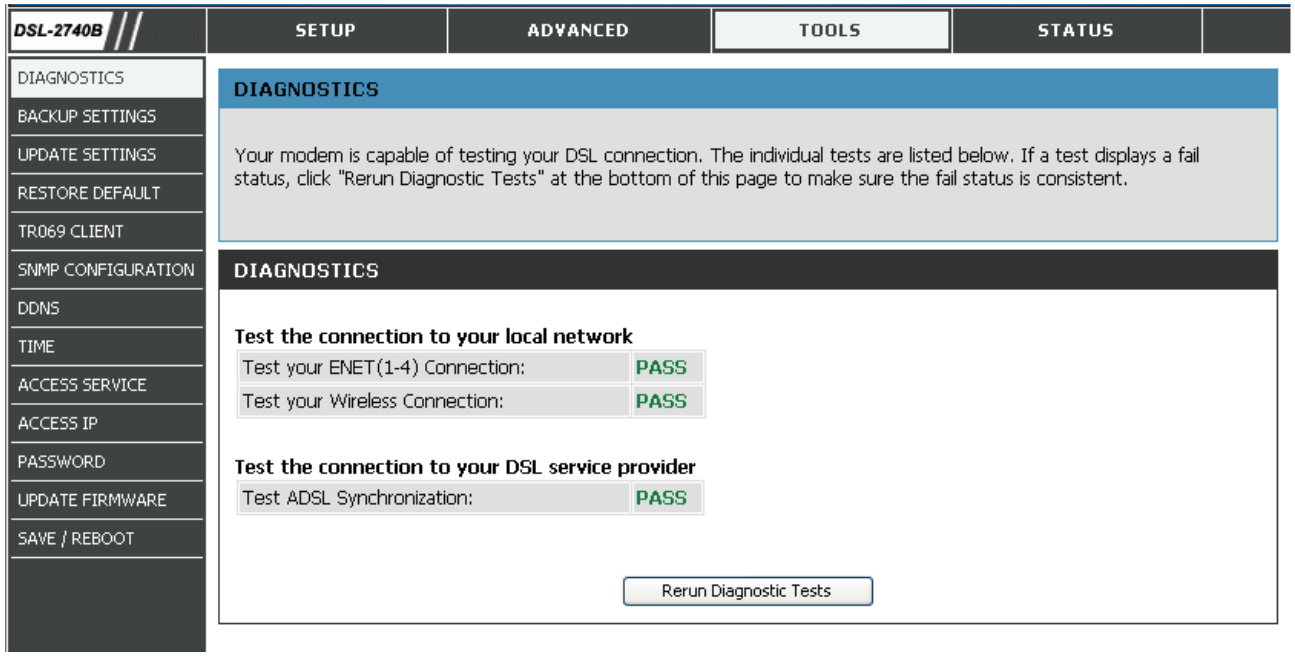


TOOLS

Click the **Tools** tab to reveal the window buttons for various functions located in this directory. The **Diagnostics** window is the first item in the **Tools** directory.

Diagnostics

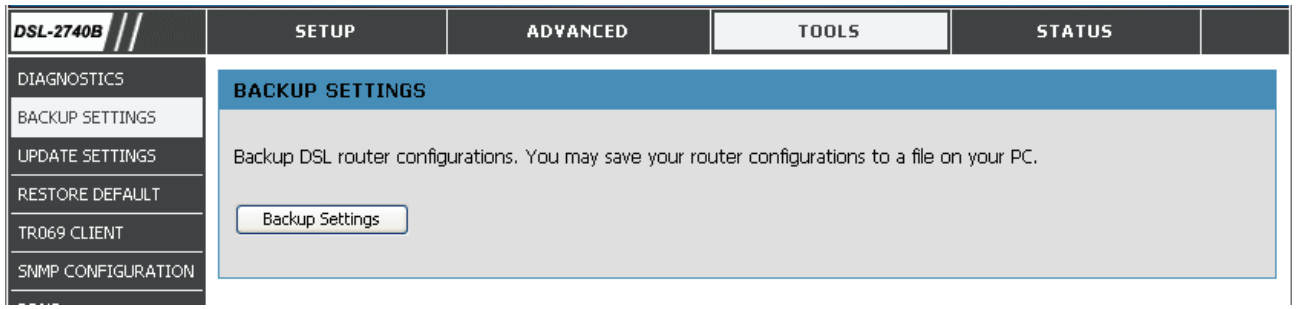
The **Diagnostic Test** window is used to test connectivity of the Router. A Ping test may be done through the local or external interface to test connectivity to known IP addresses. The diagnostics feature executes a series of test of your system software and hardware connections. Use this window when working with your ISP to troubleshoot problems.



BACKUP SETTINGS

Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **Backup Settings** button in the **Tools** directory to display the window.

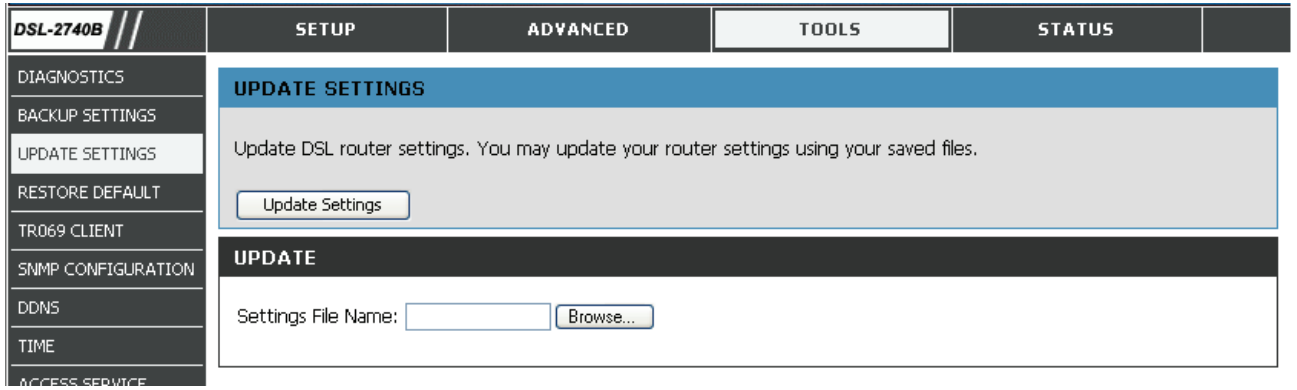
Click the **Backup Settings** button to Save Settings to Local Hard Drive. You will be prompted to select a location on your computer to put the file. The configuration file may be named anything you like.



UPDATE SETTINGS

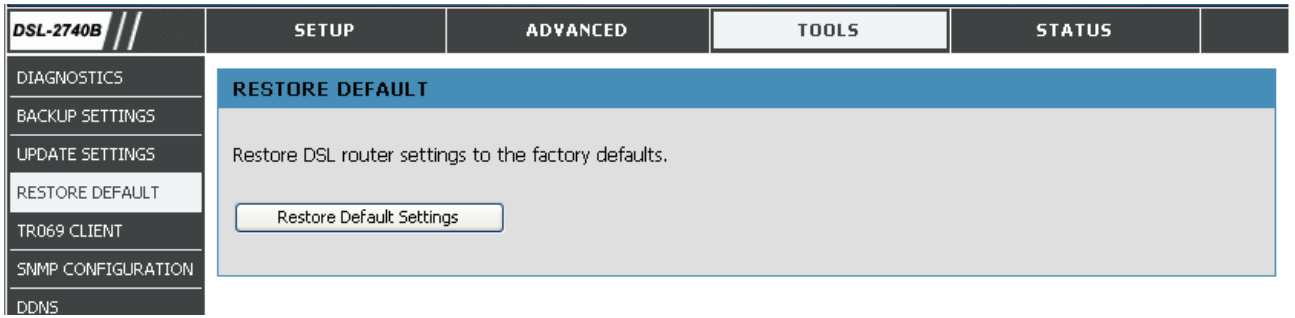
To load a previously saved configuration file, click the **Browse** button and locate the file on your computer.

Click the **Update Settings** button to load settings from local hard drive. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.



RESTORE DEFAULT

To reset the Router to its factory default settings, click the **Restore Default button**. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings (192.168.1.1) and Administrator password (admin).



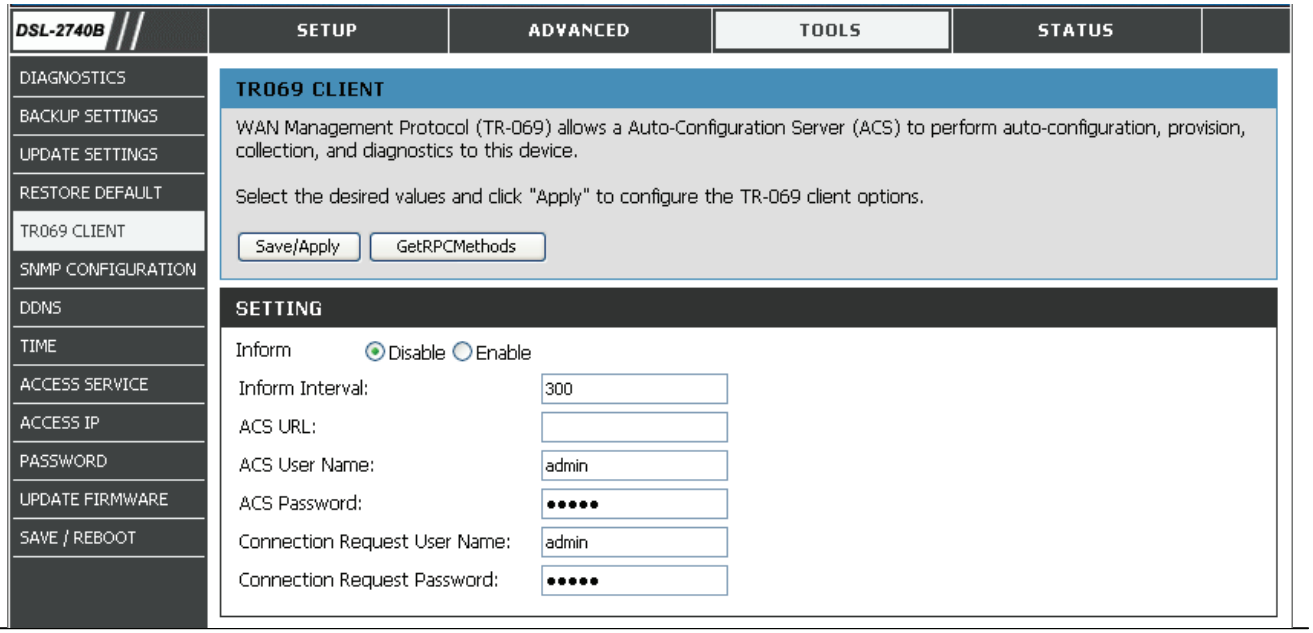
TR069 CLIENT

TR-069 is a WAN Management Protocol which allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. You should have all the necessary information from your ISP if **TR-069** is implemented by your ISP.

Click **Enable** radio button to enable **TR-069**.

Enter your ACS server data and user name/password.

Click Save/Apply to apply your settings.



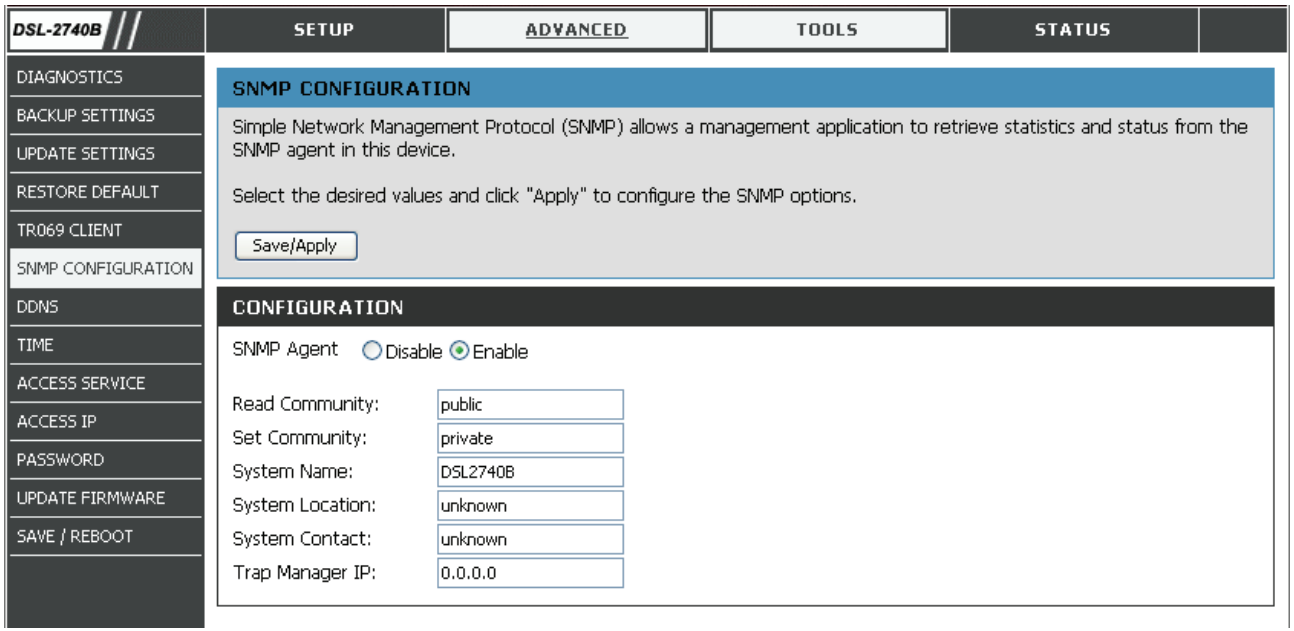
SNMP CONFIGURATION

Simple Network Management Protocol is a standard for inter-network and intra-network management. Please contact your ISP for all necessary information before configuring SNMP.

Click **Enable** radio button in **SNMP Agent**.

Enter all data provided by your ISP.

Click **Save/Apply** to apply your settings.



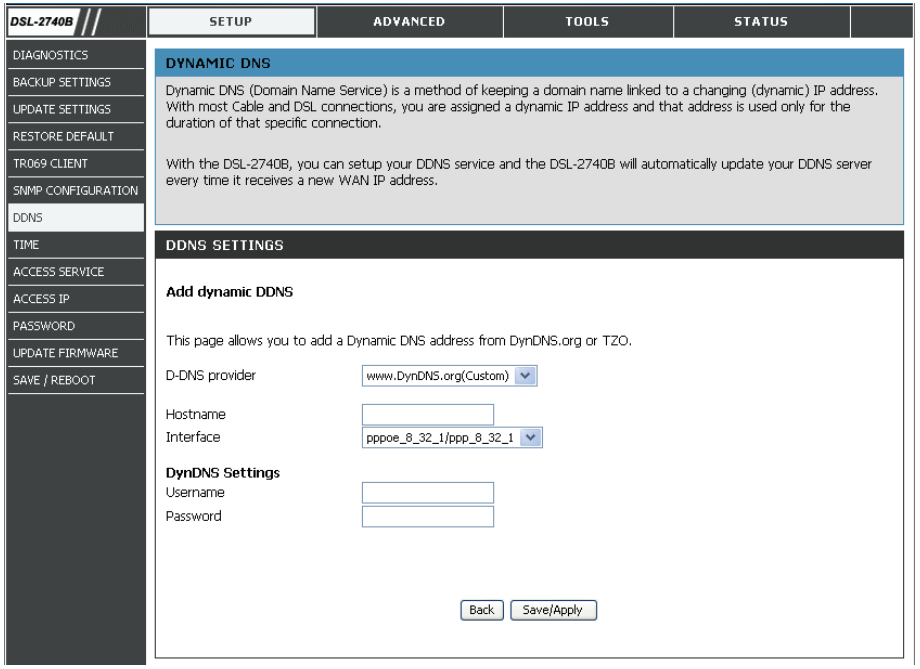
DDNS

The Router supports DDNS (Dynamic Domain Name Service). The Dynamic DNS service allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specified host from various locations on the Internet. This is enabled to allow remote access to a host by clicking a hyperlinked URL in the form hostname.dyndns.org, Many ISPs assign public IP addresses using DHCP, and this can make it difficult to locate a specific host on the LAN using standard DNS. If for example you are running a public web server or VPN server on your LAN, this ensures that the host can be located from the Internet if the public IP address changes. DDNS requires that an account be setup with one of the supported DDNS service providers (DyndDNS.org or TZO).

Click the **Add** button to enter your DDNS configuration window.

Select DDNS service provider from the **DDNS provider** drop-down list and enter your account data.

Click **Save/Apply** button to apply settings.



DDNS Server: Select one of the DDNS registration organizations form those listed in the pull-down menu. Available servers include DynDns.org and TZO.

Host Name: Enter the Host Name that you registered with your DDNS service provider.

Interface: Select your WAN interface (if more than one) that DDNS is applied to.

Username (or Key): Enter the Username for your DDNS account.

Password (or Key): Enter the Password for your DDNS account.

Email (if used): Enter the email address registered to your DDNS service provider.

Notice DDNS requires that an account be setup with one of the supported DDNS service provider prior to engaging it on the router. This function will not work without an accepted account with a DDNS service provider.

TIME

The Router provides you a method (Network Time Protocol) to maintain your router system clock via Internet.

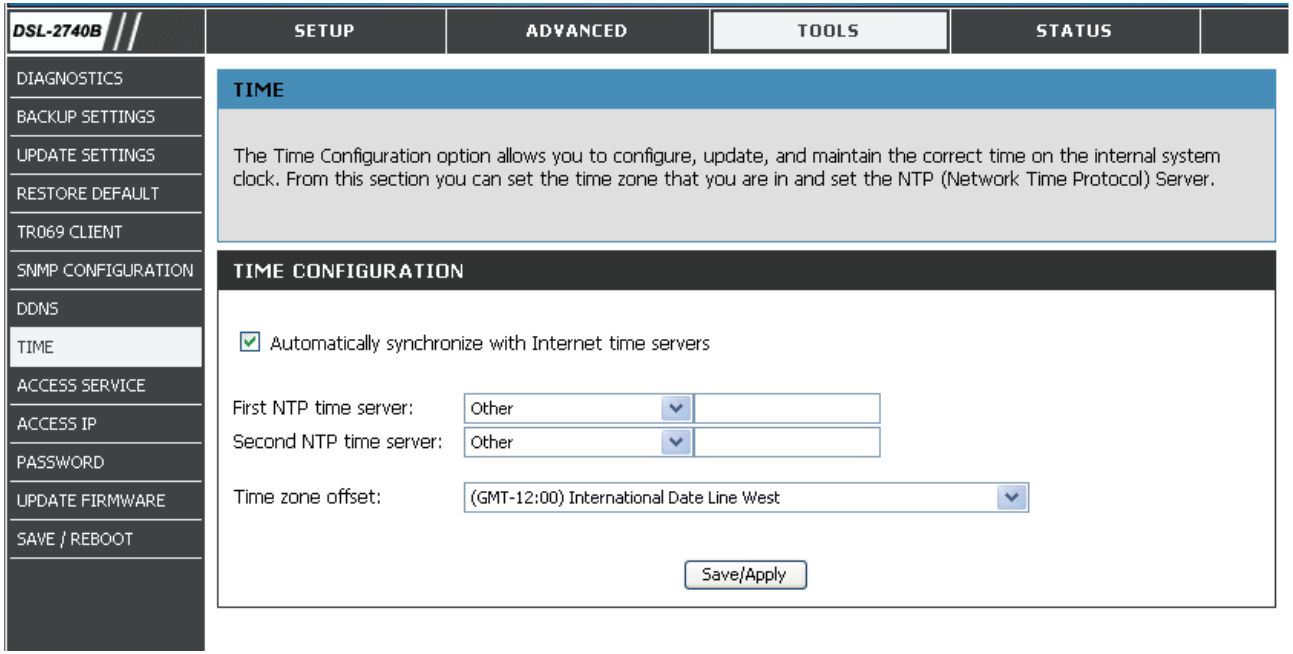
Select **Automatically synchronize with Internet time servers**.

Select specific time server to use from the **First NTP time server** drop-down list; or you can select **Other** from the drop-down list and type the preferable time server in the right field.

Configure the **Second NTP time server** for backup purpose.

Select your operating time zone from **Tine zone offset** drop-down list.

Click **Save/Apply** to apply your settings.



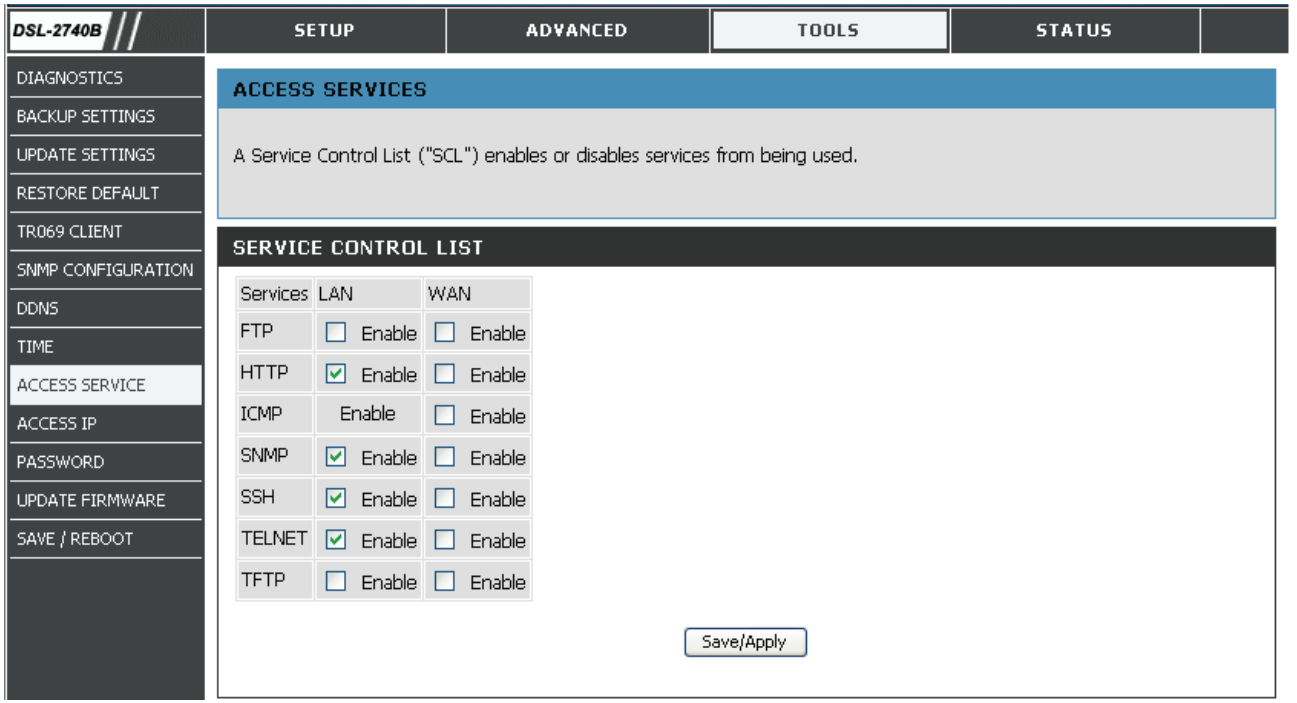
ACCESS SERVICE

You can select to enable or disable of which management services from being used in your router, for LAN and/or WAN interface. You need configure at least one WAN interface (except Bridge) before settings up service control list on WAN interface. Access Service is not available for Bridge mode.

Select the management services which you want to enable/disable on your LAN/WAN interface.

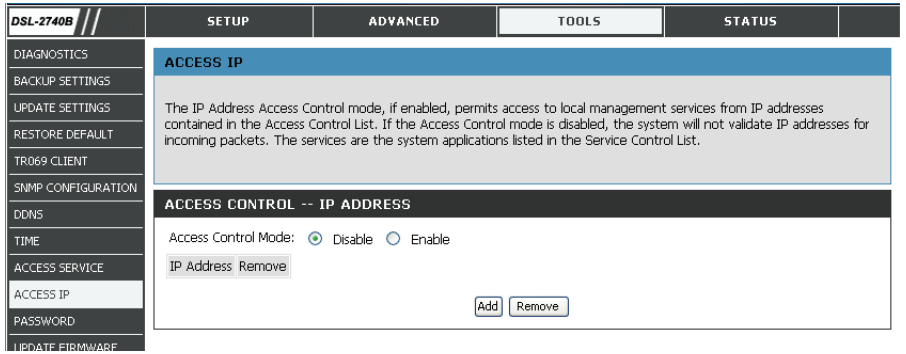
Click the **Save/Apply** button to apply your settings.

Notice If you disable HTTP service, you'll not be able to access the router's configuration window permanently.



ACCESS IP

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. The available management services are configured in the **Access Service**.



Click **Add** button to enter access IP address configuration window.

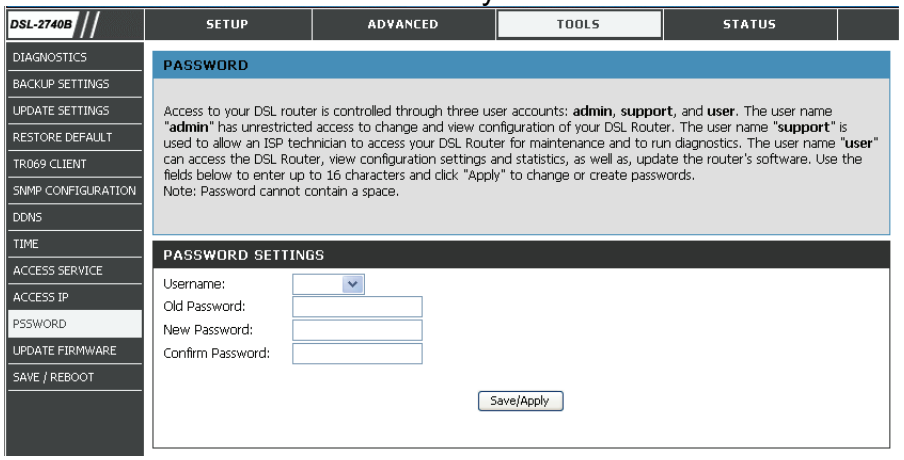
Enter the specific IP address which will be granted access and click **Save/Apply** button.

After adding all IP addresses, click **Enable** radio button to enable IP access control.

To remove configured IP address, select **Remove** box of the specific entry and click **Remove** button.

PASSWORD

Access to your router is controlled through three user accounts: **admin**, **support**, and **user**. The user name **admin** has unrestricted access to change and view configuration of your router. The user name **support** is used to allow an ISP technician to access your router for maintenance and to run diagnostics. The user name **user** can access the router, view configuration settings and statistics, as well as, update the router's software.



By default, all passwords are the same as their account name.

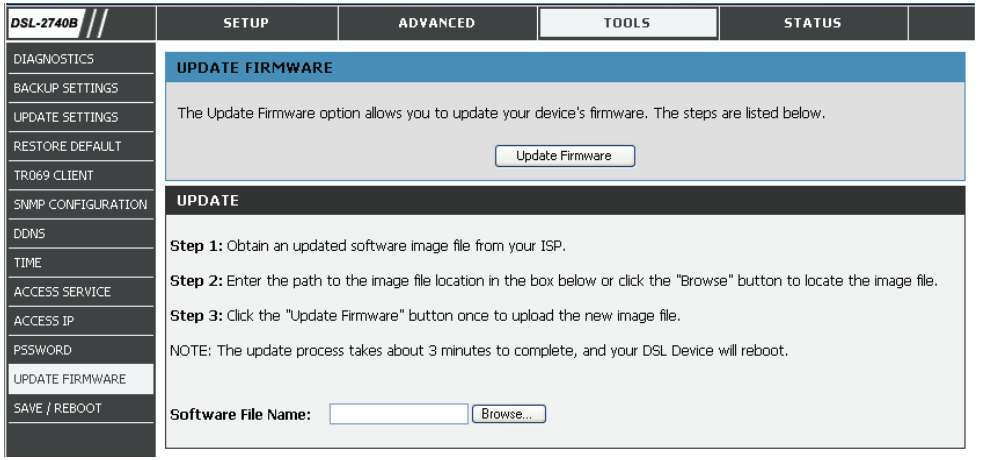
To change password, select the specific account and enter the old/new password. Click the **Save/Apply** button to apply settings.

UPDATE FIRMWARE

Use the **Firmware Upgrade** window to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the **System Settings** window described above.

To upgrade firmware, click on the **Browse** button to search for the file. Click the **Update Firmware** button to begin copying the file. The Router will load the file and restart automatically.

Notice Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the Router's configuration settings before upgrading the firmware.



SAVE / REBOOT

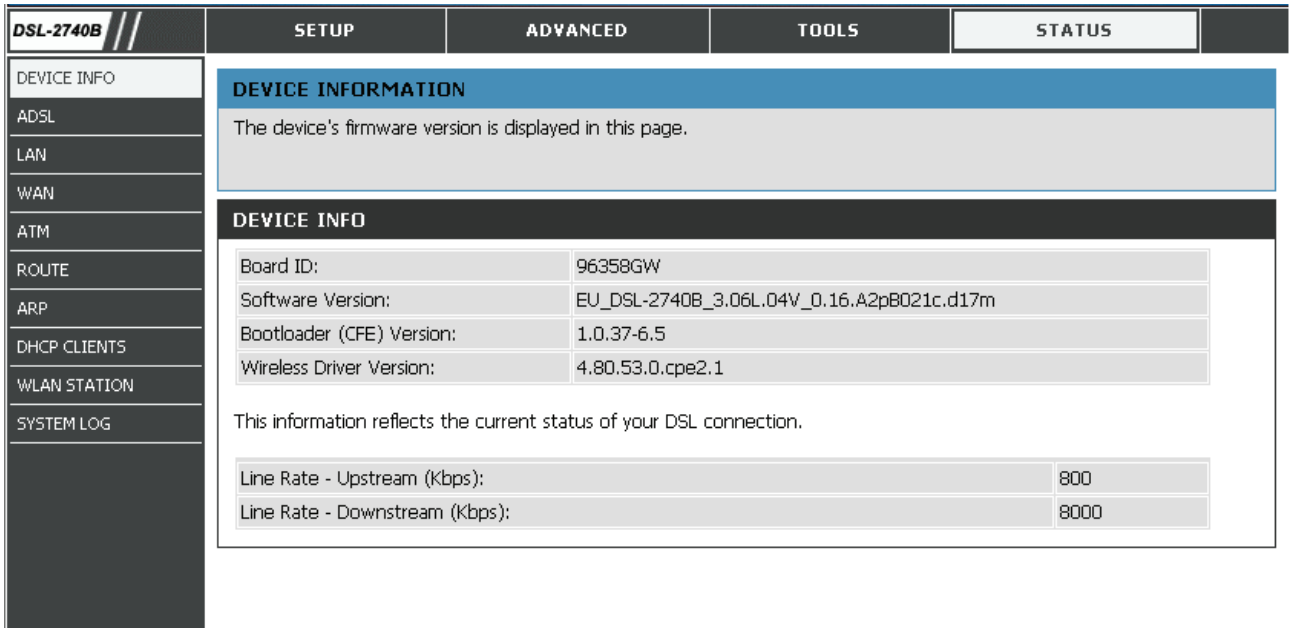
Click the **Save/Reboot** button to save the previously made configurations and reboot the router.

STATUS

Use these windows to view system information and monitor performance.

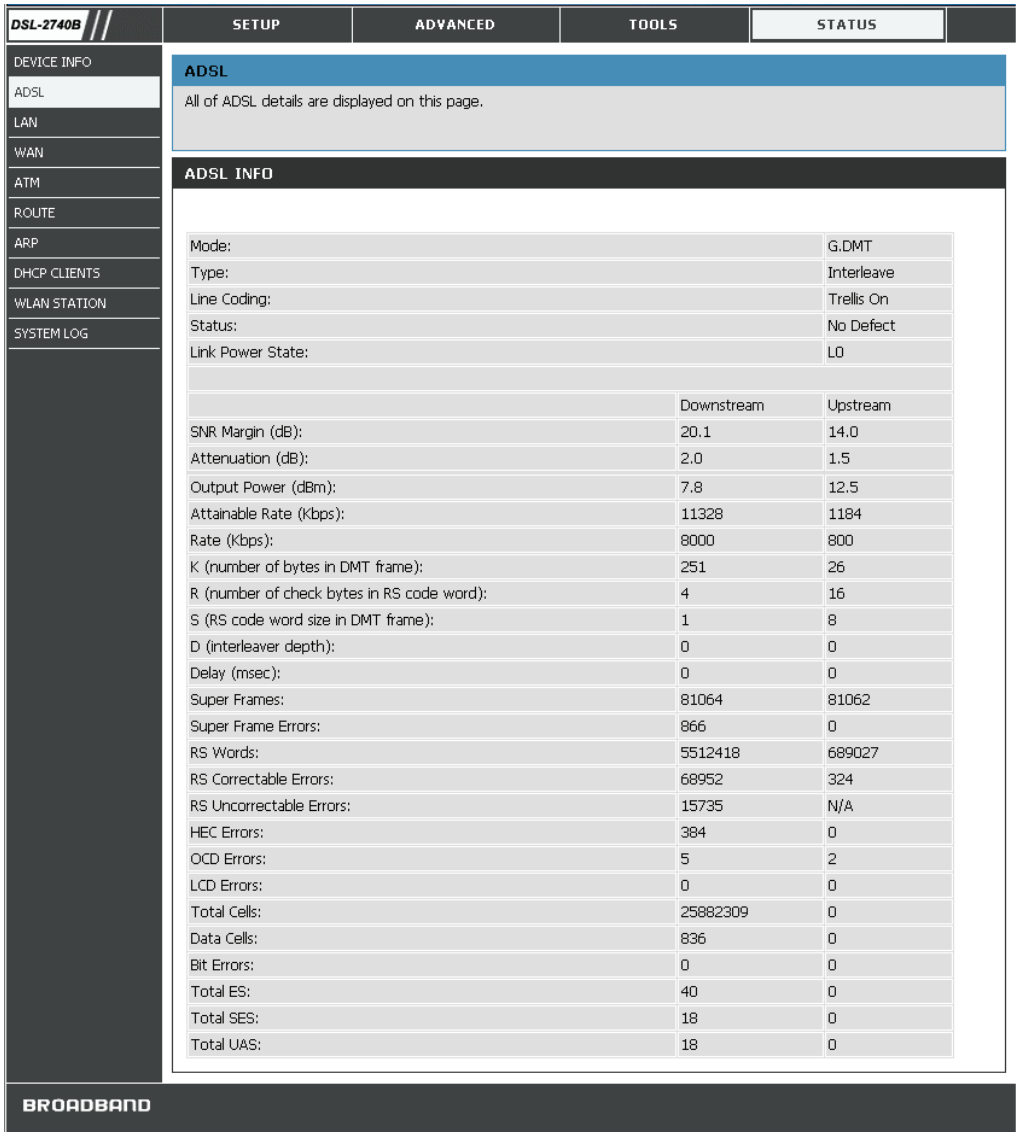
DEVICE INFO

Use the **Device Information** window to quickly view basic current information about the router and device information including Firmware Version and ADSL connection status.



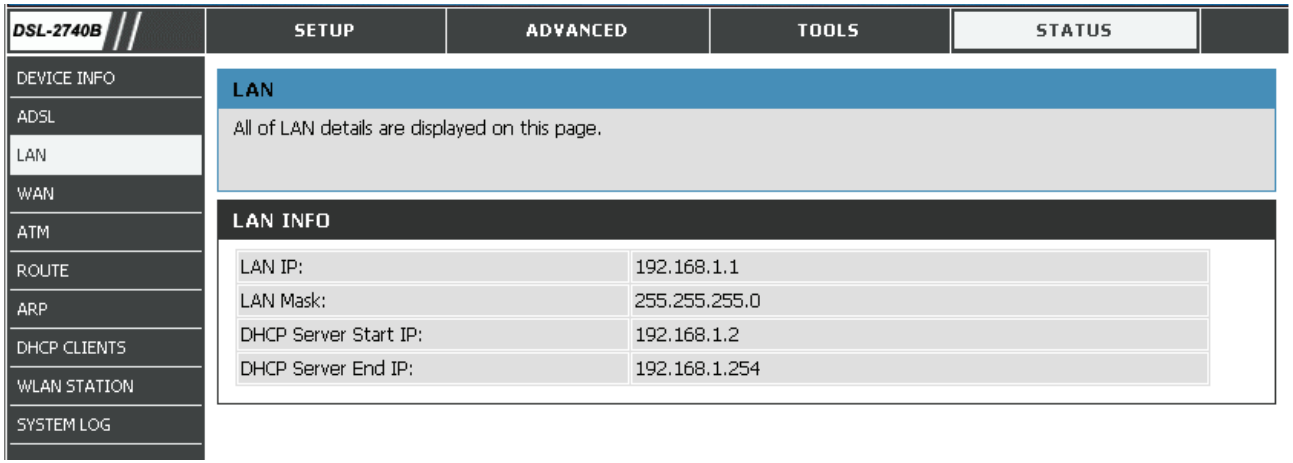
ADSL

This window displays ADSL information including Link Rate, SNR, and some Error Counters.



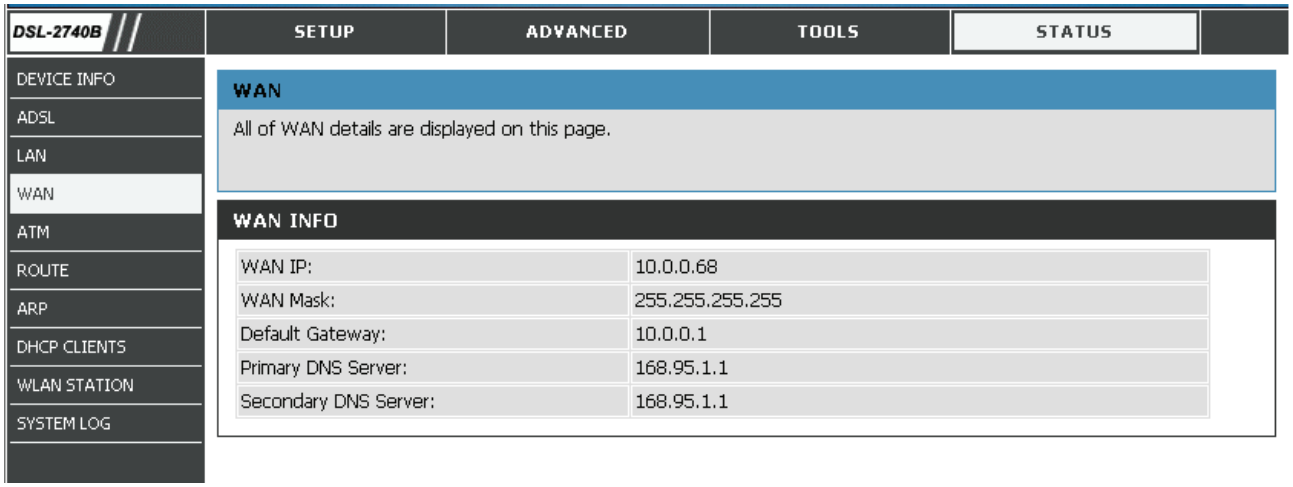
LAN

This window displays LAN information including IP address, Mask, and DCHP pool.



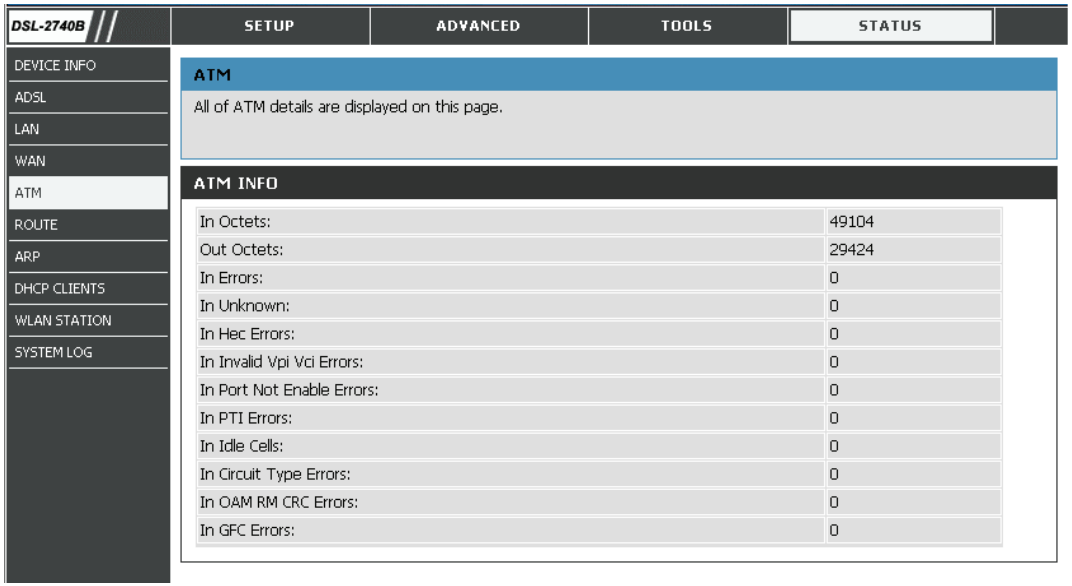
WAN

This window displays WAN information including IP address, Mask, Default Gateway, Primary/Secondary DNS Server.



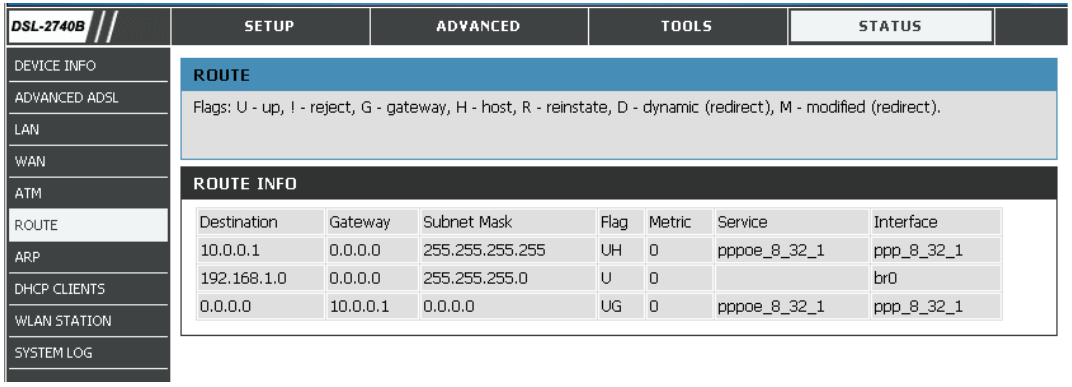
ATM

This window displays ATM information including Cell Count and some Error Counters.



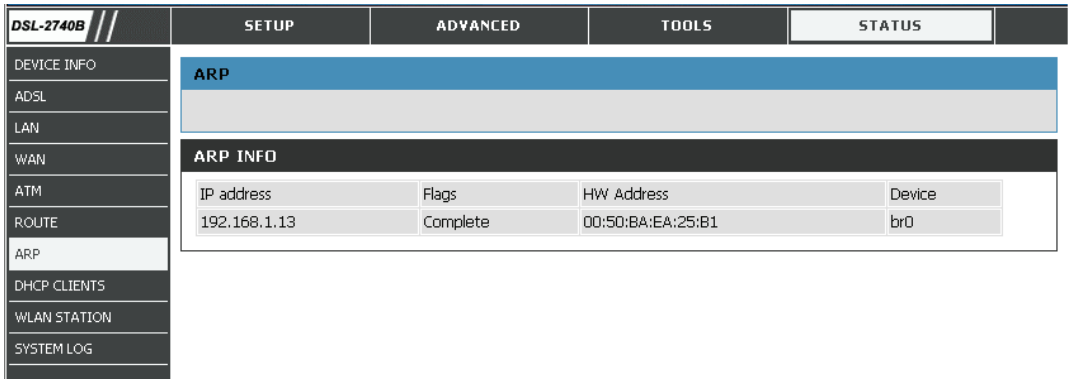
ROUTE

This window displays the Routing Table of the router.



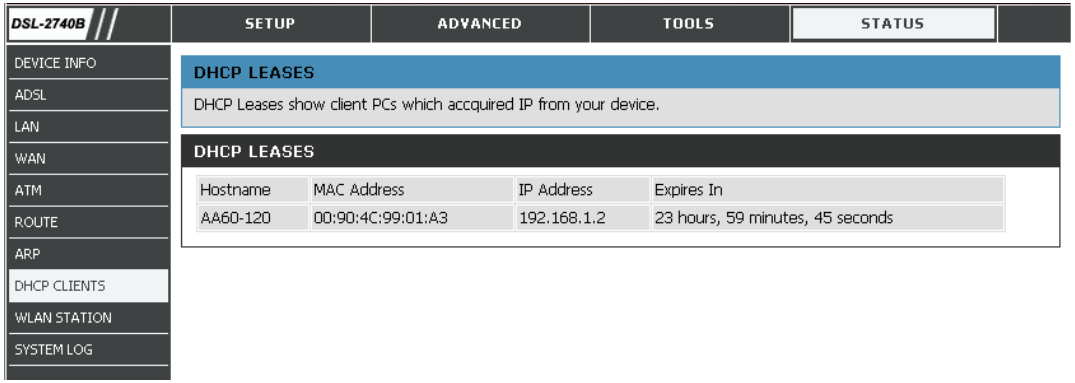
ARP

This window displays ARP Table of the router's LAN port.



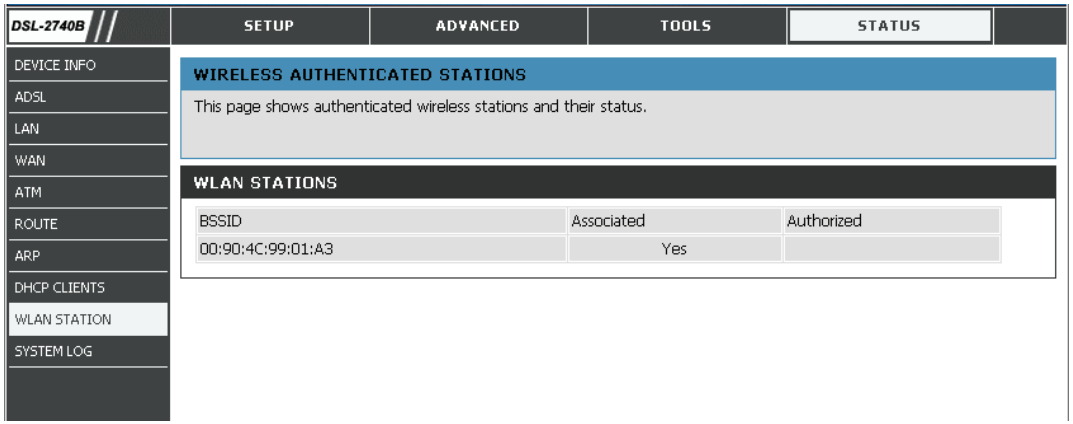
DHCP CLIENTS

This window displays all the client devices which have obtained IP addresses from the router.



WLAN STATION

This window displays authenticated wireless stations and their status.



SYSTEM LOG

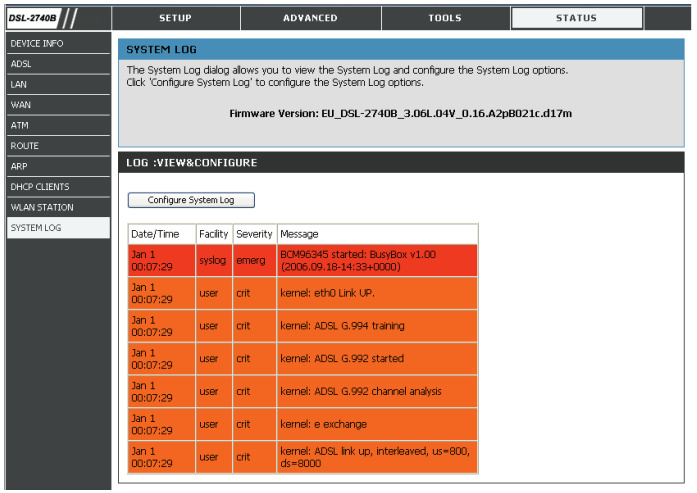
The system log displays chronological event log data. The event log can be read from local host or sent to syslog server. The available event severity levels are: **Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging**.

Click **Configure System Log** button to enter system log configuration window.

Click **Enable** radio button and select **Log/Display Level** from the drop down list.

Select display mode from the **Mode** drop-down list; enter the syslog server IP address and port number if **Both/Remote** Mode is selected.

Click **Save/Apply** button to apply your settings.



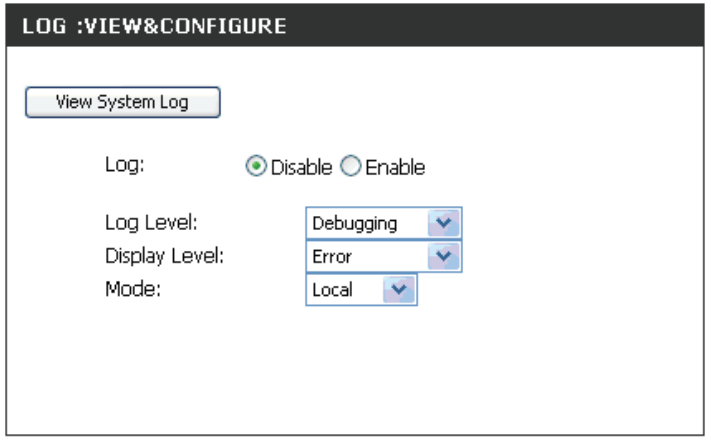
Log Level: All events above or equal to the selected level will be logged.

Display Level: All logged events above or equal to the selected level will be displayed.

Mode: Display mode of system log. Local: Display on local host only Remote: Send log file to remote syslog server only

Server IP Address: IP address of the remote syslog server

Server UDP Port: UDP port number of the remote syslog server



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-2740B. 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
  - 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. The default IP address is 192.168.1.1. When logging in, the username is **admin** and leave the password box empty.

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 security feature on the router. Refer to product manual for detail 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, such as two or more DIR-635 wireless network Cardbus adapters.

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.

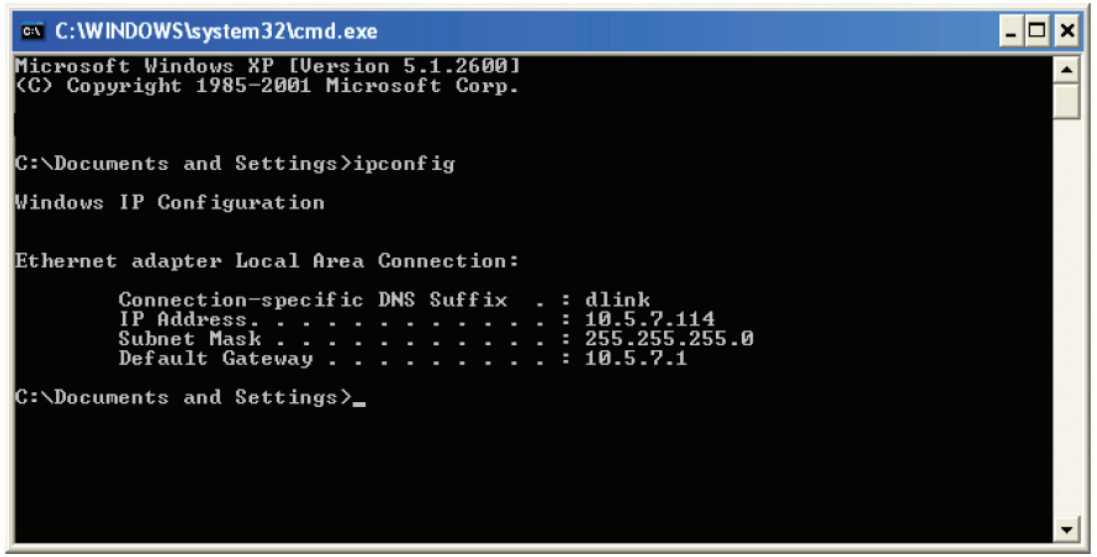
Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK**.

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.



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**.

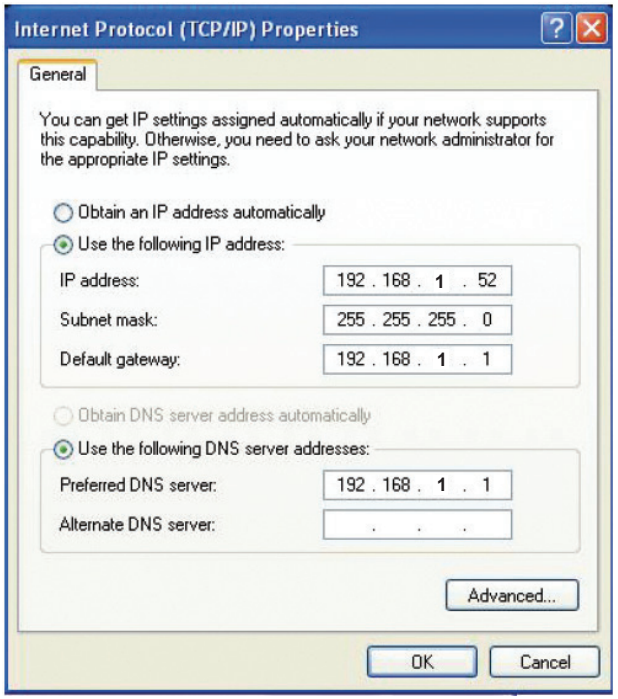
Step 2
Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.

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 192.168.1.1, make your IP address 192.168.1.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 (192.168.1.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.1.1). 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.



Technical Specifications

ADSL Standards

- ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt) AnnexA
- ITU G.992.2 (G.lite) Annex A
- ITU G.994.1 (G.hs)
- ITU G.992.5 Annex A

ADSL2 Standards

- ITU G.992.3 (G.dmt.bis) Annex A
- ITU G.992.4 (G.lite.bis) Annex A

Protocols

- IEEE 802.1d Spanning Tree
- TCP/UDP
- ARP
- RARP
- ICMP
- RFC1058 RIP v1
- RFC1213 SNMP v1 & v2c
- RFC1334 PAP
- RFC1389 RIP v2
- RFC1577 Classical IP over ATM
- RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)
- RFC1661 Point to Point Protocol
- RFC1994 CHAP
- RFC2131 DHCP Client / DHCP Server
- RFC2364 PPP over ATM
- RFC2516 PPP over Ethernet

Data Transfer Rate

- G.dmt full rate downstream: up to 8 Mbps / upstream: up to 1 Mbps
- G.lite: ADSL downstream up to 1.5 Mbps / upstream up to 512 Kbps
- G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 12 Mbps
- ADSL full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps

Media Interface

- ADSL interface: RJ-11 connector for connection to 24/26 AWG twisted pair telephone line
- LAN interface: RJ-45 port for 10/100BASE-T Ethernet connection

WIRELESS LAN

- 802.11b/g standards
- 802.11n draft
- Wireless speed: up to 54Mbps (802.11G), 270Mbps (802.11n)
- Frequency range: 2.4 GHz to 2.484G Hz
- Antennas: 3 detachable dipole antennas.
- WEP data encryption
- WPA/WPA2 (Wi-Fi Protected Access) security
- Multiple SSID
- 802.11e Wireless QoS (WMM/WME)
- MAC address-based access control

* Maximum wireless signal rate derived from IEEE Standard 802.11g and Draft 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.