USER MANUAL

DSL-2730B

VERSION 1.0

D-Link®

WIRELESS

Table of Contents

Package Contents

- DSL-2730B Wireless N 150 ADSL2+ 4-Port Ethernet Router
- Power Adapter
- CD-ROM with User Manual
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- One Quick Installation Guide

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

System Requirements

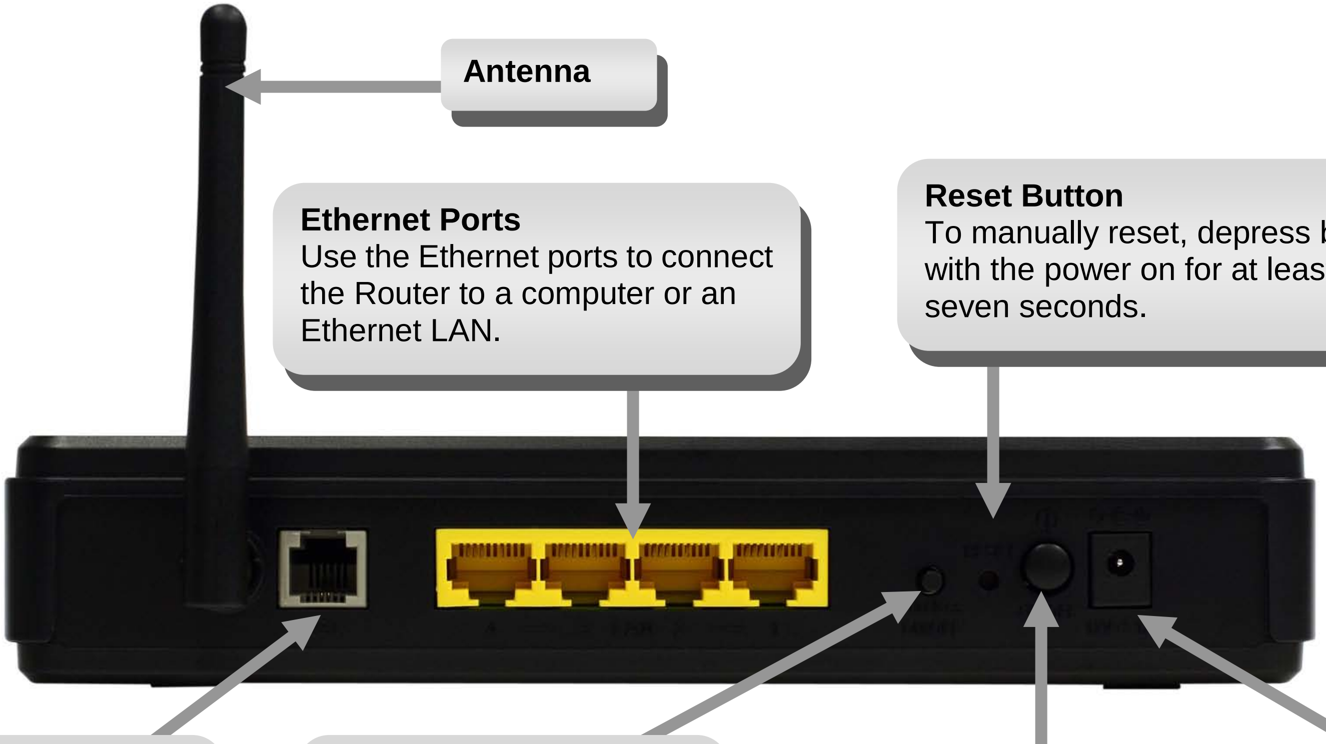
- ADSL Internet service
- Computer with:
  - 200MHz Processor
  - 64MB Memory
  - CD-ROM Drive
  - Ethernet Adapter with TCP/IP Protocol Installed
  - Internet Explorer v6 or later, FireFox v1.5, or Safari 1.3 or above
  - Windows 2000/XP/Vista
- D-Link Click'n Connect Utility

Features

- **PPP (Point-to-Point Protocol) Security –** The Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections. The Router also supports MSCHAP.
- **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 Router 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.
- **TCP/IP (Transfer Control Protocol/Internet Protocol) –** The Router supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.
- **RIP-1/RIP-2 –** The Router supports both RIP-1 and RIP-2 exchanges with other routers. Using both versions lets the Router to communicate with all RIP enabled devices.
- **Static Routing –** This allows you to select a data path to a particular network destination that will remain in the routing table and never “age out”. If you wish to define a specific route that will always be used for data traffic from your LAN to a specific destination within your LAN (for example to another router or a server) or outside your network (to an ISP defined default gateway for instance).
- **Default Routing –** This allows you to choose a default path for incoming data packets for which the destination address is unknown. This is particularly useful when/if the Router functions as the sole connection to the Internet.
- **ATM (Asynchronous Transfer Mode) –** The Router supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577), and PPP over ATM (RFC 2364).
- **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; ADSL2+ full rate supports up to 24Mbps downstream and 1Mbps upstream.
- **Full Network Management –** The Router incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or Telnet connection.
- **Telnet Connection –** The Telnet enables a network manager to access the Router’s management software remotely.
- **Easy Installation –** The Router 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.

Hardware Overview

Connections



Antenna

Ethernet Ports
Use the Ethernet ports to connect the Router to a computer or an Ethernet LAN.

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

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

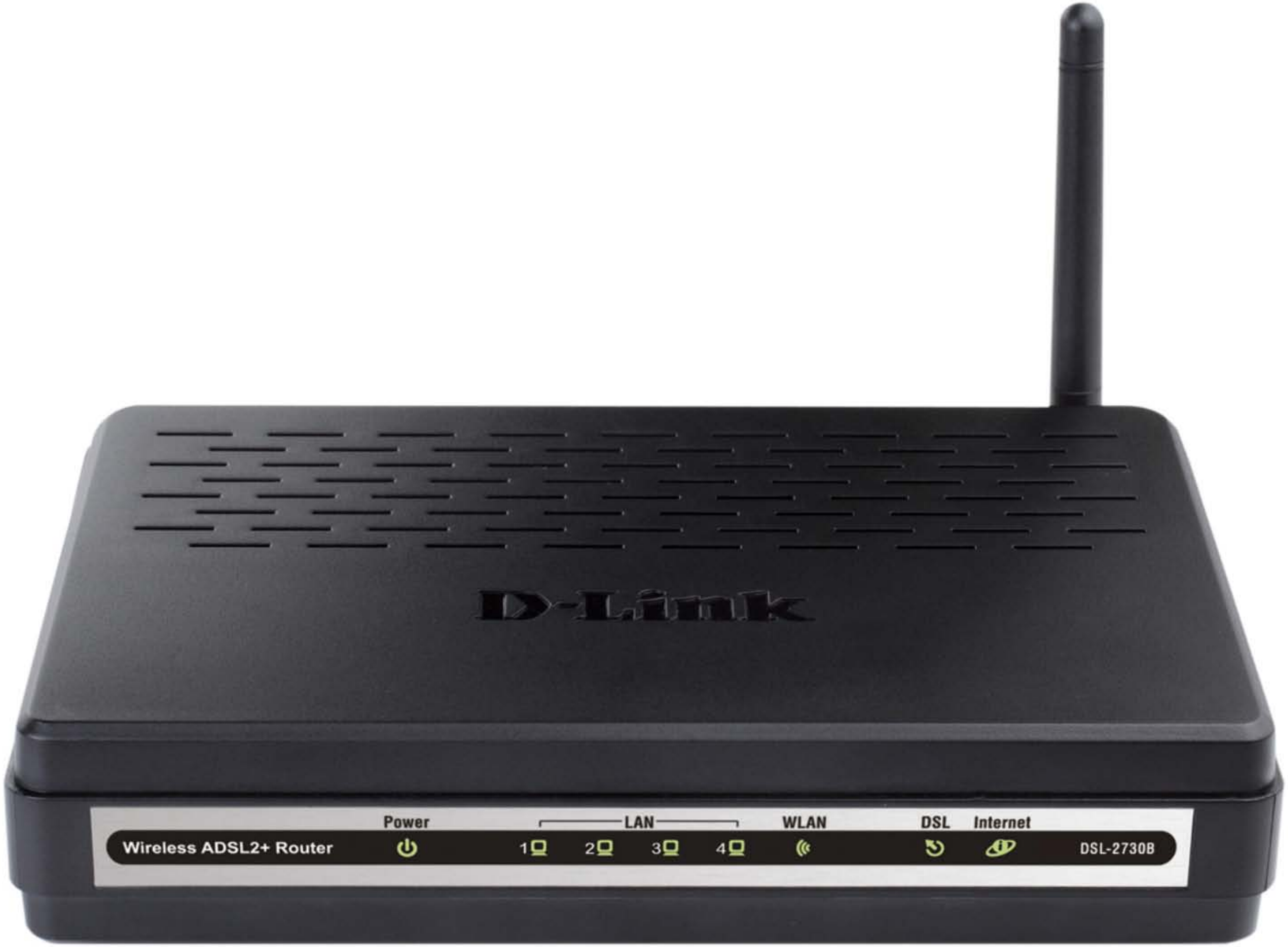
Wireless Button
Push it to enable the Wireless. Push again to disable it.

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

Power Insert
Use the adapter shipped with the Router to connect to power source.

Hardware Overview

LEDs

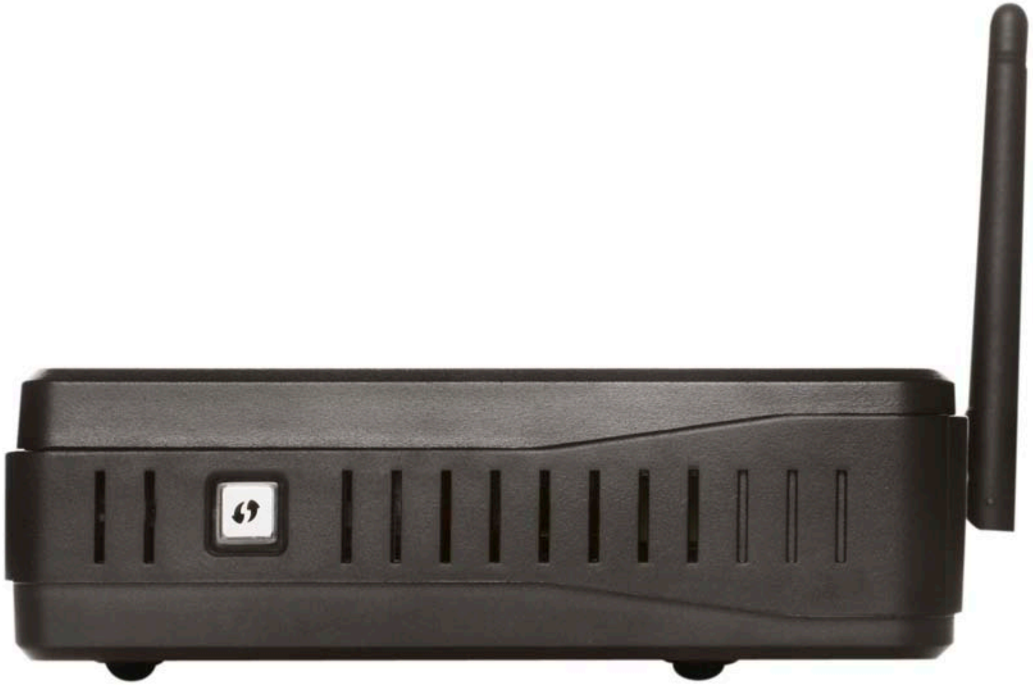


LED	**Description**
Power	A steady green light indicates the unit is powered on. When the device is powered off this remains dark. Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will light steady green. If the indicator lights steady red after the POST, the system has failed and the device should be rebooted.
LAN	A solid green light indicates a valid link on startup. This light will blink when there is activity currently passing through the Ethernet port.
WLAN	A solid green light indicates a valid link on startup. This light will blink when there is activity currently passing through the Wireless LAN.
DSL	A steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates the DLS is attempting to synchronize.
Internet	A solid green light indicates the WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured and PPP negotiation has been successfully completed. If the indicator blinks green, this means the Router is active. If the Router power is off, this remains dark. A solid red light indicates there is no DHCP response, no PPPoE response, PPPoE authentication has failed, and/or there is no IP.

Hardware Overview

WPS Button

The Router supports WPS (Wi-Fi Protected Setup). WPS is a standard for easy and secure establishment of a wireless network. With WPS you can setup and protect your wireless network in just a few easy steps.



The WPS Push Button is located at the right side of the Router. Press the button to enable the WPS function. The light blinks when WPS is successfully triggered. When the connection is successfully established between the Router and the client, the blue light will be solid and remain for five seconds. After the light is off, the Router is ready for configuring a new WPS connection.

Note: To use WPS with the Router, you need to have Wireless Clients that support WPS. If you have 1 or more Wireless Clients without WPS support, it is advised to secure your network manually using the Setup Wizard.

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-2730B 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, Windows XP, and Windows Vista.

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.

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. 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/PPPoA (PPPoE LLC, PPPoE VC-Mux, PPPoA LLC, or PPPoA VC-Mux)
- Dynamic IP Address (1483 Bridged IP LLC or 1483 Bridged IP VC-Mux)
- Static IP Address (1483 Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux)
- Bridge Mode (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 (Autosense) used for the Router automatically detects all types of ADSL, ADSL2, and ADSL2+ modulation.

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-2730B

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-2730B
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-2730B
This is the subnet mask used by the DSL-2730B, 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-2730B to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2730B to connect to other computer or Ethernet devices.

DHCP Client status

Your 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-2730B 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 you 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-2730B.

Device Installation

The DSL-2730B connects two separate physical interfaces, an ADSL (WAN) and an Ethernet (LAN) interface. 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 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 or desktop, ideally 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. Depress the Power button into the on position. 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 LAN 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, the DSL LED 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. Ensure the Router is powered on.
2. Press and hold the reset button on the back of the device for approximately 10 seconds.
3. This process should take around 1 to 2 minutes.

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. 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.

Configuration

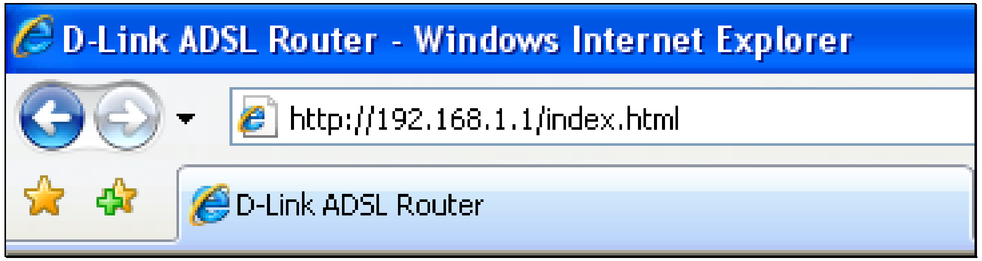
This section will show you how to set up and configure your new D-Link Router using the Web-based configuration utility.

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.

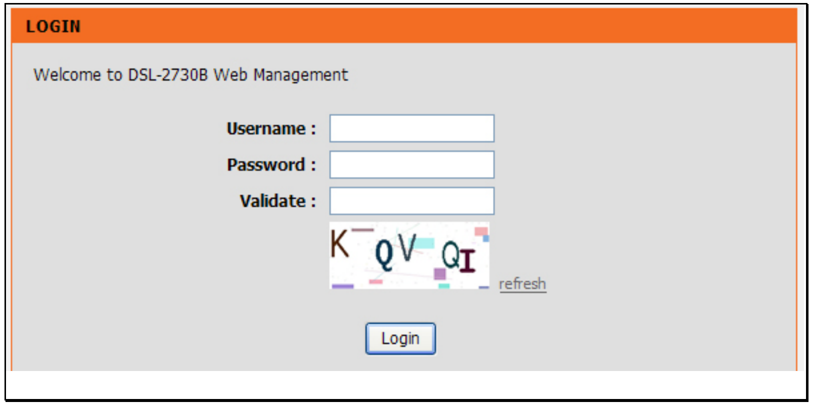
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (**192.168.1.1**).



D-Link ADSL Router - Windows Internet Explorer

http://192.168.1.1/index.html

Type **“admin**” for the Username, “**admin**” in the Password field. In the Validate entry field, type the letters that appear below. If you cannot read the letters, click on refresh to view a new randomly generated set of five letters. The Validate field is not case sensitive so upper or lower case letters work. Click Login when the you have filled in the three login fields. If you get a *Page Cannot be Displayed* error, please refer to the Troubleshooting section for assistance.



LOGIN

Welcome to DSL-2730B Web Management

Username :

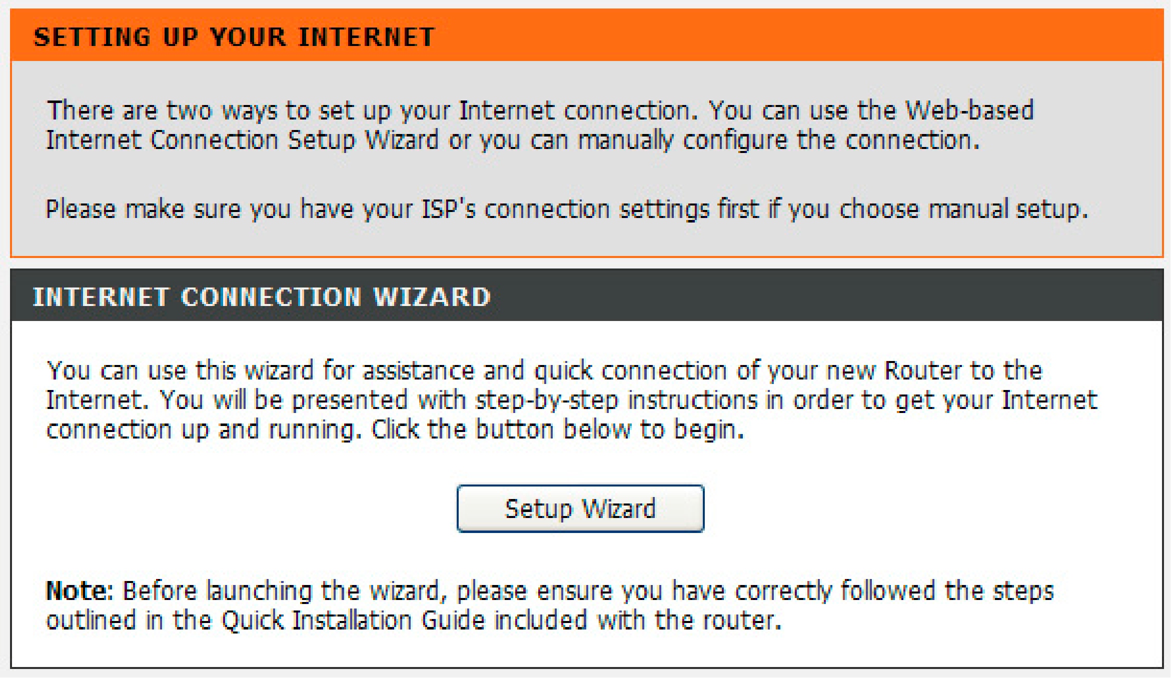
Password :

Validate :

Quick 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.

QUICK SETUP
Click the **Setup Wizard** button in the middle of the main window of the Router's opening page to launch a series of setup windows.



SETTING UP YOUR INTERNET

There are two ways to set up your Internet connection. You can use the Web-based Internet Connection Setup Wizard or you can manually configure the connection.

Please make sure you have your ISP's connection settings first if you choose manual setup.

INTERNET CONNECTION WIZARD

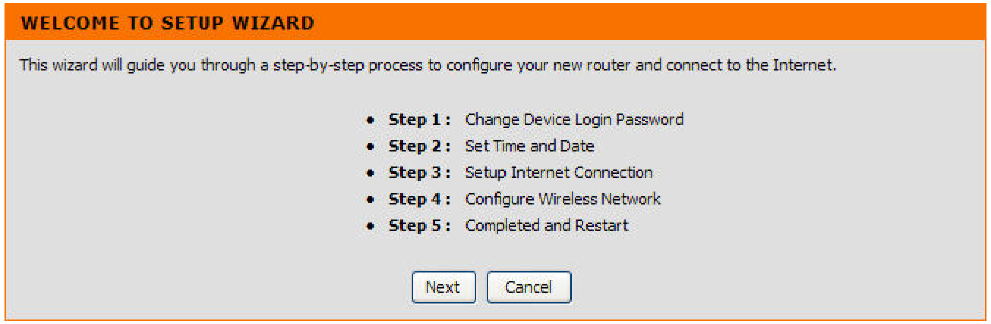
You can use this wizard for assistance and quick connection of your new Router to the Internet. You will be presented with step-by-step instructions in order to get your Internet connection up and running. Click the button below to begin.

Note: Before launching the wizard, please ensure you have correctly followed the steps outlined in the Quick Installation Guide included with the router.

QUICK SETUP – OPENING WINDOW

The first window of the Setup Wizard lists the basic steps in the process. These steps are as follows:

1. Change the Router password.
2. Configure time and date of the Router.
3. Configure the connection to the Internet.
4. Configure the connection to Wireless Network.
5. Save the new configuration settings and reboot the system.



WELCOME TO SETUP WIZARD

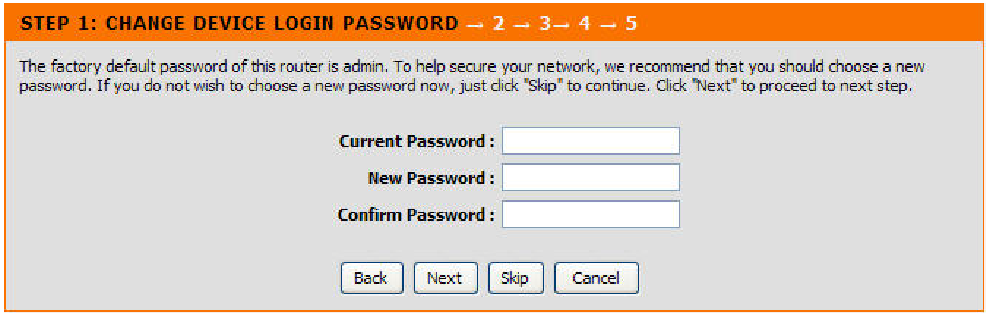
This wizard will guide you through a step-by-step process to configure your new router and connect to the Internet.

- **Step 1 :** Change Device Login Password
- **Step 2 :** Set Time and Date
- **Step 3 :** Setup Internet Connection
- **Step 4 :** Configure Wireless Network
- **Step 5 :** Completed and Restart

QUICK SETUP – CHANGE YOUR ROUTER PASSWORD

This window of the Setup Wizard is used to change the Router password. D-Link recommends to help secure your network, the user should change the Current Password from the factory default, *admin*. The New Password should be between 1 and 16 alphanumeric characters. Once you have filled out the fields in this window, including re-typing the new password in the Confirm Password field, click the **Next** button to continue.

If you do not want to change the password, click the **Skip** button to proceed to the next step.



STEP 1: CHANGE DEVICE LOGIN PASSWORD → 2 → 3→ 4 → 5

The factory default password of this router is admin. To help secure your network, we recommend that you should choose a new password. If you do not wish to choose a new password now, just click "Skip" to continue. Click "Next" to proceed to next step.

Current Password :

New Password :

Confirm Password :

QUICK SETUP – SET TIME AND DATE

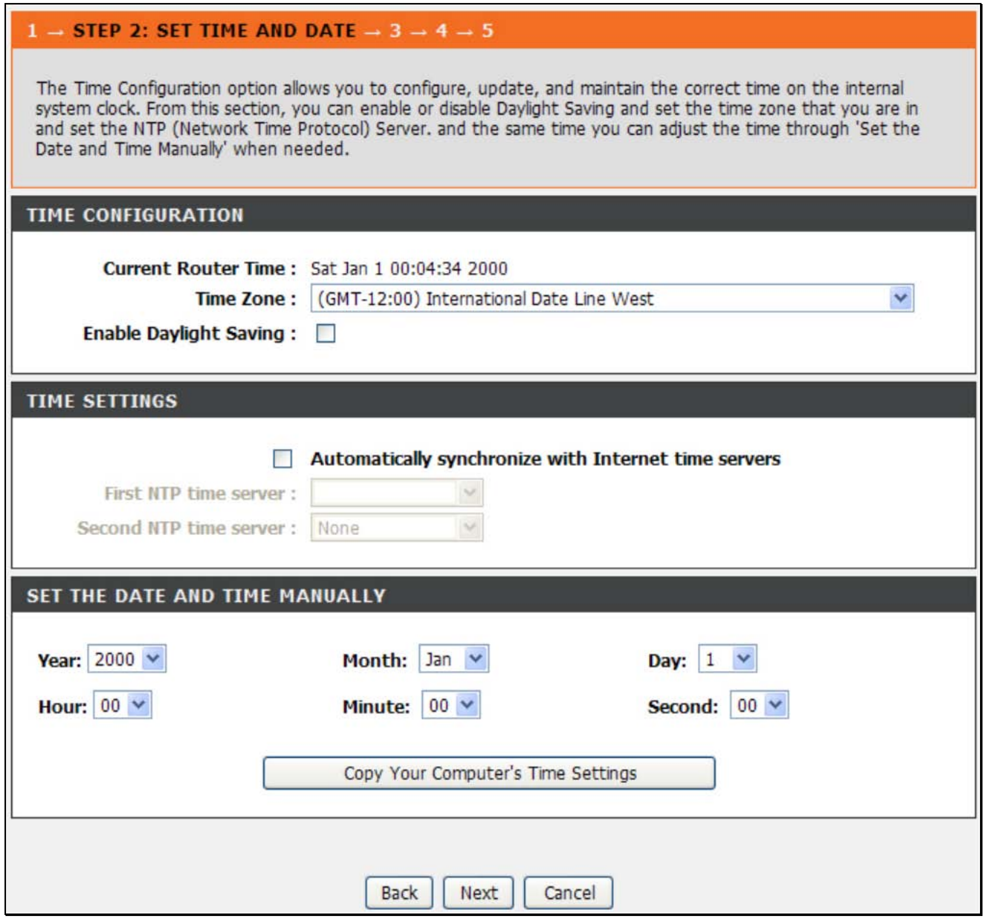
This page allows you to configure the time and date of the Router.

Select **Automatically synchronize with Internet time servers** to select first and second NTP (Network Time Protocol) server.

Select a time zone in which you are located from the **Time Zone** list.

Select **Enable Daylight Saving** and configure the daylight saving information, if the area you are located has daylight saving.

Click the **Next** button to continue.



1 → STEP 2: SET TIME AND DATE → 3 → 4 → 5

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section, you can enable or disable Daylight Saving and set the time zone that you are in and set the NTP (Network Time Protocol) Server. and the same time you can adjust the time through 'Set the Date and Time Manually' when needed.

TIME CONFIGURATION

Current Router Time : Sat Jan 1 00:04:34 2000
Time Zone : (GMT-12:00) International Date Line West
Enable Daylight Saving : □

TIME SETTINGS

□ Automatically synchronize with Internet time servers
First NTP time server :
Second NTP time server : None

SET THE DATE AND TIME MANUALLY

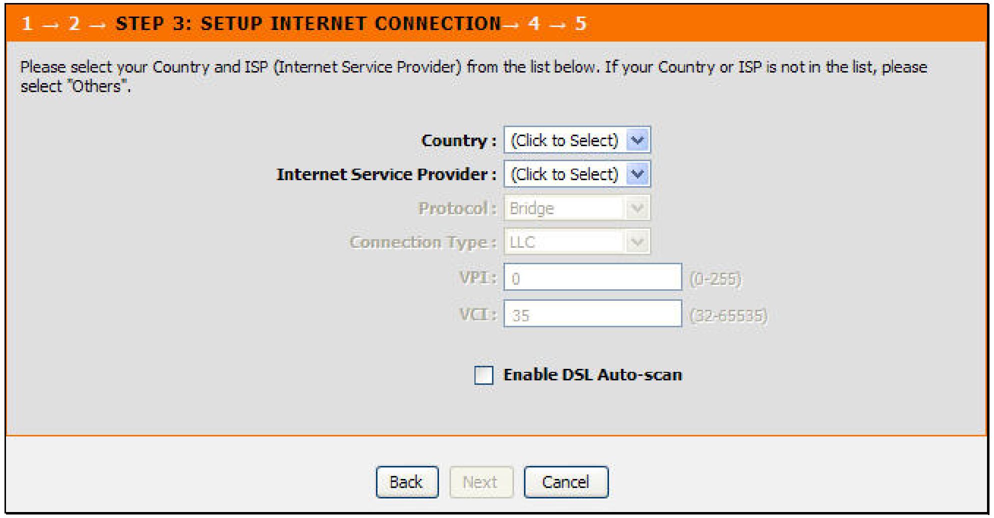
Year: 2000 Month: Jan Day: 1
Hour: 00 Minute: 00 Second: 00

QUICK SETUP – SELECT THE INTERNET CONNECTION TYPE

Now use the drop-down menus to select the Country, Internet Service Provider, Protocol, and Connection Type used for the Internet connection, and enter VPI and VCI values if applicable. Your ISP has given this information to you—any information that is not required for your provider will automatically be grayed out in this window and subsequent Quick Setup windows.

The available Protocol modes are: *PPPoE*, *PPPoA*, *Dynamic IP*, *Static IP*, and *Bridge*.

Select **PPPoE** or **PPPoA** in the **Protocol** drop-down list to see the



1 → 2 → STEP 3: SETUP INTERNET CONNECTION→ 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country : (Click to Select)
Internet Service Provider : (Click to Select)
Protocol : Bridge
Connection Type : LLC
VPI : 0 (0-255)
VCI : 35 (32-65535)

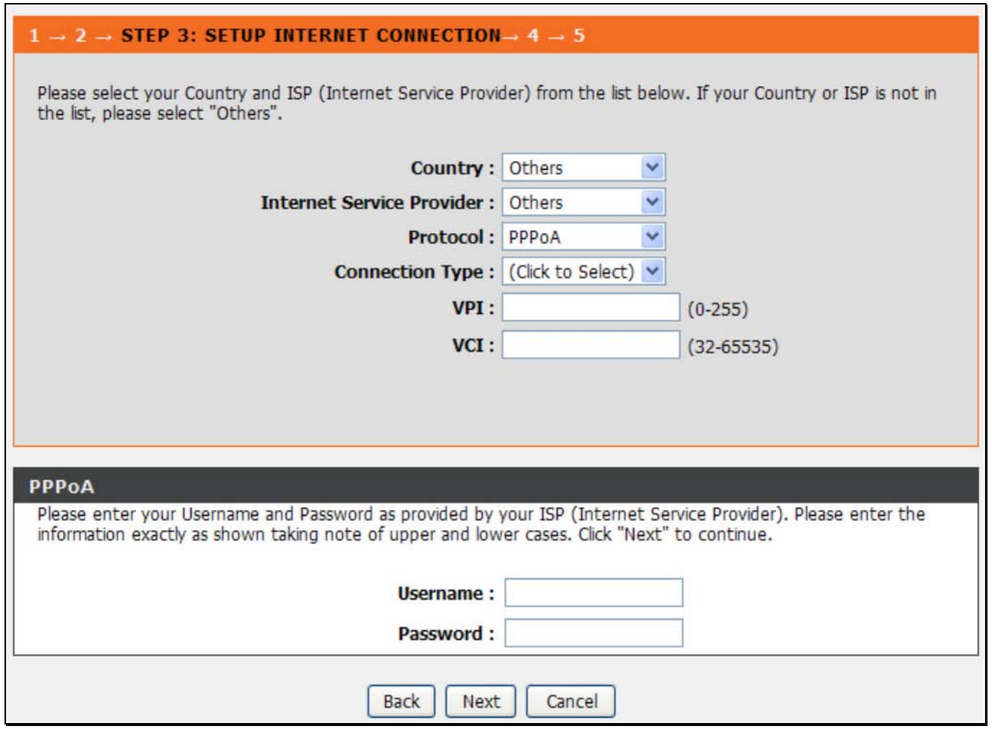
□ Enable DSL Auto-scan

QUICK SETUP – PPPOE/PPPOA CONFIGURATION

Type in the User Name and Password used to identify and verify your account to the ISP. If you are instructed to change the VPI or VCI number, type in the correct setting in the available entry fields. Most users will not need to change these settings. The Internet connection cannot function if these values are incorrect.

Some users may have to adjust the **Connection Type** from the drop-down menu. The available connection and encapsulation types are *VC-Mux*, and *LLC*.

Select **Dynamic IP** in the **Protocol** drop-down list to see the following items.



1 → 2 → STEP 3: SETUP INTERNET CONNECTION→ 4 → 5

Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :	Others
Internet Service Provider :	Others
Protocol :	PPPoA
Connection Type :	(Click to Select)
VPI :	(0-255)
VCI :	(32-65535)

PPPoA

Please enter your Username and Password as provided by your ISP (Internet Service Provider). Please enter the information exactly as shown taking note of upper and lower cases. Click "Next" to continue.

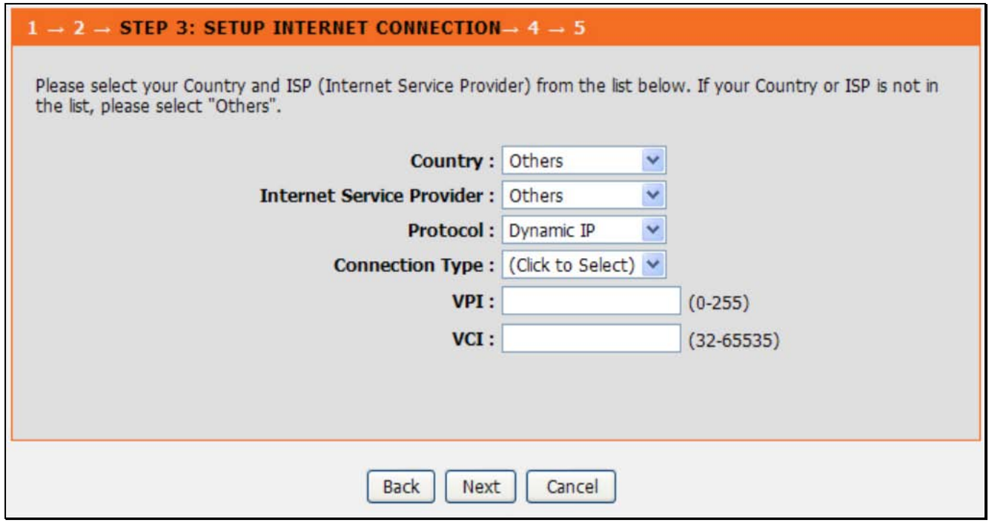
Username :

Password :

QUICK SETUP – DYNAMIC IP CONFIGURATION

If you are instructed to change the VPI or VCI numbers, type in the correct setting in the available entry fields. The Internet connection cannot function if these values are incorrect. Select the specific **Connection Type** from the drop-down menu. The available connection and encapsulation types are *LLC* and *VC-Mux*. You may want to.

Select **Static IP** in the **Protocol** drop-down list to see the following items.



1 → 2 → STEP 3: SETUP INTERNET CONNECTION→ 4 → 5

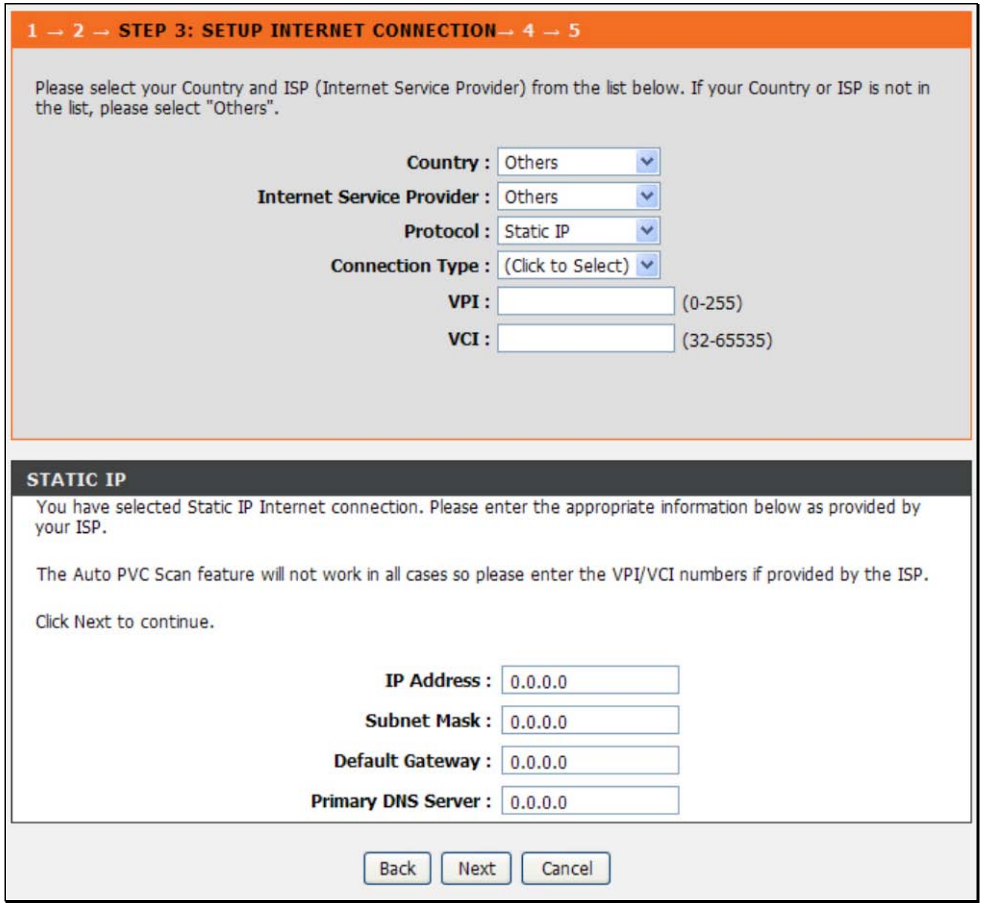
Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :	Others
Internet Service Provider :	Others
Protocol :	Dynamic IP
Connection Type :	(Click to Select)
VPI :	(0-255)
VCI :	(32-65535)

QUICK SETUP – STATIC IP CONFIGURATION
Enter values for VPI, VCI, IP Address, Subnet Mask, Default Gateway IP address, and Primary DNS Server instructed by your ISP. The Internet connection cannot function if these values are incorrect.

Select the specific **Connection Type** from the drop-down menu. The available connection and encapsulation types are *LLC*, and *VC-Mux*.

Select **Bridge** in the **Protocol** drop-down list to see the following items.



Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country : Others
Internet Service Provider : Others
Protocol : Static IP
Connection Type : (Click to Select)
VPI : (0-255)
VCI : (32-65535)

STATIC IP

You have selected Static IP Internet connection. Please enter the appropriate information below as provided by your ISP.

The Auto PVC Scan feature will not work in all cases so please enter the VPI/VCI numbers if provided by the ISP.

Click Next to continue.

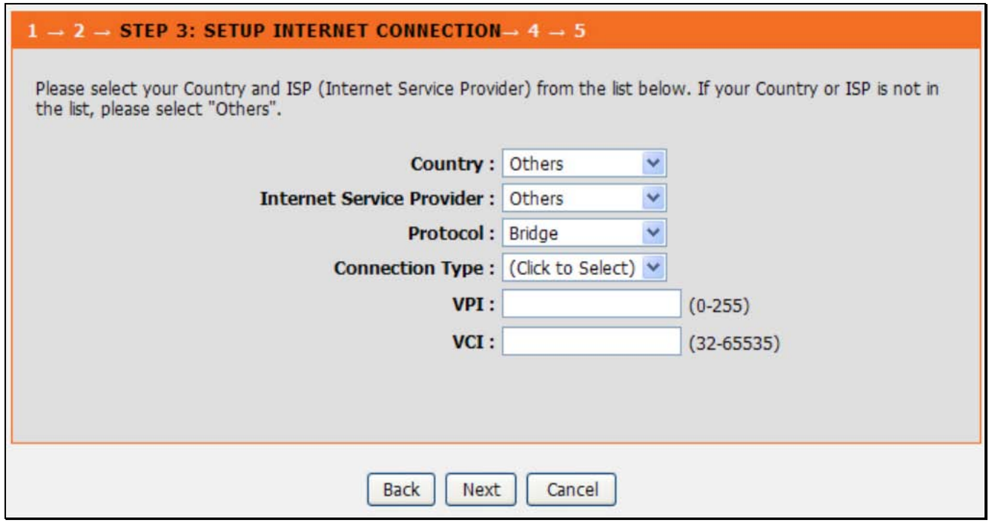
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0

QUICK SETUP – BRIDGE MODE CONFIGURATION

If you are instructed to change the VPI or VCI numbers, type in the correct setting in the available entry fields. The Internet connection cannot function if these values are incorrect.

Select the specific **Connection Type** from the drop-down menu. The available connection and encapsulation types are *LLC* and *VC-Mux*.

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



1 → 2 → STEP 3: SETUP INTERNET CONNECTION → 4 → 5

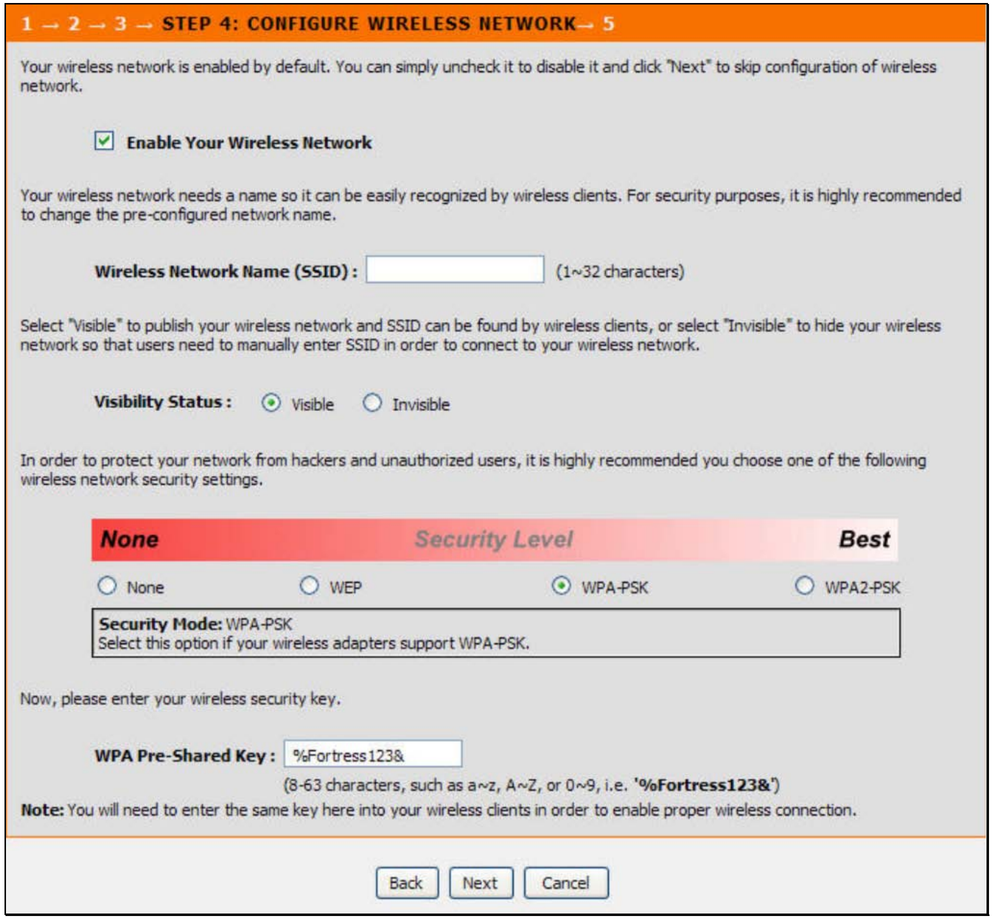
Please select your Country and ISP (Internet Service Provider) from the list below. If your Country or ISP is not in the list, please select "Others".

Country :	Others
Internet Service Provider :	Others
Protocol :	Bridge
Connection Type :	(Click to Select)
VPI :	(0-255)
VCI :	(32-65535)

QUICK SETUP – Configure Wireless Network

To enable the Wireless feature of this device, tick the **Enable Your Wireless Network** option. Enter an **SSID** (this is the wireless network name). Choose whether to make the wireless network **Visible** or **Invisible**.

The Wireless Network will be unsecure if the Security Level is set to **None**. There are 3 security options that the user can choose called **WEP**, **WPA-PSK** or **WPA2-PSK**.If the user requires no wireless security, deselect the **Enable Your Wireless Network** option. Click **Next** to continue.



1 → 2 → 3 → STEP 4: CONFIGURE WIRELESS NETWORK → 5

Your wireless network is enabled by default. You can simply uncheck it to disable it and click "Next" to skip configuration of wireless network.

☑ Enable Your Wireless Network

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name.

Wireless Network Name (SSID) : (1~32 characters)

Select "Visible" to publish your wireless network and SSID can be found by wireless clients, or select "Invisible" to hide your wireless network so that users need to manually enter SSID in order to connect to your wireless network.

Visibility Status : ● Visible ○ Invisible

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

○ None ○ WEP ● WPA-PSK ○ WPA2-PSK

Security Mode: WPA-PSK
Select this option if your wireless adapters support WPA-PSK.

Now, please enter your wireless security key.

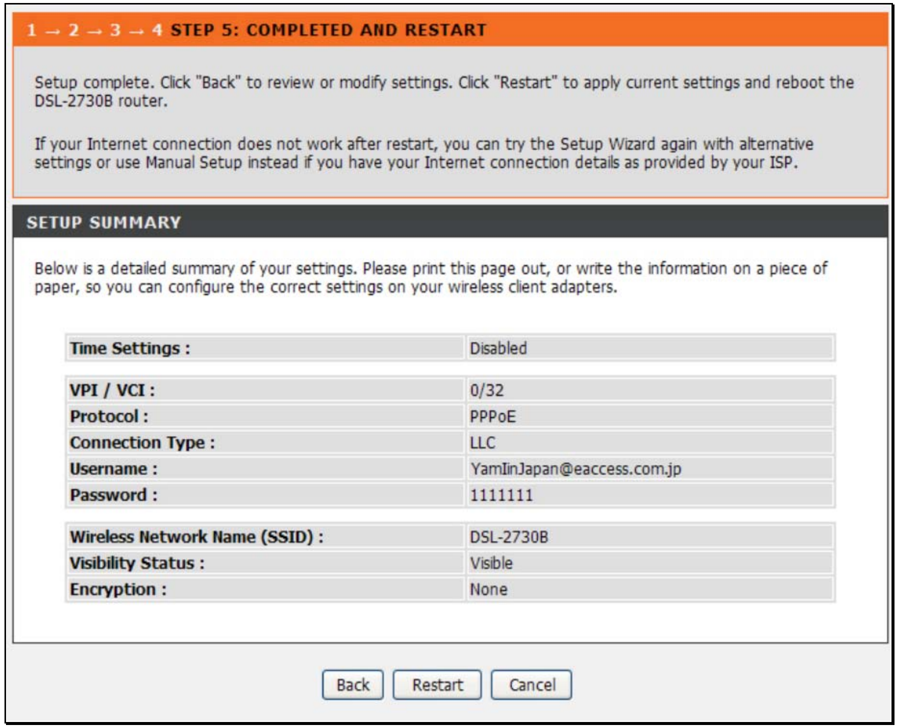
WPA Pre-Shared Key : %Fortress123&

(8-63 characters, such as a~z, A~Z, or 0~9, i.e. '**%Fortress123&**')

Note: You will need to enter the same key here into your wireless clients in order to enable proper wireless connection.

QUICK SETUP – COMPLETED & RESTART CONFIRMATION

Finally you can see the Setup Summary of the configurations you did through the wizard. If you are satisfied that you have entered all the necessary information correctly, click the **Restart** 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.



1 → 2 → 3 → 4 STEP 5: COMPLETED AND RESTART

Setup complete. Click "Back" to review or modify settings. Click "Restart" to apply current settings and reboot the DSL-2730B router.

If your Internet connection does not work after restart, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

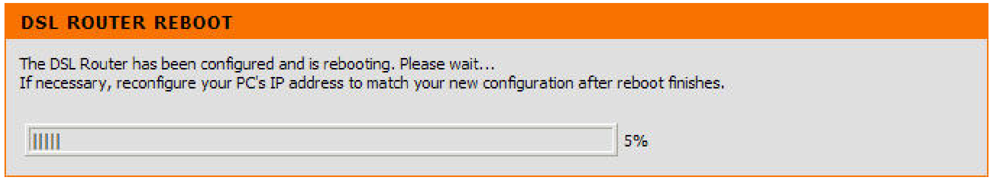
SETUP SUMMARY

Below is a detailed summary of your settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Time Settings :	Disabled
VPI / VCI :	0/32
Protocol :	PPPoE
Connection Type :	LLC
Username :	YamInJapan@eaccess.com.jp
Password :	1111111
Wireless Network Name (SSID) :	DSL-2730B
Visibility Status :	Visible
Encryption :	None

QUICK SETUP – REBOOT TIME INDICATOR

The following window opens to indicate the amount of time it will take to reboot the Router. Once the rebooting process is completed, it will go back to the main web page.



DSL ROUTER REBOOT

The DSL Router has been configured and is rebooting. Please wait…
If necessary, reconfigure your PC's IP address to match your new configuration after reboot finishes.

Internet Setup

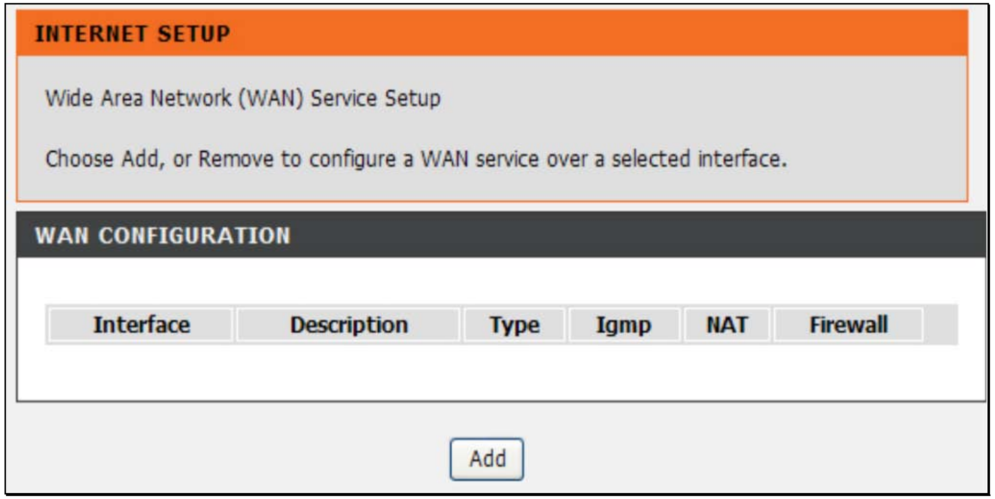
To configure the Router’s basic configuration settings without running the Setup Wizard, you can access the windows used to configure ADSL Setup, LAN Setup, Time and Date, and Parental Control settings directly from the **Setup** directory.

To access the Internet Setup window, click **Internet Setup** on the left side of the first window that appears when you successfully access the web manager.

Internet Connection Settings

Click the **Add** button to add a new Internet connection. A new menu appears.

After the Internet connection has been established, this menu will display basic information about the Internet (WAN) connection.



INTERNET SETUP

Wide Area Network (WAN) Service Setup

Choose Add, or Remove to configure a WAN service over a selected interface.

WAN CONFIGURATION

Interface	Description	Type	Igmp	NAT	Firewall

PPPoE

For a **PPPoE** connection, first choose the **EoA** option under **ATM Interface Configuration** in order to view the parameters to configure for this connection type.

VPI: Enter the correct VPI used in this field.

VCI: Enter the correct VCI used in this field.

Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE use the EoA (Ethernet over ATM) option. This is the default setting.

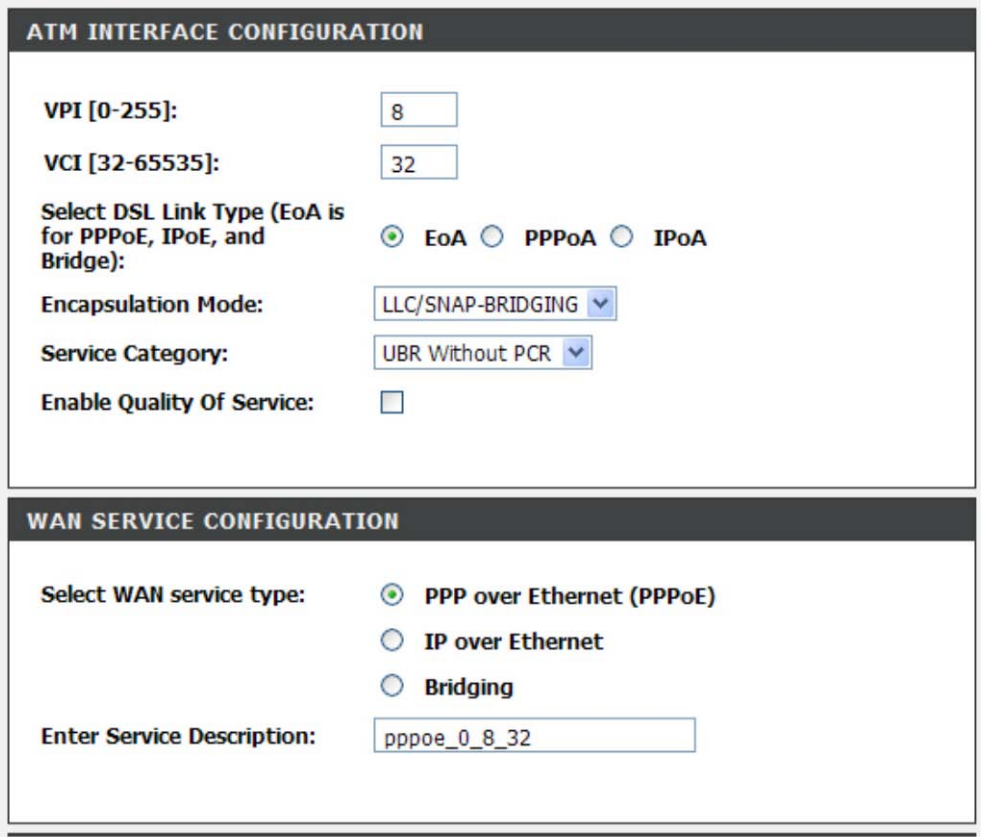
Encapsulation Mode: Choose the appropriate Encapsulation Mode here.

Service Category: Choose the appropriate Service Category here.

Enable Quality of Service: Tick this option to enable Quality of Service.

Select WAN Service Type: Choose the appropriate WAN Service Type here. Click **PPP over Ethernet (PPPoE)** for this section.

Enter Service Description: This field will display an automated service description.



ATM INTERFACE CONFIGURATION

VPI [0-255]: 8

VCI [32-65535]: 32

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge): ● EoA ○ PPPoA ○ IPoA

Encapsulation Mode: LLC/SNAP-BRIDGING

Service Category: UBR Without PCR

Enable Quality Of Service: □

WAN SERVICE CONFIGURATION

Select WAN service type: ● PPP over Ethernet (PPPoE) ○ IP over Ethernet ○ Bridging

Enter Service Description: pppoe_0_8_32

PPP Configuration

The parameters listed in the PPP Configuration menu are used for PPPoE and PPPoA connections.

PPP Username: Enter the account username in this field.

PPP Password: Enter the account password in this field.

PPPoE Service Name: Enter the service name here (optional).

Authentication Method: Choose the appropriate authentication method here. If not sure leave this option on **Auto**.

Enable NAT: Tick this option to enable NAT for this connection. NAT is enabled by default.

Enable Fullcone NAT: This option appears only if NAT is enabled (NAT is enabled by default). Tick this option to enable Fullcone NAT for this connection.

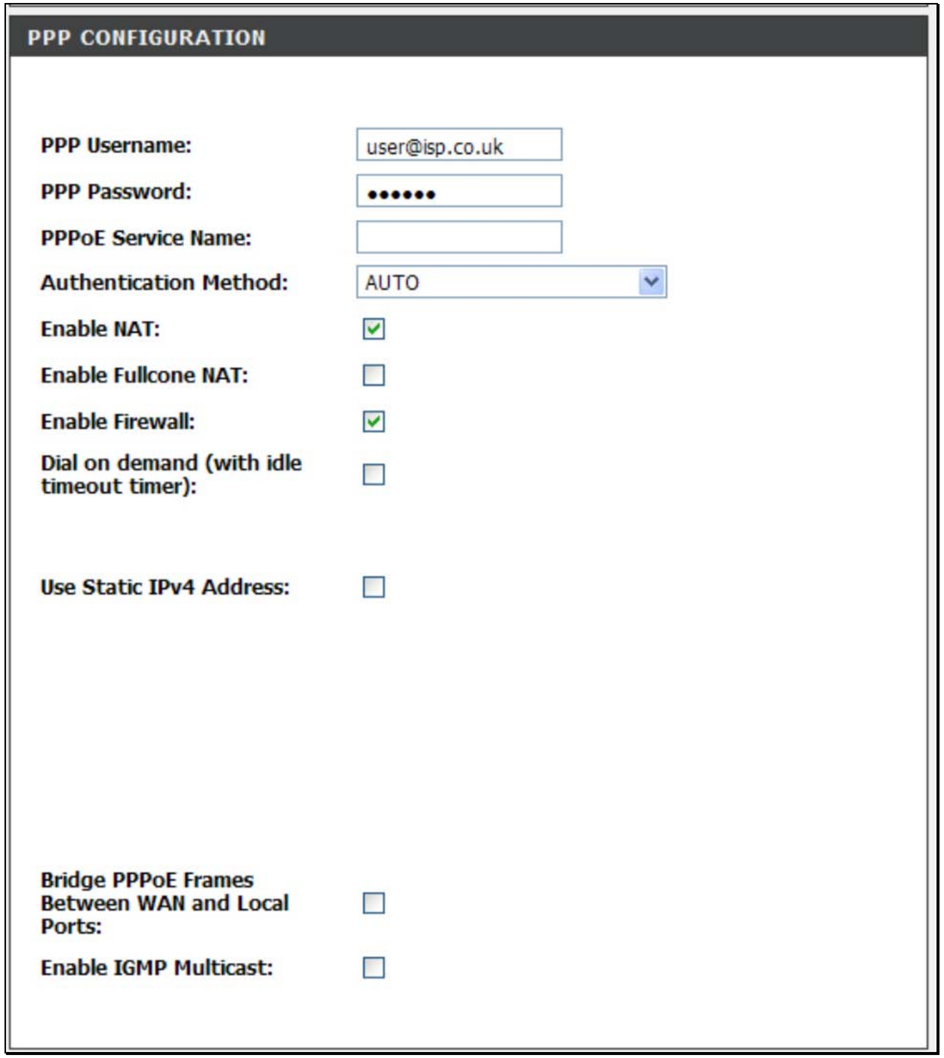
Enable Firewall: This is enabled by default. It provides basic firewall protection that closes unused ports. Click in the box to remove the check mark to disabled this function.

Dial on Demand: Tick this option to enable dial on demand for this connection. When this is enabled, the PPP session will timeout and disconnect when the connection is idle. It will automatically reconnect whenever it receives a connection request from the LAN side.

Use Static IPv4: Tick this option to use a Static IP version 4 address for this connection.

Static IPv4 Address: When **Use Static IPv4** is selected, this selection appears. Enter the Static IP version 4 address used here.

Enable IGMP Multicast: Tick this option to allow IGMP packets to go through the WAN interface in both directions.



PPP CONFIGURATION

PPP Username:	user@isp.co.uk
PPP Password:	••••••
PPPoE Service Name:	
Authentication Method:	AUTO
Enable NAT:	☑
Enable Fullcone NAT:	□
Enable Firewall:	☑
Dial on demand (with idle timeout timer):	□
Use Static IPv4 Address:	□
Bridge PPPoE Frames Between WAN and Local Ports:	□
Enable IGMP Multicast:	□

Default Gateway and DNS Settings

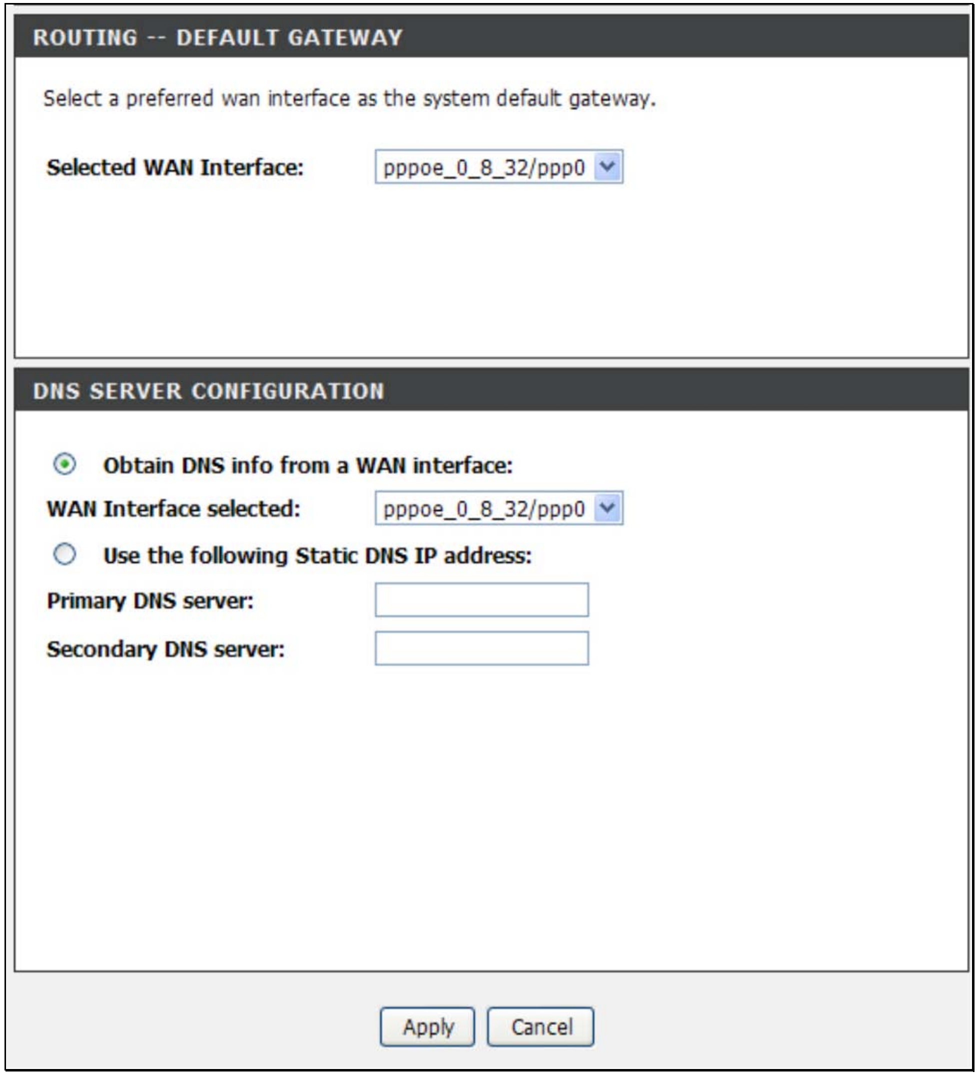
Selected WAN Interface: The user can choose the WAN interface to use this connection.

Obtain DNS info from a WAN interface: The user can choose to obtain DNS Server IP addresses automatically from the ISP.

Use the following Static DNS IP address: The user can manually enter the DNS Server IP addresses to use for this connection.

Click the **Apply** button to accept these changes.

Click the **Cancel** button to discard these changes.



ROUTING -- DEFAULT GATEWAY

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: pppoe_0_8_32/ppp0

DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoe_0_8_32/ppp0

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

IP over Ethernet

For an **IP over Ethernet** connection, first choose the **EoA** option under **ATM Interface Configuration** in order to view the parameters to configure for this connection type.

Click the **EoA** and **IP over Ethernet** radio buttons to see the following selections.

VPI: Enter the correct VPI used in this field.

VCI: Enter the correct VCI used in this field.

Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE Mode select **EoA**.

Encapsulation Mode: Choose the appropriate Encapsulation Mode here.

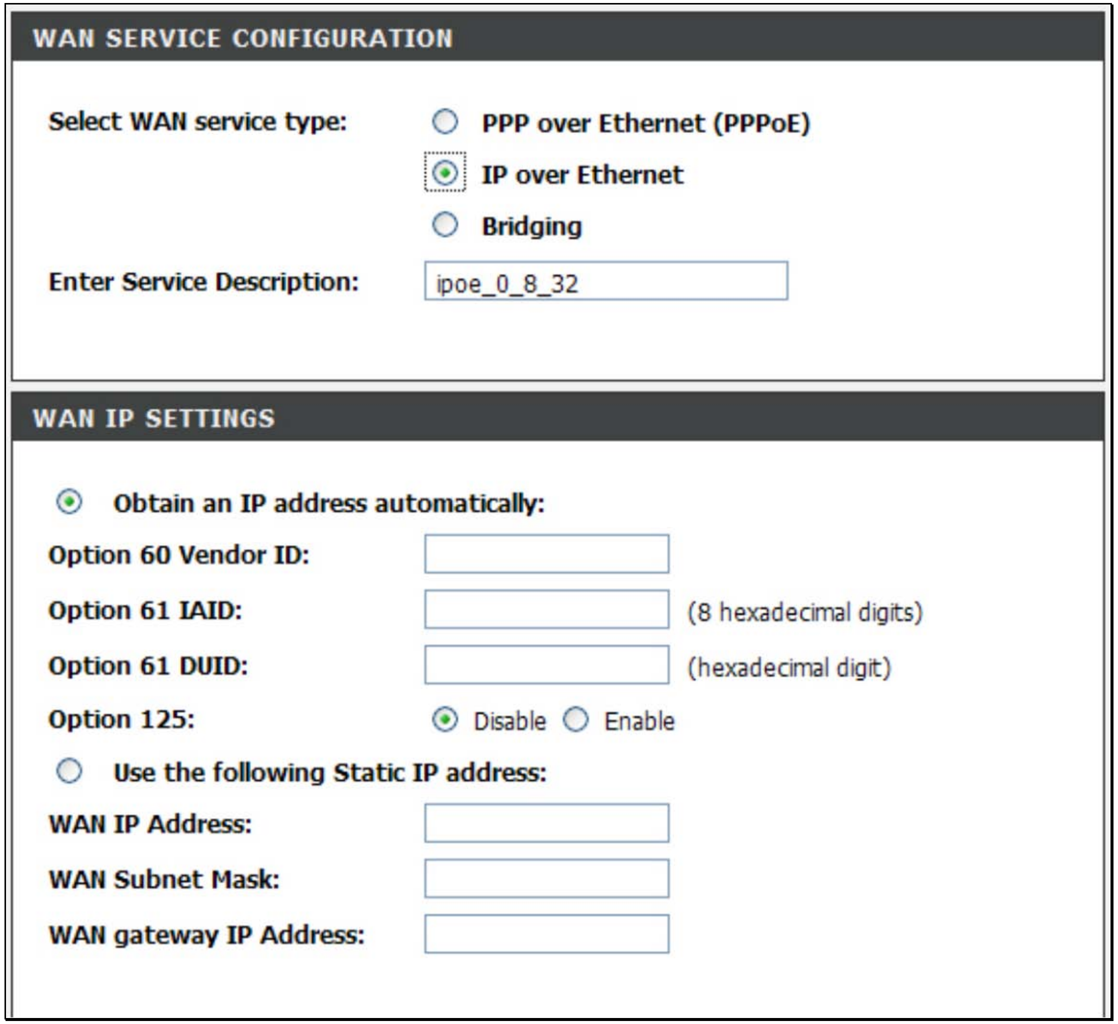
Service Category: Choose the appropriate Service Category here.

Select Connection Mode: Choose the connection mode of your Internet link here.

Enable Quality of Service: Tick this option to enable Quality of Service.

Select WAN Service Type: Choose the appropriate WAN Service Type here. Click **IP over Ethernet** for this section.

Enter Service Description: This field will display an automated service description.



WAN SERVICE CONFIGURATION

Select WAN service type: ○ PPP over Ethernet (PPPoE) ● IP over Ethernet ○ Bridging

Enter Service Description: ipoe_0_8_32

WAN IP SETTINGS

● Obtain an IP address automatically:

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: ● Disable ○ Enable

○ Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

WAN IP Settings

Obtain an IP address automatically: Choose this option to obtain an IP address automatically for this connection.

Option 60 Vender ID: Enter the Option 60 Vendor ID value used in the field.

Option 61 IAID: Enter the Option 61 IAID value used in the field.

Option 61 DUID: Enter the Option 61 DUID value used in the field.

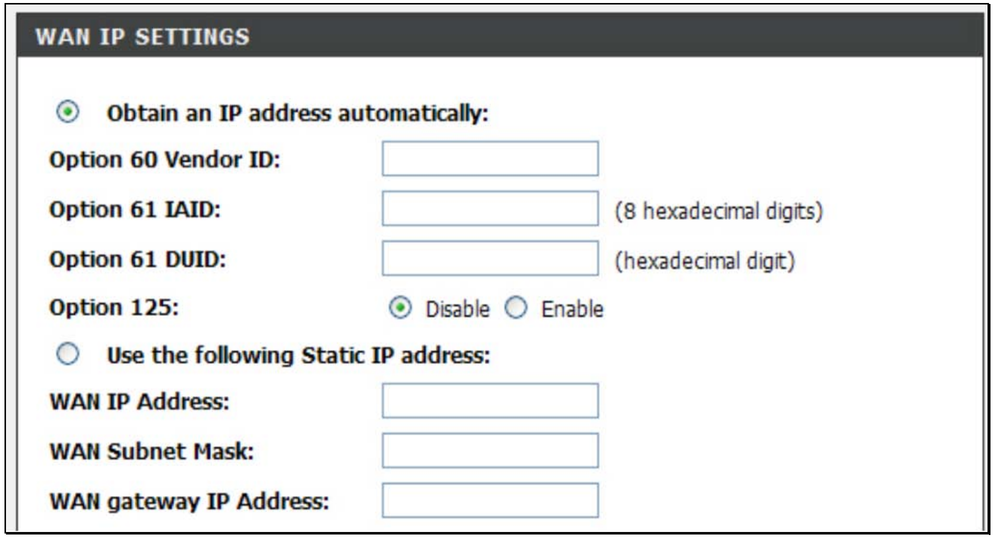
Option 125: Tick the radio buttons to enable or disable the Option 125 value.

Use the following Static IP address: Choose this option to manually enter a static IP address used for this connection. Configure the IP settings below.

WAN IP Address: Enter the WAN IP address used in the field.

WAN Subnet Mask: Enter the WAN subnet mask used in the field.

WAN Gateway IP Address: Enter the WAN gateway IP address used in the field.



WAN IP SETTINGS

● Obtain an IP address automatically:

Option 60 Vendor ID:

Option 61 IAID: (8 hexadecimal digits)

Option 61 DUID: (hexadecimal digit)

Option 125: ● Disable ○ Enable

○ Use the following Static IP address:

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

NAT, Default Gateway and DNS Settings

Enable NAT: Tick this option to enable NAT for this connection.

Enable Fullcone NAT: When **Enable NAT** is selected, this selection appears. Tick this option to enable Fullcone NAT for this connection.

Enable firewall: Tick this option to enable firewall for this connection.

Enable IGMP Multicast: Tick this option to allow IGMP packets to go through the WAN interface in both directions.

Selected WAN Interface: The user can choose the WAN interface to use this connection.

Obtain DNS info from a WAN interface: Tick the radio button to obtain DNS Server IP addresses automatically from the ISP.

WAN Interface Selected: Display the WAN interface that has been selected in the Routing – Default Gateway section.

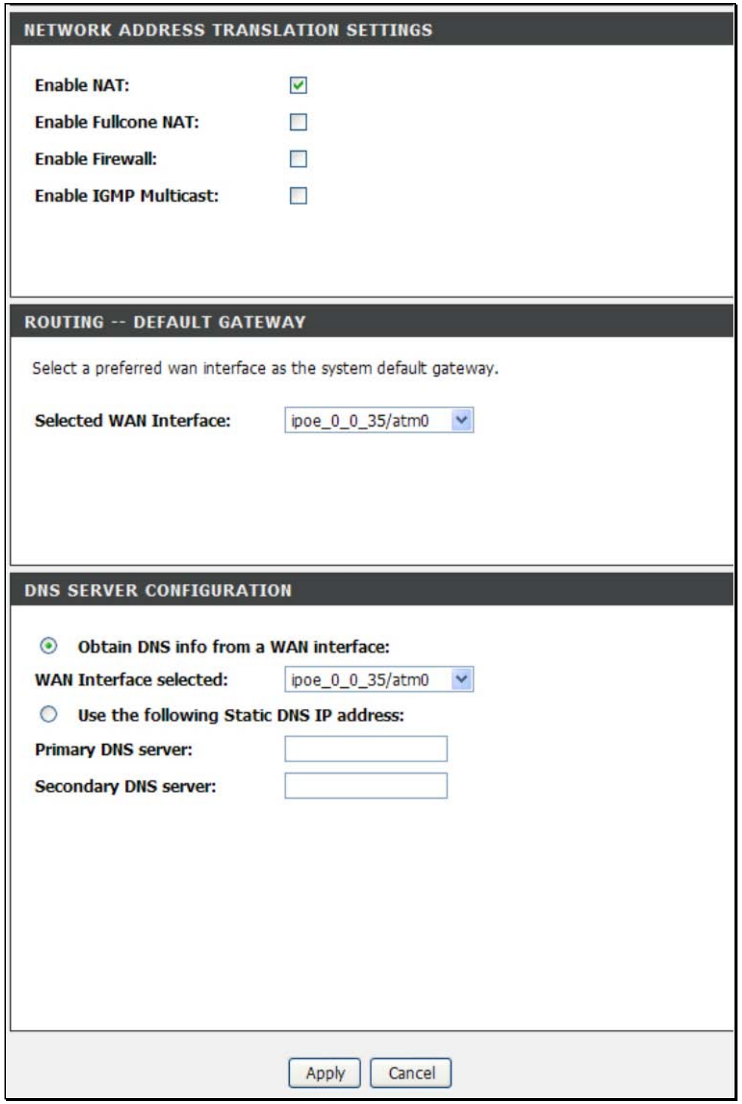
Use the following Static DNS IP address: Tick the radio button to manually enter the DNS Server IP addresses below for this connection.

Primary DNS Server: Enter the main DNS server IP address.

Secondary DNS Server: Enter the secondary DNS server IP address.

Click the **Apply** button to accept these changes.

Click the **Cancel** button to discard these changes.



NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT: ☑

Enable Fullcone NAT: □

Enable Firewall: □

Enable IGMP Multicast: □

ROUTING -- DEFAULT GATEWAY

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: ipoe_0_0_35/atm0

DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected: ipoe_0_0_35/atm0

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

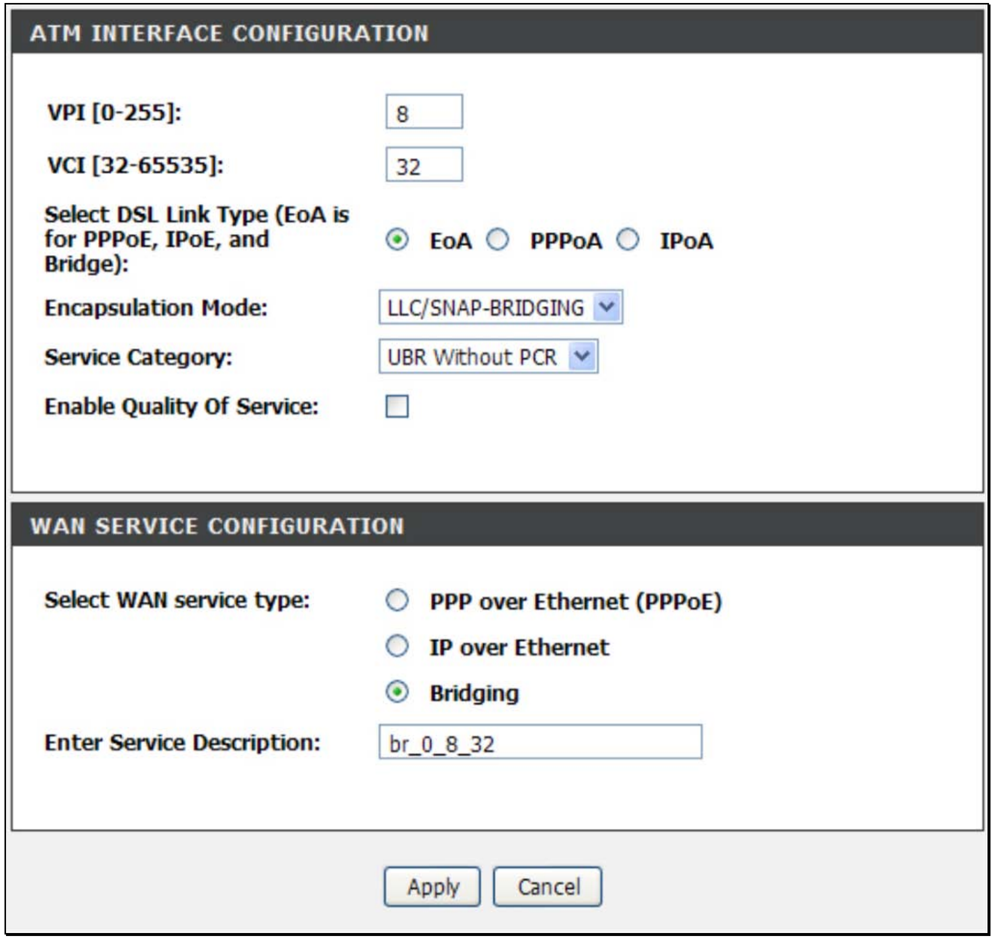
Bridge

For a **Bridge** connection, first choose the **EoA** option under **ATM Interface Configuration** in order to view the parameters to configure for this connection type.

Click the **EoA** and **Bridging** radio buttons to see the following selections.
VPI: Enter the correct VPI used in this field.
VCI: Enter the correct VCI used in this field.
Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE Mode select **EoA**.
Encapsulation Mode: Choose the appropriate Encapsulation Mode here.
Service Category: Choose the appropriate Service Category here.
Select Connection Mode: Choose the connection mode of your Internet link here.
Enable Quality of Service: Tick this option to enable Quality of Service.

Select WAN Service Type: Choose the appropriate WAN Service Type here. Click **Bridging** for this section.
Enter Service Description: This field will display an automated service description.

Click the **Apply** button to accept these changes.
Click the **Cancel** button to discard these changes.



ATM INTERFACE CONFIGURATION

VPI [0-255]:	8
VCI [32-65535]:	32
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge):	● EoA ○ PPPoA ○ IPoA
Encapsulation Mode:	LLC/SNAP-BRIDGING
Service Category:	UBR Without PCR
Enable Quality Of Service:	□

WAN SERVICE CONFIGURATION

Select WAN service type:	○ PPP over Ethernet (PPPoE) ○ IP over Ethernet ● Bridging
Enter Service Description:	br_0_8_32

PPP over ATM (PPPoA)

For a **PPPoA** connection, first choose the **PPPoA** option under **ATM Interface Configuration** in order to view the parameters to configure for this connection type.

Click the **PPPoA** radio button to see the following selections.

VPI: Enter the correct VPI used in this field.

VCI: Enter the correct VCI used in this field.

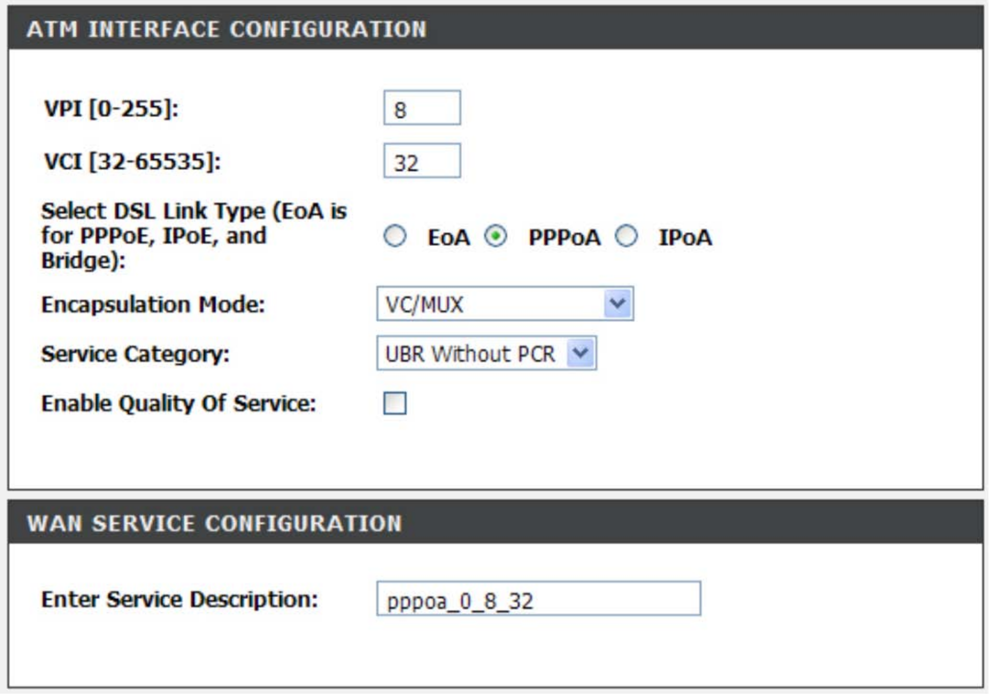
Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE Mode select **PPPoA**.

Encapsulation Mode: Choose the appropriate Encapsulation Mode here.

Service Category: Choose the appropriate Service Category here.

Enable Quality of Service: Tick this option to enable Quality of Service.

Enter Service Description: This field will display an automated service description.



ATM INTERFACE CONFIGURATION

VPI [0-255]: 8

VCI [32-65535]: 32

Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge): ○ EoA ● PPPoA ○ IPoA

Encapsulation Mode: VC/MUX

Service Category: UBR Without PCR

Enable Quality Of Service: □

WAN SERVICE CONFIGURATION

Enter Service Description: pppoa_0_8_32

PPP Configuration

The parameters listed in the PPP Configuration menu are used for PPPoE and PPPoA connections.

PPP Username: Enter the account username in this field.

PPP Password: Enter the account password in this field.

PPPoE Service Name: Enter the service name here (optional).

Authentication: Choose the appropriate authentication method here. If not sure leave this option on **Auto**.

Enable NAT: Tick this option to enable NAT for this connection.

Enable Fullcone NAT: When **Enable NAT** is selected, this selection appears. Tick this option to enable Fullcone NAT for this connection.

Enable Firewall: This is enabled by default. It provides basic firewall protection that closes unused ports. Click in the box to remove the check mark to disabled this function.

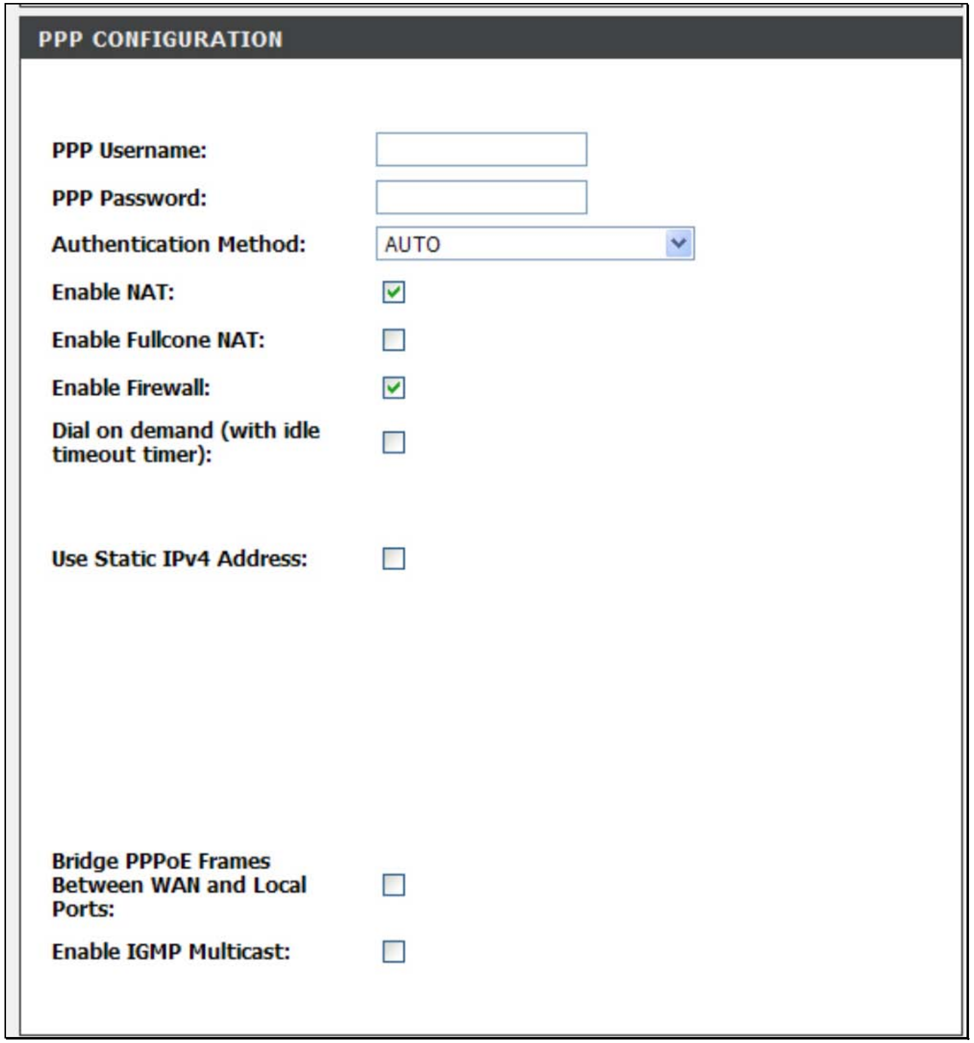
Dial on Demand: Tick this option to enable dial on demand for this connection. When this is enabled, the PPP session will timeout and disconnect when the connection is idle. It will automatically reconnect whenever it receives a connection request from the LAN side.

Use Static IPv4: Tick this option to use a Static IP version 4 address for this connection.

IPv4 Address: When **Use Static IPv4** is selected, this entry field appears. Enter the Static IP version 4 address used here.

Bridge PPPoE Frames: Tick this option if you are running services on your LAN that require PPPoE authentication or if PPPoE clients are running on your LAN that requires authentication for services on the WAN.

Enable IGMP Multicast: Tick this option to allow IGMP packets to go through the WAN interface in both directions.



PPP CONFIGURATION

PPP Username:

PPP Password:

Authentication Method: AUTO

Enable NAT: ☑

Enable Fullcone NAT: □

Enable Firewall: ☑

Dial on demand (with idle timeout timer): □

Use Static IPv4 Address: □

Bridge PPPoE Frames Between WAN and Local Ports: □

Enable IGMP Multicast: □

Default Gateway and DNS Settings

Selected WAN Interface: The user can choose the WAN interface to use this connection.

Obtain DNS info from a WAN interface: Tick the radio button to obtain DNS Server IP addresses automatically from the ISP.

WAN Interface Selected: Display the WAN interface that has been selected in the Routing – Default Gateway section.

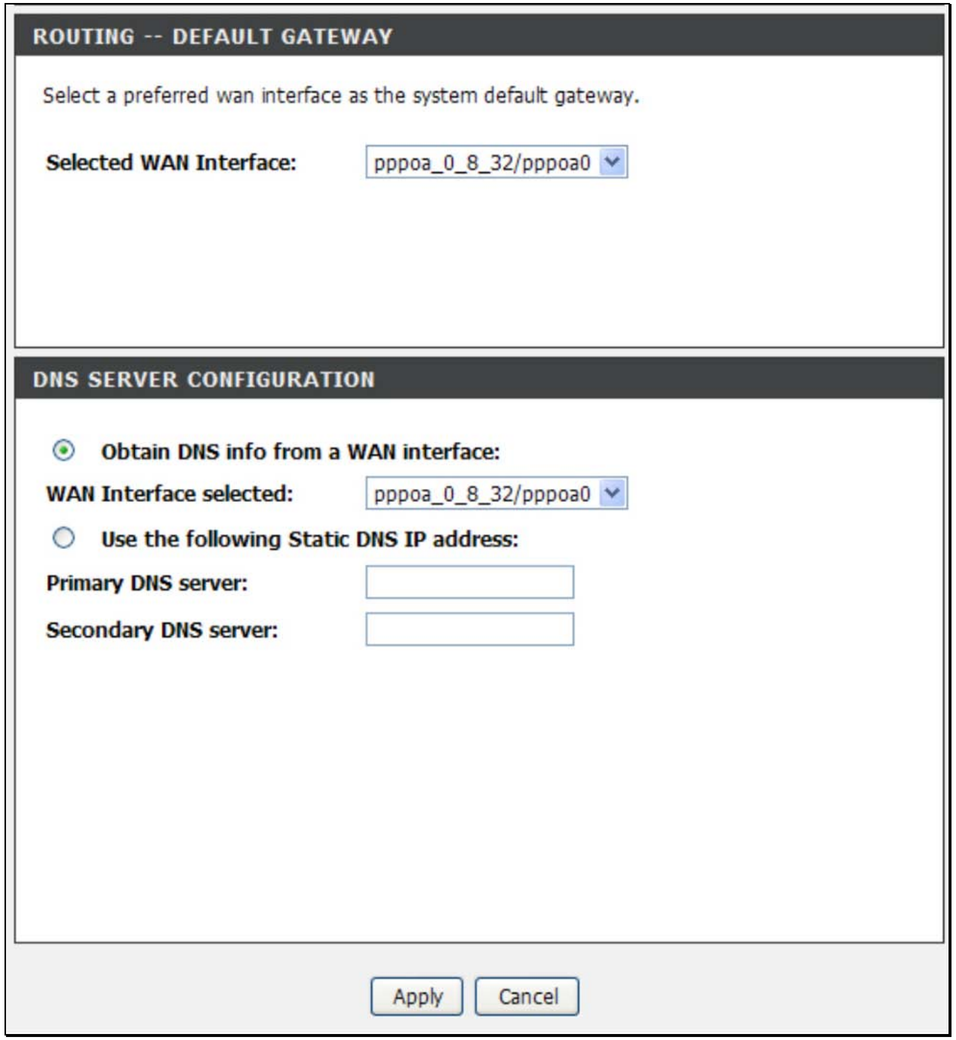
Use the following Static DNS IP address: Tick the radio button to manually enter the DNS Server IP addresses below for this connection.

Primary DNS Server: Enter the main DNS server IP address.

Secondary DNS Server: Enter the secondary DNS server IP address.

Click the **Apply** button to accept these changes.

Click the **Cancel** button to discard these changes.



ROUTING -- DEFAULT GATEWAY

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: pppoa_0_8_32/pppoa0

DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoa_0_8_32/pppoa0

○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

IP over ATM (IPoA)

For an **IPoA** connection, first choose the **IPoA** option under **ATM Interface Configuration** in order to view the parameters to configure for this connection type.

Click the **IPoA** radio button to see the following selections.

VPI: Enter the correct VPI used in this field.

VCI: Enter the correct VCI used in this field.

Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE Mode select **IPoA**.

Encapsulation Mode: Choose the appropriate Encapsulation Mode here.

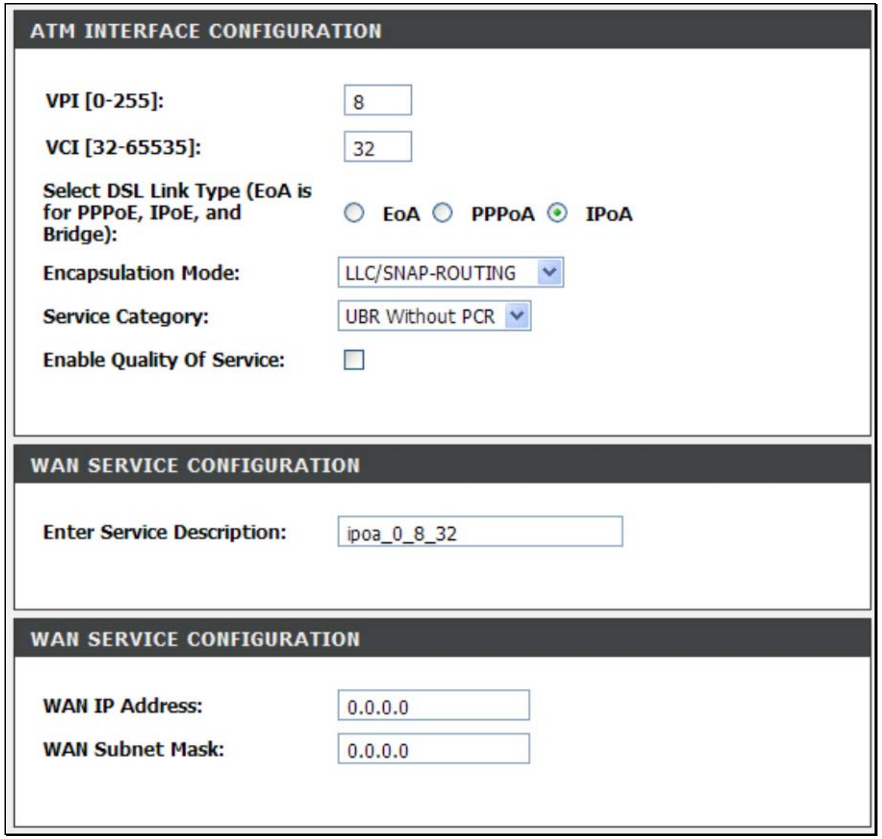
Service Category: Choose the appropriate Service Category here.

Enable Quality of Service: Tick this option to enable Quality of Service.

Enter Service Description: This field will display an automated service description.

WAN IP Address: Enter the WAN IP address used in the field.

WAN Subnet Mask: Enter the WAN subnet mask used in the field.



ATM INTERFACE CONFIGURATION

VPI [0-255]:	8
VCI [32-65535]:	32
Select DSL Link Type (EoA is for PPPoE, IPoE, and Bridge):	○ EoA ○ PPPoA ● IPoA
Encapsulation Mode:	LLC/SNAP-ROUTING
Service Category:	UBR Without PCR
Enable Quality Of Service:	□

WAN SERVICE CONFIGURATION

Enter Service Description:	ipoa_0_8_32

WAN SERVICE CONFIGURATION

WAN IP Address:	0.0.0.0
WAN Subnet Mask:	0.0.0.0

NAT, Default Gateway Settings

Enable NAT: Tick this option to enable NAT for this connection.

Enable Fullcone NAT: When **Enable NAT** is selected, this selection appears. Tick this option to enable Fullcone NAT for this connection.

Enable firewall: Tick this option to enable firewall for this connection.

Enable IGMP Multicast: Tick this option to allow IGMP packets to go through the WAN interface in both directions.

Selected WAN Interface: The user can choose the WAN interface to use this connection.

Obtain DNS info from a WAN interface: Tick the radio button to obtain DNS Server IP addresses automatically from the ISP.

WAN Interface Selected: Display the WAN interface that has been selected in the Routing – Default Gateway section.

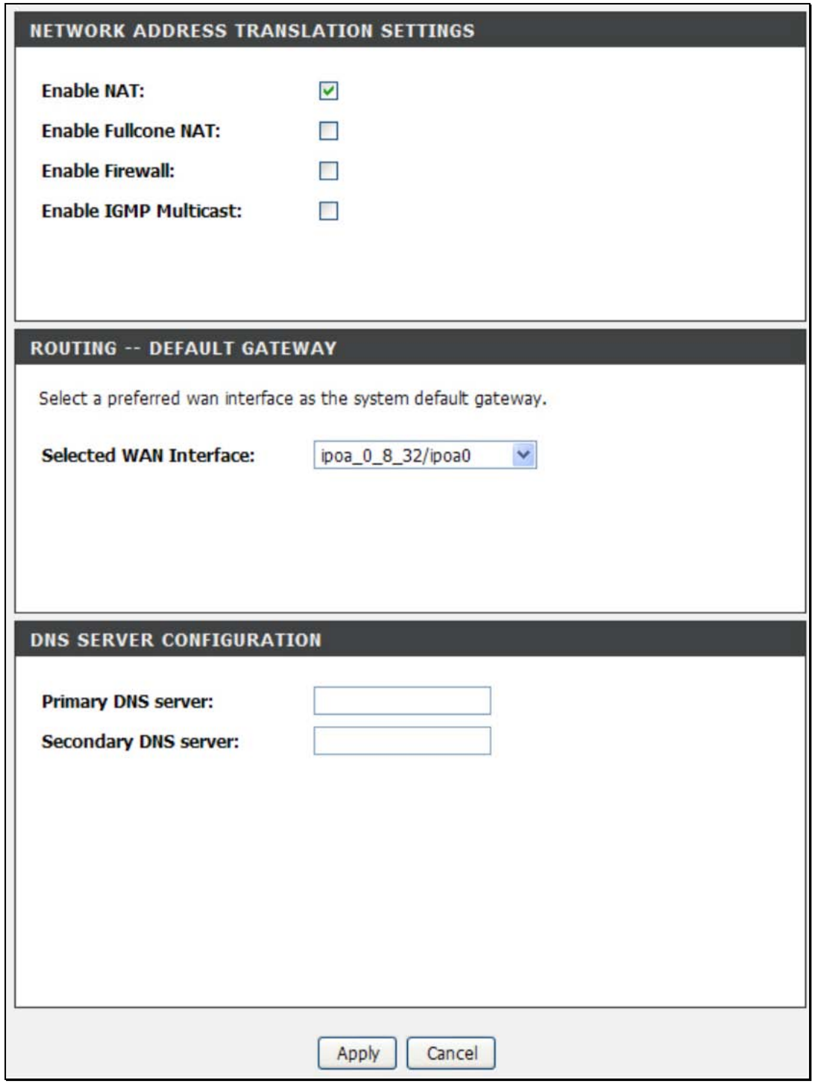
Use the following Static DNS IP address: Tick the radio button to manually enter the DNS Server IP addresses below for this connection.

Primary DNS Server: Enter the main DNS server IP address.

Secondary DNS Server: Enter the secondary DNS server IP address.

Click the **Apply** button to accept these changes.

Click the **Cancel** button to discard these changes.



NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT: ☑

Enable Fullcone NAT: □

Enable Firewall: □

Enable IGMP Multicast: □

ROUTING -- DEFAULT GATEWAY

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: ipoa_0_8_32/ipoa0

DNS SERVER CONFIGURATION

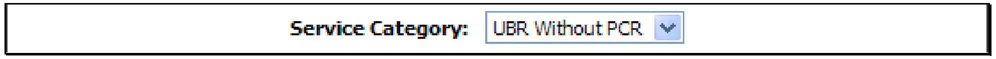
Primary DNS server:

Secondary DNS server:

Service Category

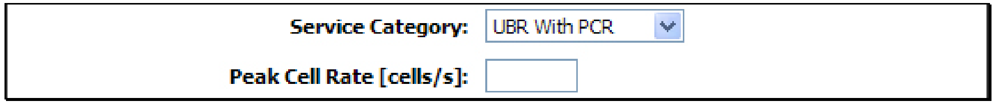
When configuring the Service Category for any of the above mentioned connection configurations there are 5 different variations to choose from.

UBR Without PCR
There are no additional fields listed when choosing this category.



Service Category: UBR Without PCR

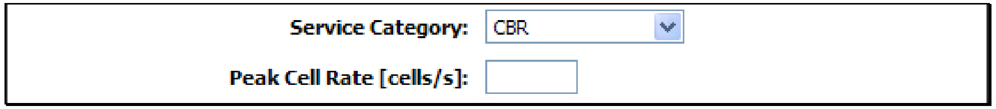
UBR With PCR
Peak Cell Rate: Enter the Peak Cell Rate used.



Service Category: UBR With PCR

Peak Cell Rate [cells/s]:

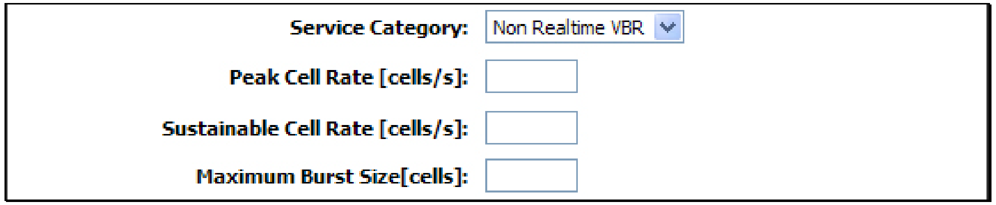
CBR
Peak Cell Rate: Enter the Peak Cell Rate used.



Service Category: CBR

Peak Cell Rate [cells/s]:

Non Realtime VBR
Peak Cell Rate: Enter the Peak Cell Rate used.
Sustainable Cell Rate: Enter the Sustainable Cell Rate used.
Maximum Burst Size: Enter the Maximum Burst Size used.



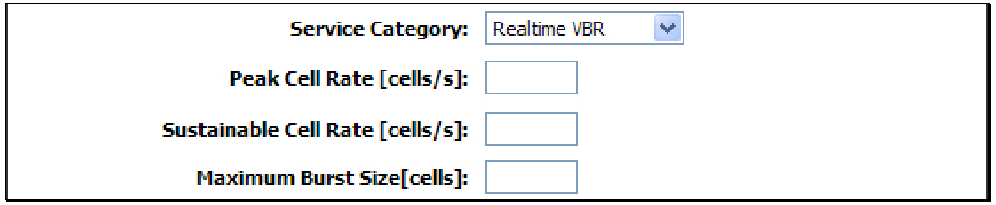
Service Category: Non Realtime VBR

Peak Cell Rate [cells/s]:

Sustainable Cell Rate [cells/s]:

Maximum Burst Size[cells]:

Realtime VBR
Peak Cell Rate: Enter the Peak Cell Rate used.
Sustainable Cell Rate: Enter the Sustainable Cell Rate used.
Maximum Burst Size: Enter the Maximum Burst Size used.



Service Category: Realtime VBR

Peak Cell Rate [cells/s]:

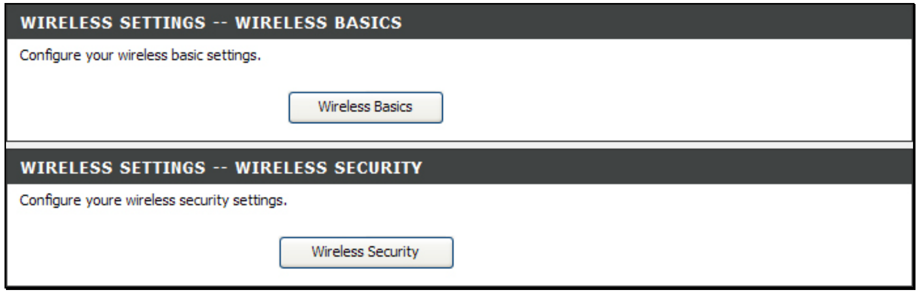
Sustainable Cell Rate [cells/s]:

Maximum Burst Size[cells]:

Wireless Settings

To access Wireless Settings, click **Wireless Settings** in the **Setup** directory.

It has two subcategories: **Wireless Basics** and **Wireless Security**. You can either point to the **Wireless Settings** on the left window and click one of the submenus, or click one of the buttons in the Wireless Settings window.



WIRELESS SETTINGS -- WIRELESS BASICS

Configure your wireless basic settings.

WIRELESS SETTINGS -- WIRELESS SECURITY

Configure youre wireless security settings.

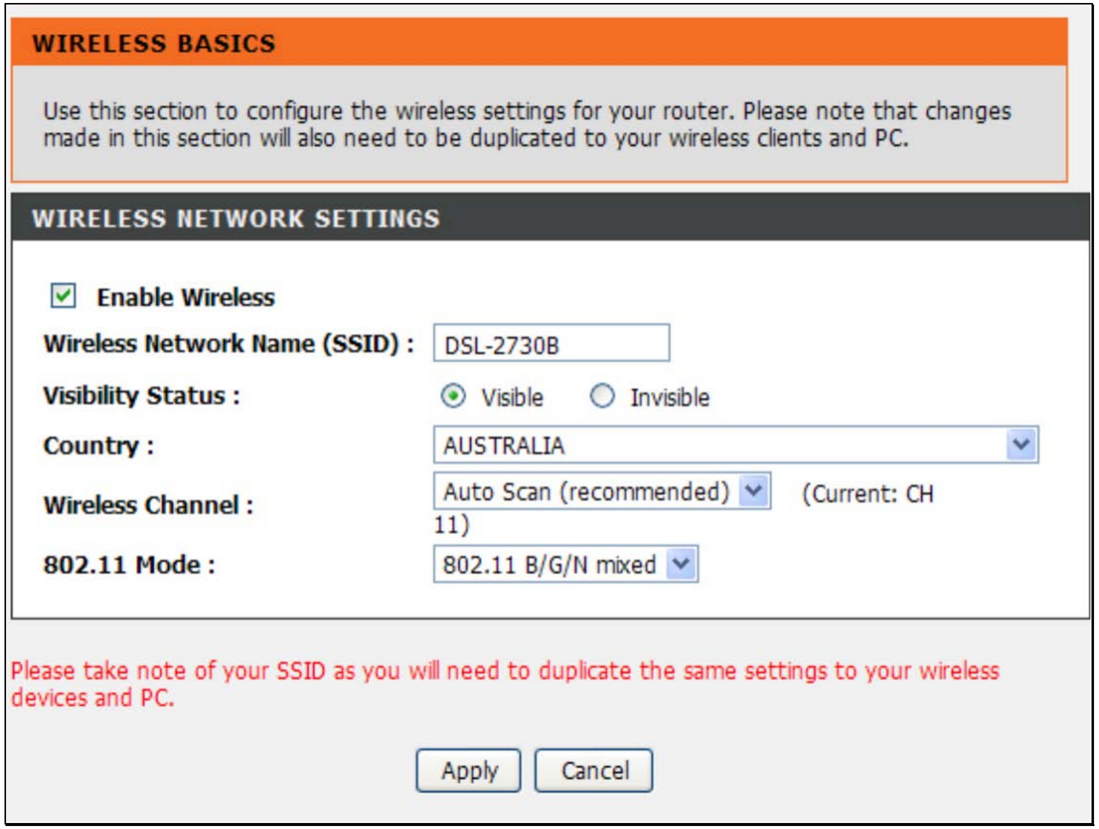
Wireless Basics

To access Wireless Basics, point to the **Wireless Settings** on the left window and click **Wireless Basics** submenu, or click the **Wireless Basics** button in the Wireless Settings window.

The two essential settings for wireless LAN operation are the Wireless Network Name (SSID) and Wireless Channel. The SSID (Service Set Identifier) is used to identify a group of wireless LAN components. The SSID can be visible (broadcast) or hidden (not broadcast).

Follow the instructions below to change basic wireless settings.

1. The Wireless LAN is enabled by default. To disable the wireless interface, click to deselect the **Enable Wireless** check box. If the wireless interface has been disabled, click the **Enable Wireless** check box again to select it.
2. The **Wireless Network Name (SSID)** can be changed to suit your wireless network. Remember that any wireless device using the access point must have the same SSID and use the same channel.
3. The Visibility Status is **Visible** by default. To disable SSID Visibility Status, click the **Invisible** radio button.
4. Select a country where the Router is located in the **Country** drop-down list.
5. The **Wireless Channel** may be changed to channels that are available in your region. Channels available for wireless LAN communication are subject to regional and national regulation.
6. Select a wireless protocol in the **802.11 Mode** drop-down list.
7. Click **Apply** to save the settings.



WIRELESS BASICS

Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

WIRELESS NETWORK SETTINGS

☑ Enable Wireless

Wireless Network Name (SSID) : DSL-2730B

Visibility Status : ● Visible ○ Invisible

Country : AUSTRALIA

Wireless Channel : Auto Scan (recommended) (Current: CH 11)

802.11 Mode : 802.11 B/G/N mixed

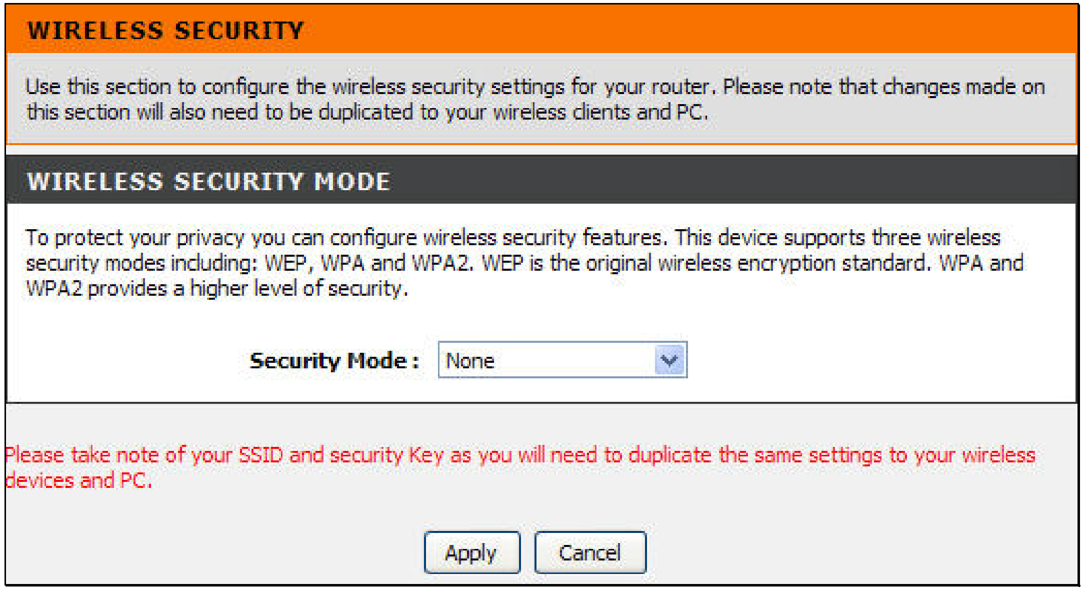
Please take note of your SSID as you will need to duplicate the same settings to your wireless devices and PC.

Wireless Security

To access Wireless Security, point to the **Wireless Settings** on the left window and click **Wireless Security** submenu, or click the **Wireless Security** button in the Wireless Settings window.

In order to protect the privacy, you can setup the wireless security. Available security modes are *WEP*, *Auto*, *WPA2 Only*, and *WPA Only*.

1. Select a wireless security mode in the **Security Mode** drop-down list.
2. Different settings based on the security mode appear at the bottom of the window.



WIRELESS SECURITY

Use this section to configure the wireless security settings for your router. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

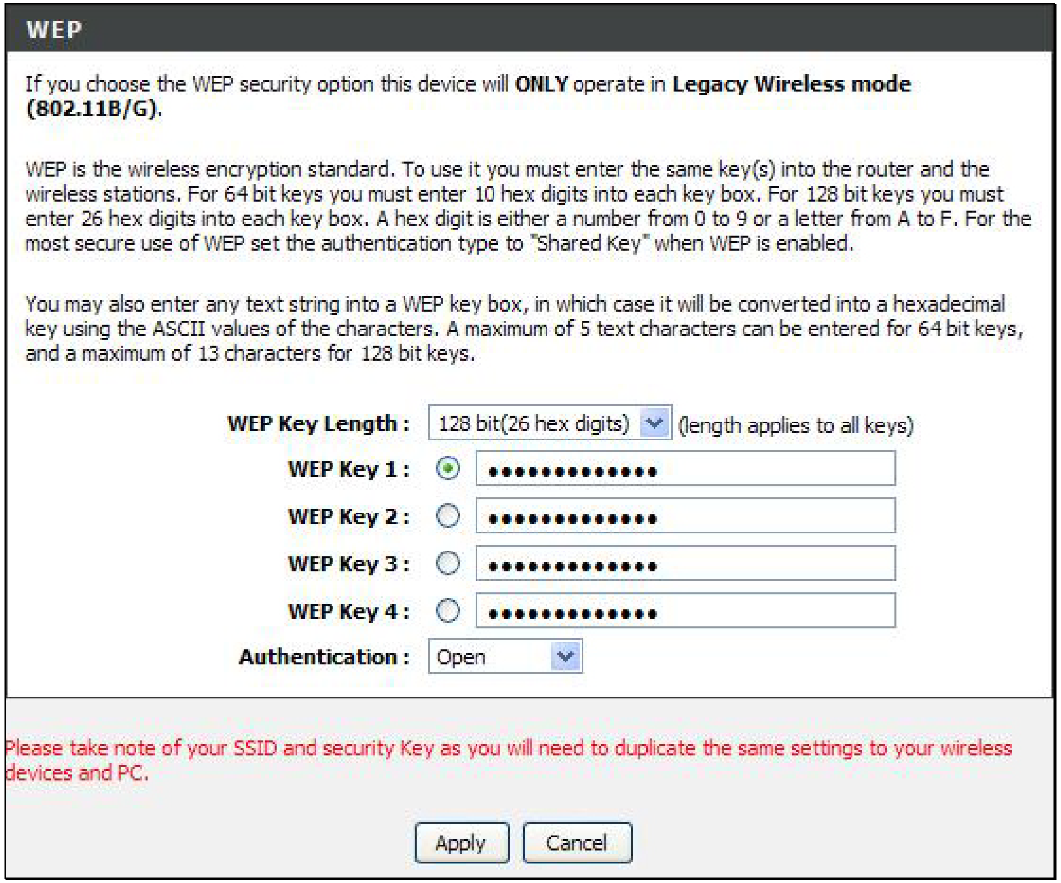
Security Mode : None

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

WEP

When selecting **WEP** from the **Security Mode** drop-down menu, the WEP section appears.

1. Select the WEP key length between 64 bit or 128 bit from the drop-down list.
2. Enter the WEP key(s) in the **WEP Key 1** to **WEP Key 4** fields.
3. Select the authentication as Open or Shared from the **Authentication** drop-down menu.
4. Click **Apply** to save the settings.



WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G).**

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : 128 bit(26 hex digits) (length applies to all keys)
WEP Key 1 : ● •••••••••••••
WEP Key 2 : ○ •••••••••••••
WEP Key 3 : ○ •••••••••••••
WEP Key 4 : ○ •••••••••••••
Authentication : Open

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

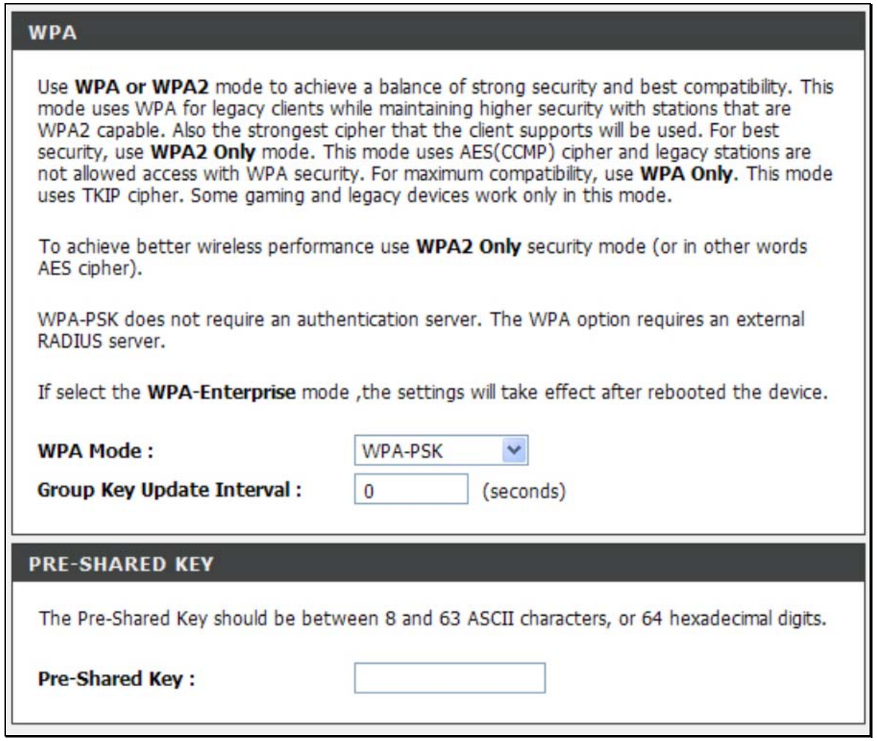
Auto, WPA or WPA2

When selecting **Auto**, **WPA2 Only** or **WPA Only** from the **Security Mode** drop-down menu, the WPA section appears.

1. In the **WPA Mode** drop-down menu, select between **WPA-PSK** and **WPA-Enterprise**. Different sections appear based on the selection.
2. Enter a period of time for key updated in the **Group Key Update Interval** field.

Pre-shared Key

When **WPA-PSK** was selected in the **WPA Mode** drop-down menu, this section appears for the user to enter a shared key.



WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

If select the **WPA-Enterprise** mode ,the settings will take effect after rebooted the device.

WPA Mode : WPA-PSK

Group Key Update Interval : 0 (seconds)

PRE-SHARED KEY

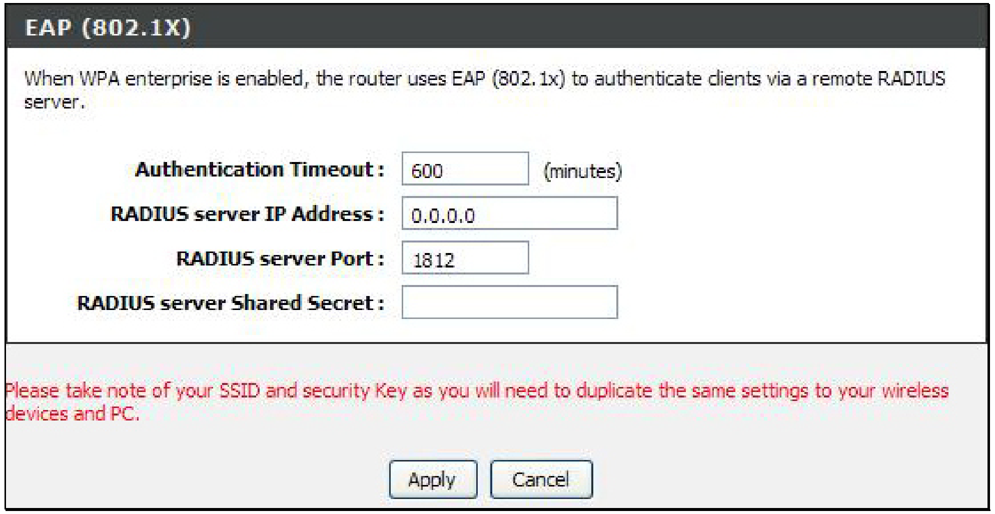
The Pre-Shared Key should be between 8 and 63 ASCII characters, or 64 hexadecimal digits.

Pre-Shared Key :

EAP (802.1X)

When **WPA-Enterprise** was selected in the **WPA Mode** drop-down menu, this section appears for the user to enter a shared key.

1. Enter the available period of time for authentication, Radius server IP address, its port, and shared secret.
2. Click **Apply** to save the settings.



EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout : 600 (minutes)
RADIUS server IP Address : 0.0.0.0
RADIUS server Port : 1812
RADIUS server Shared Secret :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Local Network

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

To access the **Local Network** window, click the **Local Network** button in the **Setup** directory.

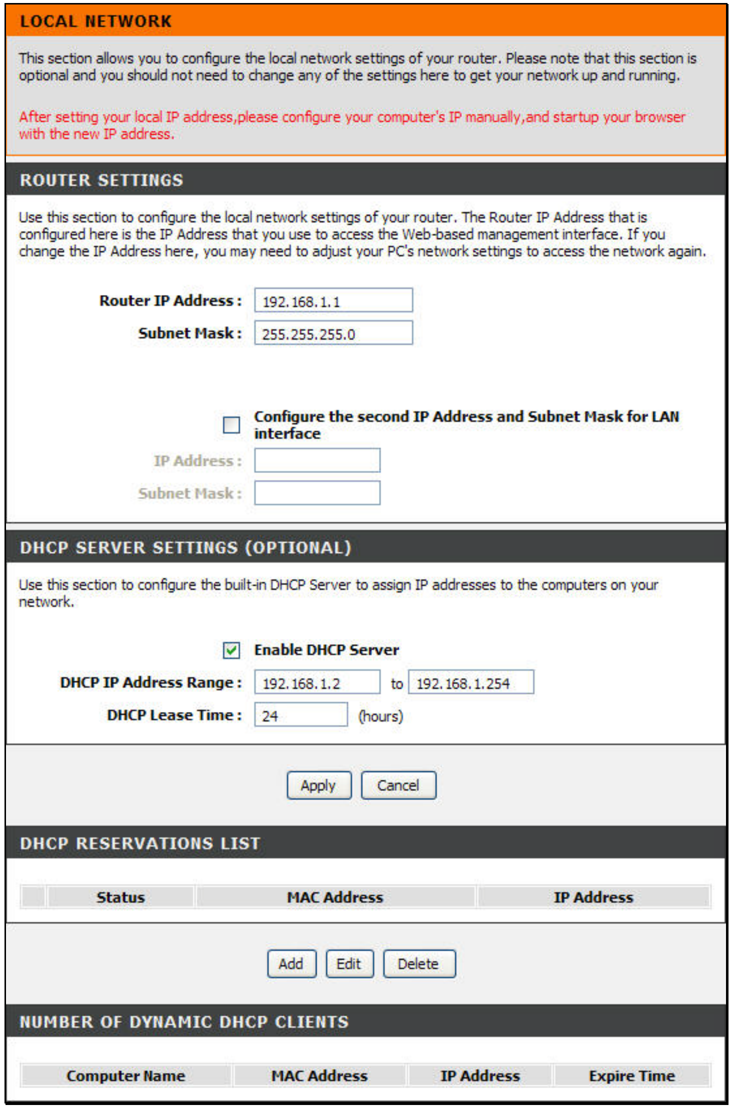
You can configure the local network IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your local network, 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. See the next section for information on DHCP setup.

To change the Router IP Address or Subnet Mask, type in the desired values in the Router Settings section and click the **Apply** button. A message pops up asking if reboot the system. Click **OK** to restart the device. Your web browser should automatically be redirected to the new IP address. You will be asked to login again to the Router's web manager.

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.

There are two options for DHCP service:

- You can use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.



LOCAL NETWORK

This section allows you to configure the local network settings of your router. Please note that this section is optional and you should not need to change any of the settings here to get your network up and running.

After setting your local IP address,please configure your computer's IP manually,and startup your browser with the new IP address.

ROUTER SETTINGS

Use this section to configure the local network settings of your router. The Router IP Address that is configured here is the IP Address that you use to access the Web-based management interface. If you change the IP Address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address : 192.168.1.1
Subnet Mask : 255.255.255.0

□ Configure the second IP Address and Subnet Mask for LAN interface
IP Address :
Subnet Mask :

DHCP SERVER SETTINGS (OPTIONAL)

Use this section to configure the built-in DHCP Server to assign IP addresses to the computers on your network.

☑ Enable DHCP Server
DHCP IP Address Range : 192.168.1.2 to 192.168.1.254
DHCP Lease Time : 24 (hours)

DHCP RESERVATIONS LIST

	Status	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS

Computer Name	MAC Address	IP Address	Expire Time

You may also configure DNS settings when using the Router in DHCP mode (**Advanced** > **DNS Setup**). When “Obtain DNS server address automatically“ is clicked under DNS Server Configuration on the DNS Setup window, the Router will automatically relay DNS settings to properly configured DHCP clients. To manually enter DNS IP addresses, click the “Use the following DNS server addresses“ radio button and type in a Preferred DNS Server and Alternate DNS Server in the fields provided. The manually configured DNS settings will be supplied to clients that are configured to request them from the Router.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured DHCP as you want, click the **Apply** button to commit the new settings. A message pops up asking if reboot the system. Click **OK** to restart the device.

Use the Router for DHCP

To use the built-in DHCP server, click the **Enable DHCP Server** radio button in the DHCP Settings section if it is not already selected. The IP address pool settings can be adjusted. The DHCP IP Address Range starts with the lowest available IP address (default = 192.168.1.2). If you change the IP address of the Router this will change automatically to be 1 more that the IP address of the Router. The DHCP IP Address Range ends with the highest IP address number in the pool. Type in the DHCP Lease Time in the entry field provided. This is the amount of time in hours that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

Disable the DHCP Server

To disable DHCP, Click the **Disable DHCP Server** radio button in the DHCP Settings section and click the **Apply** button. A message pops up asking if reboot the system. Click **OK** to restart the device. Choosing this option will gray out most of the setting options on this window and require that workstations on the local network be configured manually or use another DHCP server to obtain IP settings.

If you configure IP settings manually, make sure to use IP addresses in the subnet of the Router. You will need to use the Router’s IP address as the Default Gateway for the workstation in order to provide Internet access.

Add DHCP Reservation List

To add an entry to the DHCP Reservation List, click the **Add** button in the DHCP Reservation List section, type in an IP Address, either click the **Copy Your PC’s MAC Address** button or manually enter a MAC Address, enter a Computer Name if desired, and click the **Apply** button. To delete an entry from the DHCP Reservations List, tick the entry, and click the **Delete** button. To modify a DHCP Reservations List entry, tick the entry, click the **Edit** button, and then enter the information in the appropriate fields in the Add DHCP Reservation (Optional) section. Click the **Apply** button. A message pops up asking if reboot the system. Click **OK** to restart the device.

Time and Date

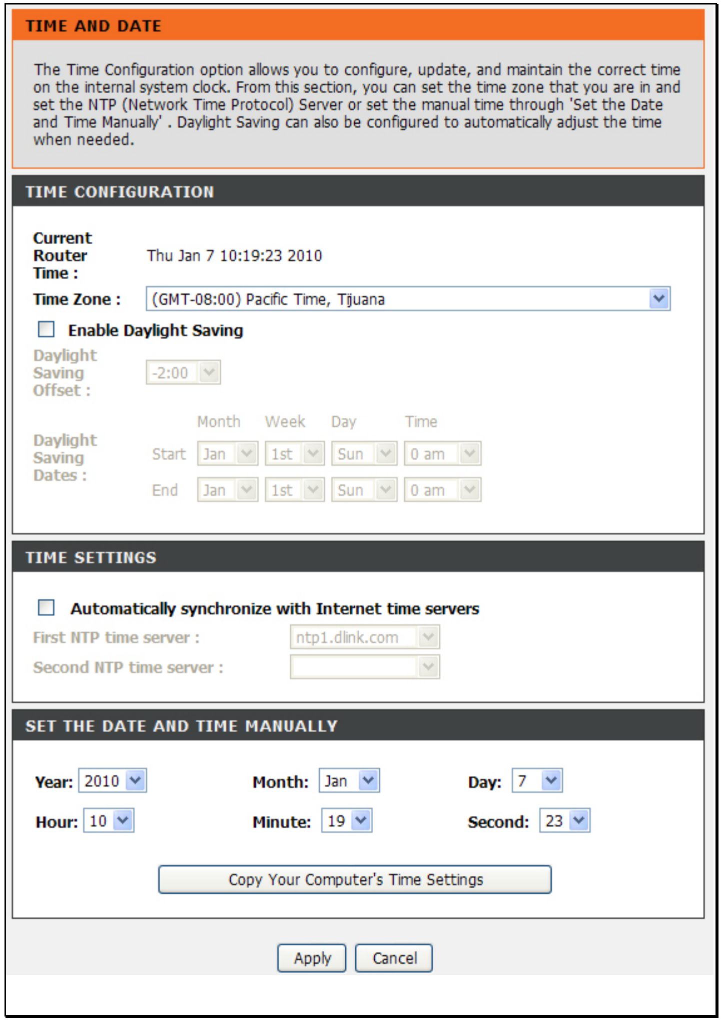
To access the **Time and Date** window, click the **Time and Date** button in the **Setup** directory.

The Router provides NTP and daylight saving to configure, update and maintain the correct time.

To configure system time on the Router, select the **Automatically synchronize with Internet time servers** check box (default) and use the drop-down menu to select the NTP server URL in the First NTP Time Server field. You may also want to choose a Second NTP Time Server using the drop-down menu.

Use the Time Zone pull-down menu to select the correct time zone. For areas that use Daylight Saving seasonal time adjustments, use the menu below Time Zone to configure the settings. To configure Daylight Savings, click on the **Enable Daylight Saving** check box and use the scheduling and offset menus to determine when to apply the adjustment and by how much. Use the **Daylight Savings Offset** pull-down menu to subtract an amount of time appropriate for the time zone. Use the **Daylight Savings Dates** menu to determine when the Daylight Savings period will **Start** and **End**.

When you are finished, click the **Apply** button. Go to **Maintenance** > **System** and click **Reboot** to restart the device and let your changes take effect.



TIME AND DATE

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section, you can set the time zone that you are in and set the NTP (Network Time Protocol) Server or set the manual time through 'Set the Date and Time Manually' . Daylight Saving can also be configured to automatically adjust the time when needed.

TIME CONFIGURATION

Current Router Time : Thu Jan 7 10:19:23 2010

Time Zone : (GMT-08:00) Pacific Time, Tijuana

□ Enable Daylight Saving

Daylight Saving Offset : -2:00

Daylight Saving Dates :

	Month	Week	Day	Time
Start	Jan	1st	Sun	0 am
End	Jan	1st	Sun	0 am

TIME SETTINGS

□ Automatically synchronize with Internet time servers

First NTP time server : ntp1.dlink.com

Second NTP time server :

SET THE DATE AND TIME MANUALLY

Year: 2010 Month: Jan Day: 7

Hour: 10 Minute: 19 Second: 23

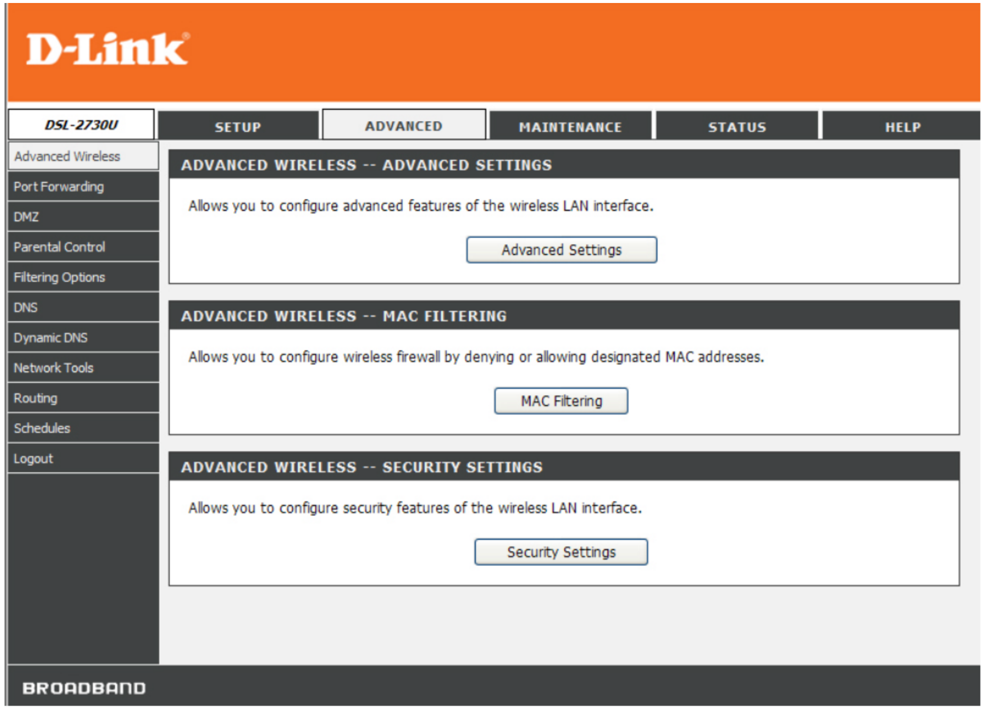
Advanced

This chapter include the more advanced features used for network management and security.

Advanced Wireless

To access Advanced Wireless, click **Advanced Wireless** in the **Advanced** directory.

It has three subcategories: **Advanced Settings**, **MAC Filtering** and **Security Settings**. You can either point to the **Advanced Wireless** on the left window and click one of the submenus, or click one of the buttons in the Wireless Settings window.



ADVANCED WIRELESS -- ADVANCED SETTINGS

Allows you to configure advanced features of the wireless LAN interface.

ADVANCED WIRELESS -- MAC FILTERING

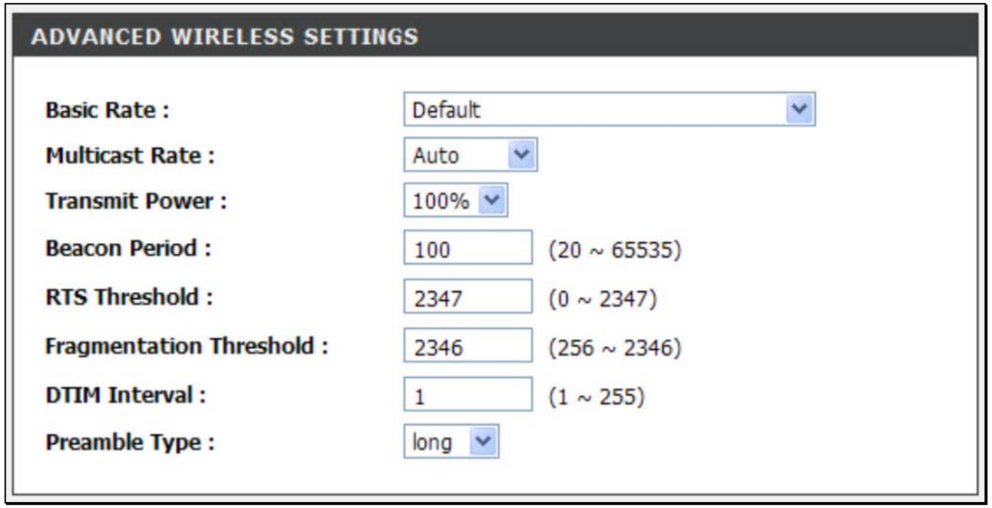
Allows you to configure wireless firewall by denying or allowing designated MAC addresses.

ADVANCED WIRELESS -- SECURITY SETTINGS

Allows you to configure security features of the wireless LAN interface.

Advanced Settings

To access Advanced Settings, point to the **Advanced Wireless** on the left window and click **Advanced Settings** submenu, or click the **Advanced Settings** button in the Wireless Settings window.



ADVANCED WIRELESS SETTINGS

Basic Rate :	Default	
Multicast Rate :	Auto	
Transmit Power :	100%	
Beacon Period :	100	(20 ~ 65535)
RTS Threshold :	2347	(0 ~ 2347)
Fragmentation Threshold :	2346	(256 ~ 2346)
DTIM Interval :	1	(1 ~ 255)
Preamble Type :	long	

In this page, you can configure more advanced settings of 802.11g wireless radio. However, it is recommended to remain as default unless your ISP requests to change it.

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

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

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

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

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

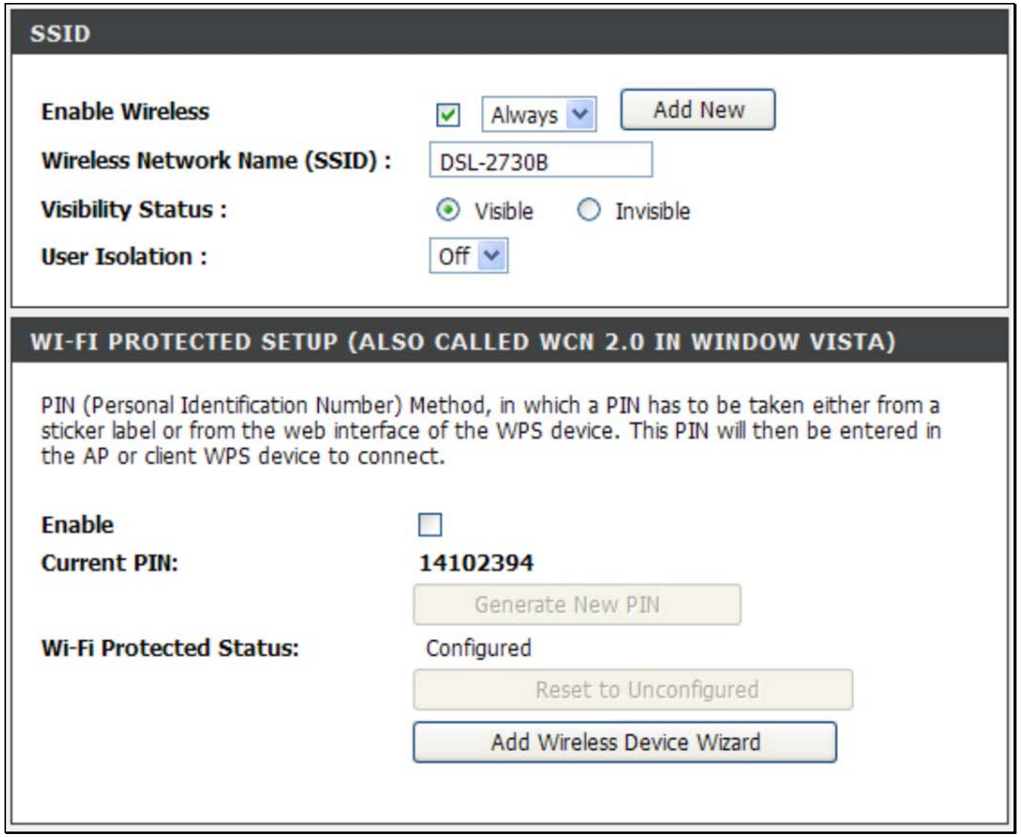
Fragment Threshold: Used to fragment packets which help improve performance in the presence of radio frequency (RF) interference.

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

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

Enable Wireless: Tick the check box to enable the wireless feature of this device. In the drop down menu select the appropriate schedule for when the wireless feature of this device should be enabled or disabled. Click the **Add New** button to go to **Advanced** -> **Schedules** page to configure more schedules.
Wireless Network Name (SSID): Enter a wireless network name (SSID).
Visibility Status: Click the radio buttons to make the wireless network visible or invisible.
User Isolation: Use the drop-down menu to enable (*On*) or disable (*Off*) wireless user isolation.

Enable: Tick to enable Wi-Fi Protection (WPS, also known as WCN).
Current PIN: The current PIN for WPS is displayed.
Generate New PIN: Click this button to generate a new WPS PIN.
Wi-Fi Protected Status: The current status of WPS is displayed.
Reset to Unconfigured: Click this button to disable WPS.
Add Wireless Device Wizard: Click this button to add a new wireless device using WPS.



SSID

Enable Wireless ☑ Always

Wireless Network Name (SSID) : DSL-2730B

Visibility Status : ● Visible ○ Invisible

User Isolation : Off

WI-FI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOW VISTA)

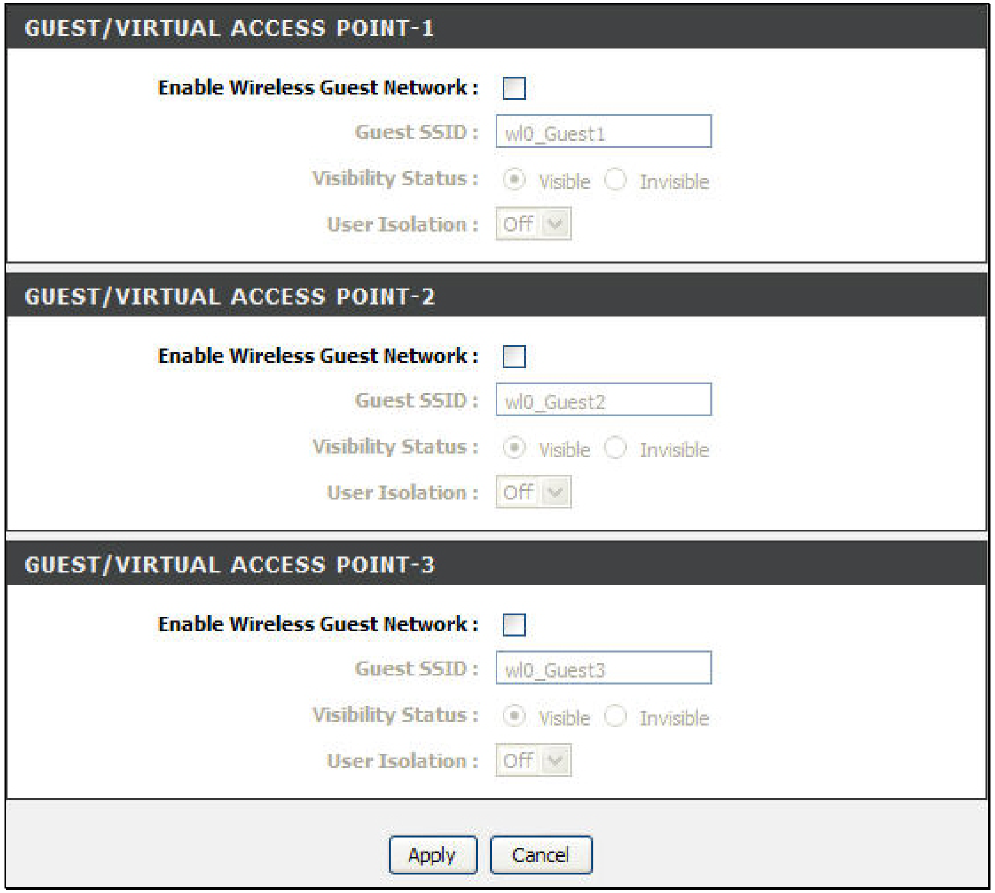
PIN (Personal Identification Number) Method, in which a PIN has to be taken either from a sticker label or from the web interface of the WPS device. This PIN will then be entered in the AP or client WPS device to connect.

Enable □

Current PIN: 14102394

Wi-Fi Protected Status: Configured

Enable Wireless Guest network: Tick the check box to enable a wireless guest network.
Guest SSID: Enter an additional SSID for the wireless guest network.
Visibility Status: Click the radio buttons to make the wireless guest network visible or invisible.
User Isolation: Use the drop-down menu to enable (*On*) or disable (*Off*) wireless user isolation.



GUEST/VIRTUAL ACCESS POINT-1

Enable Wireless Guest Network : □
Guest SSID : wl0_Guest1
Visibility Status : ● Visible ○ Invisible
User Isolation : Off

GUEST/VIRTUAL ACCESS POINT-2

Enable Wireless Guest Network : □
Guest SSID : wl0_Guest2
Visibility Status : ● Visible ○ Invisible
User Isolation : Off

GUEST/VIRTUAL ACCESS POINT-3

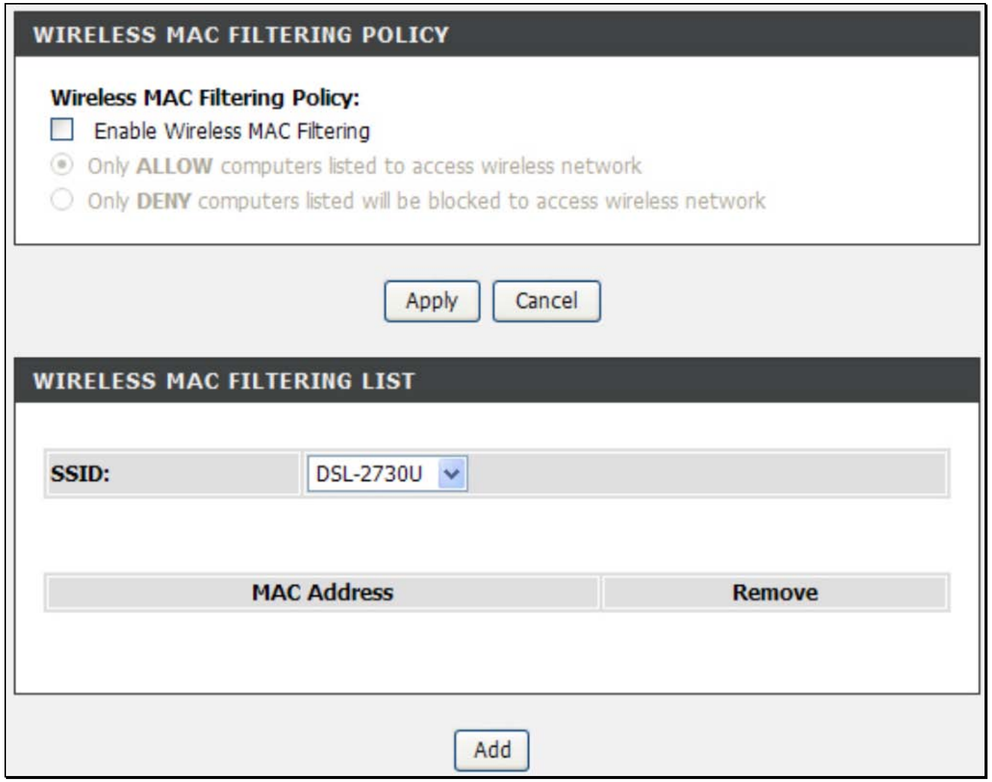
Enable Wireless Guest Network : □
Guest SSID : wl0_Guest3
Visibility Status : ● Visible ○ Invisible
User Isolation : Off

MAC Filtering

To access MAC Filtering, point to the **Advanced Wireless** on the left window and click **MAC Filtering** submenu, or click the **MAC Filtering** button in the Wireless Settings window.

This page can help you to allow or deny certain MAC addresses to pass through or block out.

Click **Add** at the bottom of the window to enter MAC address. Click **Apply** at the bottom of the page to add the MAC address to the wireless MAC filtering list.
Select **Enable Wireless MAC Filter** and click the **Only ALLOW computers listed to access wireless network** or **Only DENY computers listed to access wireless network** of the filtering policy. Click **Apply** to save the settings. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let the new settings take effect.



WIRELESS MAC FILTERING POLICY

Wireless MAC Filtering Policy:

□ Enable Wireless MAC Filtering

● Only **ALLOW** computers listed to access wireless network

○ Only **DENY** computers listed will be blocked to access wireless network

WIRELESS MAC FILTERING LIST

SSID: DSL-2730U

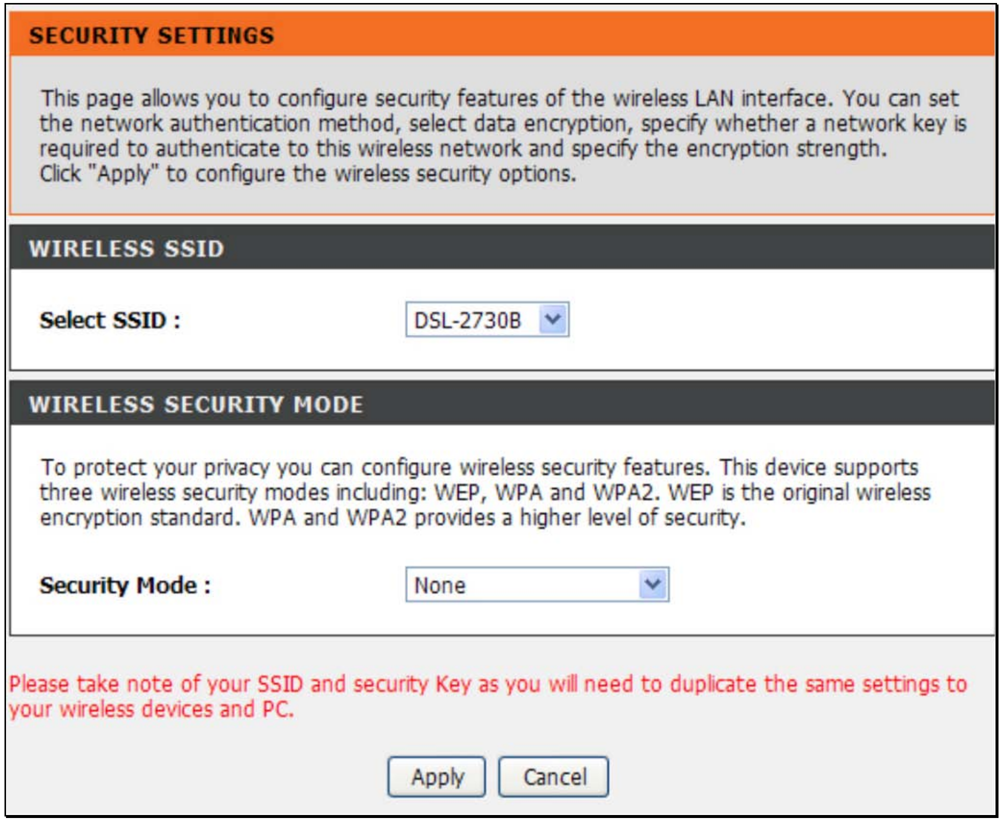
MAC Address	Remove

Security Settings

To access wireless Security Settings, point to the **Advanced Wireless** on the left window and click **Security Settings** submenu, or click the **Security Settings** button in the Wireless Settings window.

1. Select an SSID from the **Select SSID** drop-down menu.
2. Select the security type for the SSID from the **Security Mode** drop-down menu.

The detail configurations for various security types are described below.



SECURITY SETTINGS

This page allows you to configure security features of the wireless LAN interface. You can set the network authentication method, select data encryption, specify whether a network key is required to authenticate to this wireless network and specify the encryption strength.
Click "Apply" to configure the wireless security options.

WIRELESS SSID

Select SSID : DSL-2730B

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA and WPA2. WEP is the original wireless encryption standard. WPA and WPA2 provides a higher level of security.

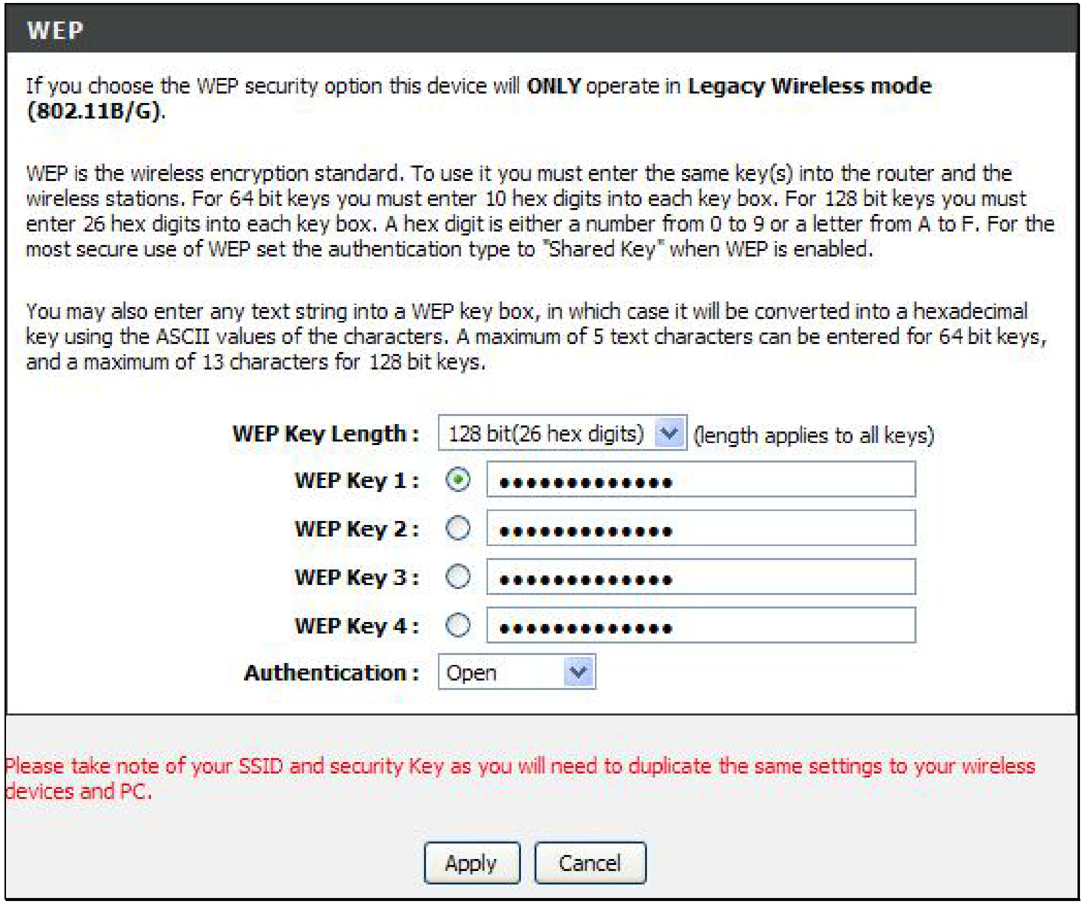
Security Mode : None

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

WEP

When selecting **WEP** from the **Security Mode** drop-down menu, the WEP section appears.

1. Select the WEP key length between 64 bit or 128 bit from the drop-down list.
2. Enter the WEP key(s) in the **WEP Key 1** to **WEP Key 4** fields.
3. Select the authentication as Open or Shared from the **Authentication** drop-down menu.
4. Click **Apply** to save the settings.



WEP

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**.

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WEP Key Length : 128 bit(26 hex digits) (length applies to all keys)

WEP Key 1 : ● •••••••••••••

WEP Key 2 : ○ •••••••••••••

WEP Key 3 : ○ •••••••••••••

WEP Key 4 : ○ •••••••••••••

Authentication : Open

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

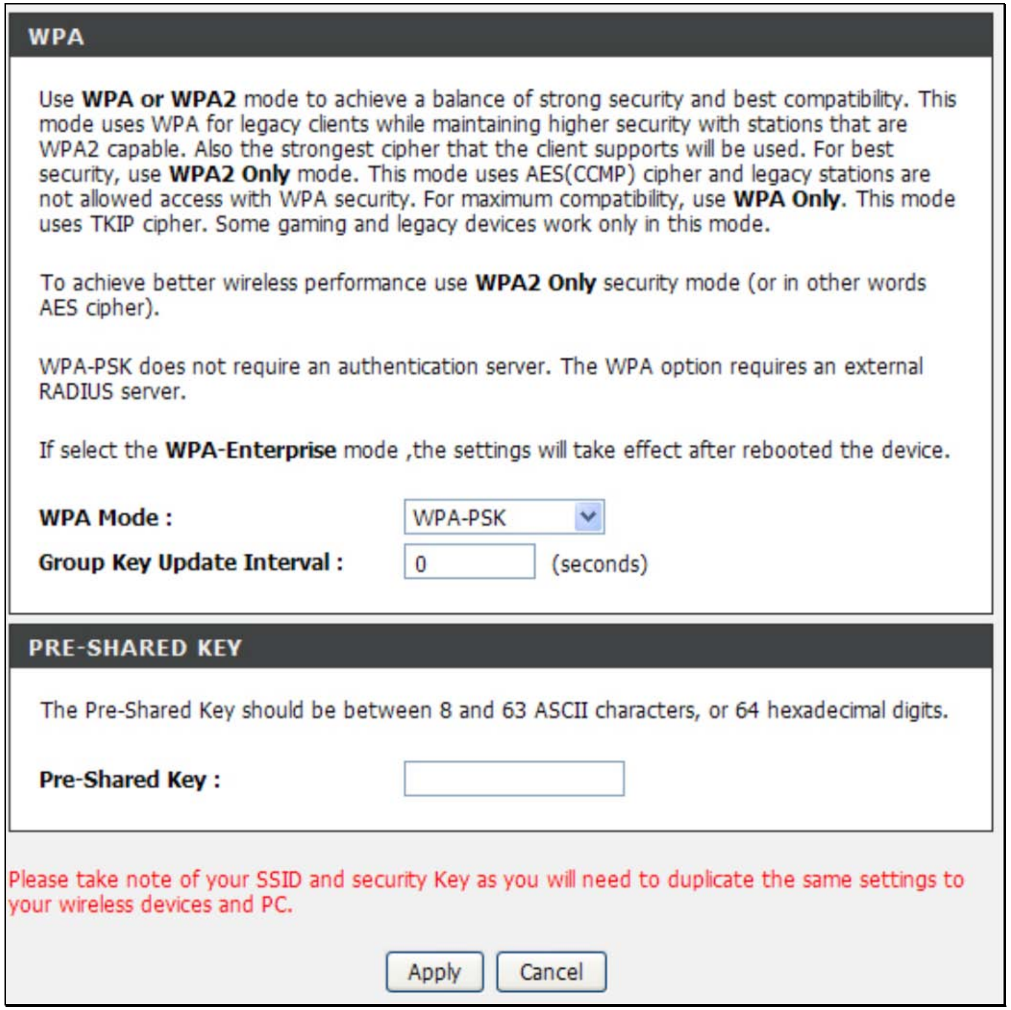
Auto, WPA or WPA2

When selecting **Auto**, **WPA2 Only** or **WPA Only** from the **Security Mode** drop-down menu, the WPA section appears.

1. In the **WPA Mode** drop-down menu, select between **WPA-PSK** and **WPA-Enterprise**. Different sections appear based on the selection.
2. Enter a period of time for key updated in the **Group Key Update Interval** field.

Pre-shared Key

When **WPA-PSK** was selected in the **WPA Mode** drop-down menu, this section appears for the user to enter a shared key.



WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA-PSK does not require an authentication server. The WPA option requires an external RADIUS server.

If select the **WPA-Enterprise** mode ,the settings will take effect after rebooted the device.

WPA Mode : WPA-PSK

Group Key Update Interval : 0 (seconds)

PRE-SHARED KEY

The Pre-Shared Key should be between 8 and 63 ASCII characters, or 64 hexadecimal digits.

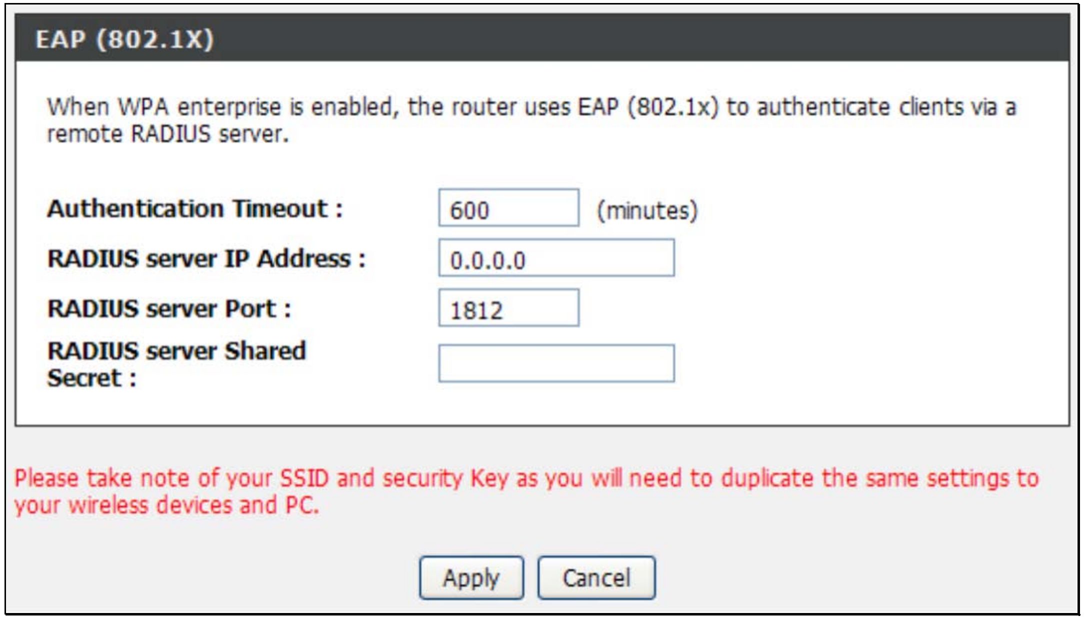
Pre-Shared Key :

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

EAP (802.1X)

When **WPA-Enterprise** was selected in the **WPA Mode** drop-down menu, this section appears for the user to enter a shared key.

1. Enter the available period of time for authentication, Radius server IP address, its port, and shared secret.
2. Click **Apply** to save the settings.



EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

Authentication Timeout :	600 (minutes)
RADIUS server IP Address :	0.0.0.0
RADIUS server Port :	1812
RADIUS server Shared Secret :	

Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

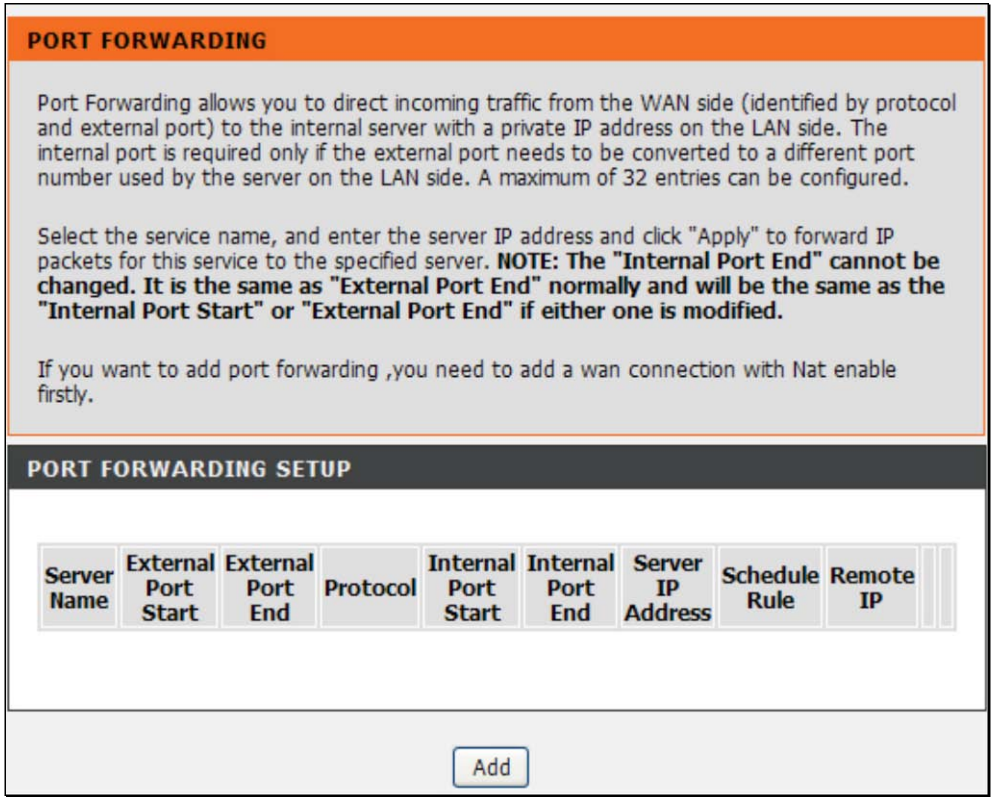
Port Forwarding

To access the **Port Forwarding** window, click the **Port Forwarding** button in the **Advanced** directory.

Multiple connections are required by some applications, such as Internet games, video conferencing, Internet telephony, and others. These applications have difficulties working through NAT (Network Address Translation). This section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network.

1. Click the **Add** button to add a new Internet connection.
2. Once there is any Internet connection in the table, the **Edit** and **Remove** buttons appears. To edit an entry in the table, tick the **Edit** check box of the entry and click the **Edit** button. To remove an entry, tick the Remove check box of the entry and click the **Remove** button.

Click the **Add** button to see the Port Forwarding Setup section.



PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 32 entries can be configured.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port End" if either one is modified.**

If you want to add port forwarding ,you need to add a wan connection with Nat enable firstly.

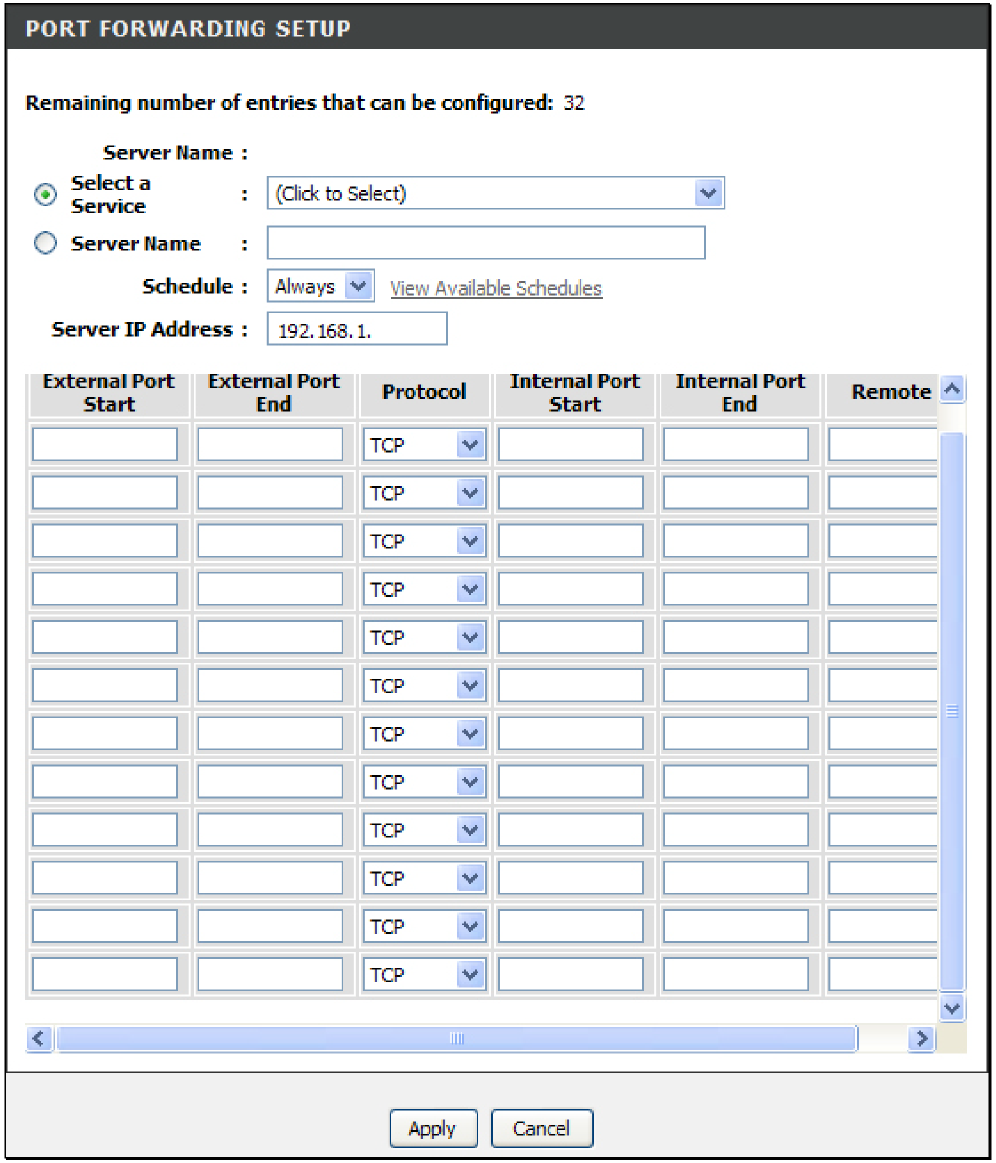
PORT FORWARDING SETUP

Server Name	External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Server IP Address	Schedule Rule	Remote IP		

Select a Service: Select a pre-defined port forwarding rule.
Server Name: **Enter a custom rule name.**
Schedule: **Select a schedule when this rule will be active. Rules in the list can be configured in** Advanced **->** Schedules**. Click the** View Available Schedules **button to go to the page.**
Server IP Address: **Enter the internal server IP address.**
External Ports: **Enter the start and end external ports used.**
Protocol: **Select a protocol applicable to this rule.**
Internal Ports: **Enter the start and end internal ports used.**
Remote IP: **Enter a remote IP address used.**

The **Internal Port End** can’t be changed. It is the same as **External Port End** normally and will be the same as the **Internal Port Start** or **External Port End** if either one is modified.

Click the **Apply** button to accept the changes.
Click the **Cancel** button to discard the changes.



PORT FORWARDING SETUP

Remaining number of entries that can be configured: 32

Server Name :
● Select a Service : (Click to Select)
○ Server Name :
Schedule : Always View Available Schedules
Server IP Address : 192.168.1.

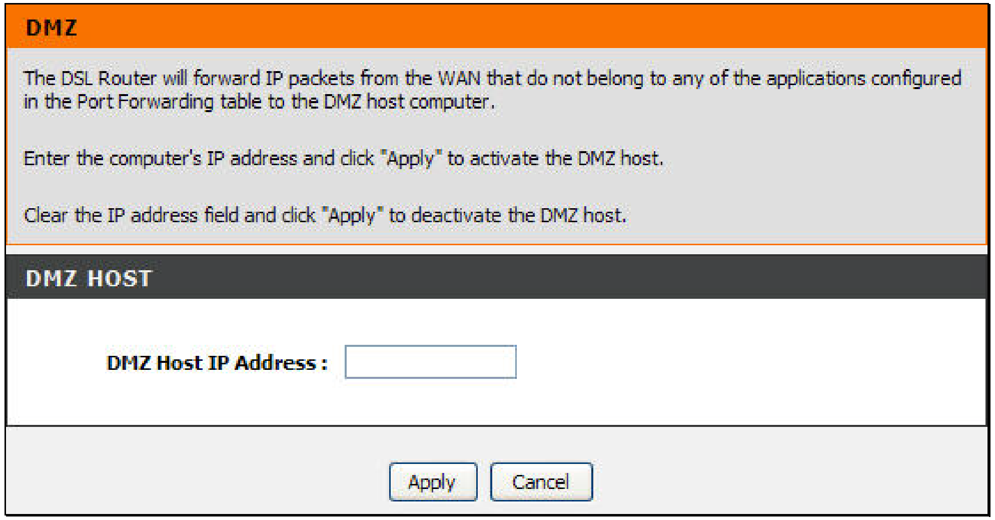
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remote
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

DMZ

To access the DMZ (Demilitarized Zone) window, click the **DMZ** button in the **Advanced** directory.

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, and click the **Apply** button.



DMZ

The DSL Router will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer.

Enter the computer's IP address and click "Apply" to activate the DMZ host.

Clear the IP address field and click "Apply" to deactivate the DMZ host.

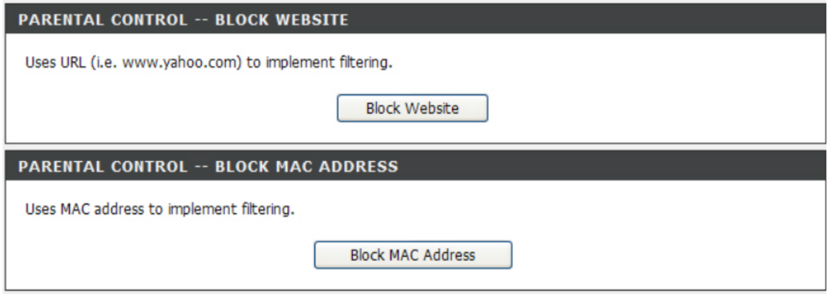
DMZ HOST

DMZ Host IP Address :

Parental Control

To access the **Parent Control** menu, click the **Parent Control** link in the **Advanced** directory.

It has one subcategories: **Block MAC Address**. You can either point to the **Parental Control** on the left window and click the submenu, or click the buttons in the Parental Control window.



PARENTAL CONTROL -- BLOCK WEBSITE

Uses URL (i.e. www.yahoo.com) to implement filtering.

PARENTAL CONTROL -- BLOCK MAC ADDRESS

Uses MAC address to implement filtering.

Block Website

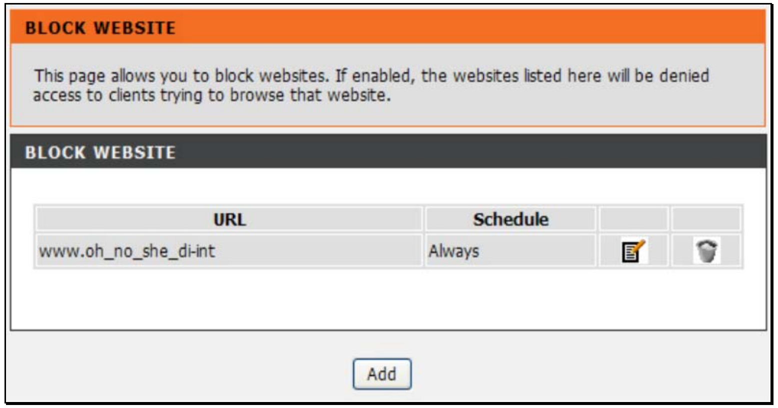
To access the Block Website menu, click the **Block Website** button in the Parental Control menu.

Use this window to deny access to specified Internet website using the URL (Universal Resource Lookup), that is, the named web address.

Click **Add** to see the **Block Website** configuration menu appear below.

To prevent access of websites using the URL for the site, enter the URL in the space provided (following the http://) and click on the **Apply** button.

The **Schedule** and **Manual Schedule** radio buttons are used to create a time schedule for enforcing the policy. For Schedule, select a rule in the drop down list. Rules in the list can be configured in **Advanced** -> **Schedules**. Click the **View Available Schedules** link to go to the page. For Manual Schedule entry, configure as follows. Use the boxes to select the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox, and then click the **Block Website** button. Click the **Apply** button to see the configured URL blocking entry is displayed in the Block Website. To remove a **Blocked URL** entry in the table, select the entry, and click the **Delete** icon. To modify a table entry, select the entry, click the **Edit** icon, make the desired changes, and then click the **Apply** button.

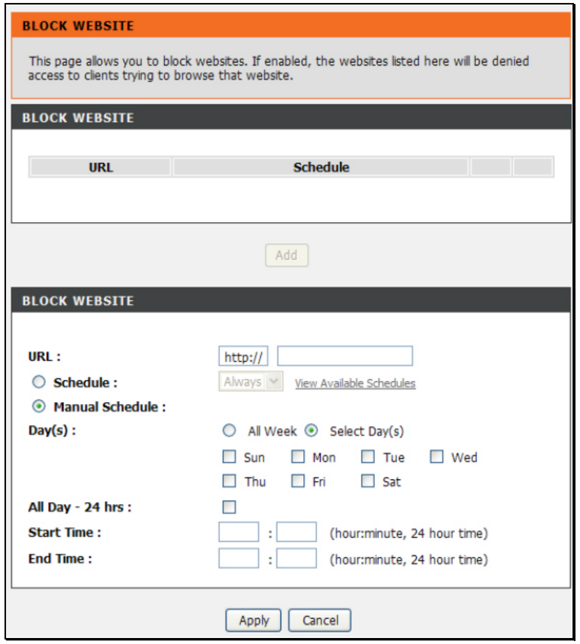


BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

URL	Schedule		
www.oh_no_she_di-int	Always	📝	🗑



BLOCK WEBSITE

This page allows you to block websites. If enabled, the websites listed here will be denied access to clients trying to browse that website.

BLOCK WEBSITE

URL	Schedule		

BLOCK WEBSITE

URL : http://

○ Schedule : Always View Available Schedules

● Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

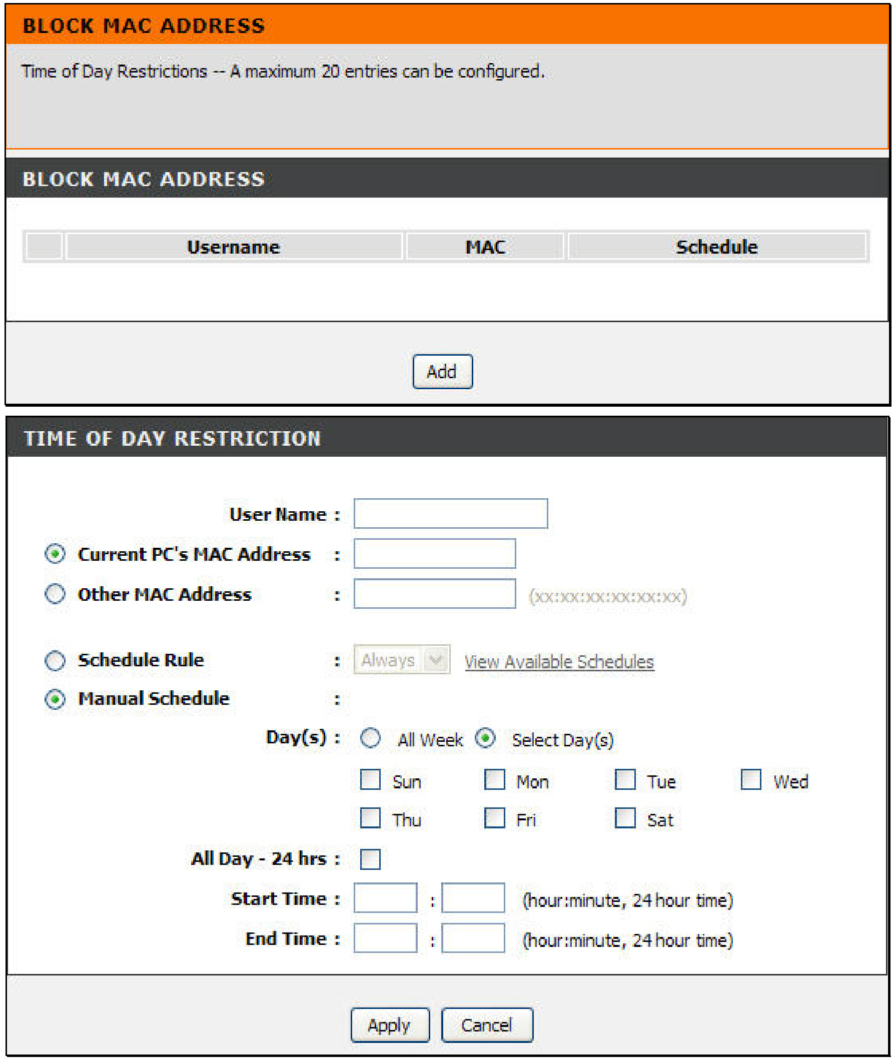
Block MAC Address

To access Block MAC Address, point to the **Parental Control** on the left window and click **Block MAC Address** submenu, or click the **Block MAC Address** button in the Parental Control window.

Use this window to deny access to specified MAC address.

Click **Add** to see the **Add Block MAC Address** section. MAC address is a specially formatted text string (xx:xx:xx:xx:xx:xx) that uniquely identification of a device. This section will allow users to block devices with certain MAC addresses on the LAN.

To configure for MAC address blocking, enter the username into the **Username** field, click **Current PC's Mac Address** to have MAC address of current computer, or click **Other MAC Address** and enter a MAC address manually. Click **Schedule Rule** or **Manual Schedule** radio button to configure the time schedule. For Schedule Rule, select a rule in the drop down list. Rules in the list can be configured in **Advanced** -> **Schedules**. Click the **View Available Schedules** button to go to the page. For manual Schedule configure as follows. Use the radio buttons to click the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox, and then click the **Block Website** button. Click the **Apply** button to see the configured URL blocking entry is displayed in the Block Website. To remove a Blocked URL entry in the table, select the entry, and click the **Delete** button. To modify a table entry, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



BLOCK MAC ADDRESS

Time of Day Restrictions -- A maximum 20 entries can be configured.

BLOCK MAC ADDRESS

	Username	MAC	Schedule

TIME OF DAY RESTRICTION

User Name :

● Current PC's MAC Address :

○ Other MAC Address : (xx:xx:xx:xx:xx:xx)

○ Schedule Rule : Always View Available Schedules

● Manual Schedule :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed

□ Thu □ Fri □ Sat

All Day - 24 hrs : □

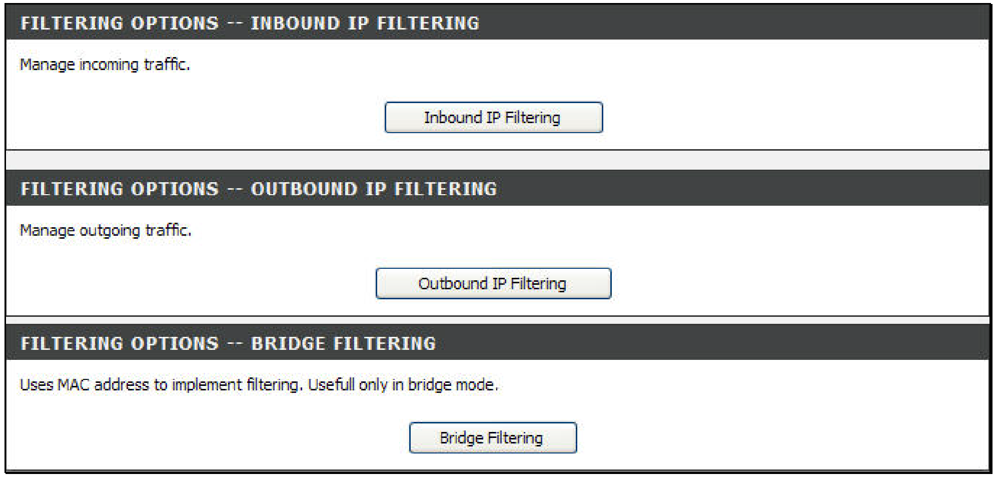
Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Filtering Options

To access the Filtering Options window, click the **Filtering Options** button in the **Advanced** directory.

It has three subcategories: **Inbound Filtering**, **Outbound Filtering** and **Bridge Filtering**. You can either point to the **Filtering Options** on the left window and click one of the submenus, or click one of the buttons in the Filtering Options window.



FILTERING OPTIONS -- INBOUND IP FILTERING

Manage incoming traffic.

FILTERING OPTIONS -- OUTBOUND IP FILTERING

Manage outgoing traffic.

FILTERING OPTIONS -- BRIDGE FILTERING

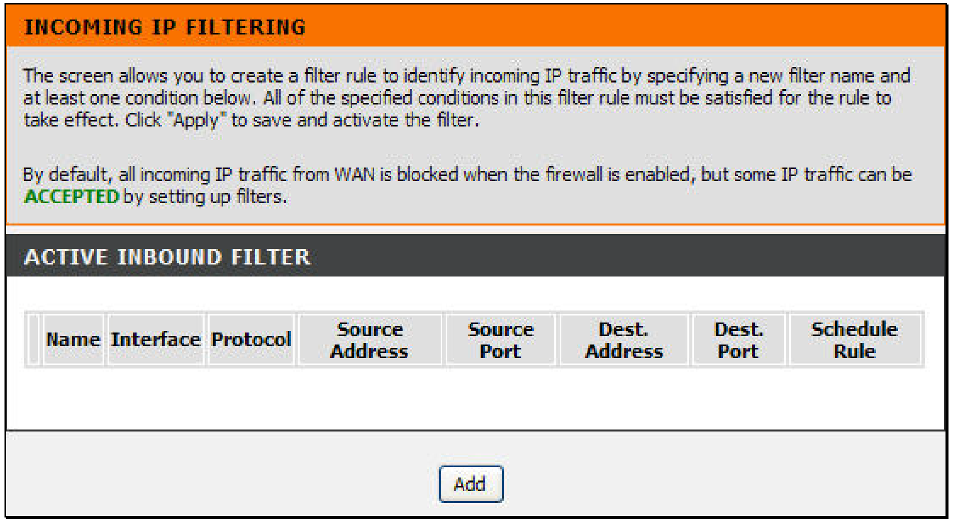
Uses MAC address to implement filtering. Usefull only in bridge mode.

Inbound Filtering

To access Inbound Filtering, point to the **Filtering Options** on the left window and click **Inbound Filtering** submenu, or click the **Inbound** button in the Filtering Options window.

The Inbound Filter allows you to create a filter rule to allow incoming IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. By default, all incoming IP traffic from the Internet is blocked when the firewall is enabled.

Click the **Add** button to see the Incoming IP Filtering section, enter the information in the section. Explanations of parameters are described below. Click the **Apply** button to add the entry in the Active Inbound IP Filtering table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



INCOMING IP FILTERING

The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

By default, all incoming IP traffic from WAN is blocked when the firewall is enabled, but some IP traffic can be ACCEPTED by setting up filters.

ACTIVE INBOUND FILTER

Name	Interface	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

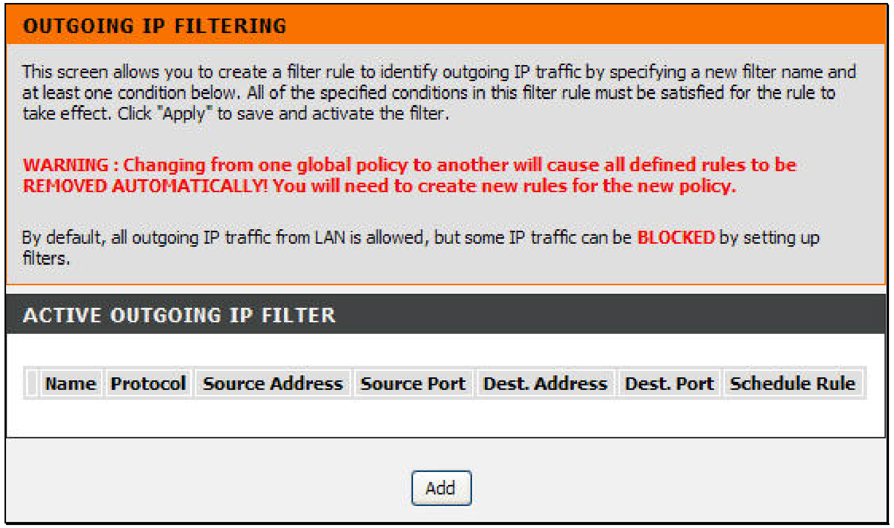
Filters Parameter	Description	
Filter Name	Enter a name for the new filter.	
Protocol	Select the transport protocol (TCP and UDP, TCP, UDP, ICMP or Any) that will be used for the filter rule.	
Select/Destination IP Type	Select the source/destination IP type. Available choices are: Any, Single IP, Network IP and IP Range.	
	Source/Destination IP Address& Source Subnet Mask	This is the IP address and their associated subnets for which you are creating the filter rule.
	Start and End Source/Destination IP Address	Enter the start and end IP address for the range of IP addresses which you are creating the filter rule.
Source/Destination Port Type	The Source/Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Inbound Filter rule. The available selections are Any, Single Port and Port Range.	
Source/Destination Port	Enter a port or range of ports for the rule.	

Outbound Filtering

To access Outbound Filtering, point to the **Filtering Options** on the left window and click **Outbound Filtering** submenu, or click the **Outbound** button in the Filtering Options window.

The Outbound Filter allows you to create a filter rule to block outgoing IP traffic by specifying a filter name and at least one condition on this window. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Filters are used to allow or deny LAN or WAN users from accessing the Internet or your internal network.

Click the **Add** button to see the Outgoing IP Filtering section, enter the information in the section. Explanations of parameters are described below. Click the **Apply** button to add the entry in the Active Outbound IP Filtering table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



OUTGOING IP FILTERING

This screen allows you to create a filter rule to identify outgoing IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.

ACTIVE OUTGOING IP FILTER

Name	Protocol	Source Address	Source Port	Dest. Address	Dest. Port	Schedule Rule

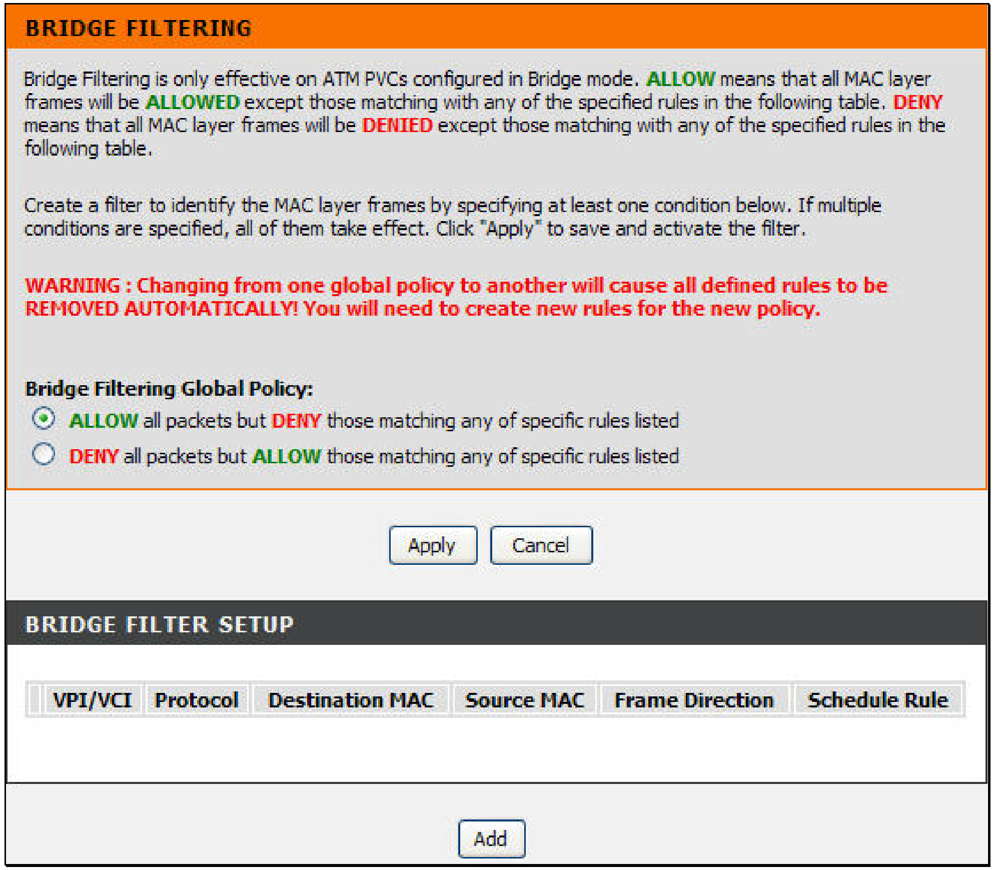
Filters Parameter	Description	
Filter Name	Enter a name for the new filter.	
Protocol	Select the transport protocol (TCP and UDP, TCP, UDP, ICMP or Any) that will be used for the filter rule.	
Select/Destination IP Type	Select the source/destination IP type. Available choices are: Any, Single IP, Network IP and IP Range.	
	Source/Destination IP Address& Source Subnet Mask	This is the IP address and their associated subnets for which you are creating the filter rule.
	Start and End Source/Destination IP Address	Enter the start and end IP address for the range of IP addresses which you are creating the filter rule.
Source/Destination Port Type	The Source/Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Inbound Filter rule. The available selections are Any, Single Port and Port Range.	
Source/Destination Port	Enter a port or range of ports for the rule.	

Bridge Filtering

To access Bridge Filtering, point to the **Filtering Options** on the left window and click **Bridge Filtering** submenu, or click the **Bridge** button in the Filtering Options window.

Bridge filters are used to block or allow various types of packets through the WAN/LAN 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. You can set up filter rules and disable the entire set of rules without loosing the rules that have been configured.

Select Bridge Filtering Global Policy: **ALLOW all packets but DENY those matching any of the specific rules listed** or **DENY all packets but ALLOW those matching any of the specific rules listed** for the rules that configured below. Click the **Add** button to see the Add Bridge Filter section. Select a protocol (PPPoE, IPv4, IPv6, Apple Talk, IPX or IGMP) in the **Protocol Type** list, type in a Source MAC, a Destination MAC or both in the entry fields. Select a direction (LAN=>WAN, WAN=>LAN, or LAN<=>WAN) in the **Frame Direction** list. Click the **Apply** button to add the entry in the Active Bridge Filters table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



BRIDGE FILTERING

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode. ALLOW means that all MAC layer frames will be ALLOWED except those matching with any of the specified rules in the following table. DENY means that all MAC layer frames will be DENIED except those matching with any of the specified rules in the following table.

Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them take effect. Click "Apply" to save and activate the filter.

WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

Bridge Filtering Global Policy:

● ALLOW all packets but DENY those matching any of specific rules listed

○ DENY all packets but ALLOW those matching any of specific rules listed

BRIDGE FILTER SETUP

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction	Schedule Rule

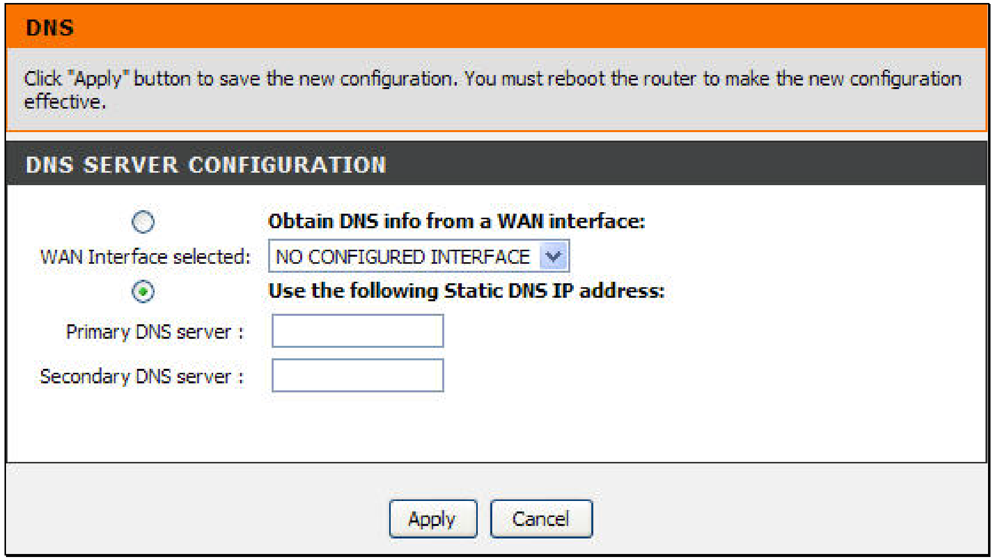
DNS Setup

To access the DNS window, click the **DNS** button in the **Advanced** directory.

Domain Name Server (DNS) is a server that translates URL/Domain Names to the corresponding IP address. Since URL/Domain Names are alphabetical, they are easier to remember. But the Internet is based on IP address.

If obtaining DNS from one of the configured WAN interface, select the **Obtain DNS info from a WAN interface** option, and select a WAN interface from the **WAN Interface selected** drop-down menu.

If you have DNS IP addresses provided by your ISP, click the **Use the following DNS server addresses** radio button and enter these IP addresses in the available entry fields for the Preferred DNS Server and the Alternative DNS Server. When you have configured the DNS settings as desired, click the **Apply** button.



DNS

Click "Apply" button to save the new configuration. You must reboot the router to make the new configuration effective.

DNS SERVER CONFIGURATION

○ Obtain DNS info from a WAN interface:

WAN Interface selected: NO CONFIGURED INTERFACE

● Use the following Static DNS IP address:

Primary DNS server :

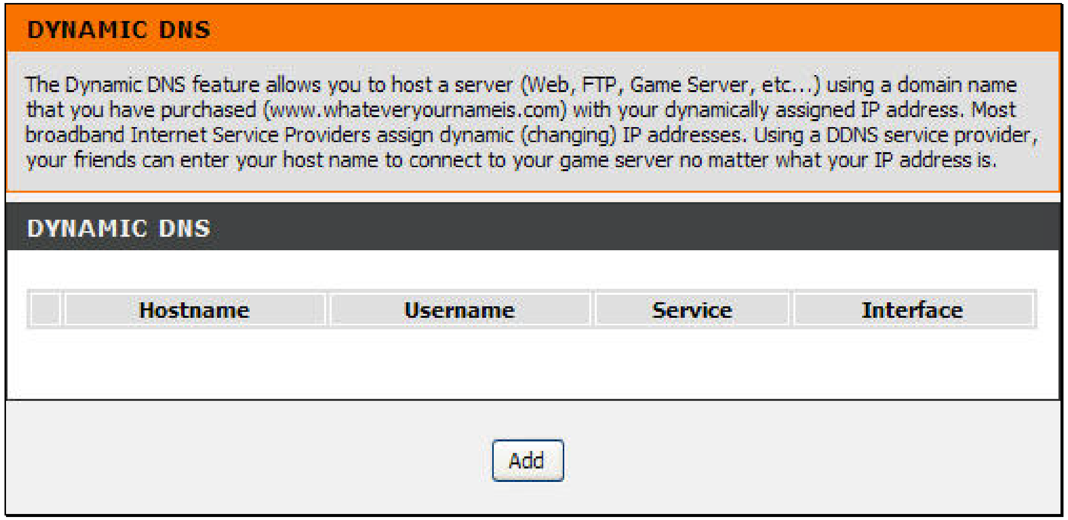
Secondary DNS server :

Dynamic DNS Setup

To access the Dynamic DNS window, click the **Dynamic DNS** button in the **Advanced** directory.

The Router supports Dynamic DNS (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, 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. Dynamic DNS requires that an account be setup with one of the supported dynamic DNS providers.

Click **Add** to see the Add Dynamic DNS section. Enter the required dynamic DNS information, click the **Apply** button to see the entry in the Dynamic DNS List table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



DYNAMIC DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is.

DYNAMIC DNS

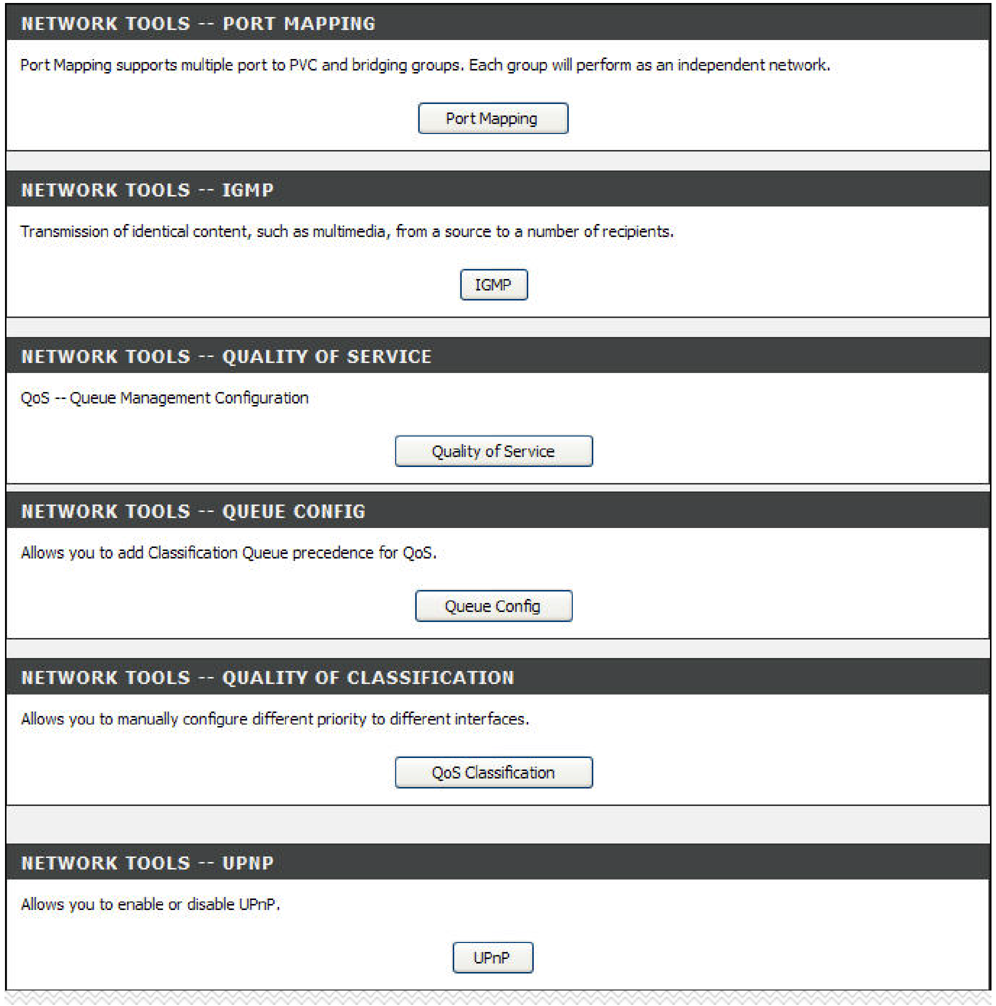
	Hostname	Username	Service	Interface

Note: Dynamic DNS requires that an account be setup with one of the supported dynamic DNS servers prior to engaging it on the Router. This function will not work without an accepted account with a dynamic DNS server.

Network Tools

To access the Network Tools window, click the **Network Tools** button in the **Advanced** directory.

There are six subcategories in Network Tools: **Port Mapping**, **IGMP**, **Quality of Service**, **Queue Config**, **Quality of Classification**, **UPnP**, **ADSL**, **SNMP**, and **TR-069**. You can either point to the **Network Tools** on the left window and click one of the submenus, or click one of the buttons in the Network Tools window.



NETWORK TOOLS -- PORT MAPPING

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network.

NETWORK TOOLS -- IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

NETWORK TOOLS -- QUALITY OF SERVICE

QoS -- Queue Management Configuration

NETWORK TOOLS -- QUEUE CONFIG

Allows you to add Classification Queue precedence for QoS.

NETWORK TOOLS -- QUALITY OF CLASSIFICATION

Allows you to manually configure different priority to different interfaces.

NETWORK TOOLS -- UPNP

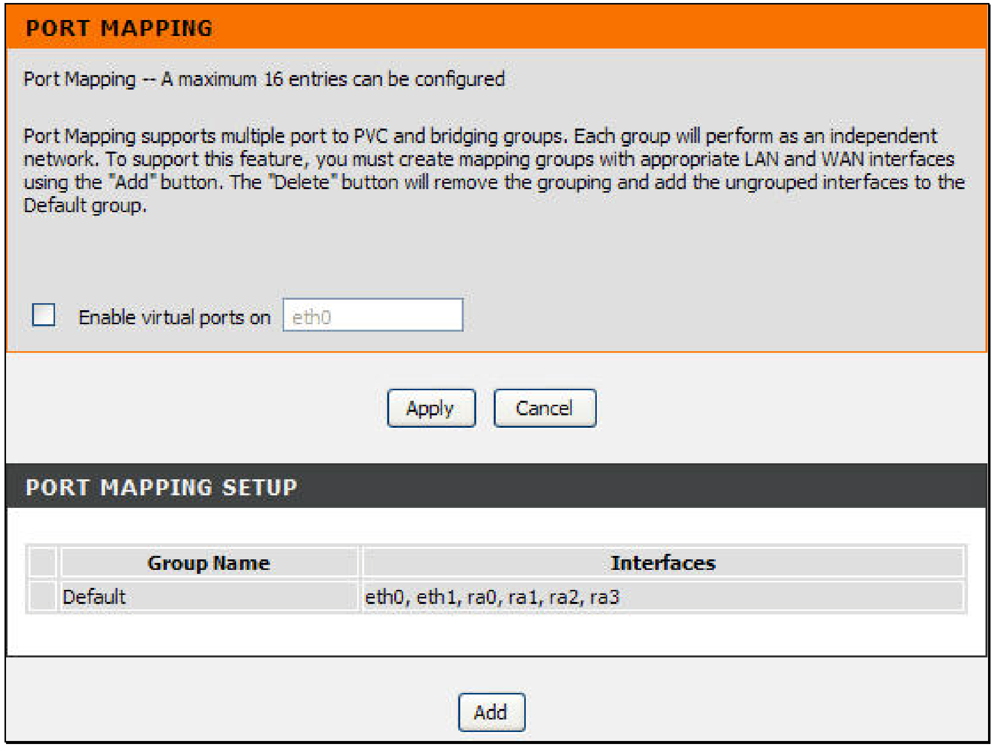
Allows you to enable or disable UPnP.

Port Mapping

To access Port Mapping, point to the **Network Tools** on the left window and click **Port Mapping** submenu, or click the **Port Mapping** button in the Network Tools window.

Port Mapping supports single or multiple (LAN) ports to be formed as a group and mapped to PVC (which is associated w/ a VLAN). As a result, each group of LAN ports will perform as an independent (logical) network (like a broadcast domain) among whom traffic broadcast would be prevented. This feature is useful while you would like to form multiple independent (logical) networks for multimedia applications at home. For instance, you can map PVC1 to port 1~3 to create a network (broadcast domain) for PCs for Internet, and map PVC2 to port 4 to create another network (broadcast domain) for IPTV service (devices). By using this feature (w/ multiple PVCs), data traffic and IPTV traffic would not affect each other.

Click the **Add** button to see the Port Mapping Configuration section. Enter a group name and select interfaces in the Available Interface field. Click **<-** to add to the Grouped Interfaced field. To remove an interface form the Grouped, select the interface in the Grouped Interfaced field and click **->**. Click the **Apply** button to see the entry in Port Mapping Setup table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



PORT MAPPING

Port Mapping -- A maximum 16 entries can be configured

Port Mapping supports multiple port 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 using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

□ Enable virtual ports on: eth0

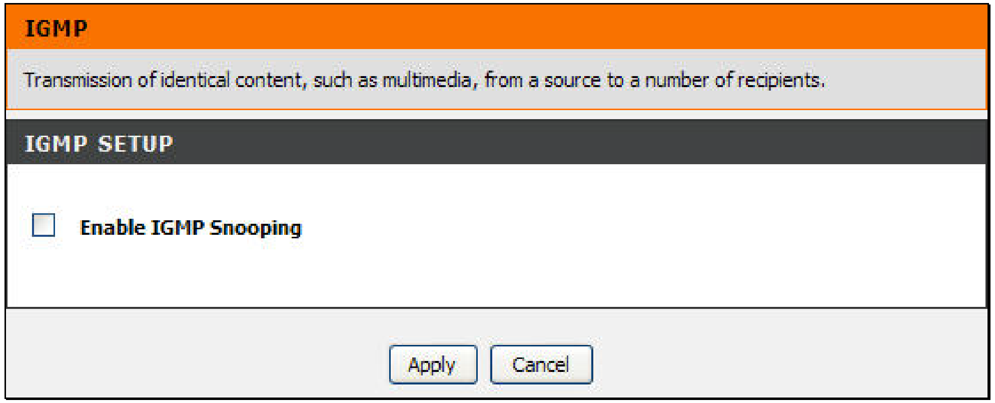
PORT MAPPING SETUP

	Group Name	Interfaces
	Default	eth0, eth1, ra0, ra1, ra2, ra3

IGMP

To access IGMP, point to the **Network Tools** on the left window and click **IGMP** submenu, or click the **IGMP** button in the Network Tools window. IGMP (Internet Group Management Protocol) page is for identical content transmission.

When the **Enable IGMP Proxy/Snooping** check box is selected, Multicast packets are allowed to pass in both directions on the WAN interface. Most users will want to leave this on.



IGMP

Transmission of identical content, such as multimedia, from a source to a number of recipients.

IGMP SETUP

□ Enable IGMP Snooping

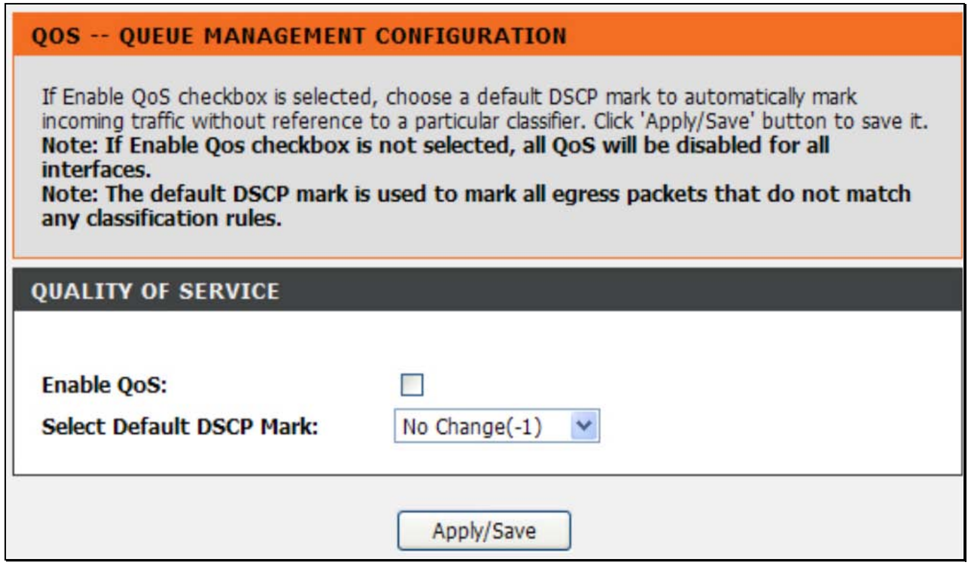
Quality of Service

To access Quality of Service, point to the **Network Tools** on the left window and click **Quality of Service** submenu, or click the **Quality of Service** button in the Network Tools window.

Quality of Service is a feature that allows you to allocate or guarantee the throughput or speed of Internet for certain computers.

Tick the **Enable QoS** check box, and Select Default DSCP mark from the list to enable the function.

When you are finished, click **Apply/Save**. Go to **Maintenance** -> **System**, and click the **Reboot** button to let your new settings take effect.



QOS -- QUEUE MANAGEMENT CONFIGURATION

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.
Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.
Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

QUALITY OF SERVICE

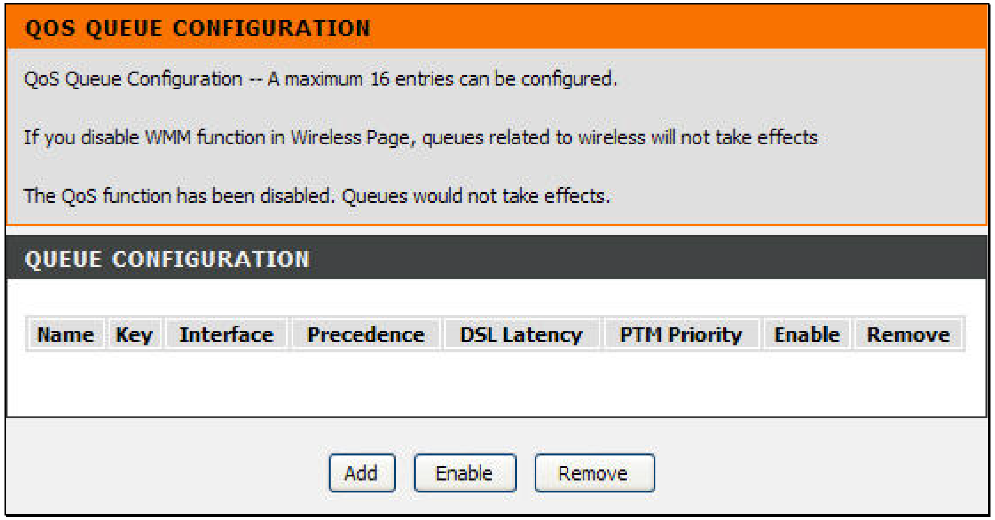
Enable QoS: □
Select Default DSCP Mark: No Change(-1)

Queue Configuration

To access Queue Configuration, point to the **Network Tools** on the left window and click **Queue Config** submenu, or click the **Queue Config** button in the Network Tools window.

This page allows you to create Assigned Classification Queue settings used in QoS. This served as the priority setting for QoS.

Click the **Add** button to see the Add Queue Config section. Enter the name of the entry, select the *Enable* option, an interface and the priority in the **Enable**, **Interface** and **Precedence** drop-down list. Click the **Apply/Save** button to see the entry in the Queue Configuration table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



QOS QUEUE CONFIGURATION

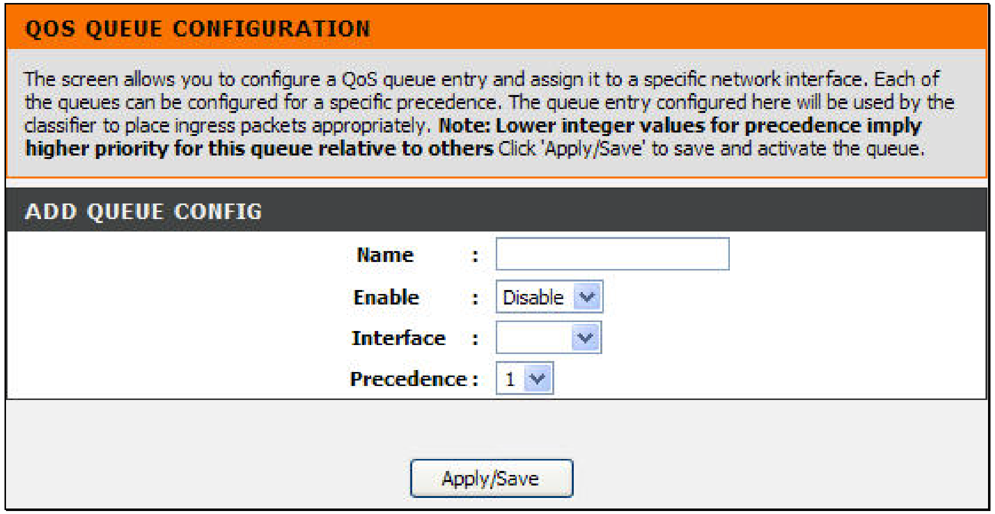
QoS Queue Configuration -- A maximum 16 entries can be configured.

If you disable WMM function in Wireless Page, queues related to wireless will not take effects

The QoS function has been disabled. Queues would not take effects.

QUEUE CONFIGURATION

Name	Key	Interface	Precedence	DSL Latency	PTM Priority	Enable	Remove



QOS QUEUE CONFIGURATION

The screen allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue entry configured here will be used by the classifier to place ingress packets appropriately. **Note: Lower integer values for precedence imply higher priority for this queue relative to others** Click 'Apply/Save' to save and activate the queue.

ADD QUEUE CONFIG

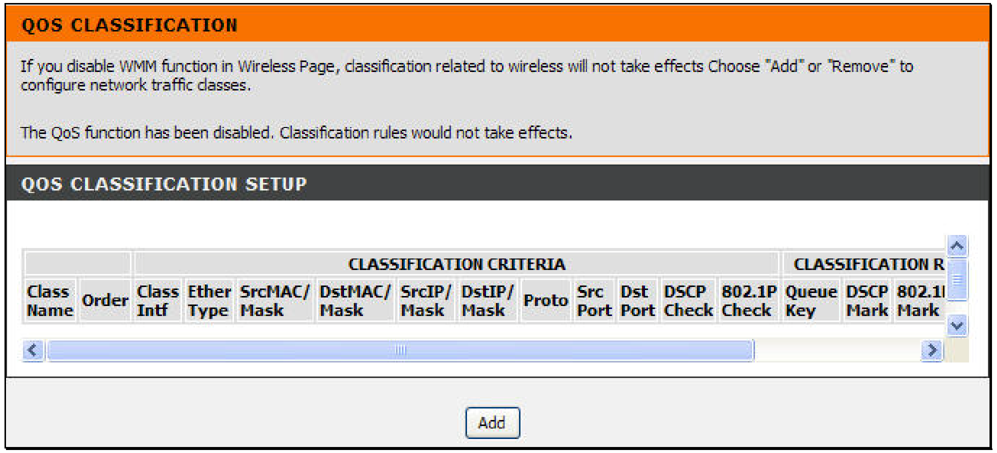
Name	:	
Enable	:	Disable
Interface	:	
Precedence	:	1

QoS Classification

To access QoS Classification, point to the **Network Tools** on the left window and click **QoS Classification** submenu, or click the **QoS Classification** button in the Network Tools window.

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface, and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect.

Click the **Add** button to see the following sections: Network Traffic Class Rule, Specify Classification Criteria and Specify Classification Results.



QOS CLASSIFICATION

If you disable WMM function in Wireless Page, classification related to wireless will not take effects Choose "Add" or "Remove" to configure network traffic classes.

The QoS function has been disabled. Classification rules would not take effects.

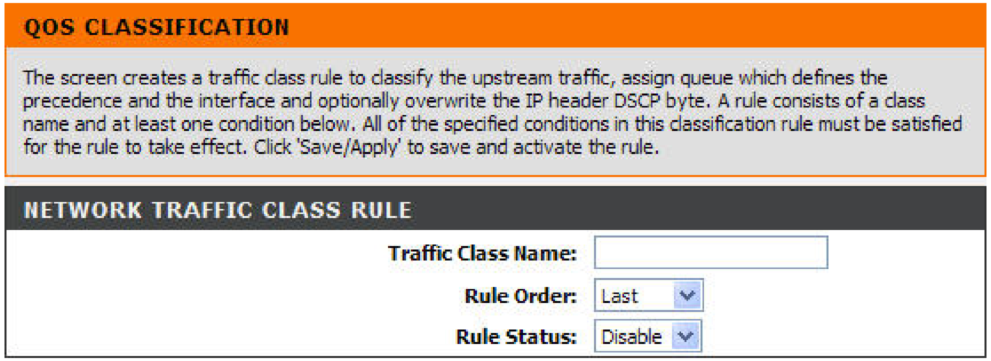
QOS CLASSIFICATION SETUP

		CLASSIFICATION CRITERIA											CLASSIFICATION R		
Class Name	Order	Class Intf	Ether Type	SrcMAC/ Mask	DstMAC/ Mask	SrcIP/ Mask	DstIP/ Mask	Proto	Src Port	Dst Port	DSCP Check	802.1P Check	Queue Key	DSCP Mark	802.1 Mark

Traffic Class Name: Enter the traffic class rule name.

Rule Order: Select the rule order.

Rule Status: Select the status of the rule.



QOS CLASSIFICATION

The screen creates a traffic class rule to classify the upstream traffic, assign queue which defines the precedence and the interface and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition below. All of the specified conditions in this classification rule must be satisfied for the rule to take effect. Click 'Save/Apply' to save and activate the rule.

NETWORK TRAFFIC CLASS RULE

Traffic Class Name:	
Rule Order:	Last
Rule Status:	Disable

Class Interface: Select the class interface used for this rule.

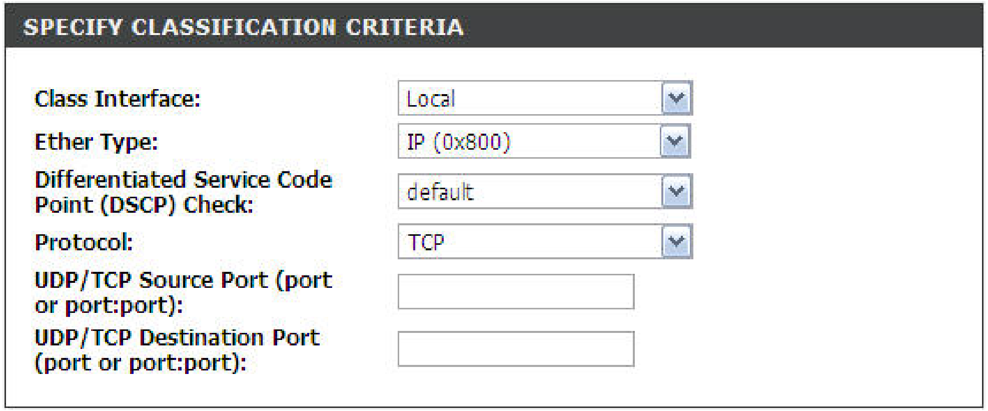
Ether Type: Select the Ethernet type used for this rule.

DSCP Check: Select the differentiated service code point check.

Protocol: Select the protocol used for this rule.

UDP/TCP Source Port: Enter the UDP/TCP source port value.

UDP/TCP Dest. Port: Enter the UDP/TCP destination port value.



SPECIFY CLASSIFICATION CRITERIA

Class Interface:	Local
Ether Type:	IP (0x800)
Differentiated Service Code Point (DSCP) Check:	default
Protocol:	TCP
UDP/TCP Source Port (port or port:port):	
UDP/TCP Destination Port (port or port:port):	

Class Interface: Select the class interface used for this rule.

Ether Type: Select the Ethernet type used for this rule.

Source/Destination MAC Address: Enter the source/destination MAC address used for this rule.

Source/Destination MAC Mask: Enter the source/destination MAC mask value used for this rule.

Source IP Address: Select **Source IP Address**, **Vendor Class ID (DHCP Option 60)**, or **User Class ID (DHCP Option 77)** from the drop-down menu, and enter the information in the field.

Source Subnet Mask: Enter the source subnet mask value used for this rule.

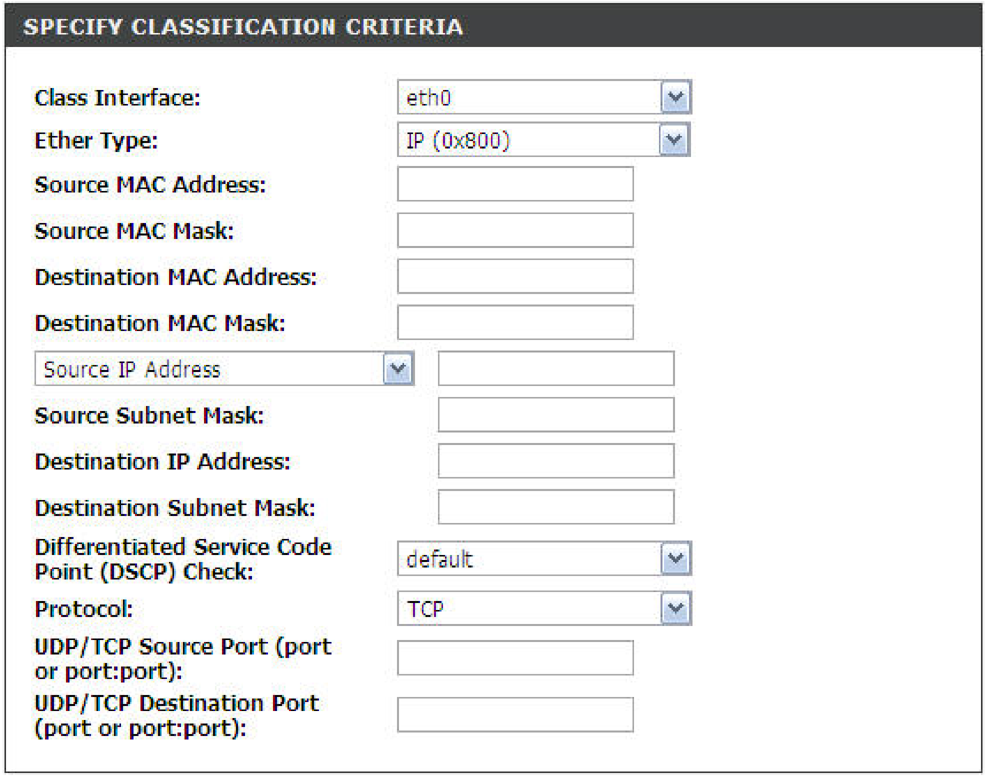
Destination IP Address: Enter the destination IP address used for this rule.

Destination Subnet Mask: Enter the destination subnet mask value used for this rule.

Differentiated Service Code Point (DSCP) Check: Select the differentiated service code point check.

Protocol: Select the protocol used for this rule.

UDP/TCP Source/Destination Port: Enter the UDP/TCP source/destination port value.



SPECIFY CLASSIFICATION CRITERIA

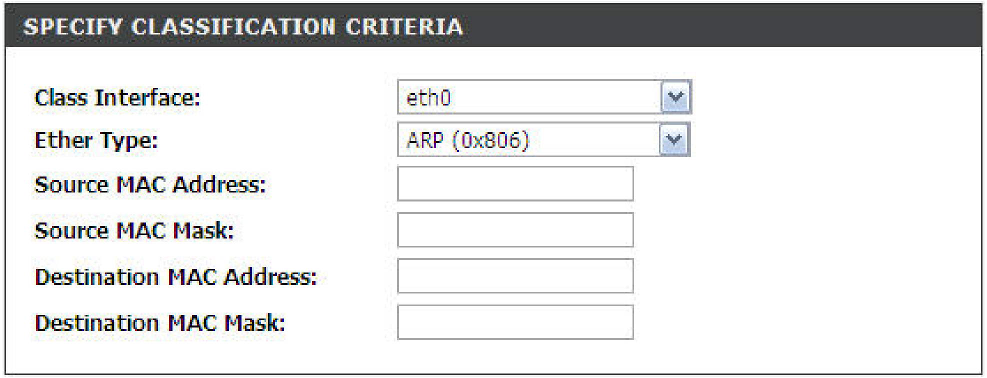
Class Interface:	eth0
Ether Type:	IP (0x800)
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	
Source IP Address	
Source Subnet Mask:	
Destination IP Address:	
Destination Subnet Mask:	
Differentiated Service Code Point (DSCP) Check:	default
Protocol:	TCP
UDP/TCP Source Port (port or port:port):	
UDP/TCP Destination Port (port or port:port):	

Class Interface: Select the class interface used for this rule.

Ether Type: Select the Ethernet type used for this rule.

Source/Destination MAC Address: Enter the source/destination MAC address used for this rule.

Source/Destination MAC Mask: Enter the source/destination MAC mask value used for this rule.



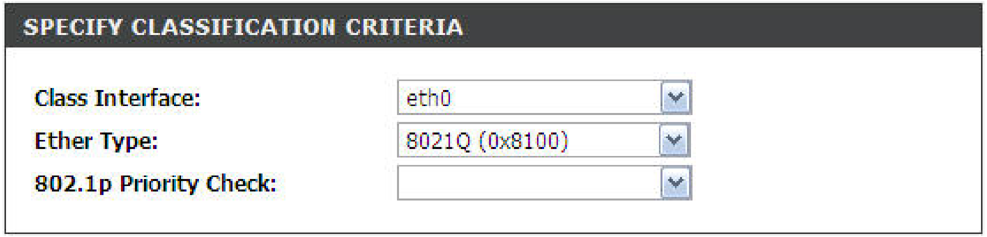
SPECIFY CLASSIFICATION CRITERIA

Class Interface:	eth0
Ether Type:	ARP (0x806)
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

Class Interface: Select the class interface used for this rule.

Ether Type: Select the Ethernet type used for this rule.

802.1p Priority Check: Select the 802.1p priority check used for this rule.

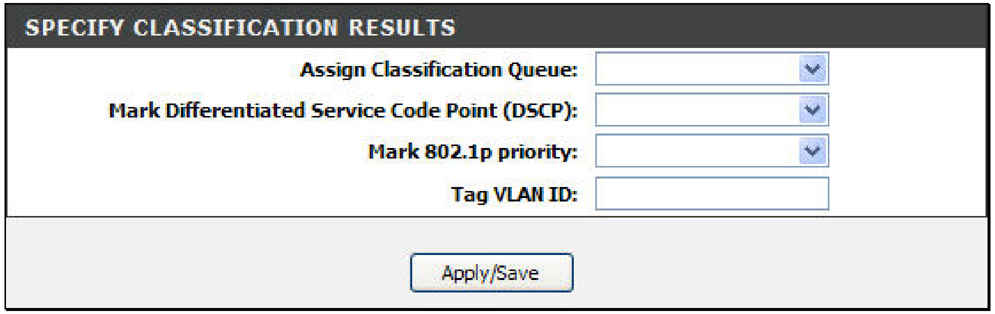


SPECIFY CLASSIFICATION CRITERIA

Class Interface:	eth0
Ether Type:	8021Q (0x8100)
802.1p Priority Check:	

Assign Classification Queue: Select the classification queue used for this rule.
Mark Differentiated Service Code Point (DSCP): Select the differentiated service code point mark.
Mark 802.1p Priority: Select the 802.1 priority mark.
Tag VLAN ID: Enter the 802.1Q VLAN ID tag used for this rule.

Click the **Apply/Save** button to see the entry appears in the QoS Classification Setup table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



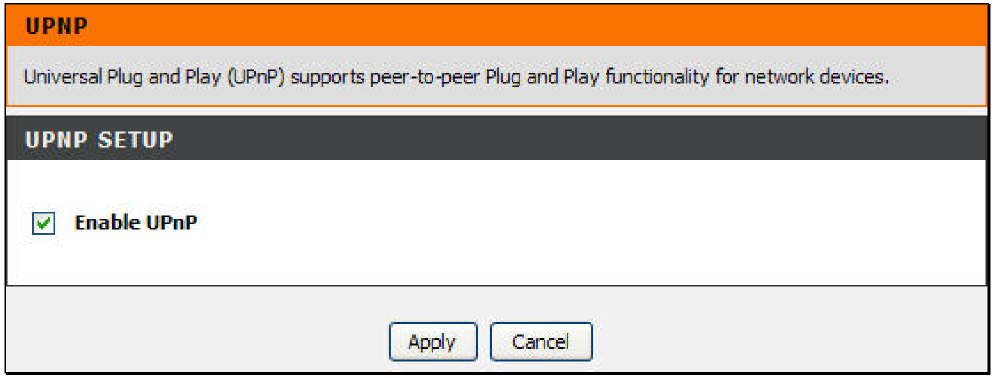
SPECIFY CLASSIFICATION RESULTS

Assign Classification Queue:	
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	
Tag VLAN ID:	

UPnP

To access UPnP, point to the **Network Tools** on the left window and click **UPnP** submenu, or click the **UPnP** button in the Network Tools window.

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. 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. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network. UPnP is a protocol supported by diverse networking media including Ethernet, Firewire, phone line, and power line networking.



UPNP

Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.

UPNP SETUP

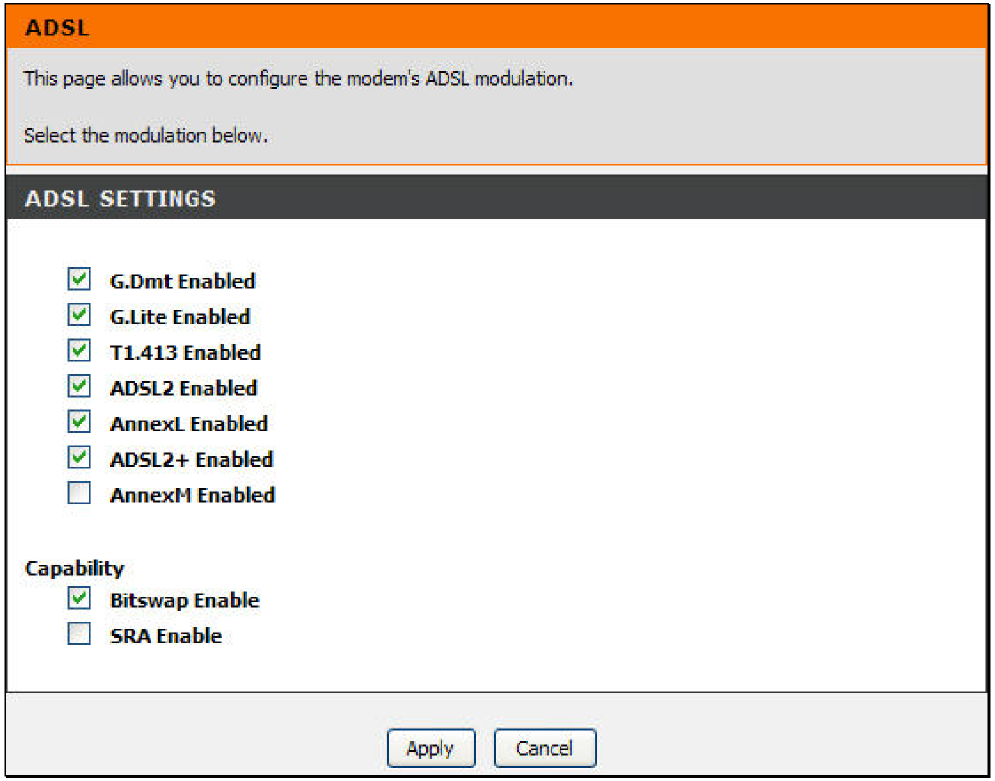
☑ Enable UPnP

To enable UPnP for any available connection, tick the **Enable UPnP** check box, and click the **Apply** button.

DSL

To access ADSL, point to the **Network Tools** on the left window and click **DSL** submenu, or click the **DSL** button in the Network Tools window.

This page contains a modulation and capability selections to be specified by your ISP. Consult with your ISP to select the correct settings for each. Click **Apply** if you to save the settings.



ADSL

This page allows you to configure the modem's ADSL modulation.

Select the modulation below.

ADSL SETTINGS

☑ G.Dmt Enabled
☑ G.Lite Enabled
☑ T1.413 Enabled
☑ ADSL2 Enabled
☑ AnnexL Enabled
☑ ADSL2+ Enabled
□ AnnexM Enabled

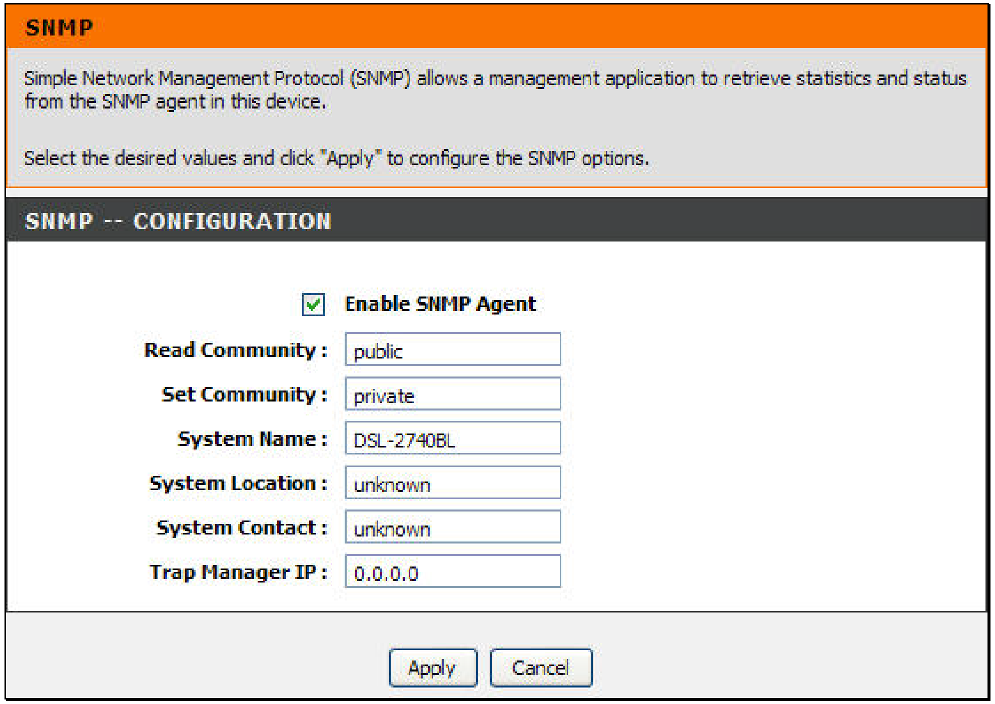
Capability
☑ Bitswap Enable
□ SRA Enable

SNMP

To access SNMP, point to the **Network Tools** on the left window and click **SNMP** submenu, or click the **SNMP** button in the Network Tools window.

Simple Network Management Protocol is a standard for internetwork and intranetwork management.

Tick the **Enable SNMP Agent** check box and configure the parameters for SNMP on this window and then click the **Apply** button.



SNMP

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device.

Select the desired values and click "Apply" to configure the SNMP options.

SNMP -- CONFIGURATION

☑ Enable SNMP Agent

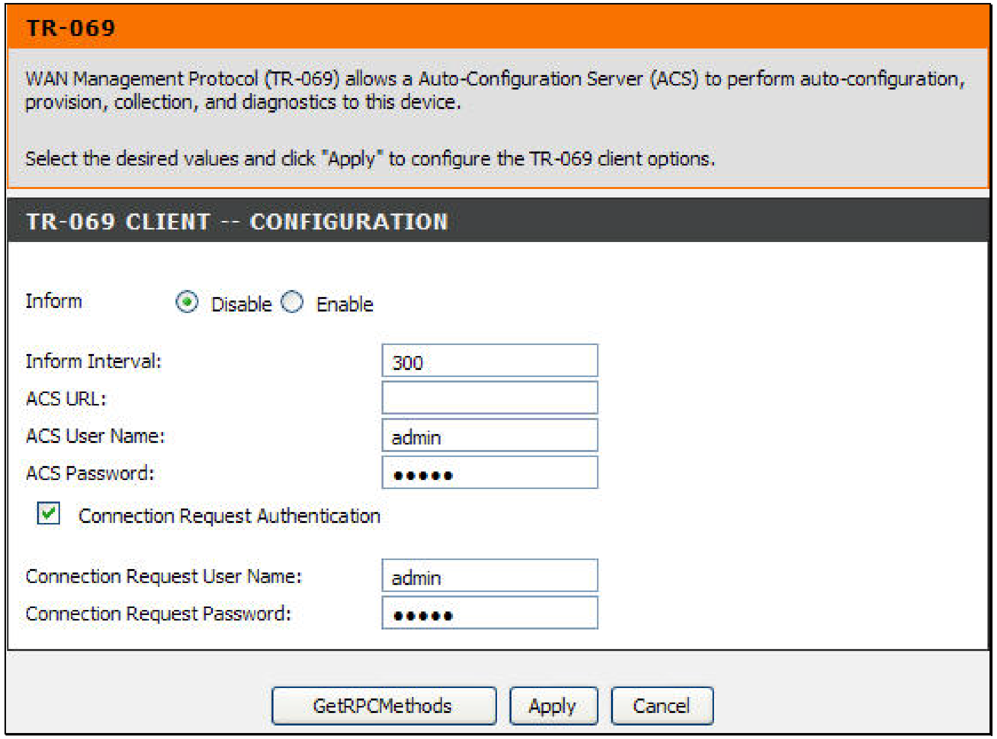
Read Community :	public
Set Community :	private
System Name :	DSL-2740BL
System Location :	unknown
System Contact :	unknown
Trap Manager IP :	0.0.0.0

TR-069

To access TR-069, point to the **Network Tools** on the left window and click **TR-069** submenu, or click the **TR-069**button in the Network Tools window.

TR-069 is a WAN management protocol. A bidirectional SOAP/HTTP based protocol it provides the communication between the ADSL router and an Auto Configuration Server (ACS).
WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Click **Disable** or **Enable** radio button under **Inform** to enable or disable the function. Configure the parameters for ACS on this window and then click the **Apply** button. Click the **GetRPCMethods** button to get RPC methods from the host.



TR-069

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device.

Select the desired values and click "Apply" to configure the TR-069 client options.

TR-069 CLIENT -- CONFIGURATION

Inform ● Disable ○ Enable

Inform Interval:	300
ACS URL:	
ACS User Name:	admin
ACS Password:	•••••

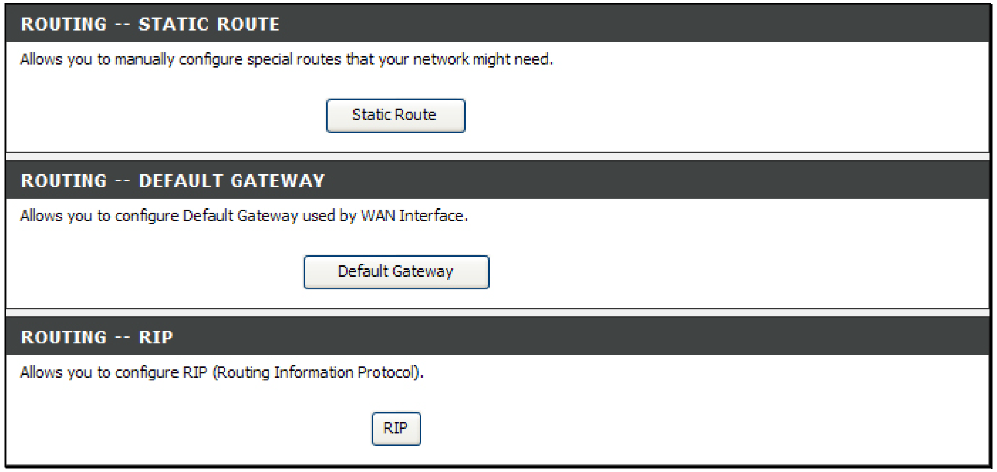
☑ Connection Request Authentication

Connection Request User Name:	admin
Connection Request Password:	•••••

Routing

To access the Routing window, click the **Routing** button in the **Advanced** directory.

It has three subcategories: **Static Route**, **Default Gateway** and **RIP**. You can either point to the **Routing** on the left window and click one of the submenus, or click one of the buttons in the Routing window.



ROUTING -- STATIC ROUTE

Allows you to manually configure special routes that your network might need.

ROUTING -- DEFAULT GATEWAY

Allows you to configure Default Gateway used by WAN Interface.

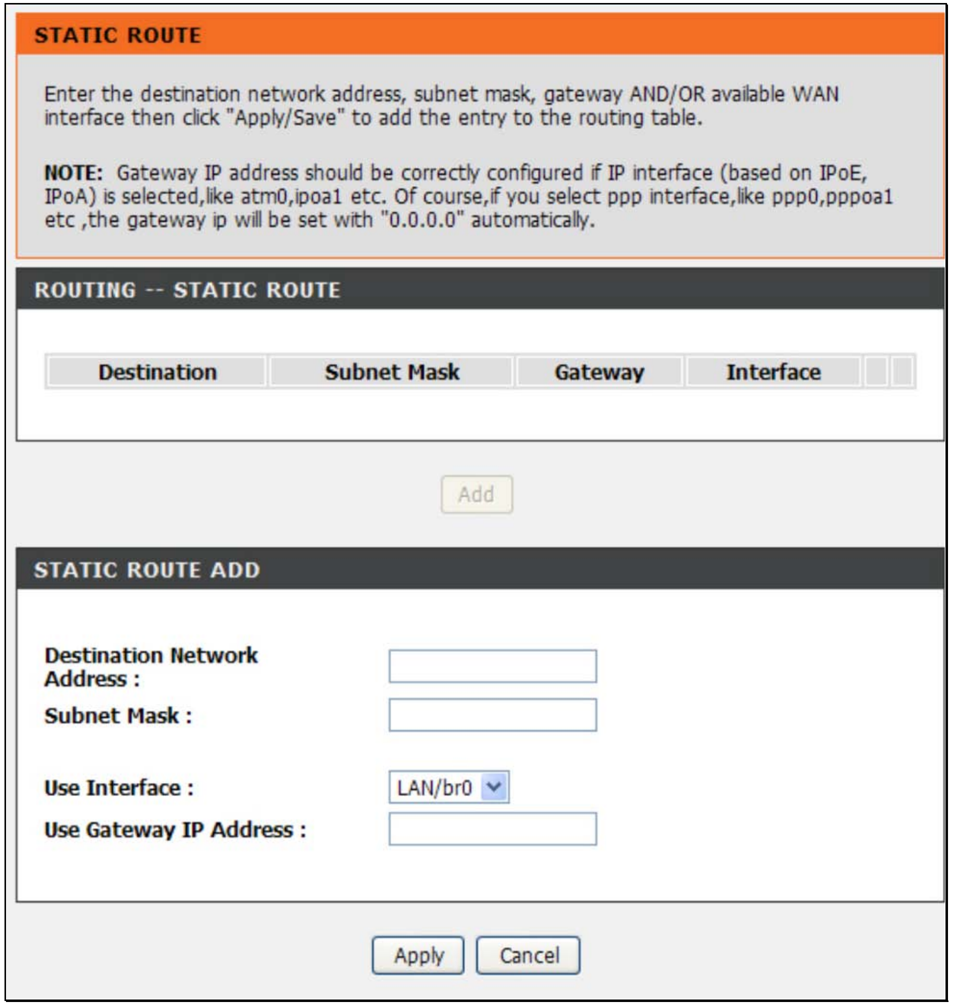
ROUTING -- RIP

Allows you to configure RIP (Routing Information Protocol).

Static Route

To access Static Route, point to the **Routing** on the left window and click **Static Route** submenu, or click the **Static Route** button in the Routing window. The page allows you to manually enter the routing table.

To define a gateway and hop to route data traffic, click **Add** to see the Static Route Add section. Enter a **Destination Network Address**, and **Subnet Mask**. Click the **Use Gateway IP Address** radio button and enter the gateway IP address, or click the **Use Interface** radio button and select an interface from the drop-down menu. Click **Apply** to see the entry in the Active Static Route table. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.



STATIC ROUTE

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply/Save" to add the entry to the routing table.

NOTE: Gateway IP address should be correctly configured if IP interface (based on IPoE, IPoA) is selected,like atm0,ipoa1 etc. Of course,if you select ppp interface,like ppp0,pppoa1 etc ,the gateway ip will be set with "0.0.0.0" automatically.

ROUTING -- STATIC ROUTE

Destination	Subnet Mask	Gateway	Interface		

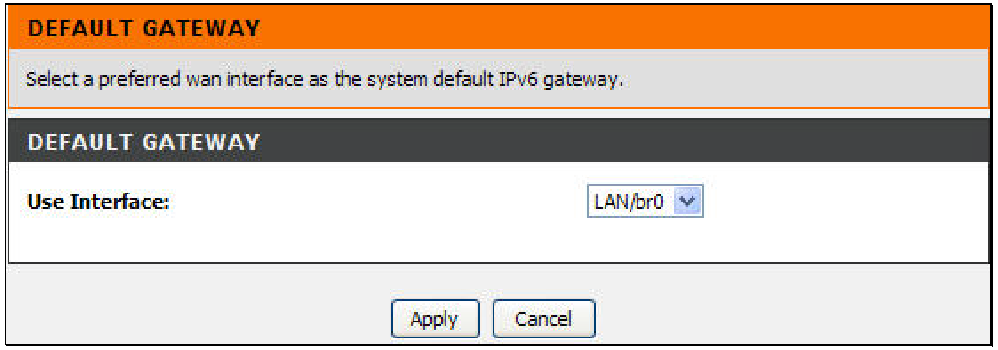
STATIC ROUTE ADD

Destination Network Address :	
Subnet Mask :	
Use Interface :	LAN/br0
Use Gateway IP Address :	

Default Gateway

To access Default Gateway, point to the **Routing** on the left window and click **Default Gateway** submenu, or click the **Default Gateway** button in the Routing window.

This page can assign a default gateway to the device. Select an interface from the **Use Interface** drop-down menu, and click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.



DEFAULT GATEWAY

Select a preferred wan interface as the system default IPv6 gateway.

DEFAULT GATEWAY

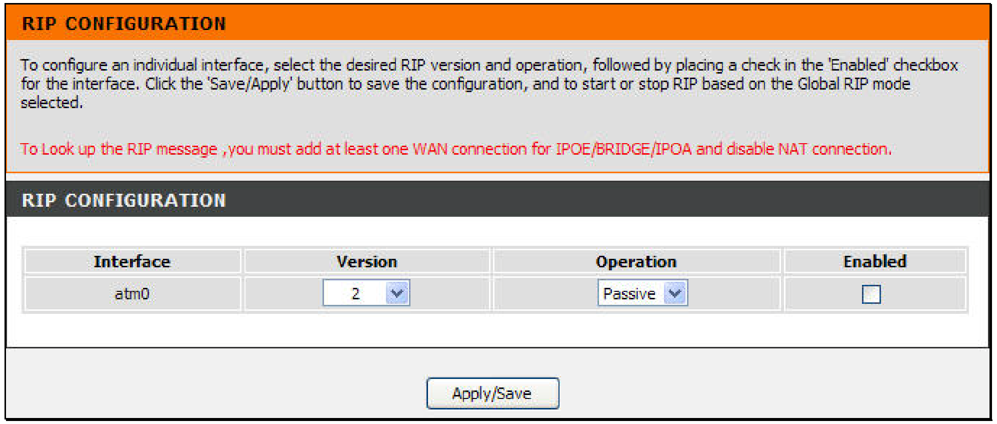
Use Interface: LAN/br0

RIP

To access RIP, point to the **Routing** on the left window and click **RIP** submenu, or click the **RIP** button in the Routing window.

The Router supports RIP version 1 and 2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN. The Operation setting refers to the RIP request. Select *Active* to allow RIP requests from other devices. Select *Passive* to instruct the Router to make RIP requests for routing tables from other devices.

To enable RIP, select the Version (1, 2, or Both) and Operation (*Active* or *Passive*), and tick the **Enable** check box in the corresponding entry. Click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device and let your changes take effect.



RIP CONFIGURATION

To configure an individual interface, select the desired RIP version and operation, followed by placing a check in the 'Enabled' checkbox for the interface. Click the 'Save/Apply' button to save the configuration, and to start or stop RIP based on the Global RIP mode selected.

To Look up the RIP message ,you must add at least one WAN connection for IPOE/BRIDGE/IPOA and disable NAT connection.

RIP CONFIGURATION

Interface	Version	Operation	Enabled
atm0	2	Passive	□

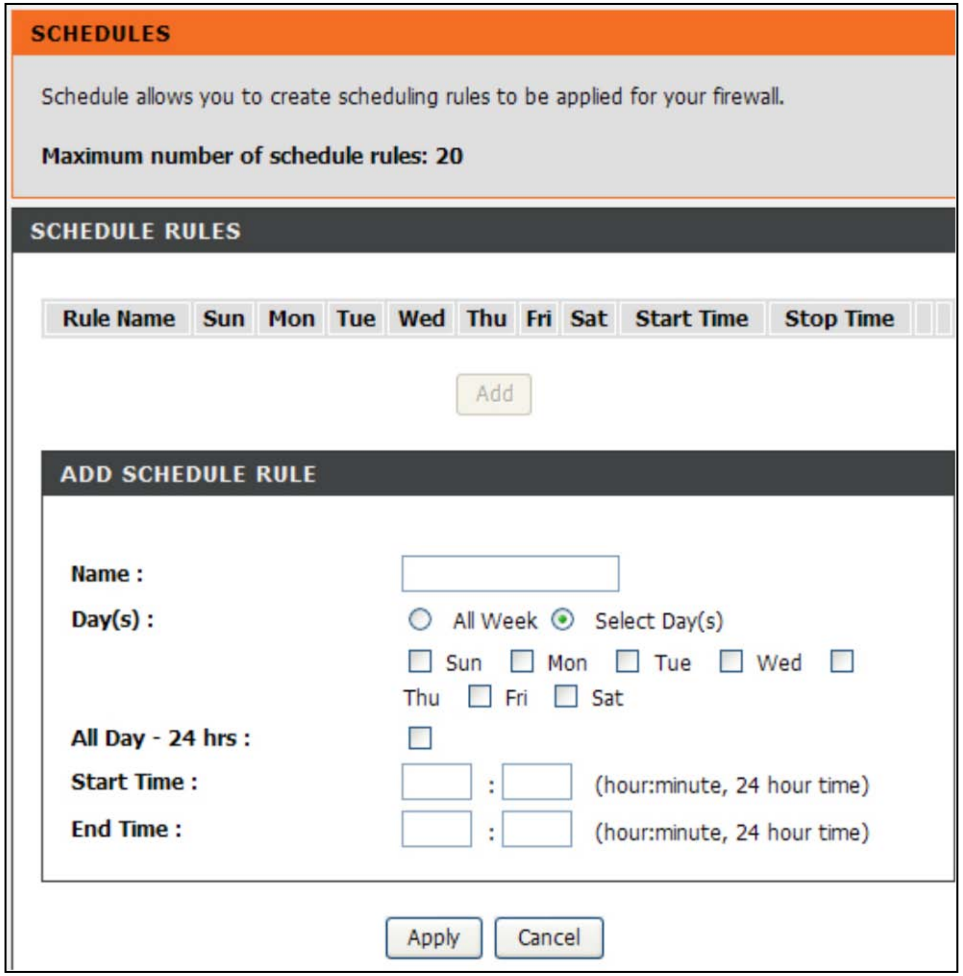
Schedules

To access the Schedules window, click the **schedules** button in the **Advanced** directory.

You can add schedules in this page and then apply them to Parental Control. Before configure the schedule, make sure **Time and Date** in the **Setup** directory is enabled.

Click **Add** to see the Add Schedule Rule section. Enter a Name for the schedule. Use the radio buttons to click the desired **Day(s)**, either **All Week** or **Select Day(s)** (in which case you must tick the checkboxes for the desired individual days of the week), select the desired **Start Time** and **End Time** or tick the **All Day – 24 hrs** checkbox. Click **Apply** to see the entry in the Schedule Rule table. To remove an entry in the table, select the entry, and click the **Delete** button. To modify an entry in the table, select the entry, click the **Edit** button, make the desired changes, and then click the **Apply** button.

Note: A schedule can only be created if the Router is configured to synchronize time settings with NTP (Network Time Protocol). To configure the NTP option, go to the **Time and Date** configuration menu in the **Setup** menu directory.



SCHEDULES

Schedule allows you to create scheduling rules to be applied for your firewall.

Maximum number of schedule rules: 20

SCHEDULE RULES

Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop Time

Add

ADD SCHEDULE RULE

Name :

Day(s) : ○ All Week ● Select Day(s)

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

All Day - 24 hrs : □

Start Time : : (hour:minute, 24 hour time)

End Time : : (hour:minute, 24 hour time)

Apply Cancel

Maintenance

The **Maintenance** directory features an array of options designed to help you get the most out of your Router.

System

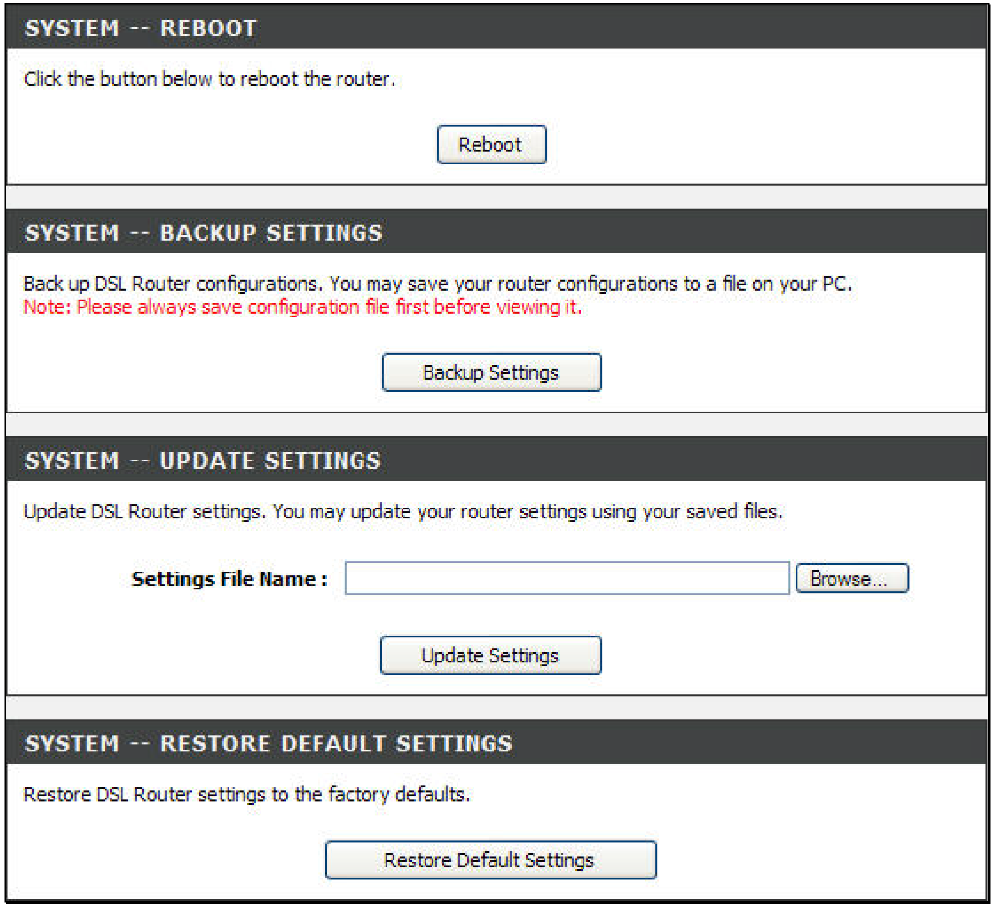
To access the System window, click the **System** button in the **Maintenance** directory.

When you configure the Router, you will need to restart the Router to take the settings effect. Click **Reboot** to restart the Router.

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. You will be prompted to select a location on your computer to put the file. The file type is bin and may be named anything you wish.

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Upload Settings** button to load the settings from your local hard drive. Confirm that you want to load the file when prompted. The Router will reboot and begin operating with the configuration settings that have just been loaded.

To reset the Router to its factory default settings, click the **Restore Default Settings** 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).



SYSTEM -- REBOOT

Click the button below to reboot the router.

SYSTEM -- BACKUP SETTINGS

Back up DSL Router configurations. You may save your router configurations to a file on your PC.
Note: Please always save configuration file first before viewing it.

SYSTEM -- UPDATE SETTINGS

Update DSL Router settings. You may update your router settings using your saved files.

Settings File Name :

SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

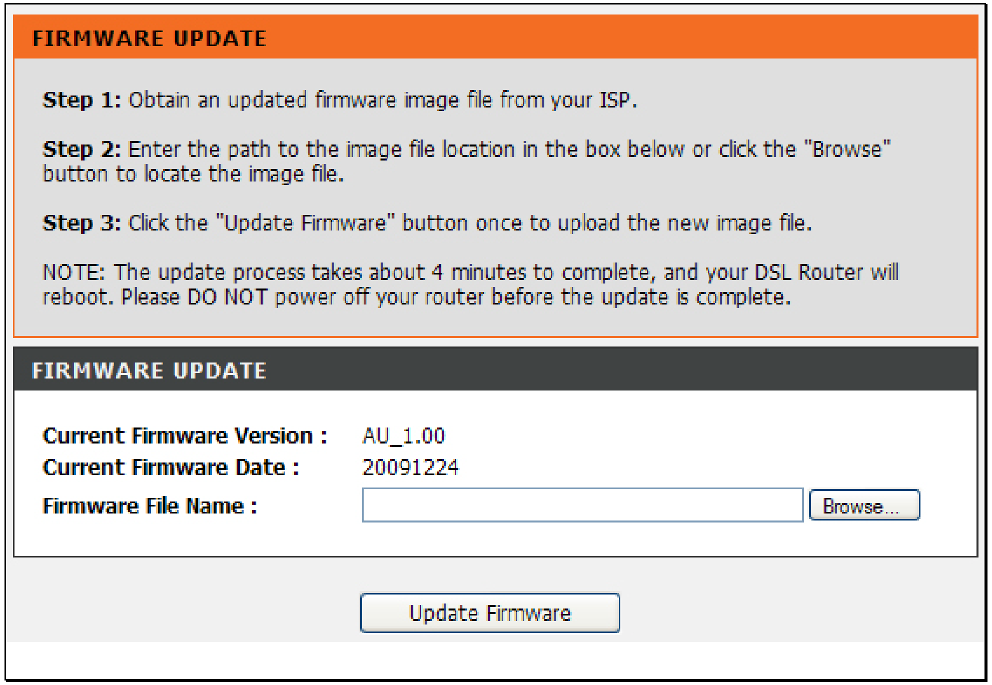
Firmware Update

To access the **Firmware Update** window, click the **Firmware Update** button in the **Maintenance** directory.

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

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

Note: Performing a Firmware Upgrade can sometimes change the configuration settings. Make sure to backup the Router's configuration settings before upgrading the firmware.



FIRMWARE UPDATE

Step 1: Obtain an updated firmware image file from your ISP.

Step 2: Enter the path to the image file location in the box below or click the "Browse" button to locate the image file.

Step 3: Click the "Update Firmware" button once to upload the new image file.

NOTE: The update process takes about 4 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

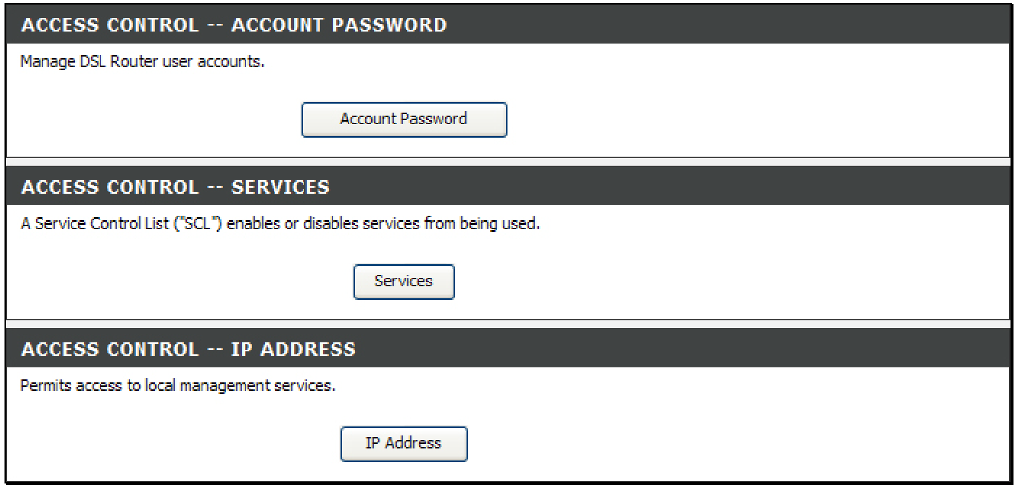
FIRMWARE UPDATE

Current Firmware Version : AU_1.00
Current Firmware Date : 20091224
Firmware File Name :

Access Controls

To access the Access Controls window, click the **Access Controls** button in the **Maintenance** directory.

In this page, you can choose to change password, manage the service control or IP address control.



ACCESS CONTROL -- ACCOUNT PASSWORD

Manage DSL Router user accounts.

ACCESS CONTROL -- SERVICES

A Service Control List ("SCL") enables or disables services from being used.

ACCESS CONTROL -- IP ADDRESS

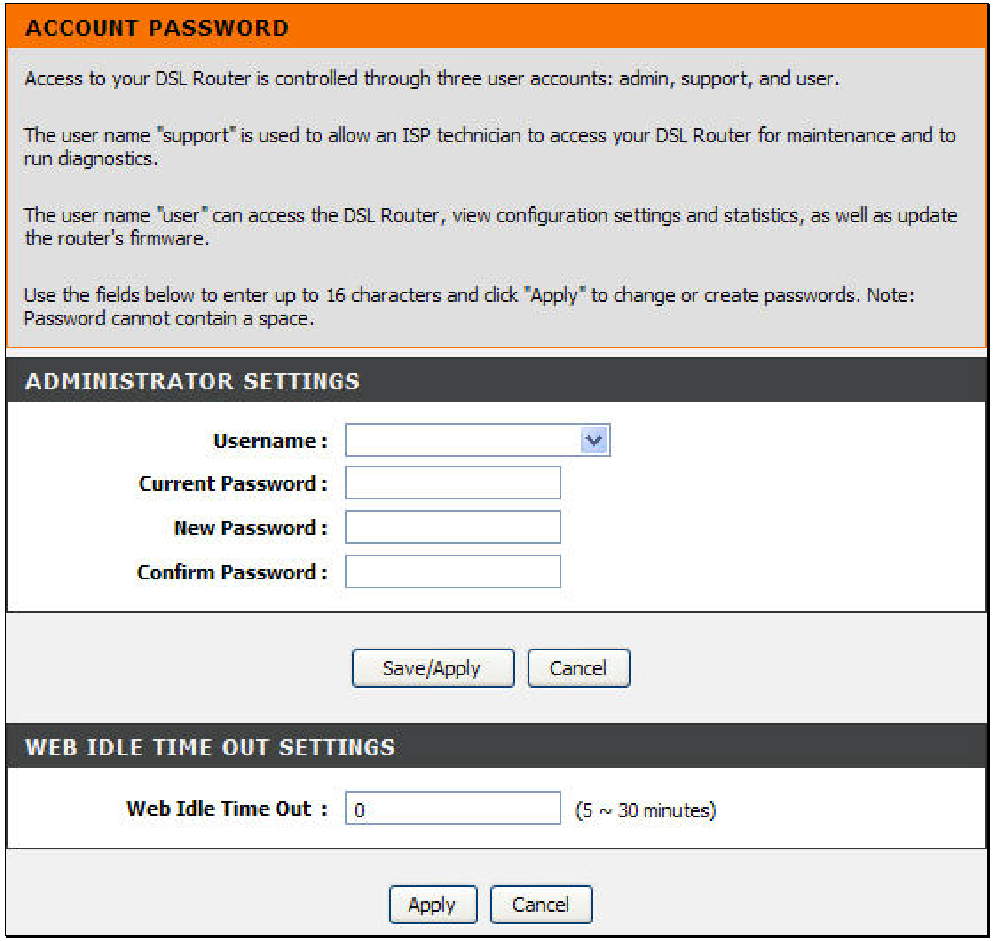
Permits access to local management services.

Account Password

To access Account Password, point to the **Access Controls** on the left window and click **Account Password** submenu, or click the **Account Password** button in the Access Controls window.

There are three different user names for different purpose. Support is for remote supporter to login from WAN and is able to adjust TR-069 settings. User and Admin are usernames to login from LAN. Select a user name (*admin*, *support* or *user*), type the Current Password (default values are *admin*, *user* or *support*) in the first field, the New Password in the second field, and enter the password again in the Confirm Password field to be certain you have typed it correctly. Click the **Save/Apply** button to save the settings.

You can configure the idle time between 5 and 30 minutes for the webpage asking you to logout.
Click the **Apply** button. Go to **Maintenance** -> **System** and click **Reboot** to restart the device.



ACCOUNT PASSWORD

Access to your DSL Router is controlled through three user accounts: admin, support, and user.

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics.

The user name "user" can access the DSL Router, view configuration settings and statistics, as well as update the router's firmware.

Use the fields below to enter up to 16 characters and click "Apply" to change or create passwords. Note: Password cannot contain a space.

ADMINISTRATOR SETTINGS

Username :
Current Password :
New Password :
Confirm Password :

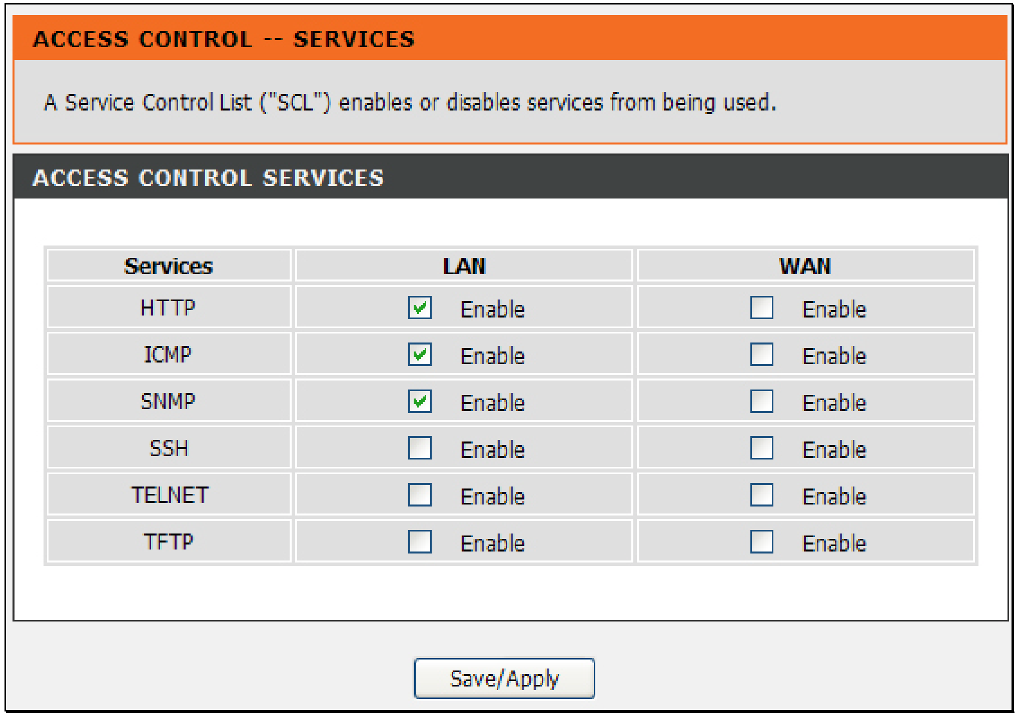
WEB IDLE TIME OUT SETTINGS

Web Idle Time Out : 0 (5 ~ 30 minutes)

Services

To access Services, point to the **Access Controls** on the left window and click **Services** submenu, or click the **Services** button in the Access Controls window.

This page lists out all the available services including Telnet, HTTP, ICMP, SNMP, SSH, and TFTP that can enable at LAN, WAN or both. Tick to enable the services, or deselect to disable them. Click the **Save/Apply** button to save the settings.



ACCESS CONTROL -- SERVICES

A Service Control List ("SCL") enables or disables services from being used.

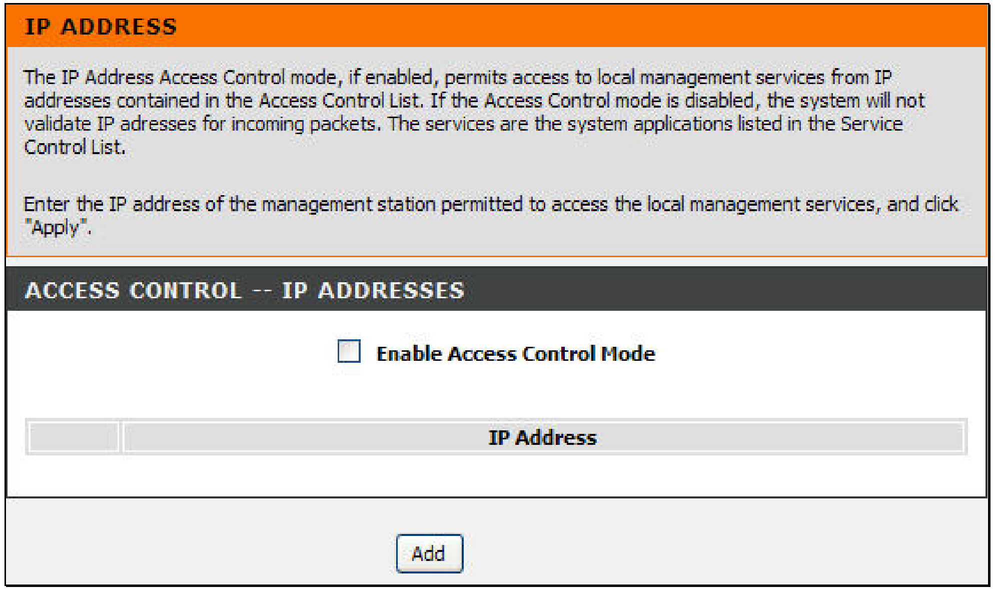
ACCESS CONTROL SERVICES

Services	LAN	WAN
HTTP	☑ Enable	□ Enable
ICMP	☑ Enable	□ Enable
SNMP	☑ Enable	□ Enable
SSH	□ Enable	□ Enable
TELNET	□ Enable	□ Enable
TFTP	□ Enable	□ Enable

IP Address

To access IP Address, point to the **Access Controls** on the left window and click **IP Address** submenu, or click the **IP Address** button in the Access Controls window.

Click **Add** to see the Add IP Address section. Enter an IP address and click **Apply** in the section. The IP address will show in the table in the Remote Web and Telnet Management section. Tick the **Enable Access Control Mode** check box to enable the function.



IP ADDRESS

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP adresses for incoming packets. The services are the system applications listed in the Service Control List.

Enter the IP address of the management station permitted to access the local management services, and click "Apply".

ACCESS CONTROL -- IP ADDRESSES

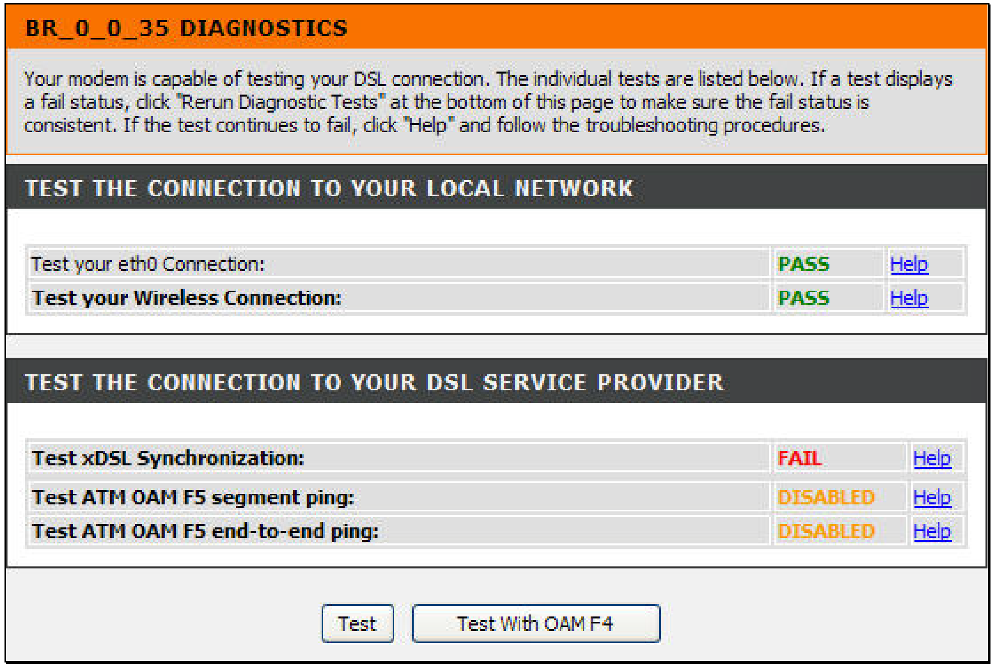
□ Enable Access Control Mode

	IP Address

Diagnostics

To access the Diagnostic window, click the **Diagnostics** button in the **Maintenance** directory.

This 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 tests of your system software and hardware connections. Use this window when working with your ISP to troubleshoot problems.



BR_0_0_35 DIAGNOSTICS

Your modem is capable of testing your DSL connection. The individual tests are listed below. If a test displays a fail status, click "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent. If the test continues to fail, click "Help" and follow the troubleshooting procedures.

TEST THE CONNECTION TO YOUR LOCAL NETWORK

Test your eth0 Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

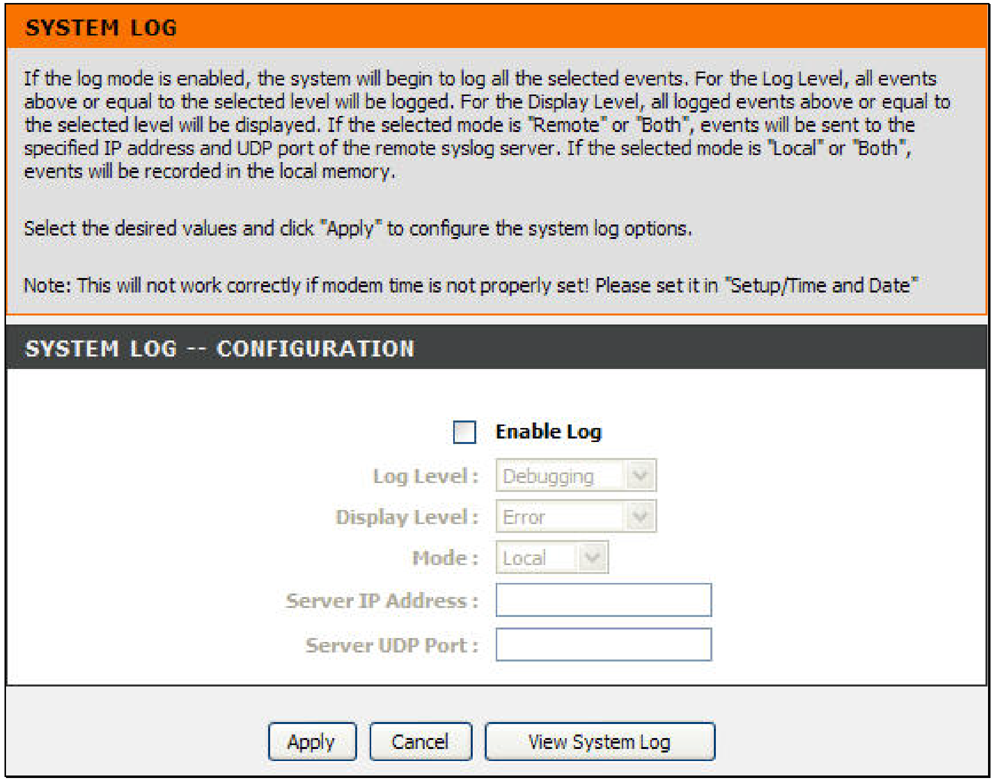
Test xDSL Synchronization:	FAIL	Help
Test ATM OAM F5 segment ping:	DISABLED	Help
Test ATM OAM F5 end-to-end ping:	DISABLED	Help

System Log

To access the System Log window, click the **System Log** button in the **Maintenance** directory.

The system log allows you to configure local and remote logging, and to view the logs that have been created.

To generate a system log, tick the **Enable Log** check box. Select the **Log Level** and **Display Level** from the drop-down lists. The levels available are the same for each type of level: Emergency, Alert, Critical, Error, Warning, Notice, Informational and Debugging. Click the **Apply** button to allow your new settings to take effect. Click **View System Log** to go to **Status** -> **Logs** to see the detail log information.



SYSTEM LOG

If the log mode is enabled, the system will begin to log all the selected events. For the Log Level, all events above or equal to the selected level will be logged. For the Display Level, all logged events above or equal to the selected level will be displayed. If the selected mode is "Remote" or "Both", events will be sent to the specified IP address and UDP port of the remote syslog server. If the selected mode is "Local" or "Both", events will be recorded in the local memory.

Select the desired values and click "Apply" to configure the system log options.

Note: This will not work correctly if modem time is not properly set! Please set it in "Setup/Time and Date"

SYSTEM LOG -- CONFIGURATION

□ Enable Log

Log Level : Debugging

Display Level : Error

Mode : Local

Server IP Address :

Server UDP Port :

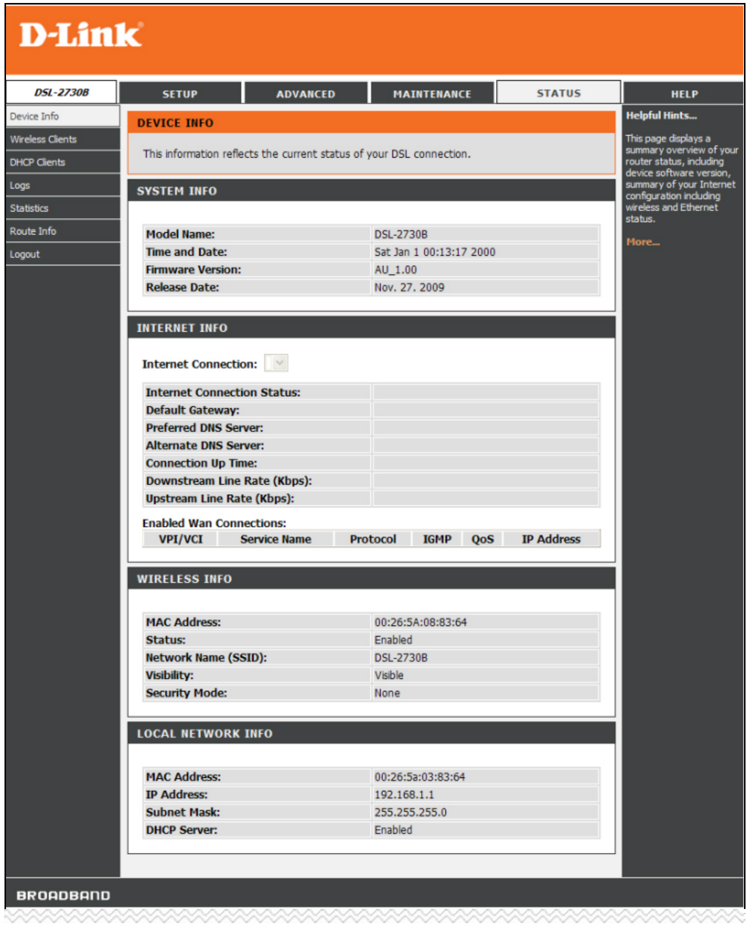
Status

Use the various read-only windows to view system information and monitor performance.

Device Info

To access the Device Info window, click the **Device Info** button in the **Status** directory.

Use this window to quickly view basic current information about the LAN and WAN interfaces and device information including Firmware Version and MAC address.



DEVICE INFO

This information reflects the current status of your DSL connection.

SYSTEM INFO

Model Name:	DSL-2730B
Time and Date:	Sat Jan 1 00:13:17 2000
Firmware Version:	AU_1.00
Release Date:	Nov. 27. 2009

INTERNET INFO

Internet Connection:

Internet Connection Status:	
Default Gateway:	
Preferred DNS Server:	
Alternate DNS Server:	
Connection Up Time:	
Downstream Line Rate (Kbps):	
Upstream Line Rate (Kbps):	

Enabled Wan Connections:

VPI/VCI	Service Name	Protocol	IGMP	QoS	IP Address

WIRELESS INFO

MAC Address:	00:26:5A:08:83:64
Status:	Enabled
Network Name (SSID):	DSL-2730B
Visibility:	Visible
Security Mode:	None

LOCAL NETWORK INFO

MAC Address:	00:26:5a:03:83:64
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enabled

Helpful Hints...

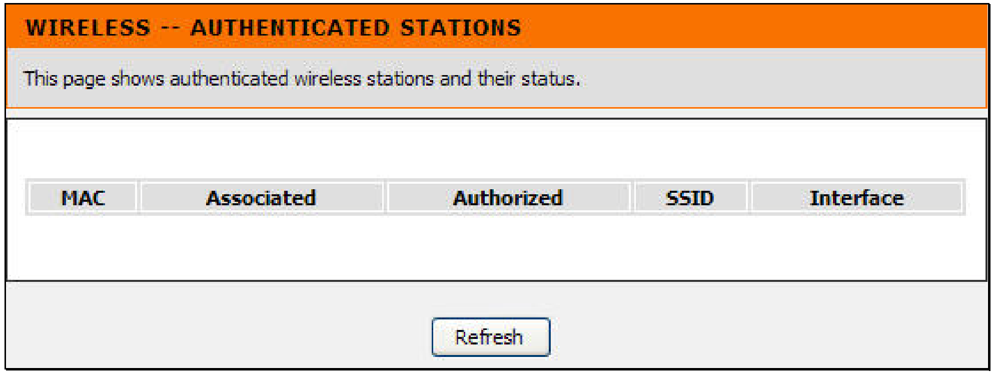
This page displays a summary overview of your router status, including device software version, summary of your Internet configuration including wireless and Ethernet status.

More...

Wireless Clients

To access the DHCP Clients window, click the **Wireless Clients** button in the **Status** directory.

The Connected Wireless LAN Clients list displays in this page.



WIRELESS -- AUTHENTICATED STATIONS

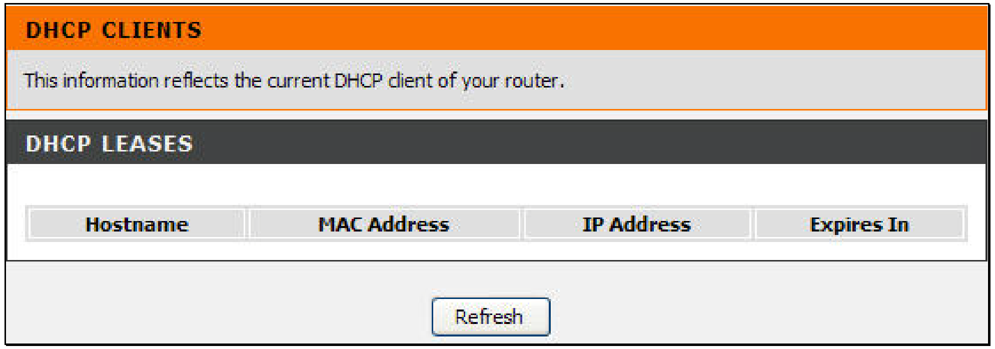
This page shows authenticated wireless stations and their status.

MAC	Associated	Authorized	SSID	Interface

DHCP Clients

To access the DHCP Clients window, click the **DHCP Clients** button in the **Status** directory.

The Connected LAN Clients list displays active DHCP clients when the Router is acting as a DHCP server.



DHCP CLIENTS

This information reflects the current DHCP client of your router.

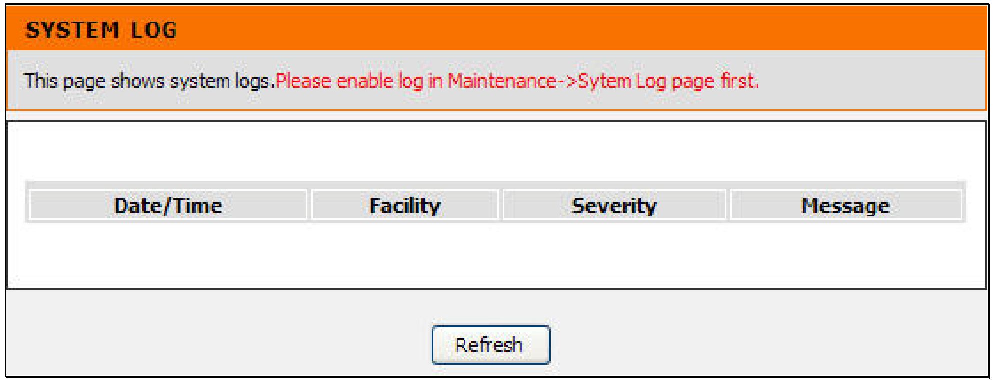
DHCP LEASES

Hostname	MAC Address	IP Address	Expires In

Logs

To access the Logs window, click the **Logs** button in the **Status** directory.

This page displays the event logs of the Router. Before seeing the log information, make sure the system log function is enabled in the **Maintenance** -> **System Log**. Click **Refresh** to update the log information.



SYSTEM LOG

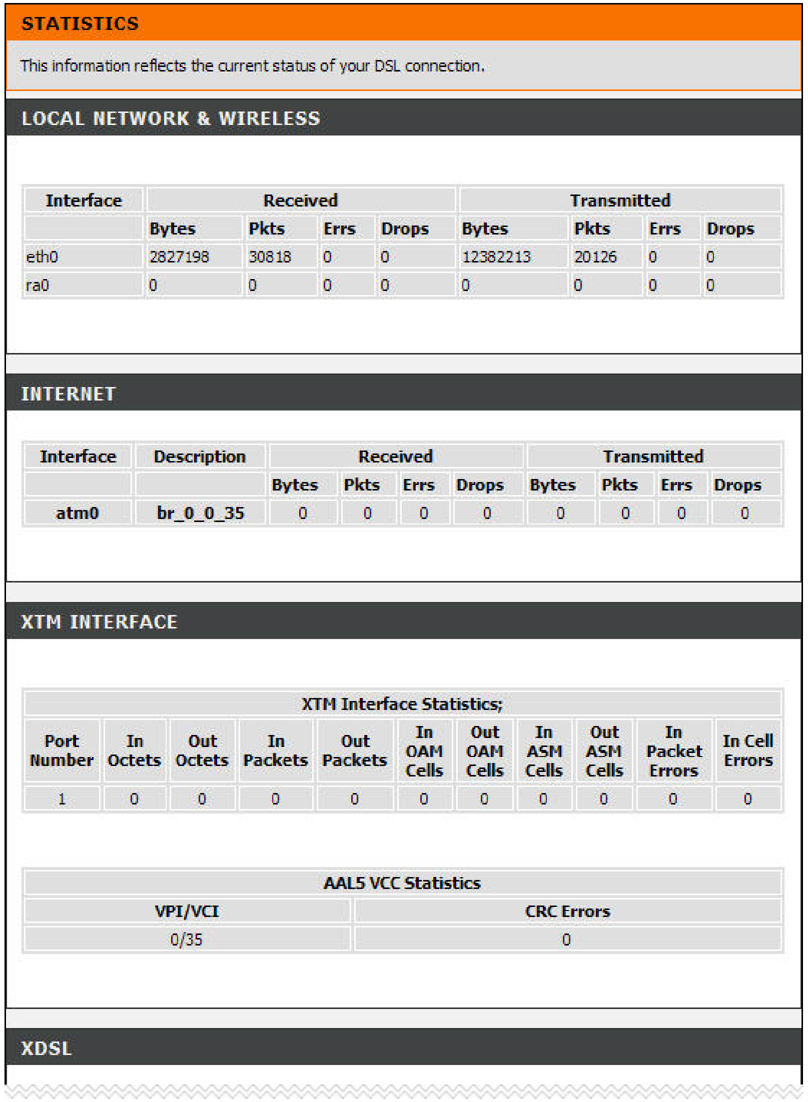
This page shows system logs.Please enable log in Maintenance->Sytem Log page first.

Date/Time	Facility	Severity	Message

Statistics

To access the Statistics window, click the **Statistics** button in the **Status** directory.

This page allows you to monitor traffic on the Local Network, Internet or ADSL connection. This window also displays information concerning ADSL status.



STATISTICS

This information reflects the current status of your DSL connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	2827198	30818	0	0	12382213	20126	0	0
ra0	0	0	0	0	0	0	0	0

INTERNET

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
atm0	br_0_0_35	0	0	0	0	0	0	0	0

XTM INTERFACE

XTM Interface Statistics;

Port Number	In Octets	Out Octets	In Packets	Out Packets	In OAM Cells	Out OAM Cells	In ASM Cells	Out ASM Cells	In Packet Errors	In Cell Errors
1	0	0	0	0	0	0	0	0	0	0

AAL5 VCC Statistics

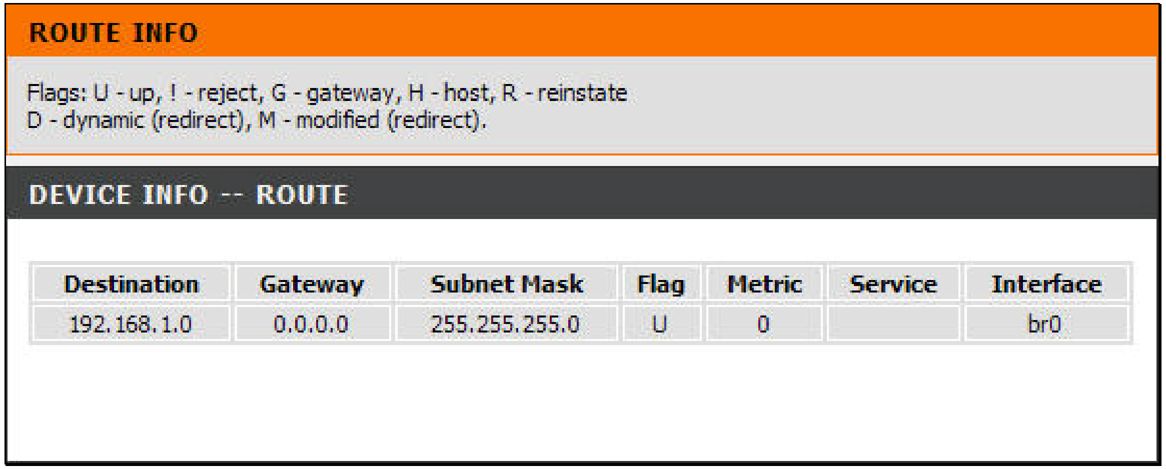
VPI/VCI	CRC Errors
0/35	0

XDSL

Routing Info

To access the Routing Info window, click the **Routing Info** button in the **Status** directory.

This page is used to direct forwarding by matching destination addresses to the network paths used to reach them.



ROUTE INFO

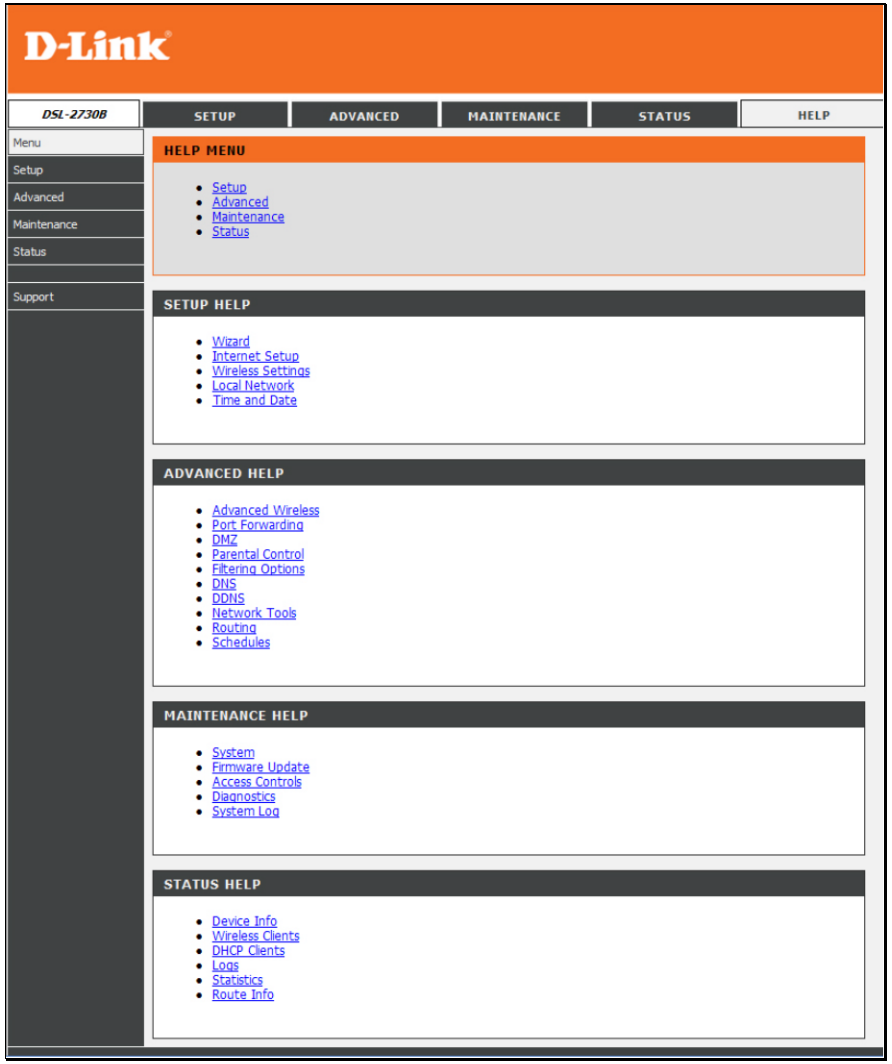
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

DEVICE INFO -- ROUTE

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

Help

To access the Help window, click the **Help** directory.



HELP MENU

- Setup
- Advanced
- Maintenance
- Status

SETUP HELP

- Wizard
- Internet Setup
- Wireless Settings
- Local Network
- Time and Date

ADVANCED HELP

- Advanced Wireless
- Port Forwarding
- DMZ
- Parental Control
- Filtering Options
- DNS
- DDNS
- Network Tools
- Routing
- Schedules

MAINTENANCE HELP

- System
- Firmware Update
- Access Controls
- Diagnostics
- System Log

STATUS HELP

- Device Info
- Wireless Clients
- DHCP Clients
- Logs
- Statistics
- Route Info

Troubleshooting

This chapter provides solutions to problems that might occur during the installation and operation of the DSL-2730B. 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. How do I configure my DSL-2730B Router without the CD-ROM?

- Connect your PC to the Router using an Ethernet cable.
- Open a web browser and enter the address http://192.168.1.1
- The default username is ‘admin’ and the default password is ‘admin’.
- If you have changed the password and cannot remember it, you will need to reset the Router to the factory default setting (see question 2), which will set the password back to ‘admin’.

Note: Please refer to the next section “Networking Basics” to check your PC’s IP configuration if you can’t see the login windows.

2. How do I reset my Router to the factory default settings?

- Ensure the Router is powered on.
- Press and hold the reset button on the back of the device for approximately 10 seconds.
- This process should take around 1 to 2 minutes.

Note: Resetting the Router to the factory default settings will erase the current configuration settings. To reconfigure your settings, login to the Router as outlined in question 1, then run the Quick Setup wizard.

3. What can I do if my Router is not working correctly?

There are a few quick steps you can take to try and resolve any issues:

- Follow the directions in Question 2 to reset the Router.
- Check that all the cables are firmly connected at both ends.
- Check the LEDs on the front of the Router. The Power indicator should be on, the Status indicator should flash, and the DSL and LAN indicators should be on as well.

- Please ensure that the settings in the Web-based configuration manager, e.g. ISP username and password, are the same as the settings that have been provided by your ISP.

4. Why can’t I get an Internet connection?

For ADSL ISP users, please contact your ISP to make sure the service has been enabled/connected by your ISP and that your ISP username and password are correct.

5. What can I do if my Router can’t be detected by running the installation CD?

- Ensure the Router is powered on.
- Check that all the cables are firmly connected at both ends and all LEDs work correctly.
- Ensure only one network interface card on your PC is activated.
- Click on **Start** > **Control Panel** > **Security Center** to disable the firewall.

Note: There is a potential security issue if the firewall is disabled on your PC. Please remember to turn it back on once you have finished the whole installation procedure. This will enable you to be able to surf the Internet without any problem.

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.

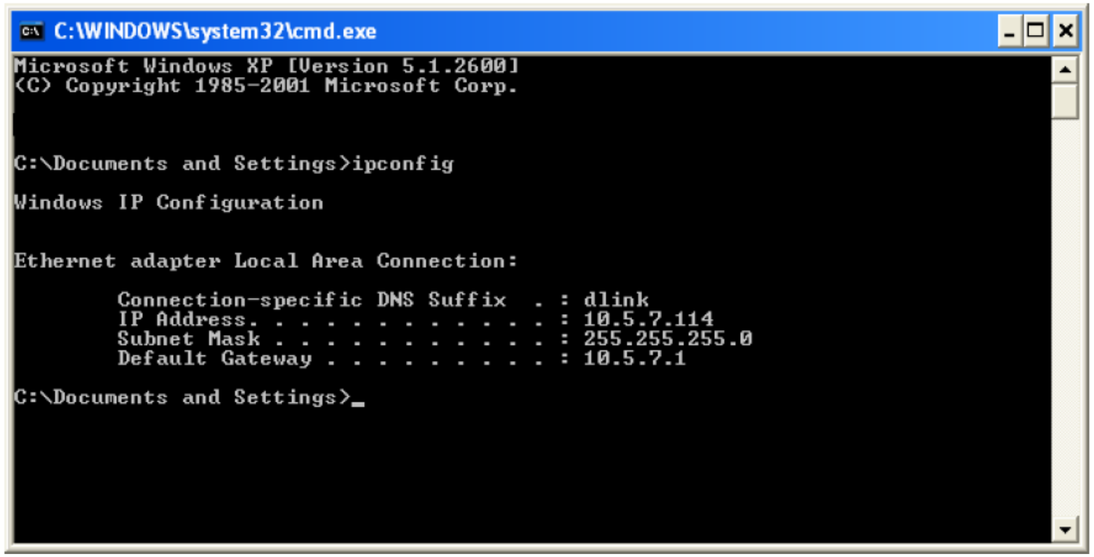
Click on **Start** > **Run**. In the run box type ***cmd*** and click on the **OK**.

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.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : dlink
        IP Address. . . . . . . . . . . . : 10.5.7.114
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.5.7.1

C:\Documents and 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 on the **My Network Places** > **Properties**.

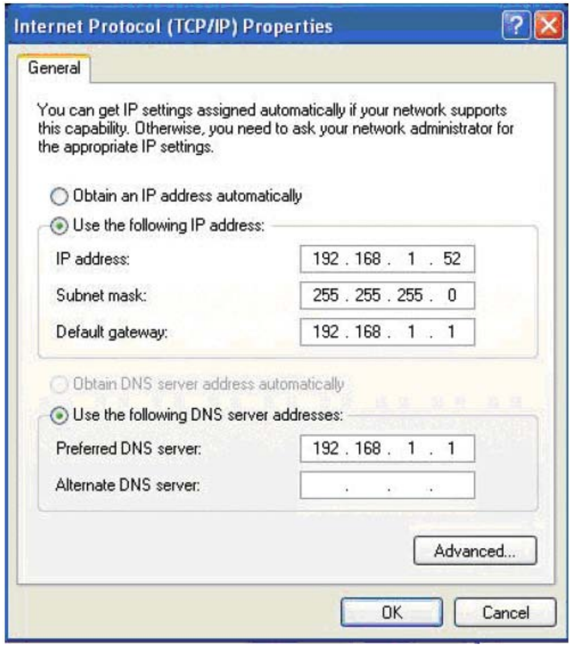
Step 2
Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.

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

Step 4
Click on the **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.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 52
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: . . .

Step 5
Click on the **OK** twice to save your settings.

Technical Specifications

ADSL Standards

- ANSI T1.413 Issue 2
- ITU G.992.1 (G.dmt) Annex A/C/I
- ITU G.992.2 (G.lite) Annex A/C
- ITU G.994.1 (G.hs)

ADSL2 Standards

- ITU G.992.3 (G.dmt.bis) Annex A/J/K/L/M
- ITU G.992.4 (G.lite.bis) Annex A

ADSL2+ Standards

- ITU G.992.5 Annex A/L/M

Protocols

- IEEE 802.1d; up to 128 MAC Learning Address supported
- TCP/UDP
- ARP
- RARP
- RFC792 ICMP
- RFC1058 RIP, RIP v2
- RFC1213 SNMP v1 & v2c
- RFC1332 IPCP
- RFC1334 PAP
- RFC1389 RIP v2
- RFC1577 Classical IP over ATM
- RFC1483 MER
- RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5)
- RFC1631 NAT; maximum 4096 NAT sessions
- RFC1661 Point to Point Protocol
- RFC1994 CHAP
- RFC2131 DHCP Client / DHCP Server
- RFC2364 PPP over ATM
- RFC2433 Microsoft PPP CHAP extensions
- 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 1 Mbps
- ADSL2+ full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps

Wireless Transfer Rates

- IEEE 802.11b: 11, 5.5, 2, and 1Mbps
- IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps
- Optional 802.11n Capabilities
- 20MHz BW: 150, 130, 117, 104, 78, 52, 39, 26, 13Mbps
- 40MHz BW: 150, 130, 117, 104, 78, 52, 39, 26, 13Mbps

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