USER MANUAL

DSL-2642B

VERSION 1.00

D-Link®

BROADBAND

Table of Contents

Package Contents

- DSL-2642B Wireless ADSL 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

Note: Using a power supply with a different voltage rating than the one included with the DSL-2642B will cause damage and void the warranty for this product.

System Requirements

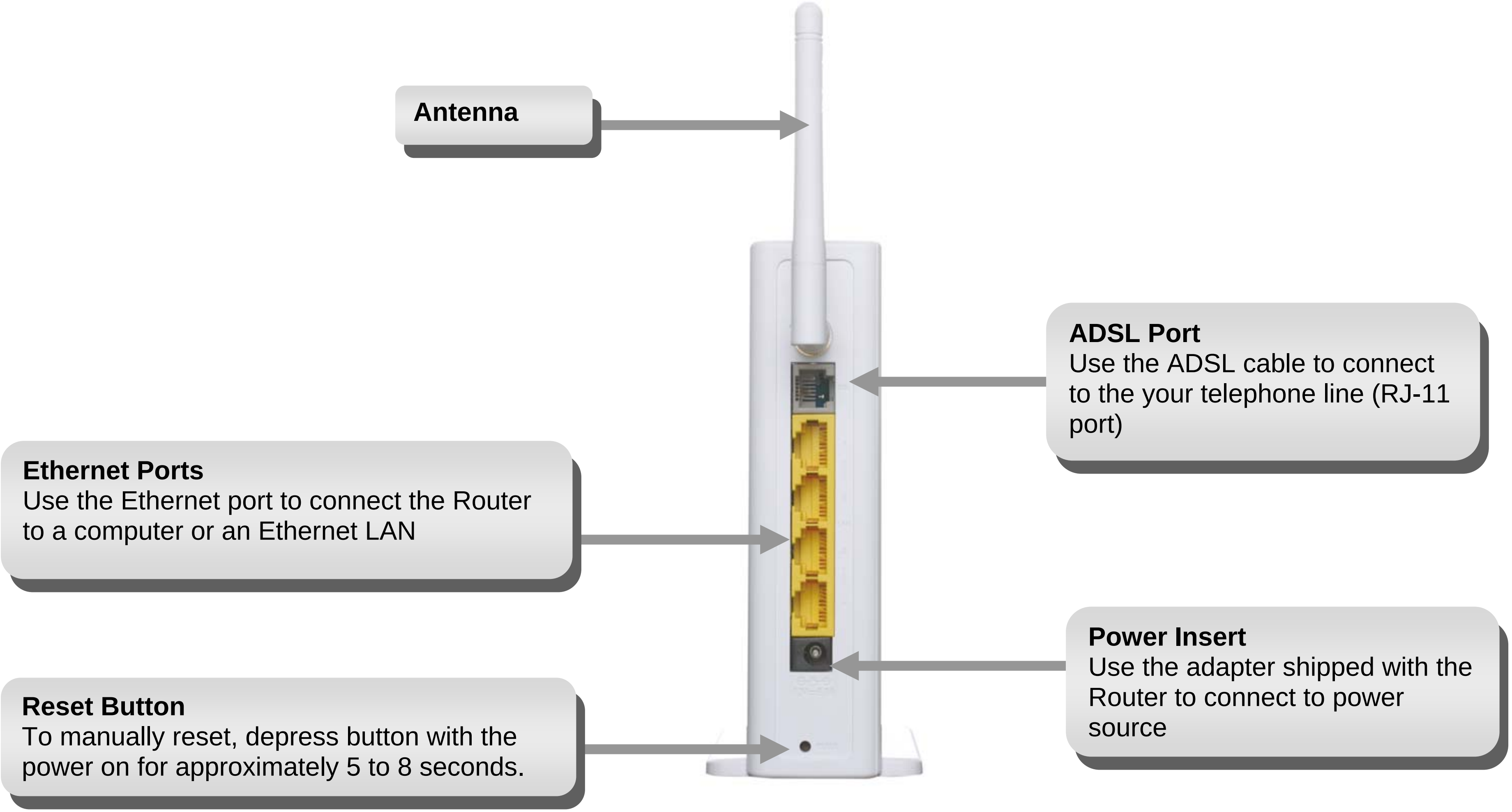
- ADSL Internet service
- Computer with:
  - 200MHz Processor
  - 64MB Memory
  - CD-ROM Drive
  - Ethernet Adapter with TCP/IP Protocol Installed
  - Internet Explorer v6 or later, FireFox v1.5
  - Computer with Windows 2000, Windows XP, or Windows Vista
- D-Link Click'n Connect Utility

Features

- **PPP (Point-to-Point Protocol) Security –** The DSL-2642B ADSL 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 DSL-2642B 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 DSL-2642B 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 DSL-2642B 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 DSL-2642B 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.
- **G.hs (Auto-handshake) –** This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.
- **High Performance –** Very high rates of data transfer are possible with the Router. Up to 8 Mbps downstream bit rate using the G.dmt standard.
- **Full Network Management –** The DSL-2642B 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 DSL-2642B 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

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

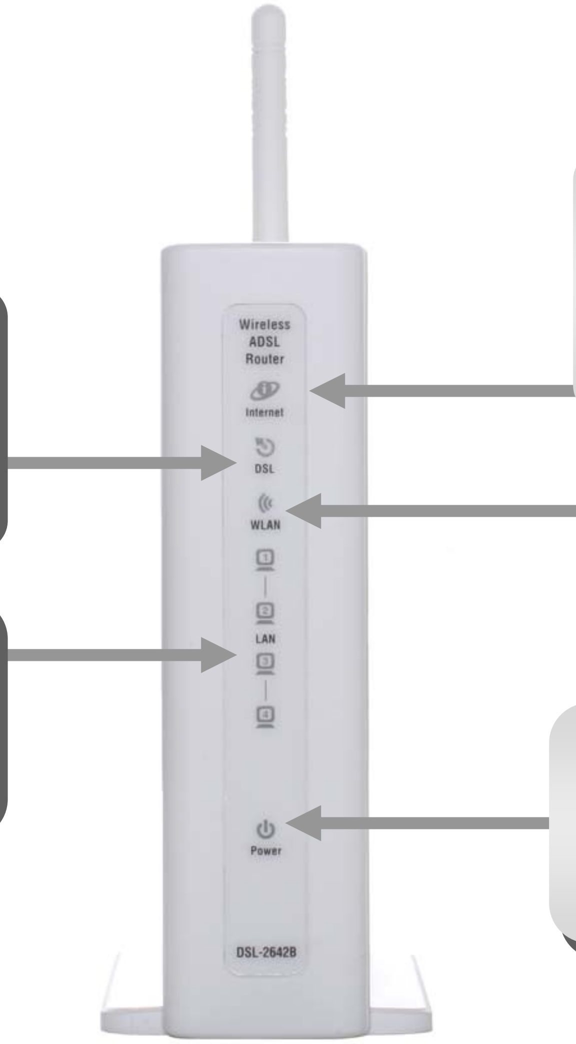
Ethernet Ports
Use the Ethernet port to connect the Router to a computer or an Ethernet LAN

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

Reset Button
To manually reset, depress button with the power on for approximately 5 to 8 seconds.

Hardware Overview

LEDs



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 that ADLS is attempting to sync.

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.

Internet
LED will light green when obtaining WAN IP address from IPCP or DHCP, and DSL connection is build up. It also will light green when a static IP address is configured and PPP negotiation is successfully established.

WLAN
This LED will be lit green when a Wireless LAN connection is detected. It will blink when there is data activity on the connection.

Power
A steady green light indicates the unit is powered on. When the device is powered off this remains dark. Lights steady red during power on self-test (POST) or the device is malfunction.

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-2642B 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/PPoA (PPPoE LLC, PPPoA LLC or PPPoA VC-Mux)
- Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC Mux)
- IPoA/MER (Static IP Address) (Bridged IP LLC, 1483 Bridged IP VC Mux, 1483 Routed IP LLC, 1483 Routed IP VC-Mux or IPoA)
- MER (Dynamic IP Address) (1483 Bridged IP LLC or 1483 Bridged IP VC-Mux)

Modulation Type
ADSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (ADSL2+ Multi-Mode) used for the Router automatically detects all types of ADSL, ADSL2, and ADSL2+ modulation.

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-2642B

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-2642B
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-2642B
This is the subnet mask used by the DSL-2642B, 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-2642B to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2642B to connect to other computer or Ethernet devices.

DHCP Client status

Your DSL-2642B ADSL Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-2642B will assign are from 192.168.1.2 to 192.168.1.254. Your computer (or computers) needs to be configured to obtain an IP address automatically (that is, they need to be configured as DHCP clients.)

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

Once you have the above information, you are ready to setup and configure your DSL-2642B ADSL Router.

Device Installation

The DSL-2642B 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. You should see the Power LED indicator light up red, and then turn green.
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 this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Router can establish a connection.

Factory Reset Button

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

1. Ensure the Router is powered on.
2. Press and hold the reset button on the back of the device for approximately 5 to 8 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

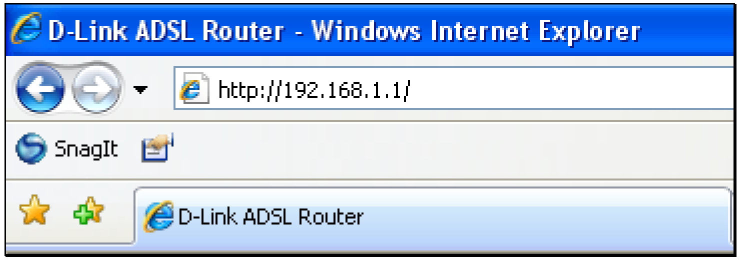
This section will show you how to set up and configure your new D-Link Router using the Web-based configuration utility.

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.

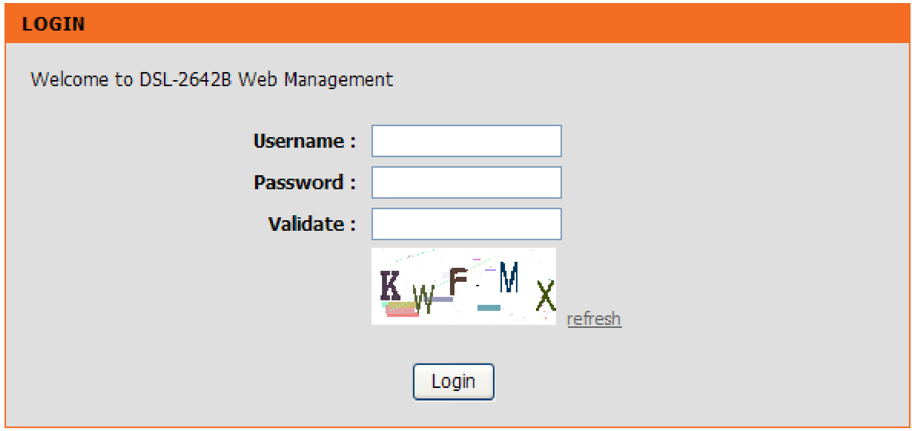
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (**192.168.1.1**).



D-Link ADSL Router - Windows Internet Explorer

http://192.168.1.1/

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



LOGIN

Welcome to DSL-2642B Web Management

Username :

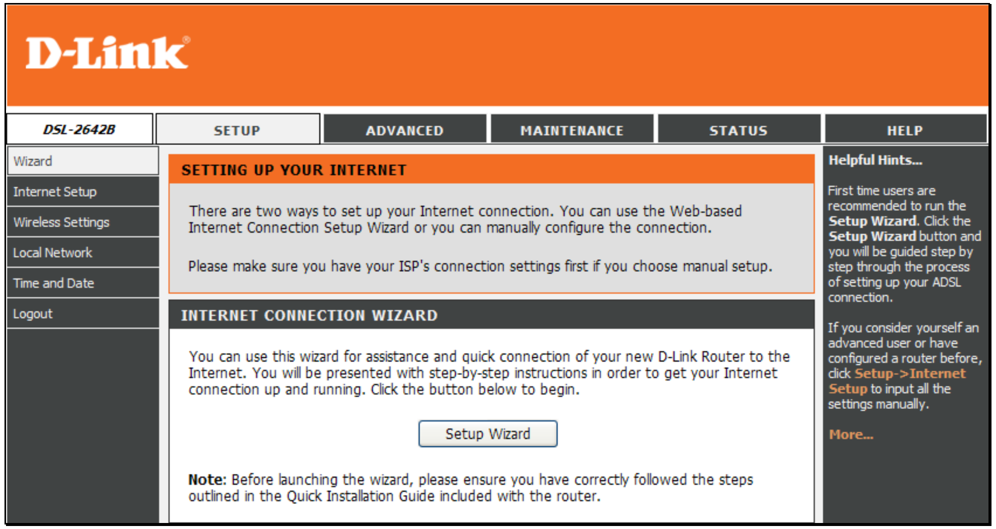
Password :

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 D-Link 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.

Helpful Hints...

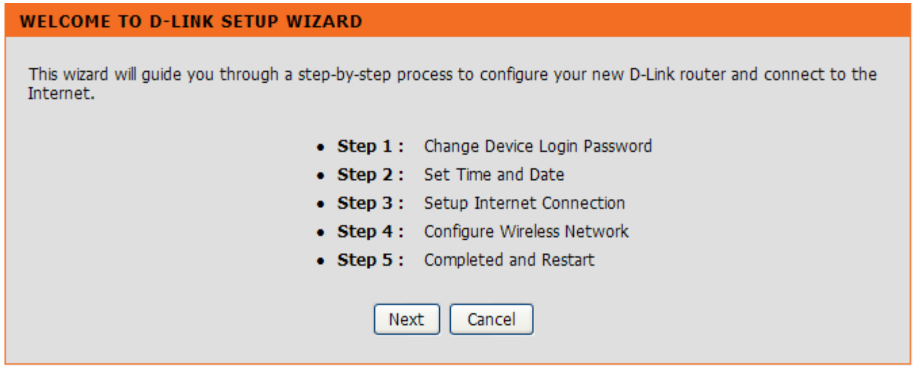
First time users are recommended to run the **Setup Wizard**. Click the **Setup Wizard** button and you will be guided step by step through the process of setting up your ADSL connection.

If you consider yourself an advanced user or have configured a router before, click **Setup->Internet Setup** to input all the settings manually.

QUICK SETUP – WELCOME TO D-LINK SETUP WIZARD

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 D-LINK SETUP WIZARD

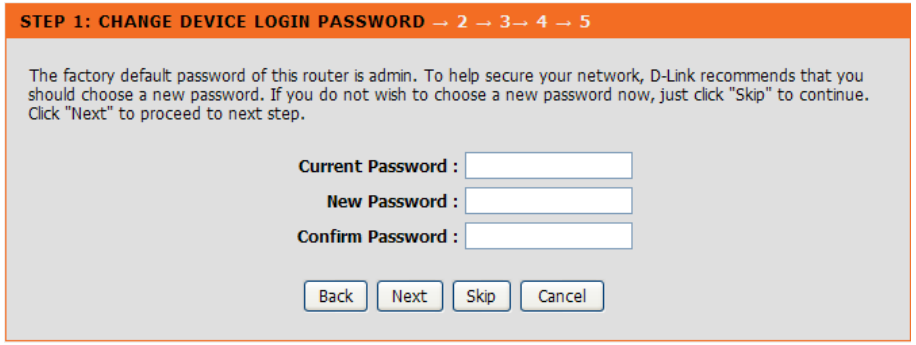
This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

- **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 DEVICE LOGIN PASSWORD

This window of the Setup Wizard is used to change the Router password. D-Link recommends to help secure your network, the user 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, D-Link recommends 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.

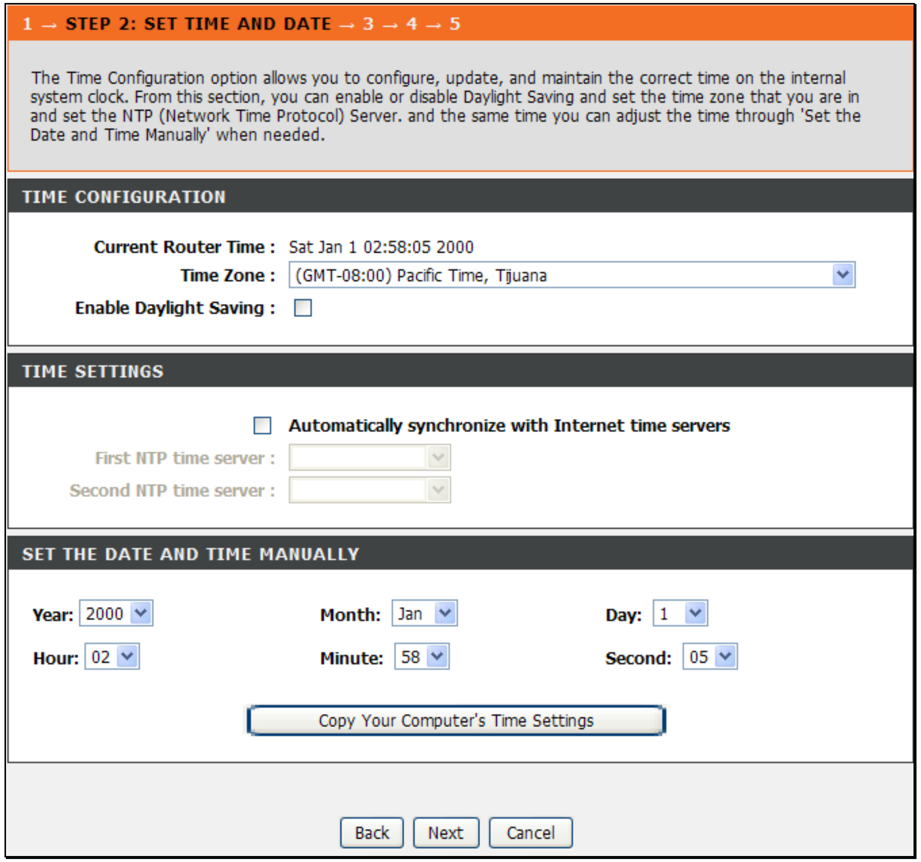
Select a time zone in which you are located from the **Time Zone** list.

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

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

Click **Copy Your computer's Time Settings** to synchronize the Router's time with your computer.

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 02:58:05 2000

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

Enable Daylight Saving : □

TIME SETTINGS

□ Automatically synchronize with Internet time servers

First NTP time server :

Second NTP time server :

SET THE DATE AND TIME MANUALLY

Year: 2000 Month: Jan Day: 1

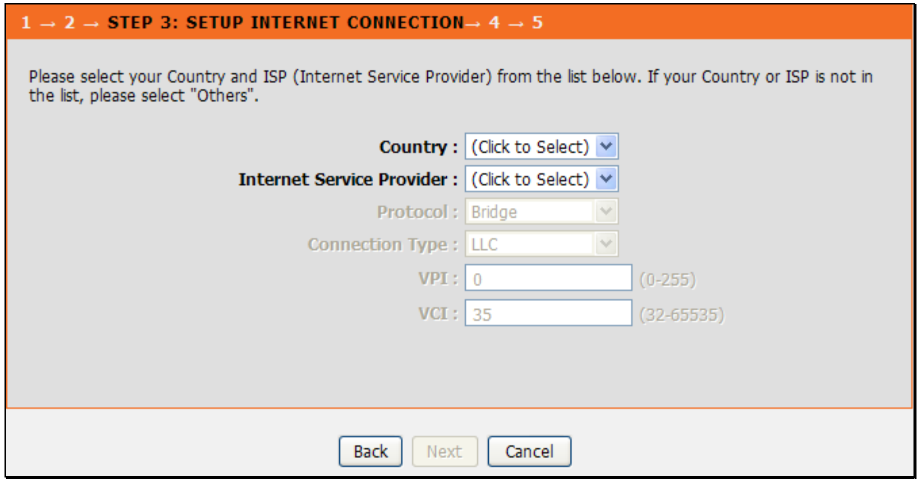
Hour: 02 Minute: 58 Second: 05

QUICK SETUP – SETUP INTERNET CONNECTION

Now use the drop-down menus to select the Country, Internet Service Provider (ISP), 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 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 : (Click to Select)
Internet Service Provider : (Click to Select)
Protocol : Bridge
Connection Type : LLC
VPI : 0 (0-255)
VCI : 35 (32-65535)

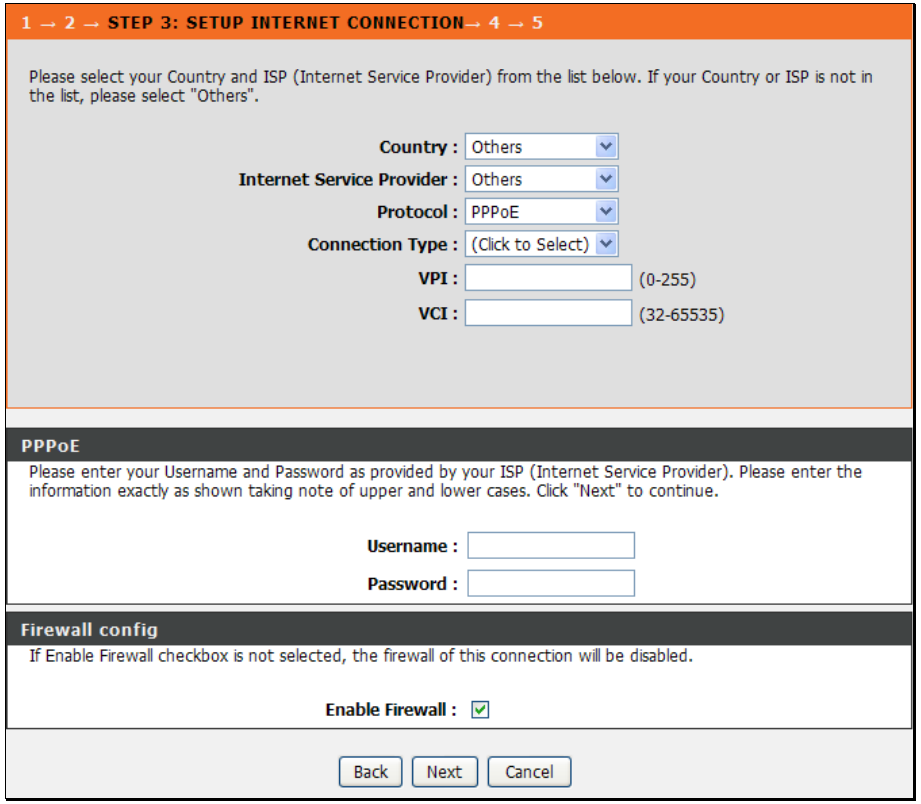
QUICK SETUP – PPPOE/PPPOA CONFIGURATION

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 at the bottom of this Setup Wizard window. For PPPoE/PPPoA protocol, the available connection and encapsulation types are *VC-Mux* and *LLC*.

Tick the **Enable Firewall** check box to enable the firewall function of this connection.

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 : PPPoE

Connection Type : (Click to Select)

VPI : (0-255)

VCI : (32-65535)

PPPoE

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 :

Firewall config

If Enable Firewall checkbox is not selected, the firewall of this connection will be disabled.

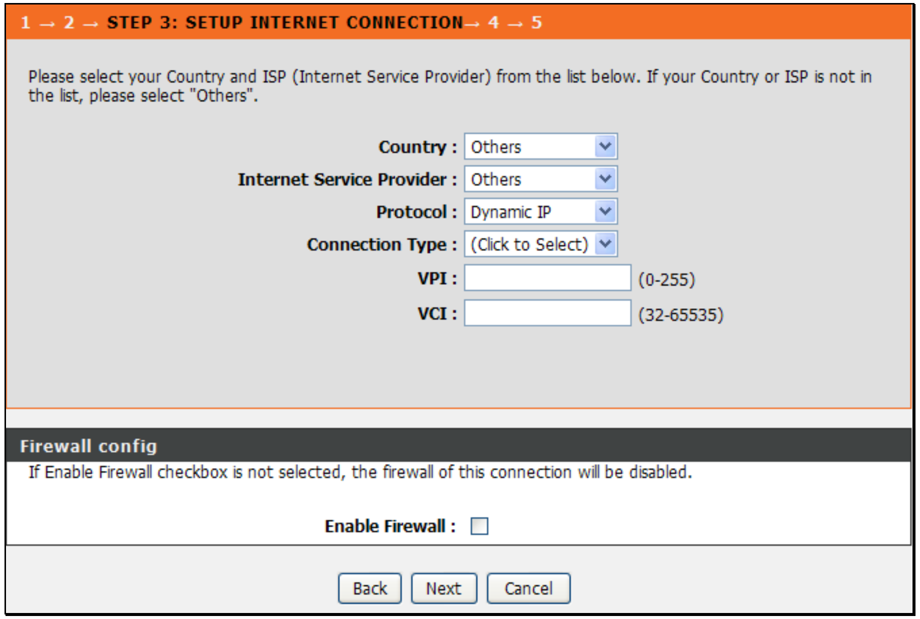
Enable Firewall : ☑

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*.

Tick the **Enable Firewall** check box to enable the firewall function of this connection

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)

Firewall config

If Enable Firewall checkbox is not selected, the firewall of this connection will be disabled.

Enable Firewall : □

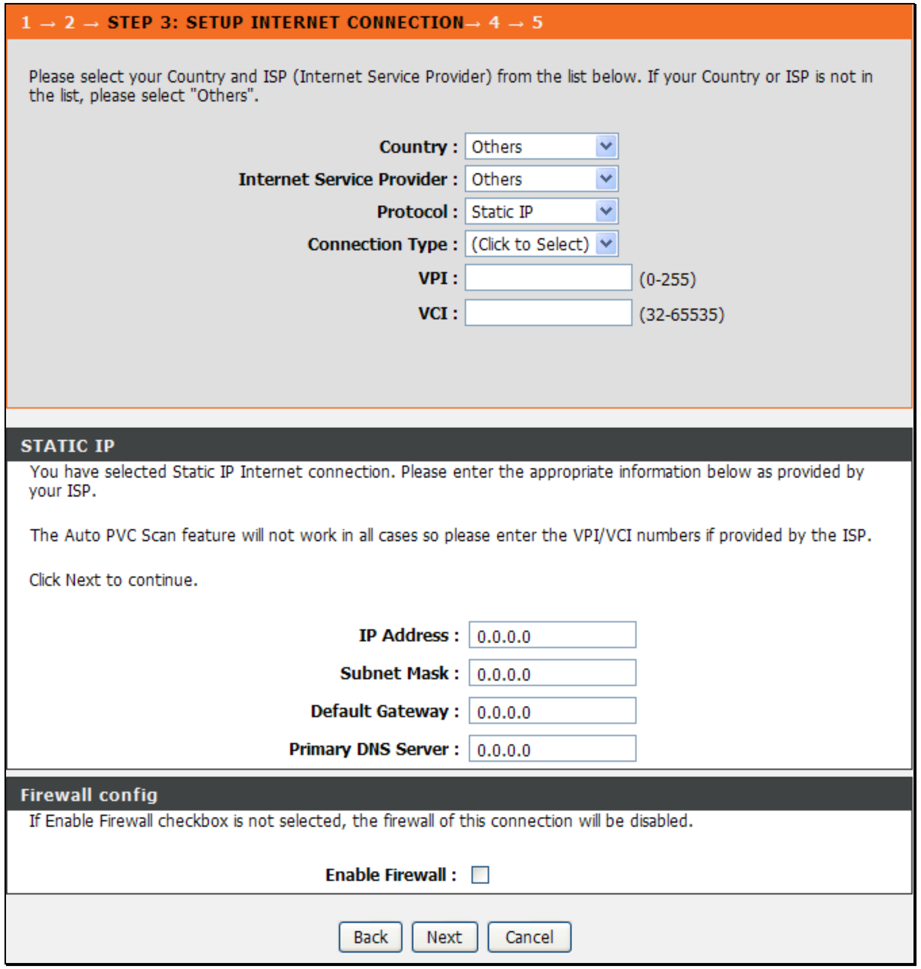
QUICK SETUP – STATIC IP CONFIGURATION

Enter values for VPI, VCI, IP Address, Subnet Mask, Default Gateway IP address, and Primary DNS as 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*.

Tick the **Enable Firewall** check box to enable the firewall function of this connection

Select **Bridge** 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 :	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

Firewall config

If Enable Firewall checkbox is not selected, the firewall of this connection will be disabled.

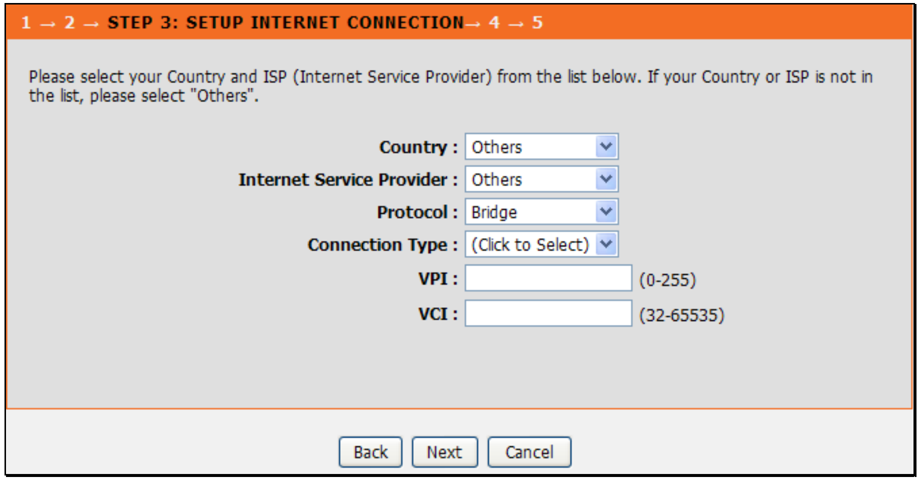
Enable Firewall : □

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 the **Next** button to continue.



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".

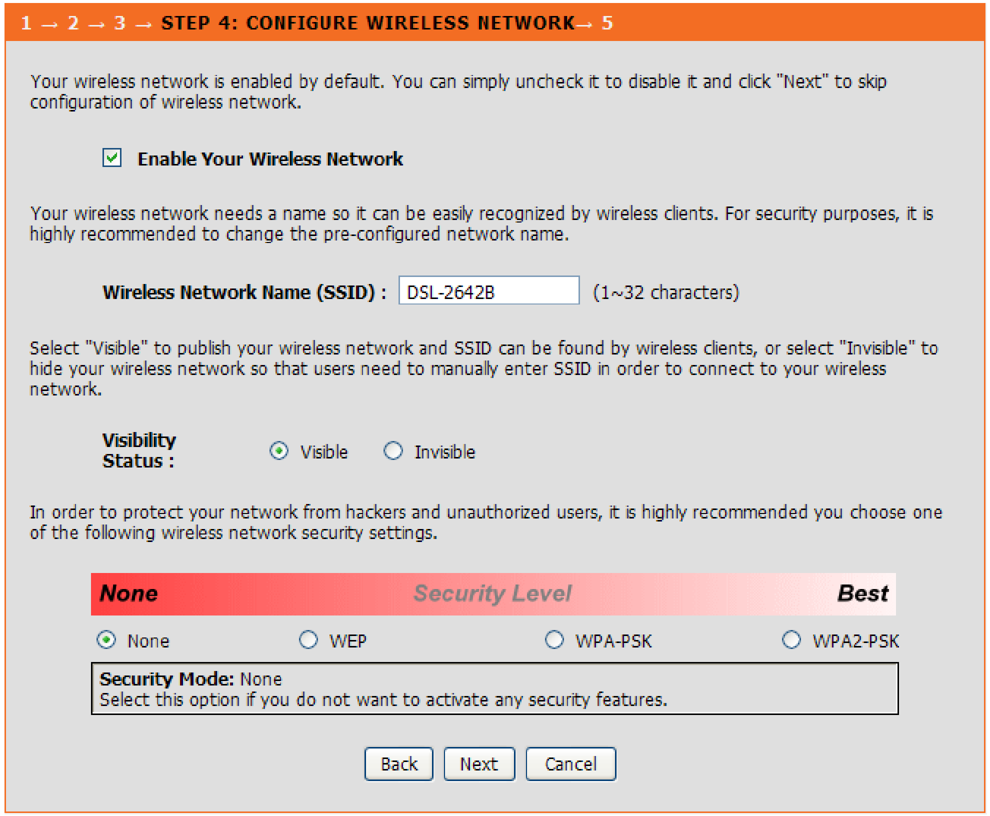
Country :	Others
Internet Service Provider :	Others
Protocol :	Bridge
Connection Type :	(Click to Select)
VPI :	(0-255)
VCI :	(32-65535)

QUICK SETUP – CONFIGURE WIRELESS NETWORK

Select **Enable your Wireless Network** by default and configure the SSID, the Visibility Status of SSID and the Wireless network security. The Wireless Network will be unsecure if the **Security Level** is set to **None**. There are 3 security options the user can choose: **WEP, WPA-PSK** or **WPA2-PSK**. After selecting the Security mode, enter the security key below.

Deselect **Enable your Wireless Network** for skipping the wireless configurations.

Click the **Next** button to go to the last step.



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) : DSL-2642B (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.

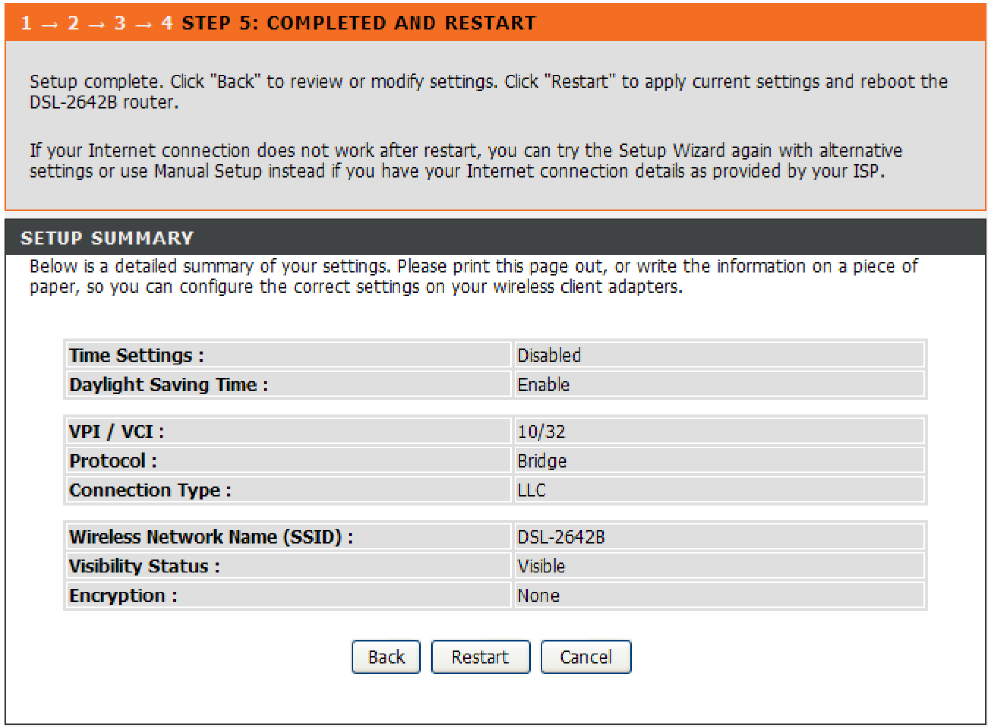
None *Security Level* *Best*

● None ○ WEP ○ WPA-PSK ○ WPA2-PSK

Security Mode: None
Select this option if you do not want to activate any security features.

QUICK SETUP – COMPLETED & RESTART

Finally you can see the Setup Summary of the configurations you did through the wizard. If all the necessary information that you have entered is correct, 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-2642B 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.

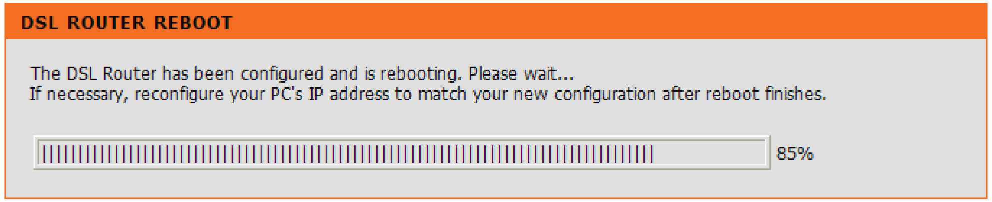
SETUP SUMMARY

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
Daylight Saving Time :	Enable
VPI / VCI :	10/32
Protocol :	Bridge
Connection Type :	LLC
Wireless Network Name (SSID) :	DSL-2642B
Visibility Status :	Visible
Encryption :	None

QUICK SETUP – DSL ROUTER REBOOT

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



DSL ROUTER REBOOT

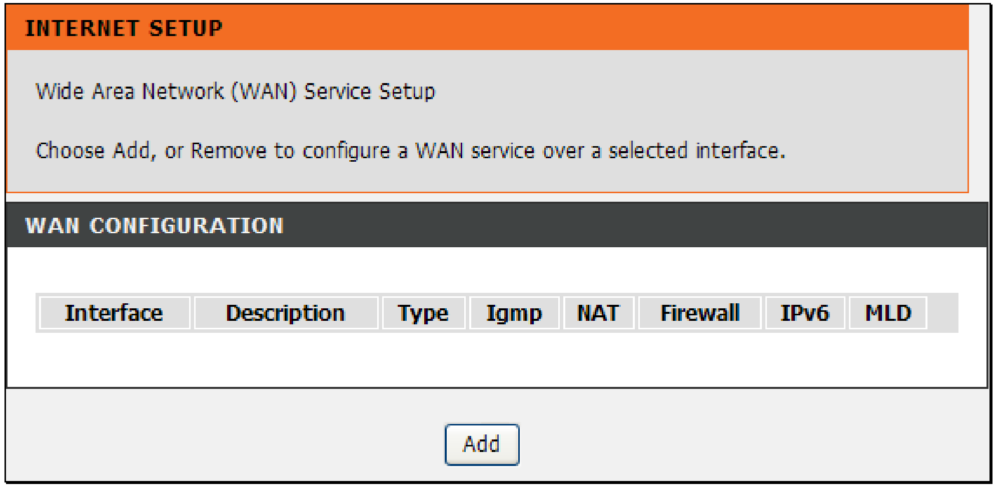
The DSL Router has been configured and is rebooting. Please wait...
If necessary, reconfigure your PC's IP address to match your new configuration after reboot finishes.

Internet Setup

To access the **Internet Setup** window, click **Internet Setup** in the **Setup** directory.

In this page, all available WAN connection displays in the table. Click the corresponding 📝 button to edit the connection. Click the corresponding 🗑 button to delete the connection.

Click the **Add** button to see the window in the next page for adding a WAN connection.



INTERNET SETUP

Wide Area Network (WAN) Service Setup

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

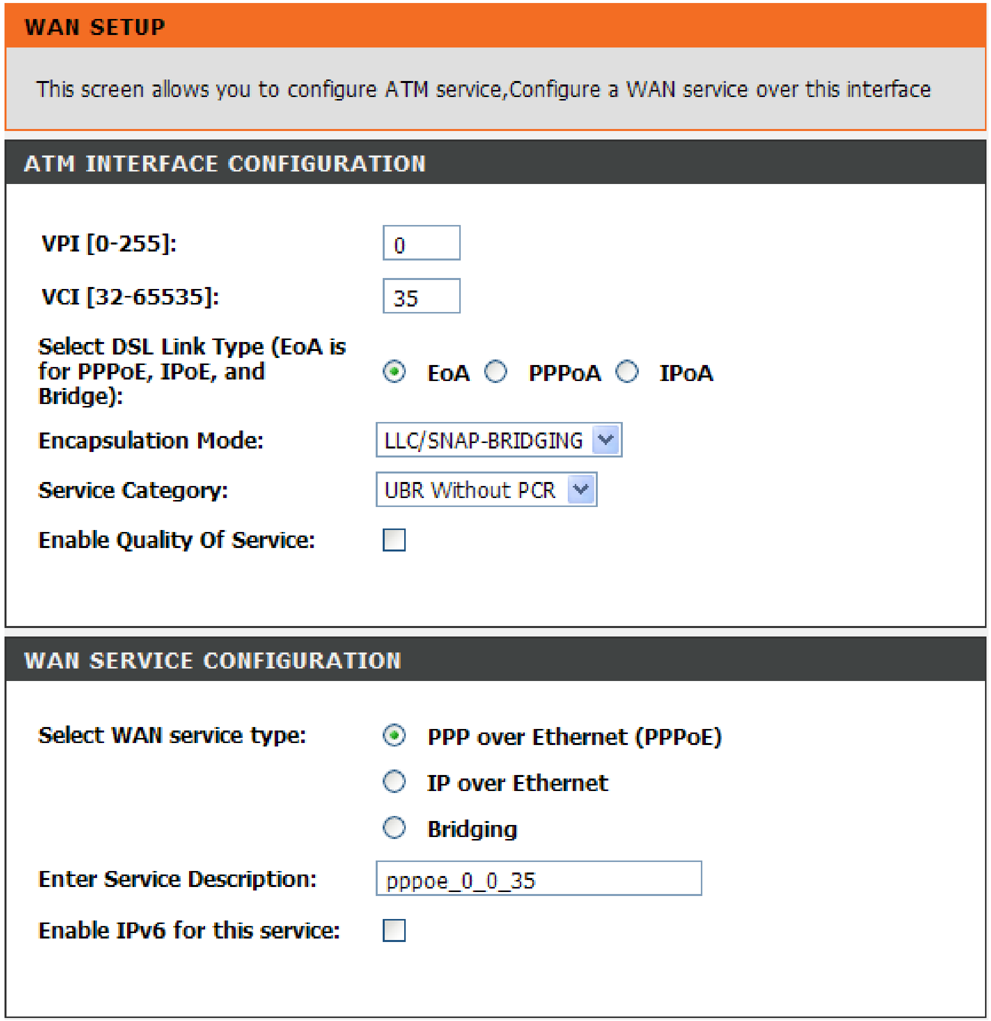
WAN CONFIGURATION

Interface	Description	Type	Igmp	NAT	Firewall	IPv6	MLD

PPP over Ethernet (PPPoE)

VPI: Enter the correct VPI used here.
VCI: Enter the correct VCI used here.
Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE, IPoE and Bridge Modes, select EoA.
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 the **PPP over Ethernet (PPPoE)** radio button to configure PPPoE mode.
Enter Service Description: This field will display an automated service description.
Enable IPv6 for this service: Tick this option to enable IPv6.



WAN SETUP

This screen allows you to configure ATM service,Configure a WAN service over this interface

ATM INTERFACE CONFIGURATION

VPI [0-255]: 0

VCI [32-65535]: 35

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: □

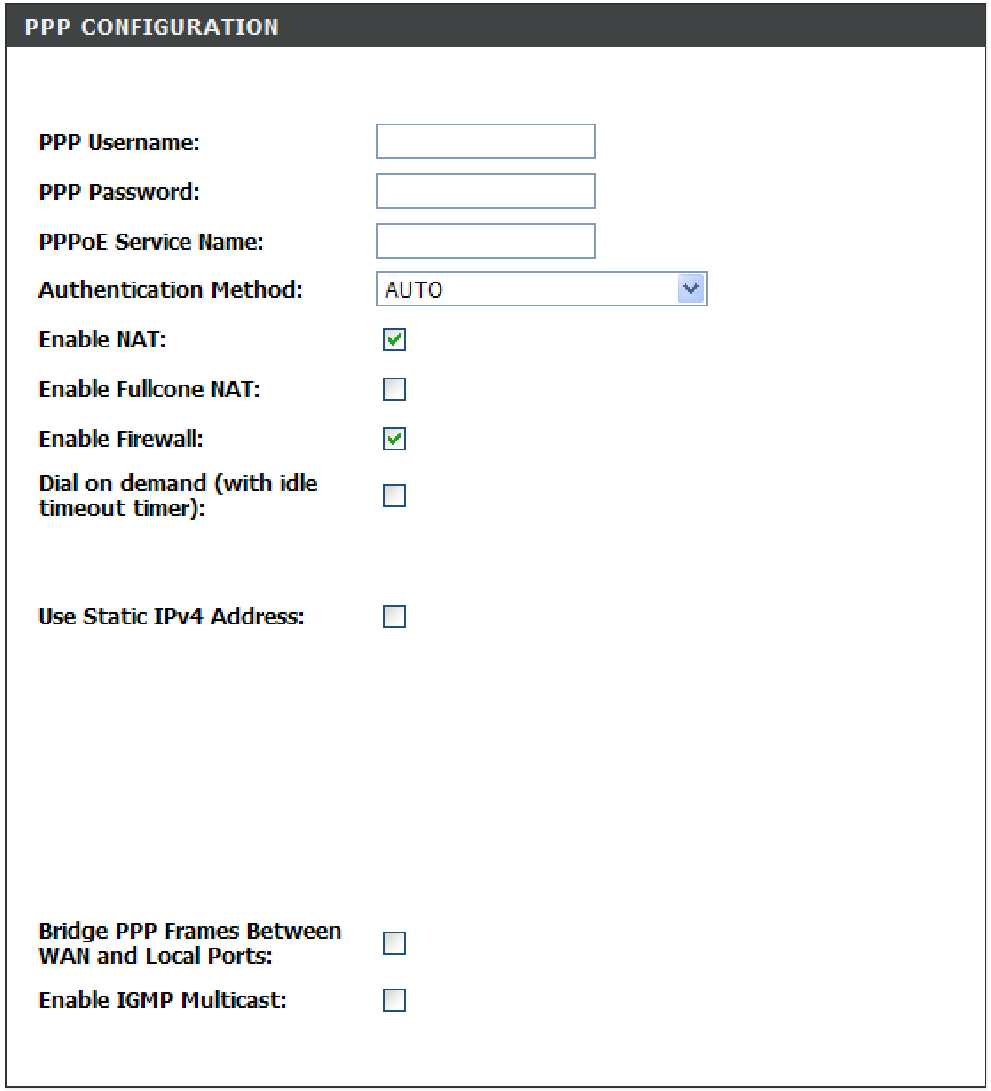
WAN SERVICE CONFIGURATION

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

Enter Service Description: pppoe_0_0_35

Enable IPv6 for this service: □

PPP Username: Enter the account username in here.
PPP Password: Enter the account password in here.
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.
Enable Fullcone NAT: Tick this option to enable Fullcone NAT for this connection.
Enable Firewall: Tick this option to enable firewall for this connection.
Dial on demand: Tick this option to enable dial on demand for this connection.
Inactivity Timeout: The option appears when **Dial on demand** is selected. Enter an inactivity timeout value here. Leave this option on 0 to disable this option.
Use Static IPv4 Address: Tick this option to use a Static IP version 4 address for this connection.
IPv4 Address: The option appears when **Use Static IPv4 Address** is selected. Enter the Static IP version 4 address used here.
Bridge PPP Frames Between WAN and Local Ports: Tick this option to bridge PPPoE frames between WAN and local ports.
Enable IGMP Multicast: Tick this option to allow IGMP packets to go through the WAN interface in both directions.



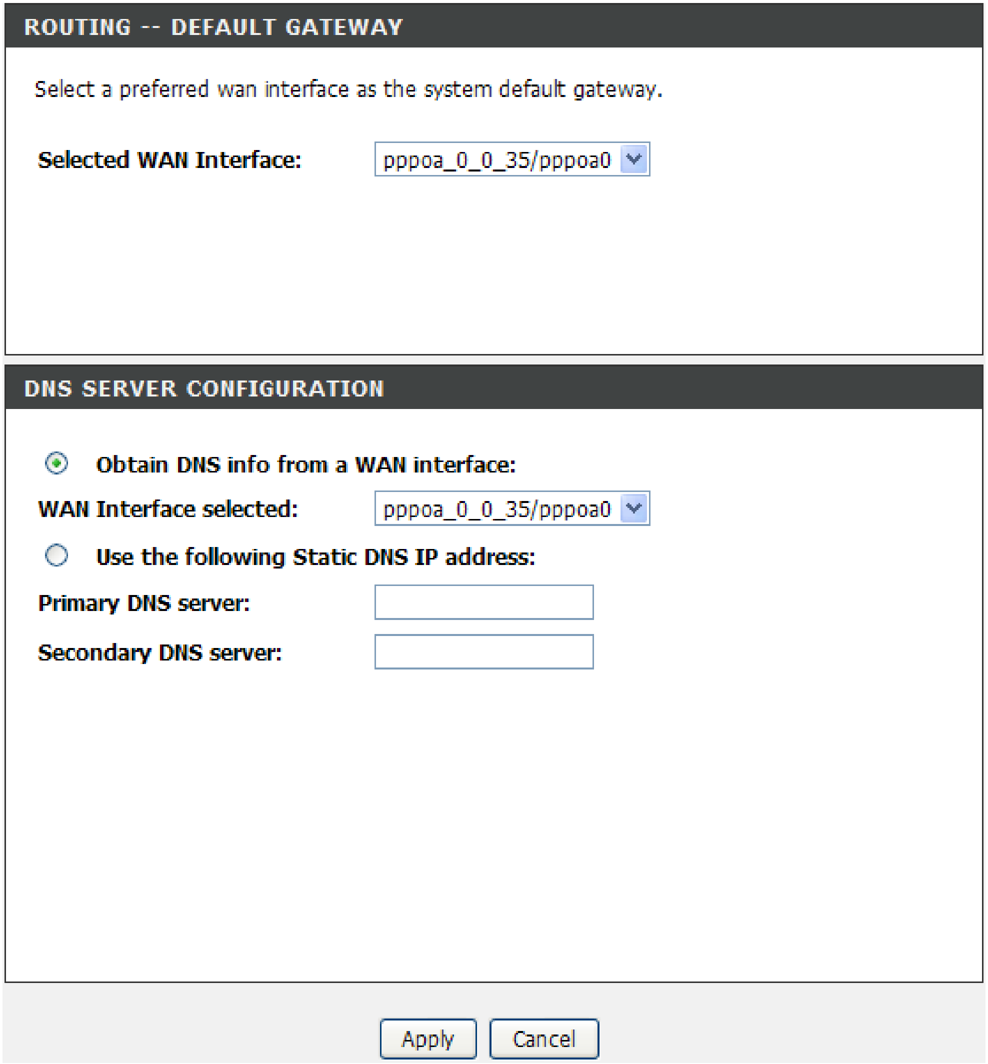
PPP CONFIGURATION

PPP Username:	
PPP Password:	
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 PPP Frames Between WAN and Local Ports:	□
Enable IGMP Multicast:	□

Selected WAN Interface: Use the drop-down menu to choose the WAN interface to use this connection.

Obtain DNS info from a WAN interface: Click the radio button to obtain DNS Server IP addresses automatically from the ISP.
User the following Static DNS IP address: click the radio button to manually enter the Primary and Secondary DNS Server IP addresses 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: pppoa_0_0_35/pppoa0

DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoa_0_0_35/pppoa0

○ Use the following Static DNS IP address:

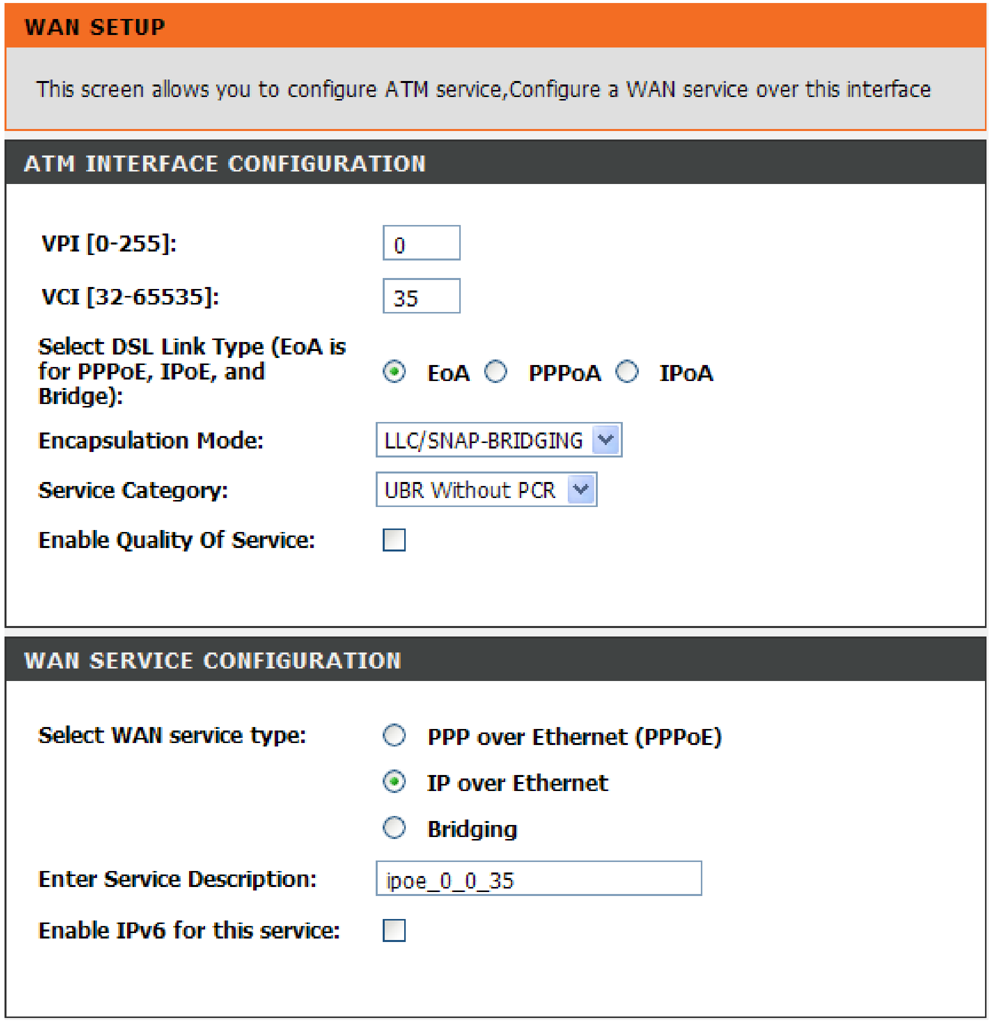
Primary DNS server:

Secondary DNS server:

IP over Ethernet (IPoE)

VPI: Enter the correct VPI used here.
VCI: Enter the correct VCI used here.
Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE, IPoE and Bridge Modes, select EoA.
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 the **IP over Ethernet** radio button to configure IPoE mode.
Enter Service Description: This field will display an automated service description.
Enable IPv6 for this service: Tick this option to enable IPv6.



WAN SETUP

This screen allows you to configure ATM service,Configure a WAN service over this interface

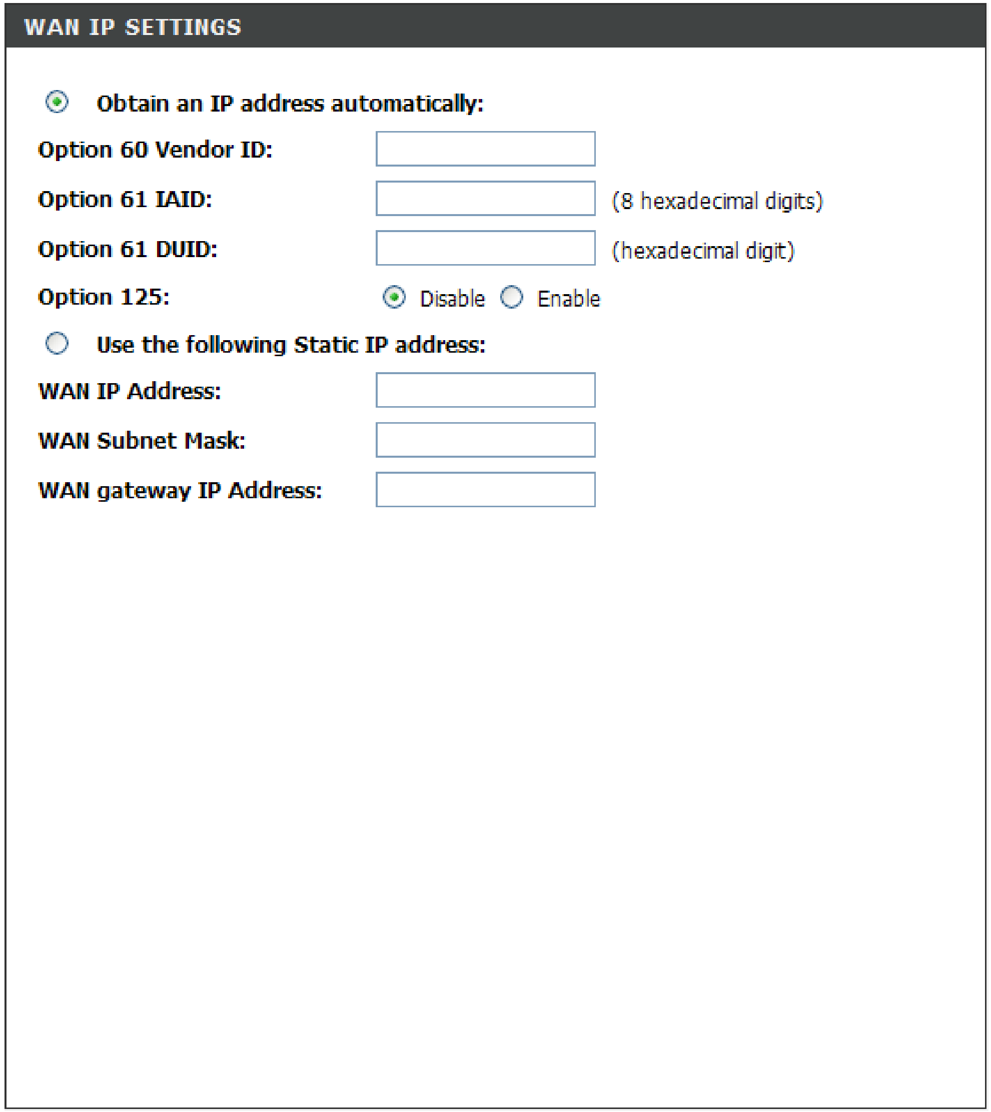
ATM INTERFACE CONFIGURATION

VPI [0-255]:	0
VCI [32-65535]:	35
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:	ipoe_0_0_35
Enable IPv6 for this service:	□

Obtain an IP address automatically: Click the radio button to automatically obtain an IP address from the DHCP server.
Option 60 Vendor ID: The option code 60 used to identify Vendor class.
Option 61 IAID: Identity Association ID (IAID) assigns an IAID to individual interfaces. If the device is functioning with a single DHCP client identity, it must use value 1 for IAID for all DHCP interactions. If the device is functioning with multiple DHCP client identities, the values of IAID have to start at 1 for the first identity and be incremented for each subsequent identity.
Option 61 DUID: Enter the unique name of the interface when exchange the DHCP messages.
Option 125: Click the **Enable** radio button to allow DHCP server to be pre-configured with policy for handling classes of devices in a certain way without requiring DHCP server to be able to parse the unique format used in client-identifier option.
Use the following Static IP address: Click the radio button to use static IP for the connection.
WAN IP Address: Enter the static IP address for the connection.
WAN Subnet mask: Enter the subnet mask of the static IP address.
WAN gateway IP Address: Enter the gateway of the static IP address.



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

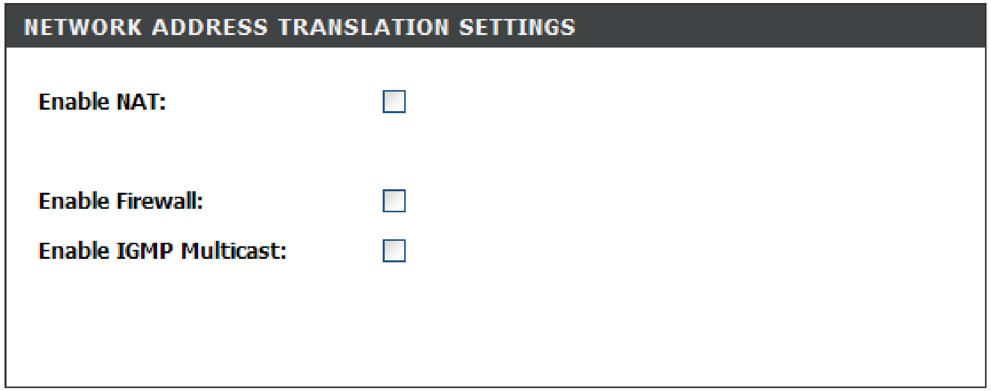
○ **Use the following Static IP address:**

WAN IP Address:

WAN Subnet Mask:

WAN gateway IP Address:

Enable NAT: Tick this option to enable NAT for this connection.
Enable Fullcone NAT: The option appears only when **Enable NAT** is selected. 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.



NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT: □

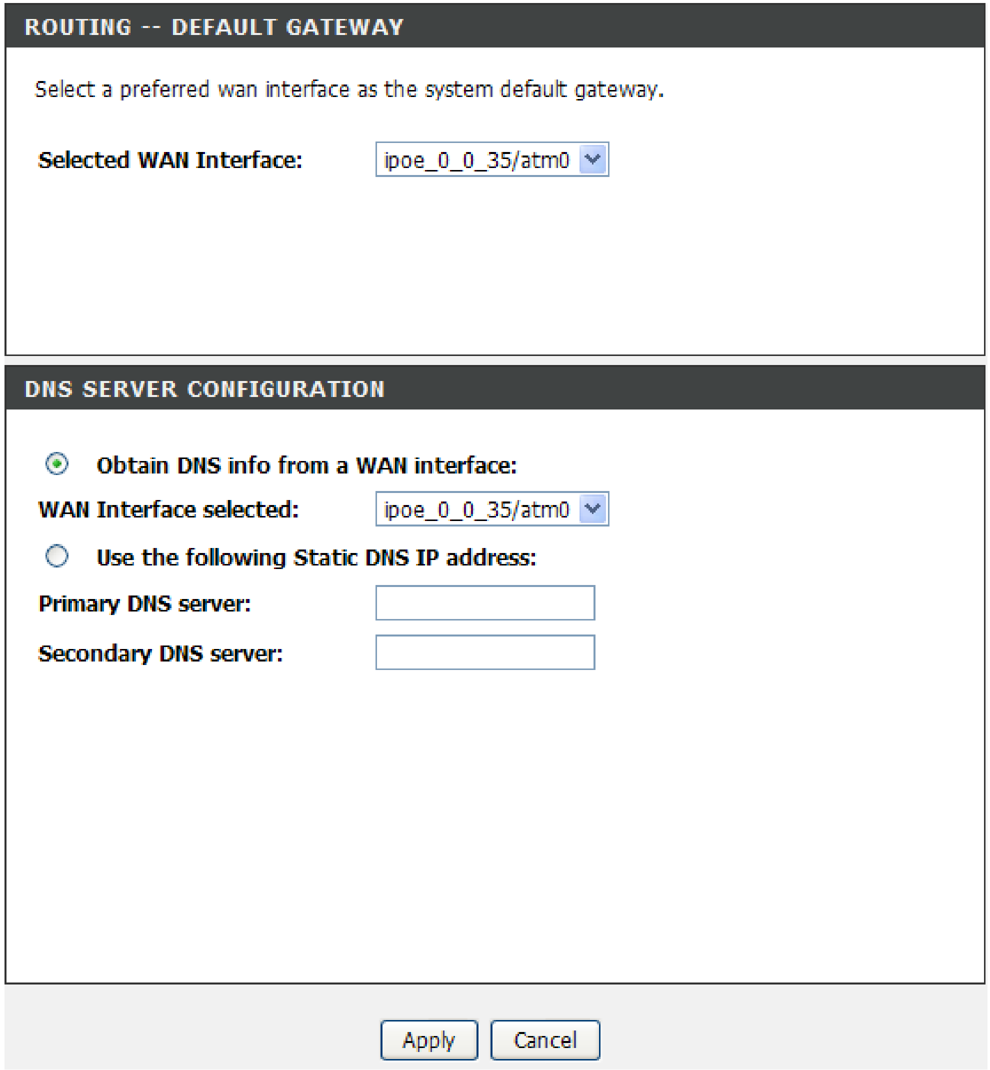
Enable Firewall: □

Enable IGMP Multicast: □

Selected WAN Interface: Use the drop-down menu to choose the WAN interface to use this connection.

Obtain DNS info from a WAN interface: Click the radio button to obtain DNS Server IP addresses automatically from the ISP.
User the following Static DNS IP address: click the radio button to manually enter the Primary and Secondary DNS Server IP addresses 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: ipoe_0_0_35/atm0

DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected: ipoe_0_0_35/atm0

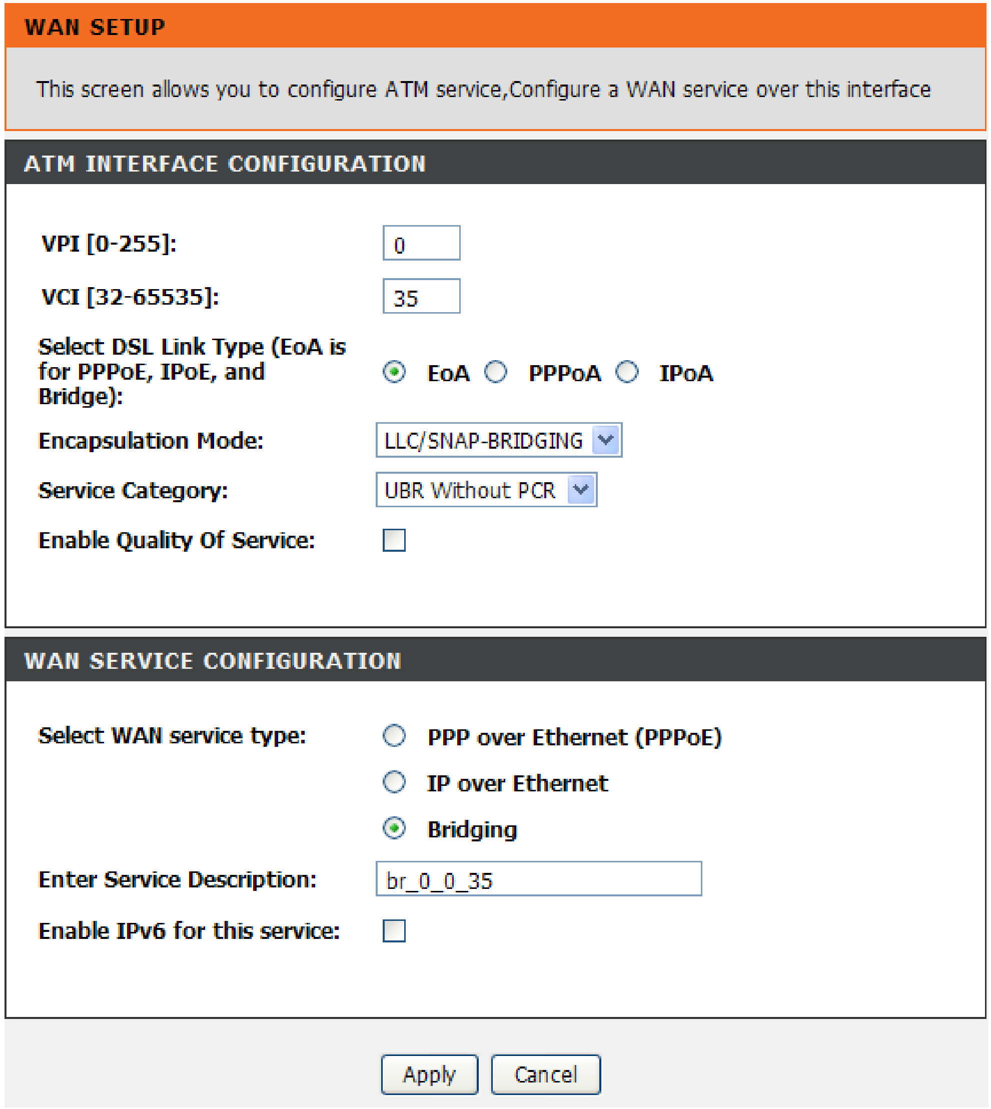
○ Use the following Static DNS IP address:

Primary DNS server:

Secondary DNS server:

Bridging

VPI: Enter the correct VPI used here.
VCI: Enter the correct VCI used here.
Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE, IPoE and Bridge Modes, select EoA.
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.



WAN SETUP

This screen allows you to configure ATM service,Configure a WAN service over this interface

ATM INTERFACE CONFIGURATION

VPI [0-255]:	0
VCI [32-65535]:	35
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_0_35
Enable IPv6 for this service:	□

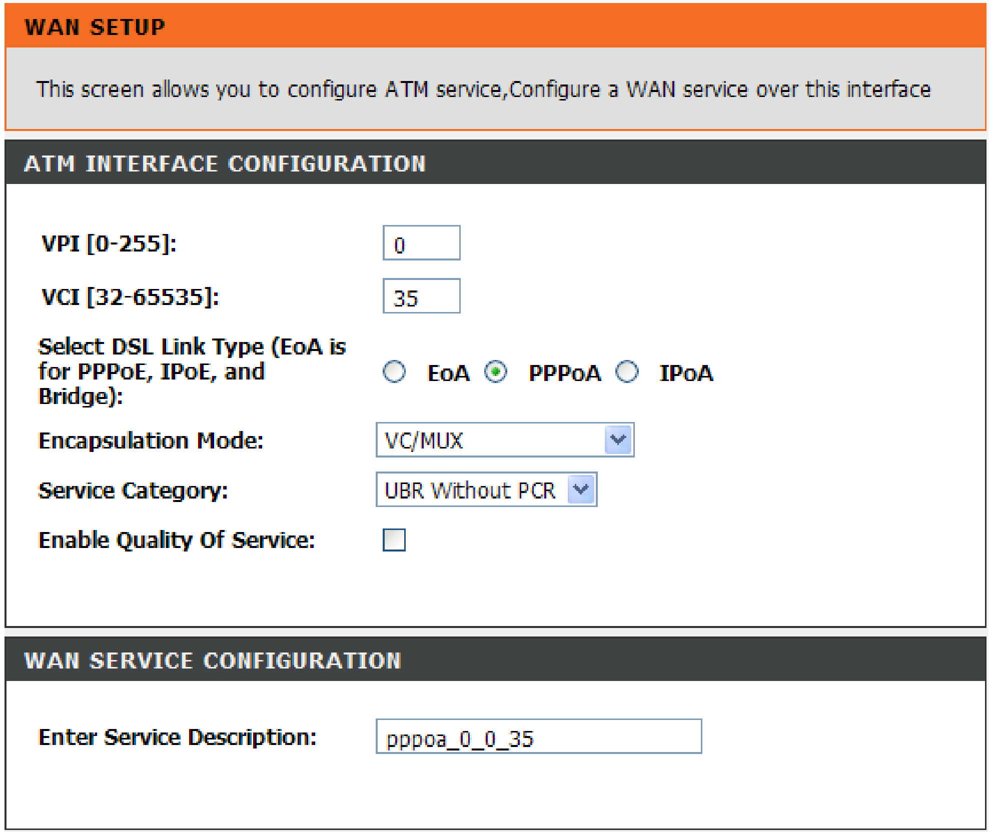
Select WAN service type: Choose the appropriate WAN Service Type here. Click the **Bridging** radio button to configure bridge mode.
Enter Service Description: This field will display an automated service description.
Enable IPv6 for this service: Tick this option to enable IPv6.

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

PPP over ATM (PPPoA)

VPI: Enter the correct VPI used here.
VCI: Enter the correct VCI used here.
Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE, IPoE and Bridge Modes, select EoA.
Encapsulation Mode: Choose the appropriate Encapsulation Mode here. Click the **PPPoA** radio button to configure PPPoA mode.
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 SETUP

This screen allows you to configure ATM service,Configure a WAN service over this interface

ATM INTERFACE CONFIGURATION

VPI [0-255]: 0

VCI [32-65535]: 35

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

Encapsulation Mode: VC/MUX

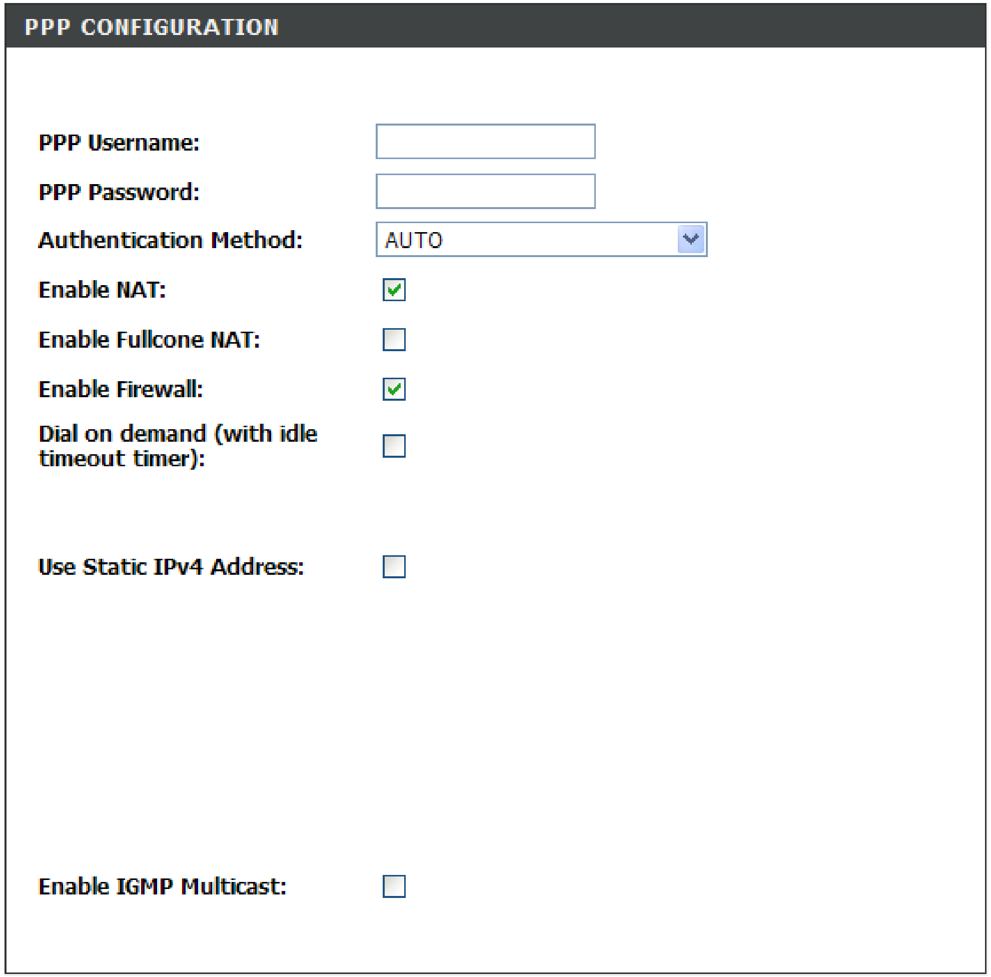
Service Category: UBR Without PCR

Enable Quality Of Service: □

WAN SERVICE CONFIGURATION

Enter Service Description: pppoa_0_0_35

PPP Username: Enter the account username in here.
PPP Password: Enter the account password in here.
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.
Enable Fullcone NAT: Tick this option to enable Fullcone NAT for this connection.
Enable Firewall: Tick this option to enable firewall for this connection.
Dial on demand: Tick this option to enable dial on demand for this connection.
Inactivity Timeout: The option appears when **Dial on demand** is selected. Enter an inactivity timeout value here. Leave this option on 0 to disable this option.
Use Static IPv4 Address: Tick this option to use a Static IP version 4 address for this connection.
IPv4 Address: The option appears when **Use Static IPv4 Address** is selected. 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.



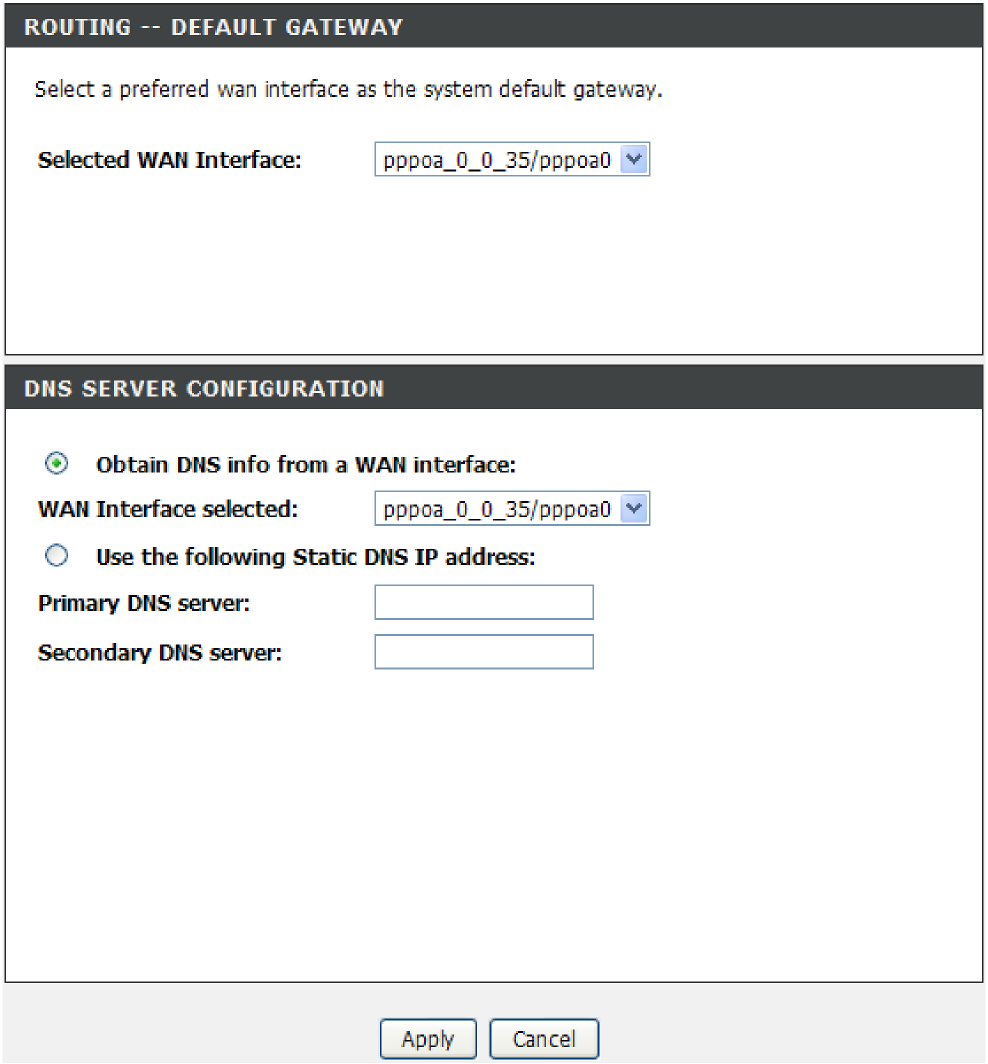
PPP CONFIGURATION

PPP Username:	
PPP Password:	
Authentication Method:	AUTO
Enable NAT:	☑
Enable Fullcone NAT:	□
Enable Firewall:	☑
Dial on demand (with idle timeout timer):	□
Use Static IPv4 Address:	□
Enable IGMP Multicast:	□

Selected WAN Interface: Use the drop-down menu to choose the WAN interface to use this connection.

Obtain DNS info from a WAN interface: Click the radio button to obtain DNS Server IP addresses automatically from the ISP.
User the following Static DNS IP address: click the radio button to manually enter the Primary and Secondary DNS Server IP addresses 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: pppoa_0_0_35/pppoa0

DNS SERVER CONFIGURATION

● Obtain DNS info from a WAN interface:

WAN Interface selected: pppoa_0_0_35/pppoa0

○ Use the following Static DNS IP address:

Primary DNS server:

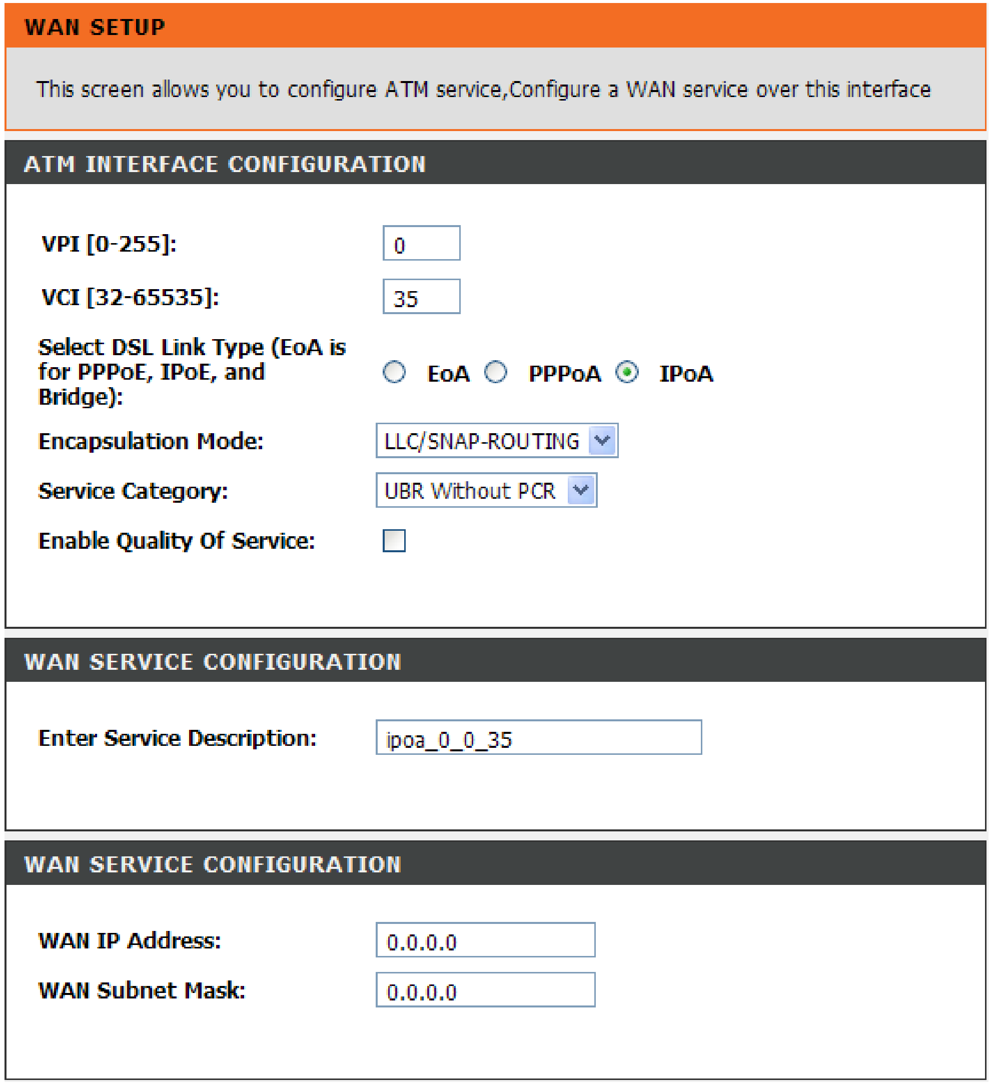
Secondary DNS server:

IP over ATM (IPoA)

VPI: Enter the correct VPI used here.
VCI: Enter the correct VCI used here.
Select DSL Link Type: Select the correct DSL Link Type here. For PPPoE, IPoE and Bridge Modes, select EoA. Click the **IPoA** radio button to configure IPoA mode.
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 Configureation: Choose the appropriate WAN Service Type here.

WAN IP Address: Enter the WAN IP address used here.
WAN Subnet Mask: Enter the subnet of the WAN IP address.



WAN SETUP

This screen allows you to configure ATM service,Configure a WAN service over this interface

ATM INTERFACE CONFIGURATION

VPI [0-255]:	0
VCI [32-65535]:	35
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_0_35

WAN SERVICE CONFIGURATION

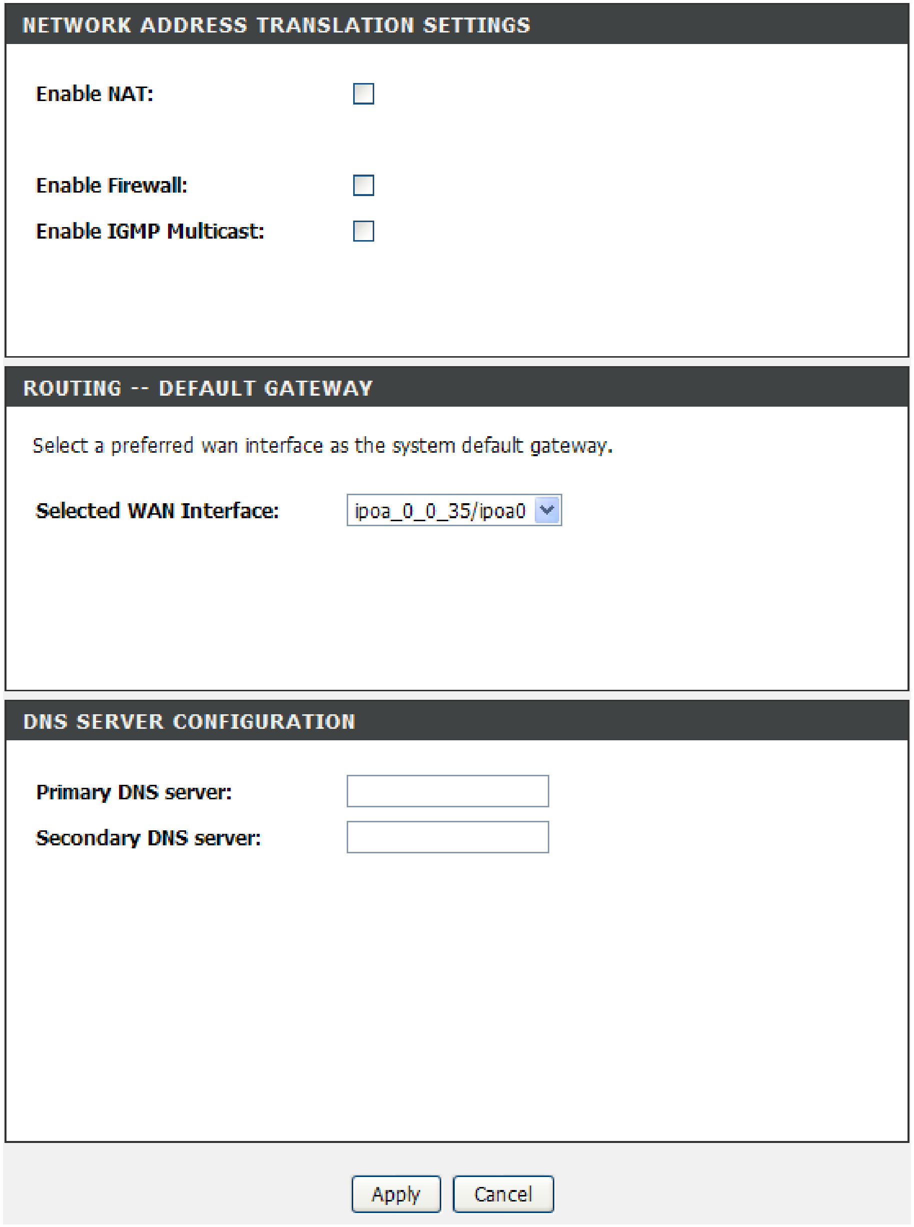
WAN IP Address:	0.0.0.0
WAN Subnet Mask:	0.0.0.0

Enable NAT: Tick this option to enable NAT for this connection.
Enable Fullcone NAT: he option appears when **Enable NAT** is selected. 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: Use the drop-down menu to choose the WAN interface to use this connection.

Primary/Secondary DNS server: Enter the Primary and Secondary DNS Server IP addresses for this connection.

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



NETWORK ADDRESS TRANSLATION SETTINGS

Enable NAT: □

Enable Firewall: □

Enable IGMP Multicast: □

ROUTING -- DEFAULT GATEWAY

Select a preferred wan interface as the system default gateway.

Selected WAN Interface: ipoa_0_0_35/ipoa0

DNS SERVER CONFIGURATION

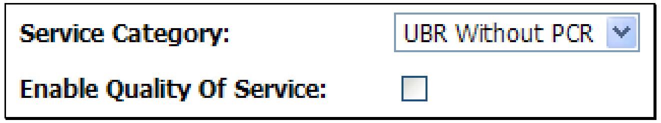
Primary DNS server:

Secondary DNS server:

There are 5 different variations in the **Service Category** drop-down menu when configuring the abovementioned connections.

UBR Without PCR

There is no additional field listed when choosing this category.

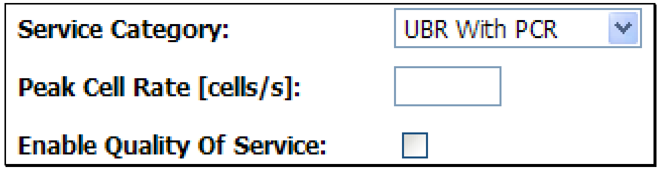


Service Category: UBR Without PCR

Enable Quality Of Service: □

UBR With PCR

Peak Cell Rate: Here the user can enter the Peak Cell Rate used.



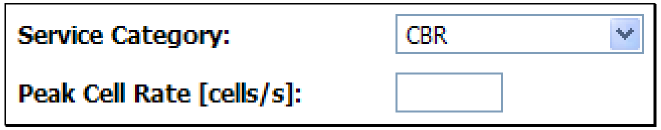
Service Category: UBR With PCR

Peak Cell Rate [cells/s]:

Enable Quality Of Service: □

CBR

Peak Cell Rate: Here the user can enter the Peak Cell Rate used.

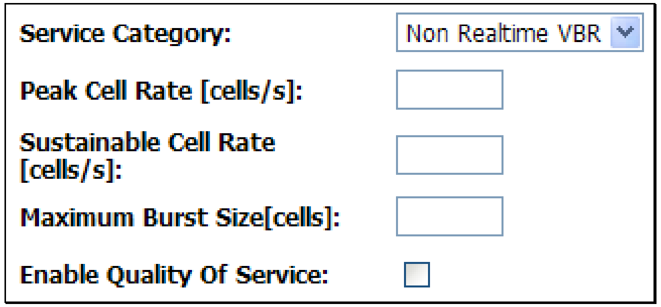


Service Category: CBR

Peak Cell Rate [cells/s]:

Non Realtime VBR

Peak Cell Rate: Here the user can enter the Peak Cell Rate used.
Sustainable Cell Rate: Here the user can enter the Sustainable Cell Rate used.
Maximum Burst Size: Here the user can enter the Maximum Burst Size used.



Service Category: Non Realtime VBR

Peak Cell Rate [cells/s]:

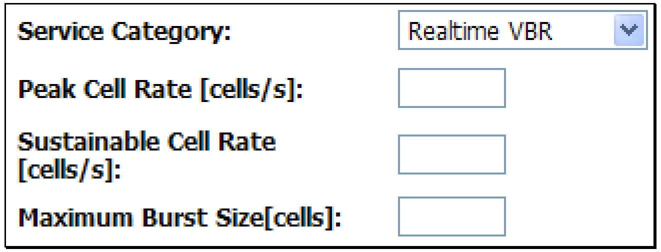
Sustainable Cell Rate [cells/s]:

Maximum Burst Size[cells]:

Enable Quality Of Service: □

Realtime VBR

Peak Cell Rate: Here the user can enter the Peak Cell Rate used.
Sustainable Cell Rate: Here the user can enter the Sustainable Cell Rate used.
Maximum Burst Size: Here the user can enter the Maximum Burst Size used.



Service Category: Realtime VBR

Peak Cell Rate [cells/s]:

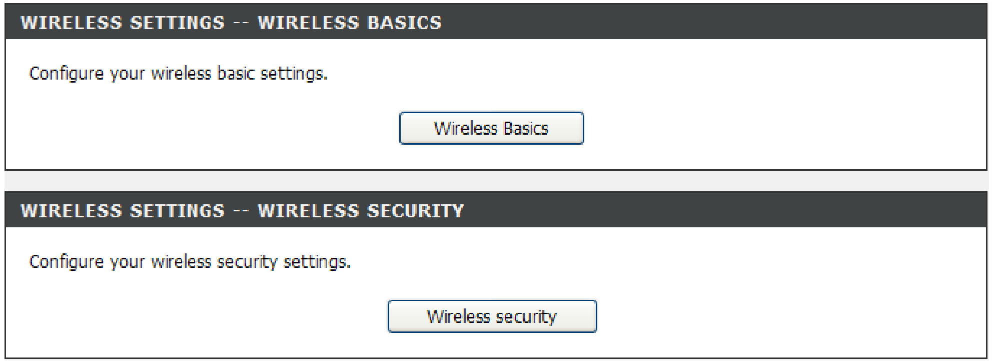
Sustainable Cell Rate [cells/s]:

Maximum Burst Size[cells]:

Wireless Settings

The wireless section is used to configure the wireless settings for the Router. Note that changes made in this section may also need to be duplicated on wireless clients that you want to connect to your wireless network.
To protect your privacy, use the wireless security mode to configure the wireless security features.
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 your wireless security settings.

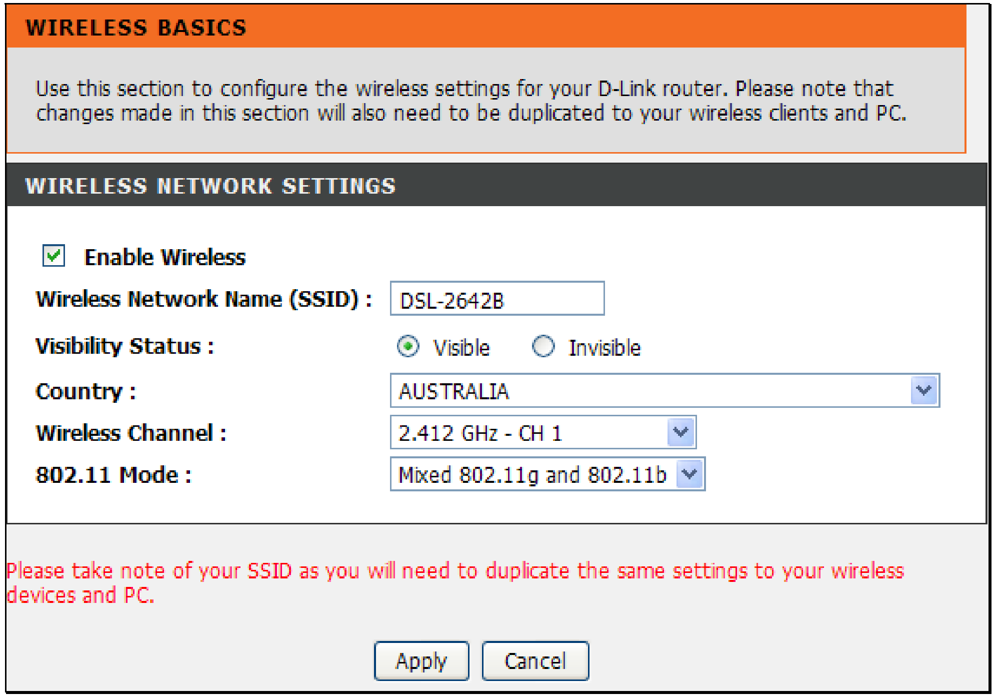
Wireless Basics

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 invisible (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 D-Link 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-2642B

Visibility Status : ● Visible ○ Invisible

Country : AUSTRALIA

Wireless Channel : 2.412 GHz - CH 1

802.11 Mode : Mixed 802.11g and 802.11b

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

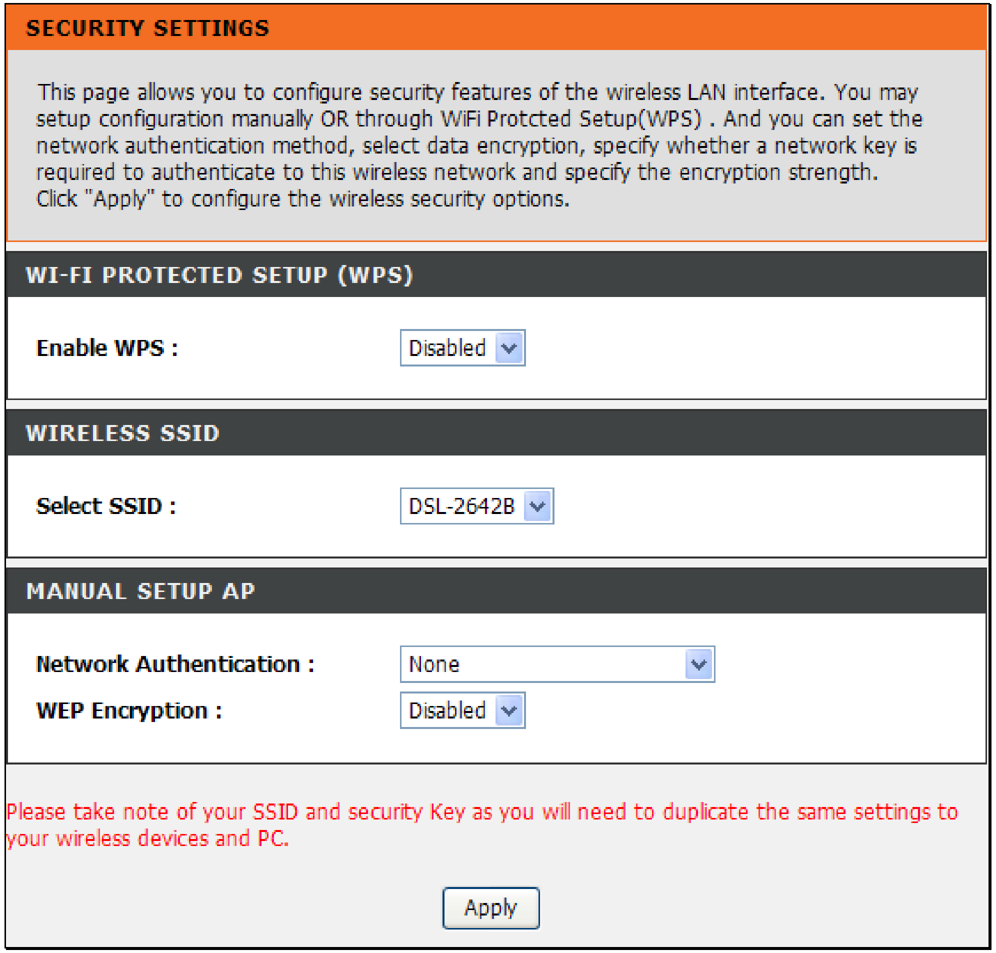
Wireless Security

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.

This page allows you to configure the security of wireless LAN interface. In order to protect the privacy, you can use WiFi Protected Setup (WPS) or setup the wireless security manually. Available security modes are *WEP*, *WPA*, *WPA2* and *Auto*. WPS function will be described in the next section.

For manually configure the wireless security,

1. Select a SSID in the **Wireless Network Name (SSID)** drop-down list.
2. Select a wireless security mode in the **Network Authentication** drop-down menu. Network Authentication methods are *Open*, *Shared*, *802.1X*, *WPA*, *WPA-PSK*, *WPA2*, *WPA2-PSK*, *Mixed WPA2/WPA* and *Mixed WPA2/WPA-PSK*.
3. Configure the security information below.
4. Click the **Apply** button to save the settings.



SECURITY SETTINGS

This page allows you to configure security features of the wireless LAN interface. You may setup configuration manually OR through WiFi Protcted Setup(WPS) . And 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.

WI-FI PROTECTED SETUP (WPS)

Enable WPS : Disabled

WIRELESS SSID

Select SSID : DSL-2642B

MANUAL SETUP AP

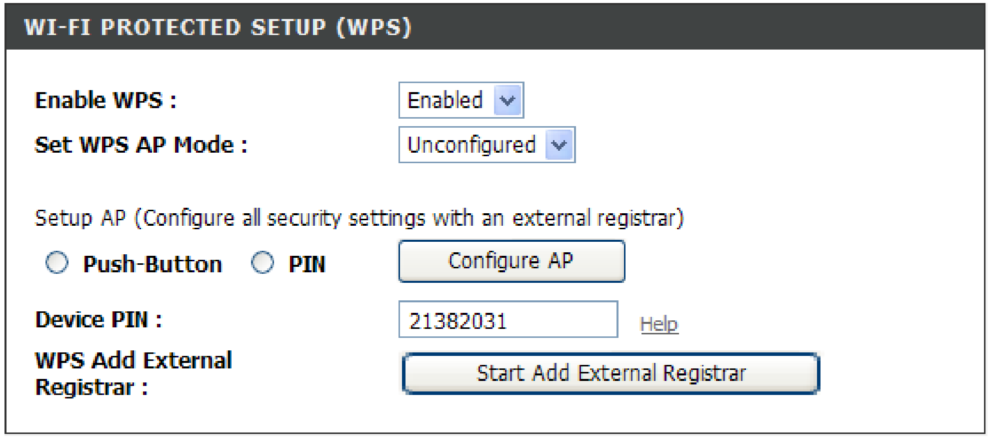
Network Authentication : None

WEP Encryption : Disabled

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

WiFi Protected Setup (WPS)

To implement Wi-Fi protection, select **Enabled** from the **Enable WSC** drop-down menu.
Set WPS AP Mode: Use the drop-down menu to select **Configured** or **Unconfigured**. Select **Configured** to use the device's wireless security settings. Select **Unconfigured** to manually change the wireless security settings.
Push-Button: Select this radio button to start using push-button configuration of WPS.
PIN: Select this radio button to configure the wireless station's wireless settings.
Configure AP: click this button after choosing **Push-Button** or **PIN** to start connecting the wireless connections with WPS function.
Device PIN: The pin number that is used to have wireless connection with WPS station.
WPS Add External Registrar: Click the button to search for the external registrar.



WI-FI PROTECTED SETUP (WPS)

Enable WPS : Enabled

Set WPS AP Mode : Unconfigured

Setup AP (Configure all security settings with an external registrar)

○ Push-Button ○ PIN

Device PIN : 21382031

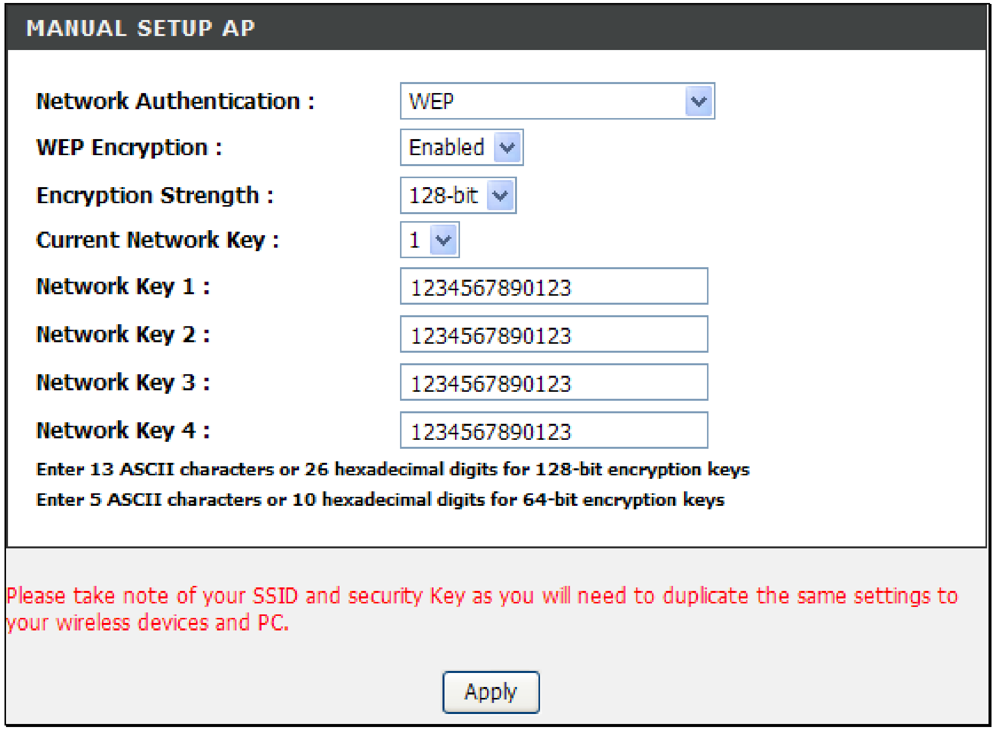
WPS Add External Registrar :

Wireless Encryption Mode – Wired Equivalent Privacy (WEP)

WEP is the most basic form of wireless security. There are two variations of WEP known as Open System and Shared authentication. Use the **Network Authentication** drop-down menu to select these. Open System allows for a two-way hand shake authentication whereas Shared authentication allows for a four-way handshake before authentication is completed. Select **Enabled** from the **WEP Encryption** drop-down menu to choose the Encryption Strength.

Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys.

Click the **Apply** button to save the settings.



MANUAL SETUP AP

Network Authentication :	WEP
WEP Encryption :	Enabled
Encryption Strength :	128-bit
Current Network Key :	1
Network Key 1 :	1234567890123
Network Key 2 :	1234567890123
Network Key 3 :	1234567890123
Network Key 4 :	1234567890123

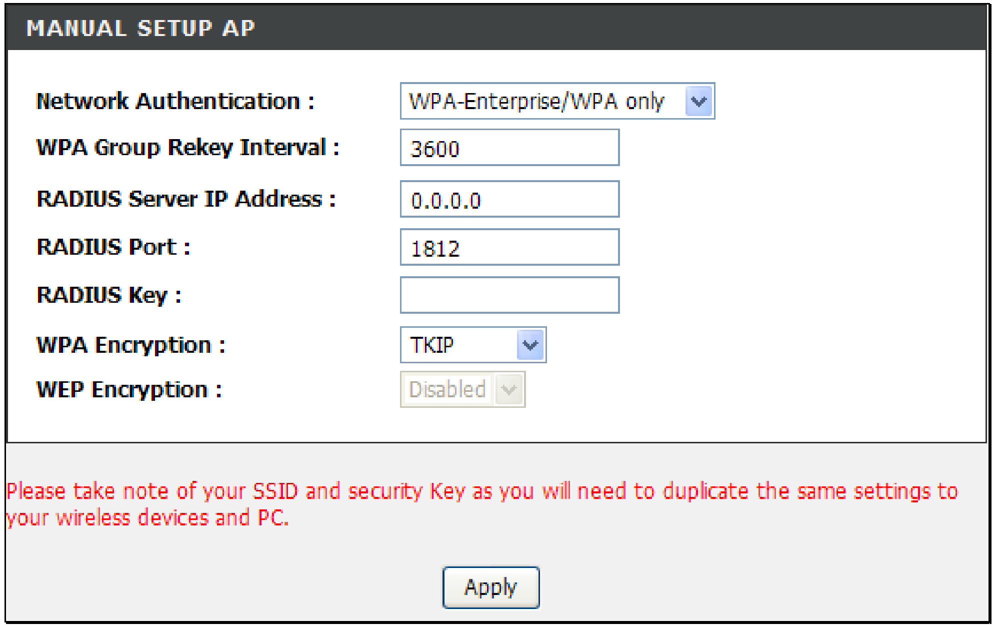
Enter 13 ASCII characters or 26 hexadecimal digits for 128-bit encryption keys
Enter 5 ASCII characters or 10 hexadecimal digits for 64-bit encryption keys

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

Wireless Encryption Mode – Wi-Fi Protected Access (WPA)-Enterprise

WPA is the replacement for WEP (which is seen by many administrators as a ‘weak’ security method). There are two variations of WPA known as WPA-Enterprise and WPA-Personal.
Use the **Network Authentication** drop-down menu to select **WPA-Enterprise/WPA only**. Specify a Radius Server IP Address, Radius Server Port and a Radius Key.

Click the **Apply** button to save the settings.



MANUAL SETUP AP

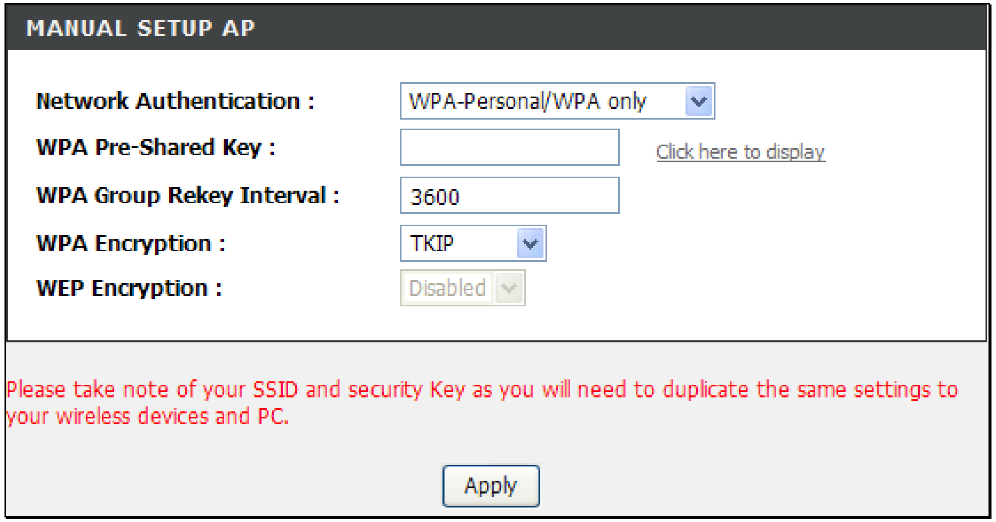
Network Authentication :	WPA-Enterprise/WPA only
WPA Group Rekey Interval :	3600
RADIUS Server IP Address :	0.0.0.0
RADIUS Port :	1812
RADIUS Key :	
WPA Encryption :	TKIP
WEP Encryption :	Disabled

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

Wireless Encryption Mode – Wi-Fi Protected Access (WPA)-Personal

Use the **Network Authentication** drop-down menu to select **WPA-Personal/WPA only**. Specify a Pre-Shared Key. Note that there is NO Radius Server settings required when configuring WPA-PSK.
Enter the Group Key Interval and Encryption if needed.

Click the **Apply** button to save the settings.



MANUAL SETUP AP

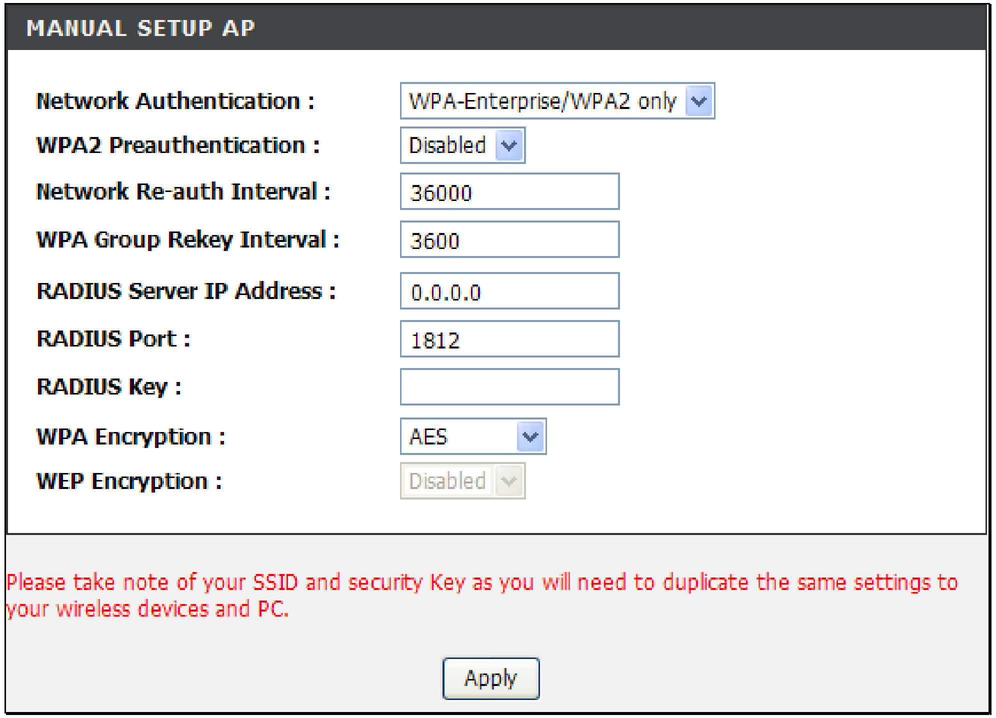
Network Authentication :	WPA-Personal/WPA only
WPA Pre-Shared Key :	Click here to display
WPA Group Rekey Interval :	3600
WPA Encryption :	TKIP
WEP Encryption :	Disabled

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

Wireless Encryption Mode – Wi-Fi Protected Access (WPA2)-Enterprise

WPA2 is the upgrade for WPA. WPA2 sorts out a couple of security vulnerabilities the WPA might encounter. There are also two variations of WPA2 known as WPA2-EAP (Enterprise) and WPA2- PSK (Personal).
Use the **Network Authentication** drop-down menu to select **WPAA-Enterprise/WPA2 only** Specify a Radius Server IP Address, Radius Server Port and a Radius Key.

Click the **Apply** button to save the settings.



MANUAL SETUP AP

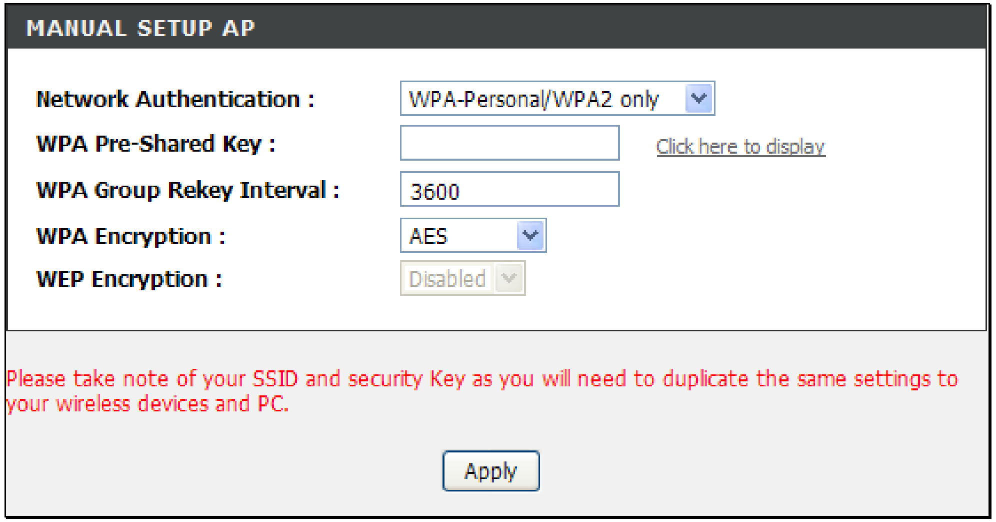
Network Authentication :	WPA-Enterprise/WPA2 only
WPA2 Preauthentication :	Disabled
Network Re-auth Interval :	36000
WPA Group Rekey Interval :	3600
RADIUS Server IP Address :	0.0.0.0
RADIUS Port :	1812
RADIUS Key :	
WPA Encryption :	AES
WEP Encryption :	Disabled

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

Wireless Encryption Mode – Wi-Fi Protected Access (WPA2)-Personal

Use the **Network Authentication** drop-down menu to select **WP-Personal/WPA2 only**. Specify a Pre-Shared Key. Note that there is NO Radius Server settings required when configuring WPA2-PSK.
Enter the Group Key Interval and Encryption if needed.

Click the **Apply** button to save the settings.



MANUAL SETUP AP

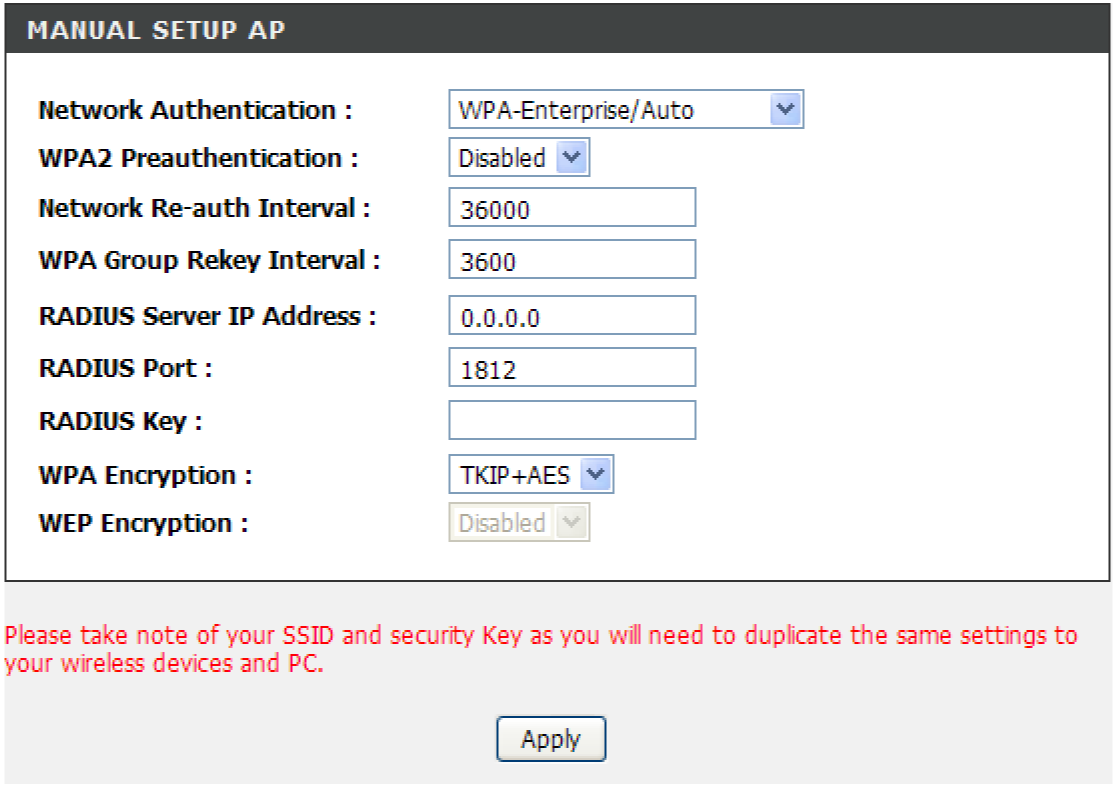
Network Authentication :	WPA-Personal/WPA2 only
WPA Pre-Shared Key :	Click here to display
WPA Group Rekey Interval :	3600
WPA Encryption :	AES
WEP Encryption :	Disabled

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

Wireless Encryption Mode – Mixed Wi-Fi Protected Access (WPA2/WPA)-Enterprise

Mixed WPA2/WPA-EAP provides the functionality of having wireless clients running WPA2-EAP or WPA-EAP. It provides backwards compatibility from WPA2 to WPA.
Use the **Network Authentication** drop-down menu to select **WPA-Enterprise/Auto**. Specify a Radius Server IP Address, Radius Server Port and a Radius Key.

Click the **Apply** button to save the settings.



MANUAL SETUP AP

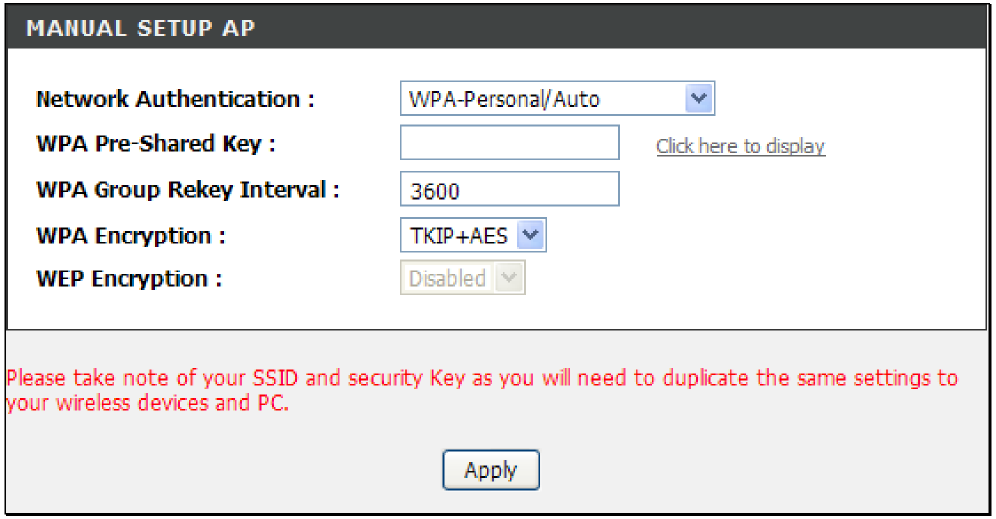
Network Authentication :	WPA-Enterprise/Auto
WPA2 Preauthentication :	Disabled
Network Re-auth Interval :	36000
WPA Group Rekey Interval :	3600
RADIUS Server IP Address :	0.0.0.0
RADIUS Port :	1812
RADIUS Key :	
WPA Encryption :	TKIP+AES
WEP Encryption :	Disabled

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

Wireless Encryption Mode – Mixed Wi-Fi Protected Access (WPA2/WPA)-Personal

Use the **Network Authentication** drop-down menu to select **WPA-Personal/Auto**. Specify a Pre-Shared Key. Note that there is NO Radius Server settings required when configuring Mixed WPA2/WPA-PSK.
Enter the Group Key Interval and Encryption if needed.

Click the **Apply** button to save the settings.



MANUAL SETUP AP

Network Authentication :	WPA-Personal/Auto
WPA Pre-Shared Key :	
WPA Group Rekey Interval :	3600
WPA Encryption :	TKIP+AES
WEP Encryption :	Disabled

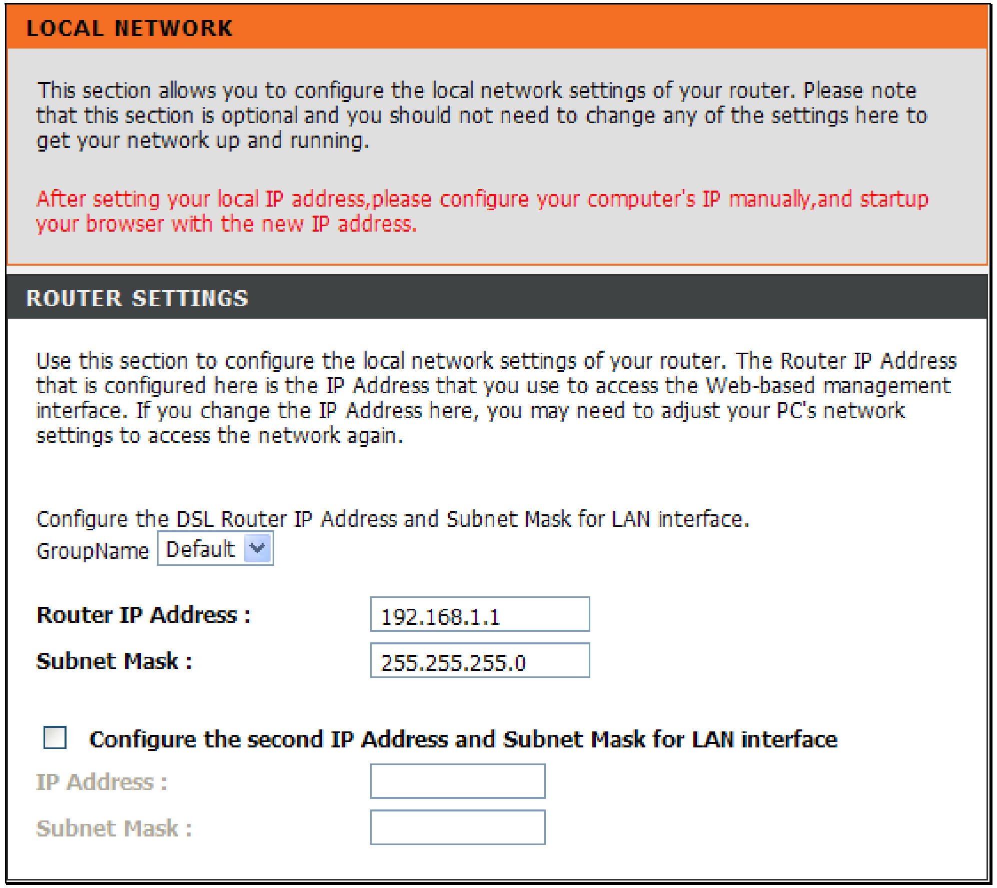
Please take note of your SSID and security Key as you will need to duplicate the same settings to your wireless devices and PC.

Local Network

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

These are the settings of the LAN (Local Area Network) interface for the router. The router's local network (LAN) settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

DHCP stands for Dynamic Host Configuration Protocol. The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network (LAN).
Router IP Address: Enter the device’s new IP address here.
Subnet Mask: Enter the device’s new subnet mask here.
Configure the second IP Address and Subnet Mask for LAN Interface: Tick this option to enable the use of a second IP address for this device.
IP Address: Enter the device’s new second IP here.
Subnet Mask: Enter the device’s new second subnet mask here.



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.

Configure the DSL Router IP Address and Subnet Mask for LAN interface.
GroupName: Default

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 :

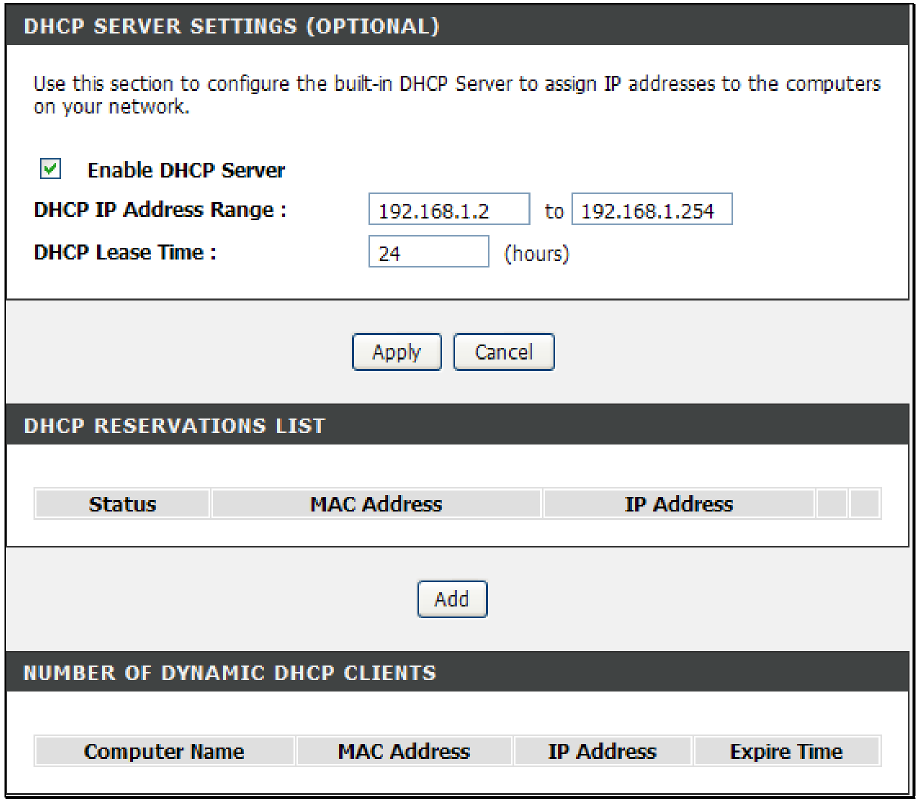
DHCP Server Settings: Here the user can add a DHCP Reserved address.

Enable DHCP Server: Tick this option to enable this entry.
DHCP IP Address Range: Enter a reserved user’s IP address in here.
DHCP Lease Time: Enter a reserved user’s MAC address in here.

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

DHCP Reservations 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, click the corresponding 🗑 button. To modify a DHCP Reservations List entry, click the corresponding 📝 button and then enter the information in the appropriate fields in the DHCP Reservation List section.

Number of Dynamic DHCP Clients: Here the number of dynamic DHCP clients will be listed. Information shown is Computer Name, MAC Address, IP Address and Expire Time.



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

Time and Date

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

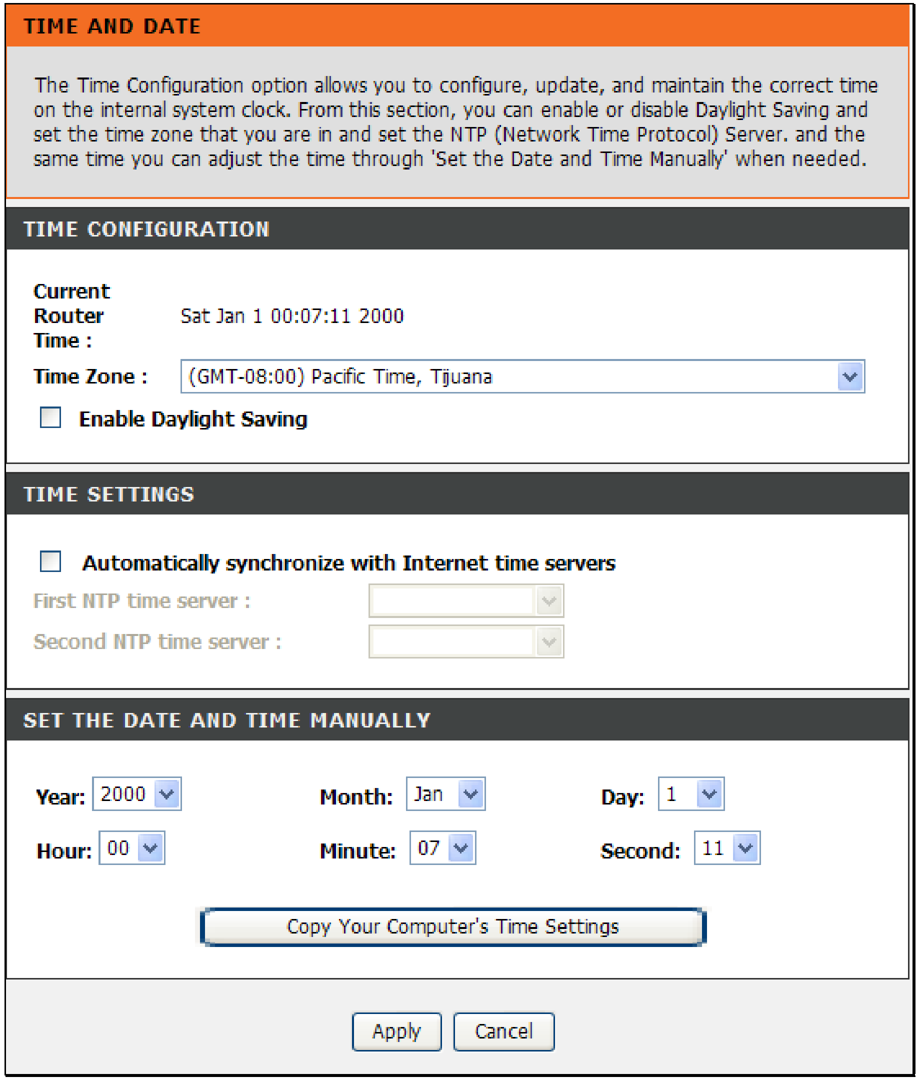
The Router provides manually time and date setup, NTP, and daylight saving to configure, update and maintain the correct time.

The Router allows you to set the time zone you are in by using the Time Zone drop-down menu. In addition, you can enable Daylight Saving by ticking the **Enable Daylight Saving** check.

To configure system time on the Router, select the **Automatically synchronize with Internet time servers** check box 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.

You can also manually configure the system time on Router. Select the Year, Month, Day, Hour, Minute and Second in the Set the Date and Time Manually system, or just click **Copy Your Computer's Time Settings** button to synchronize the time with the computer.

When you are finished, click the **Apply** button to 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 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 00:07:11 2000

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

□ Enable Daylight Saving

TIME SETTINGS

□ Automatically synchronize with Internet time servers

First NTP time server :

Second NTP time server :

SET THE DATE AND TIME MANUALLY

Year: 2000 Month: Jan Day: 1

Hour: 00 Minute: 07 Second: 11

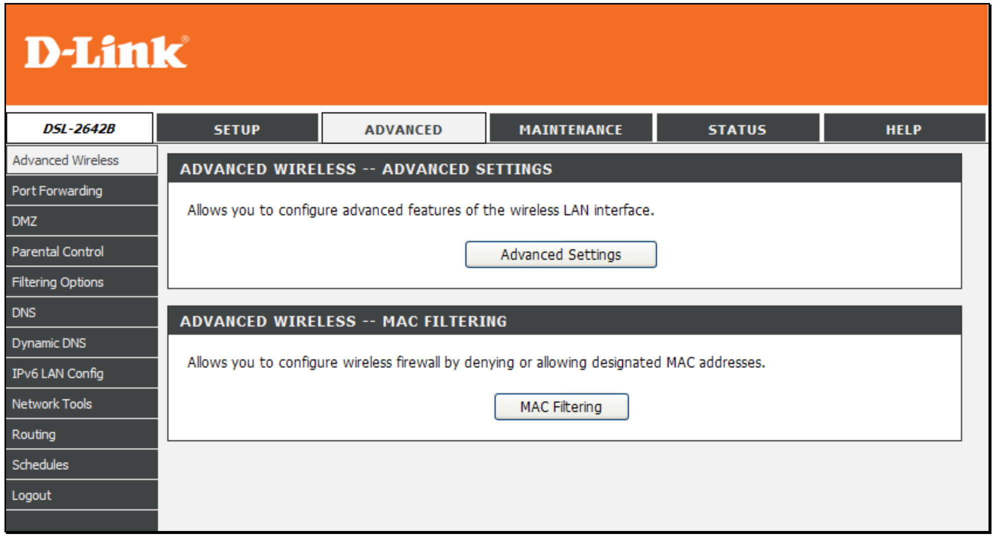
Advanced

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 two subcategories: **Advanced Settings**, and **MAC Filtering**. 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.

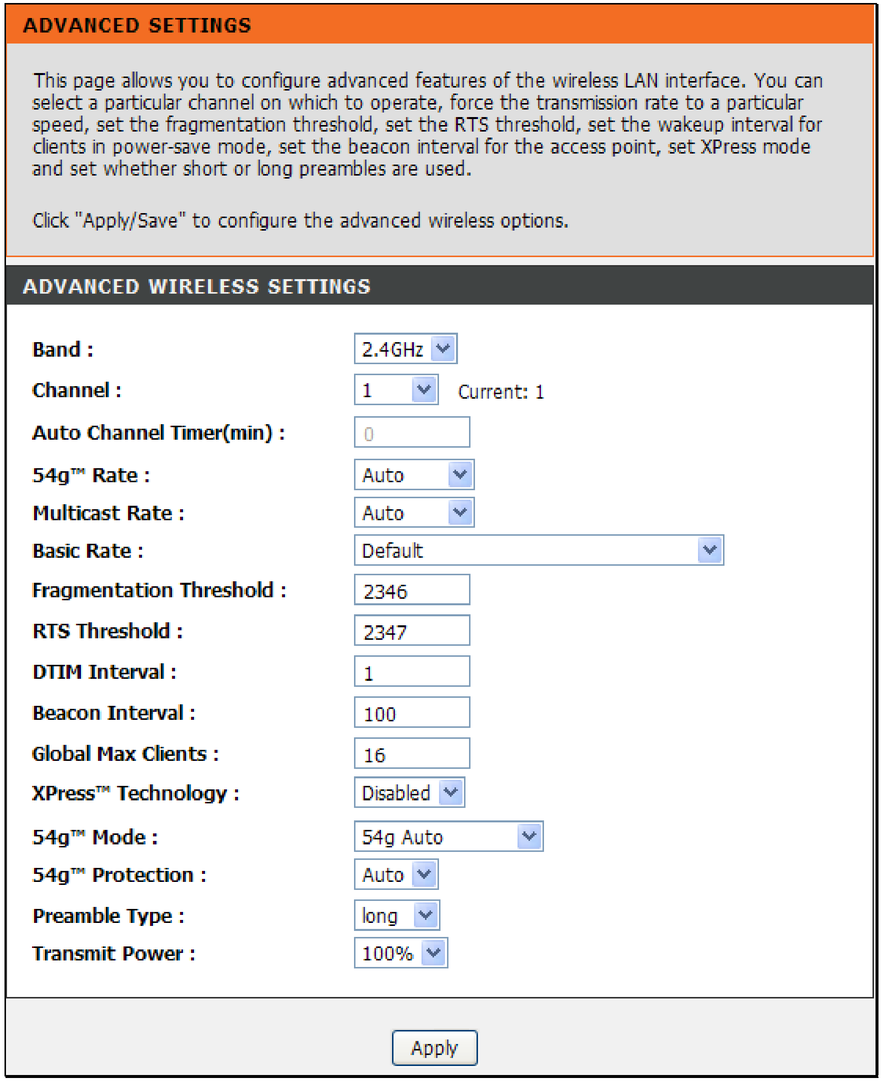
ADVANCED WIRELESS -- MAC FILTERING

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

Advanced 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.

The user can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used and more.



ADVANCED SETTINGS

This page allows you to configure advanced features of the wireless LAN interface. You can select a particular channel on which to operate, force the transmission rate to a particular speed, set the fragmentation threshold, set the RTS threshold, set the wakeup interval for clients in power-save mode, set the beacon interval for the access point, set XPress mode and set whether short or long preambles are used.

Click "Apply/Save" to configure the advanced wireless options.

ADVANCED WIRELESS SETTINGS

Band :	2.4GHz
Channel :	1 Current: 1
Auto Channel Timer(min) :	0
54g™ Rate :	Auto
Multicast Rate :	Auto
Basic Rate :	Default
Fragmentation Threshold :	2346
RTS Threshold :	2347
DTIM Interval :	1
Beacon Interval :	100
Global Max Clients :	16
XPress™ Technology :	Disabled
54g™ Mode :	54g Auto
54g™ Protection :	Auto
Preamble Type :	long
Transmit Power :	100%

MAC Filtering

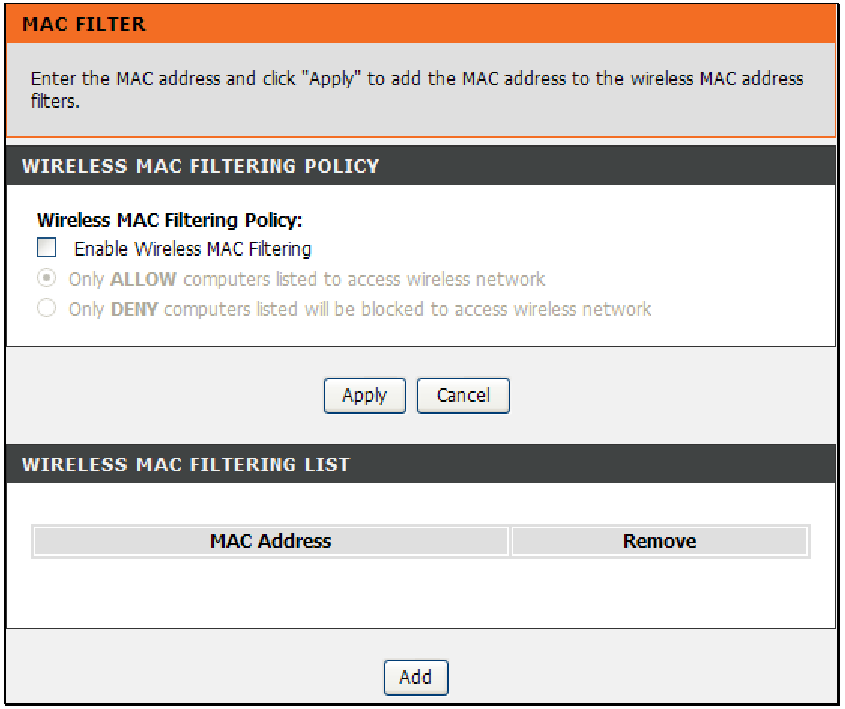
To access MAC Filtering, point to the **Advanced Wireless** on the left window and click **MAC Filtering** submenu, or click the **MAC Filtering** button in the Wireless Settings window.

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

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 **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.

Click **Apply** to take effect.



MAC FILTER

Enter the MAC address and click "Apply" to add the MAC address to the wireless MAC address filters.

WIRELESS MAC FILTERING POLICY

Wireless MAC Filtering Policy:

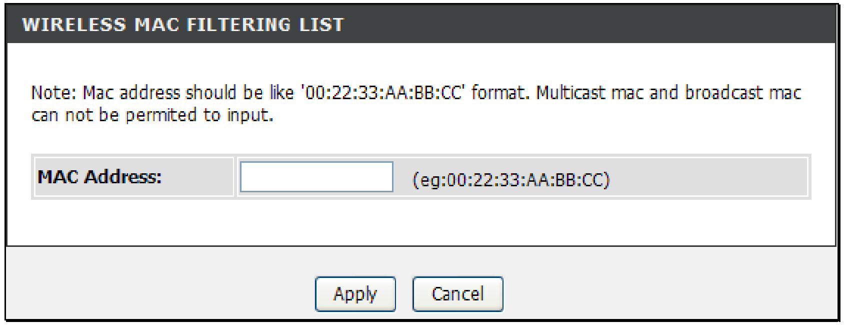
□ Enable Wireless MAC Filtering

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

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

WIRELESS MAC FILTERING LIST

MAC Address	Remove



WIRELESS MAC FILTERING LIST

Note: Mac address should be like '00:22:33:AA:BB:CC' format. Multicast mac and broadcast mac can not be permited to input.

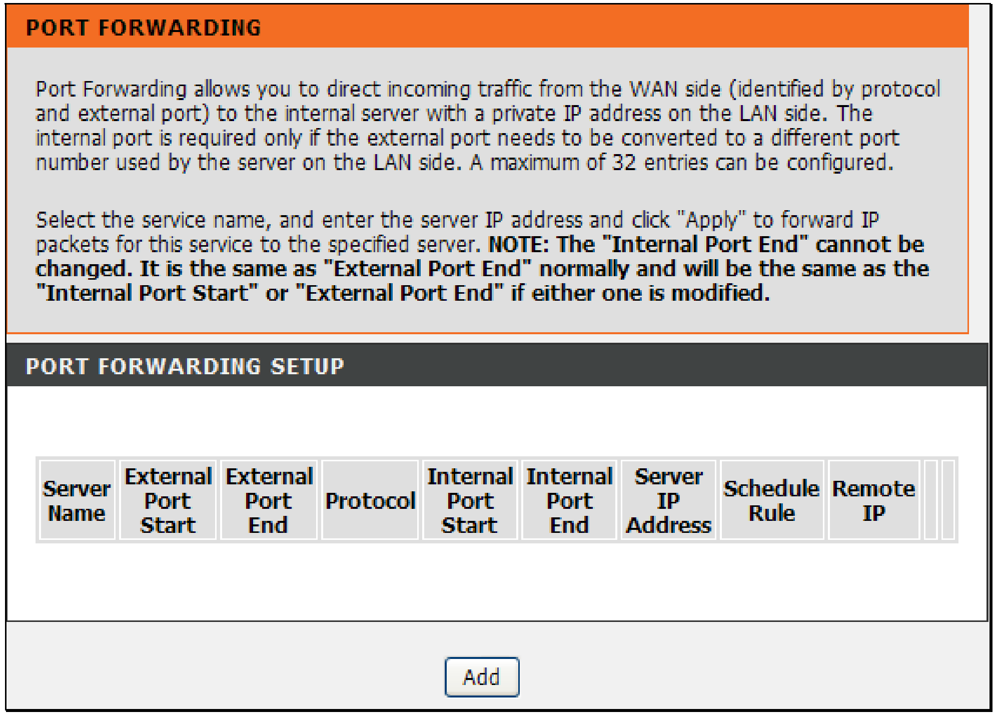
MAC Address: (eg:00:22:33:AA:BB:CC)

Port Forwarding

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

To access the Port Forwarding window, click the **Port Forwarding** button in the **Advanced** directory. Port Forwarding is used to redirect data to a single PC.

To remove an Active Port Forwarding entry in the table, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 button, make the desired changes, and then click the **Apply** button.



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.

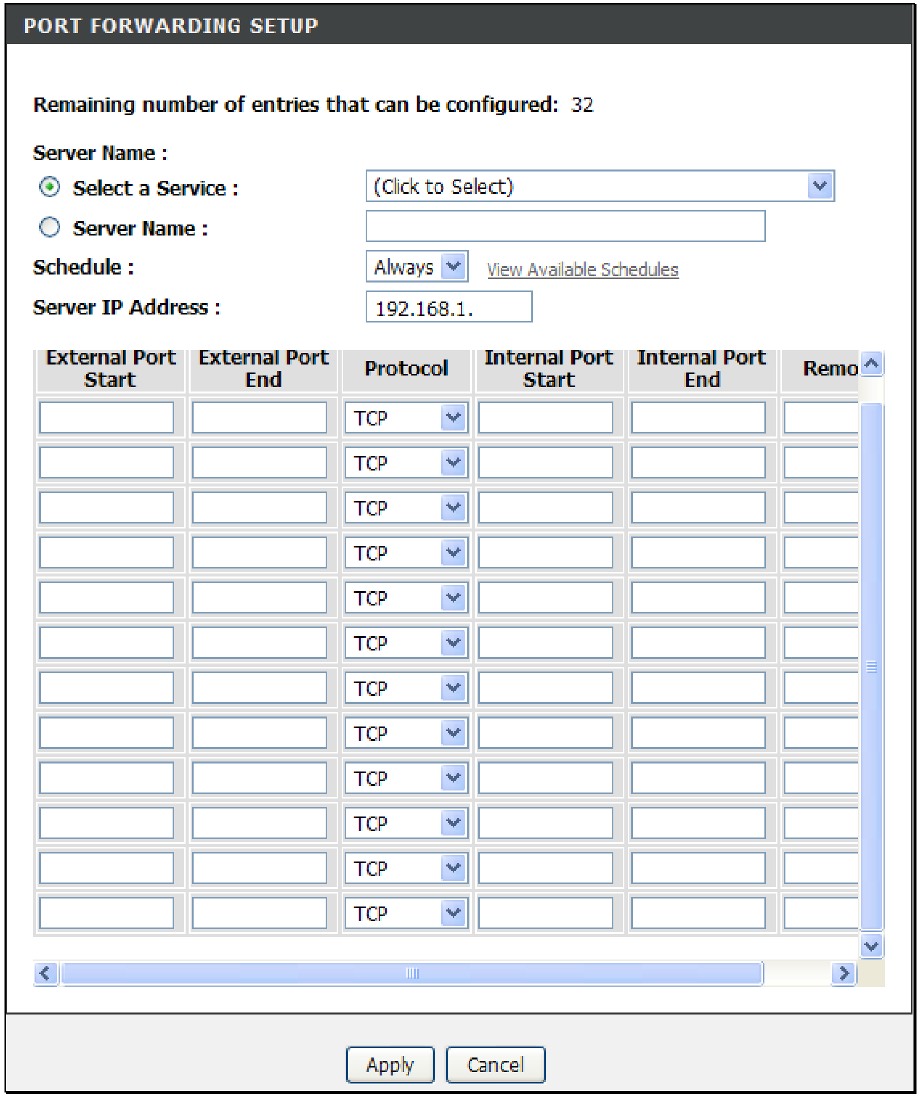
Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. **NOTE: The "Internal Port End" cannot be changed. It is the same as "External Port End" normally and will be the same as the "Internal Port Start" or "External Port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

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

Click the **Add** button to set up a rule as follows.

Click the **Select a Service** radio button and use the drop-down menu to elect a pre-defined port forwarding rule. Or, click the **Sever Name** radio button to enter a custom rule name. Choose Schedule that has been configured in **Advanced** -> **Schedules**, and enter the Server IP Address. Enter a range of ports in the External Start Port and External End Port fields, and then click the **Apply** button to see the customized rule in the Port Forwarding Setup section.



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.

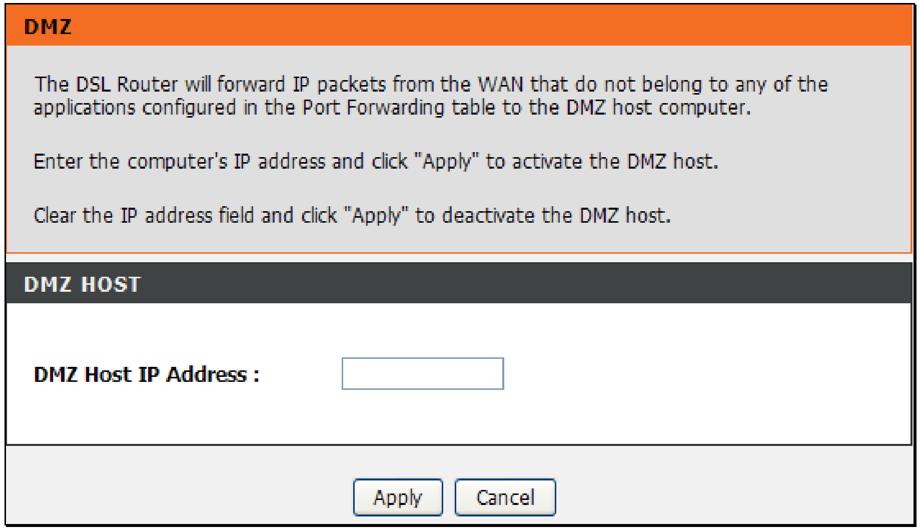
External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End	Remo
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			
		TCP			

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, select **Enabled DMZ**, type in the IP Address of the server or device on your LAN, and click the **Apply** button. To remove DMZ status from the designated IP address, deselect the **Enable DMZ** and click **Apply**. It will be necessary to save the settings and reboot the Router before the DMZ is activated.



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.

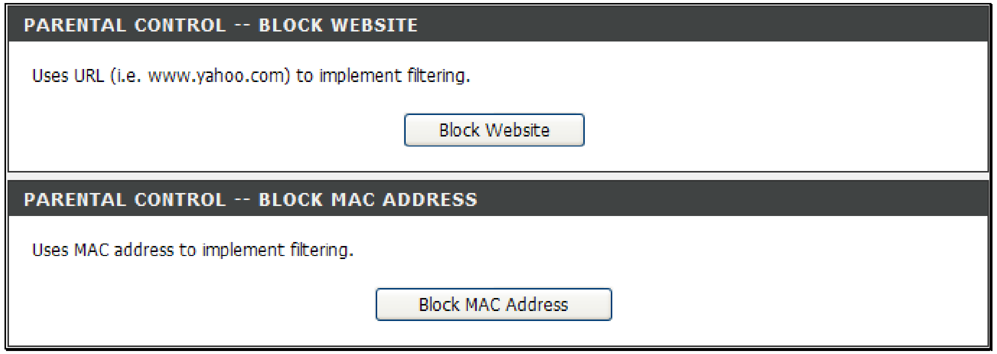
DMZ HOST

DMZ Host IP Address :

Parental Control

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

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

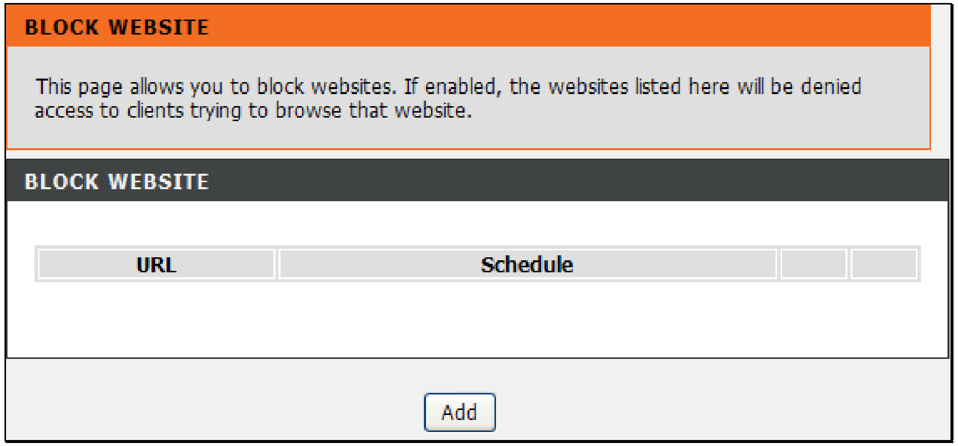
Use this window to deny access to specified websites.

Click **Add** to see the **Block Website** section. URL (Uniform Resource Locator) is a specially formatted text string that uniquely defines an Internet website. This section will allow users to block computers on the LAN from accessing certain URLs. This may be accomplished by simply entering the URL to be blocked in the **URL** field.

To configure for URL blocking, enter the website's address into the **URL** field, click **Schedule Rule** or **Manual Schedule** radio button. For Schedule Rule, select a rule in the drop down list. Rules in the list can be configured in **Advanced** -> **Schedules**. 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, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 button, make the desired changes, and then click the **Apply** button.

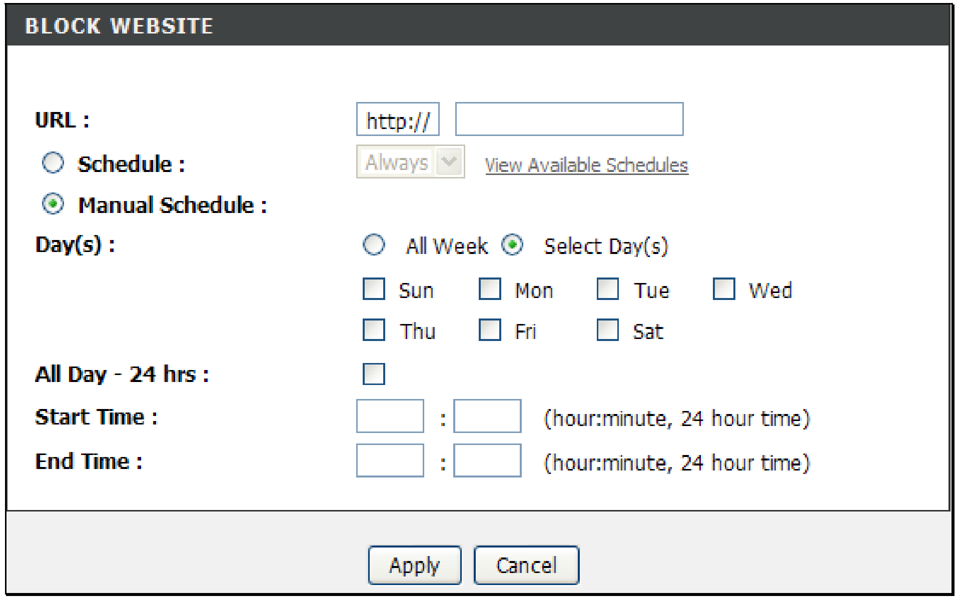


BLOCK WEBSITE

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		



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.

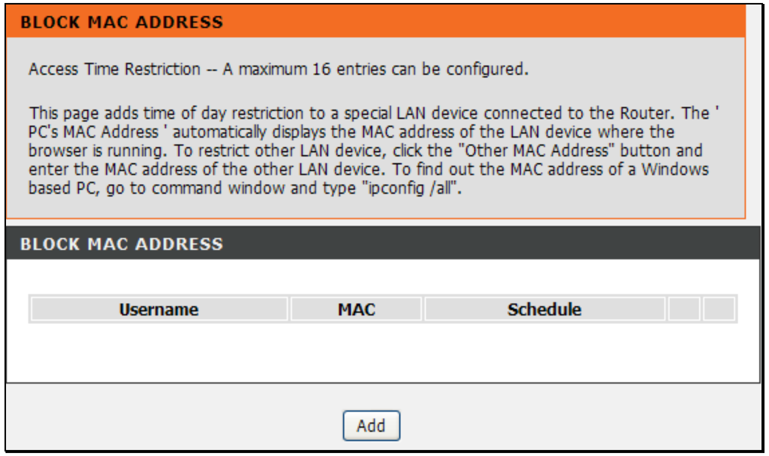
Use this window to deny access to specified MAC address.

Click **Add** to see the **Time of Day Restriction** 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**. 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, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 button, make the desired changes, and then click the **Apply** button.



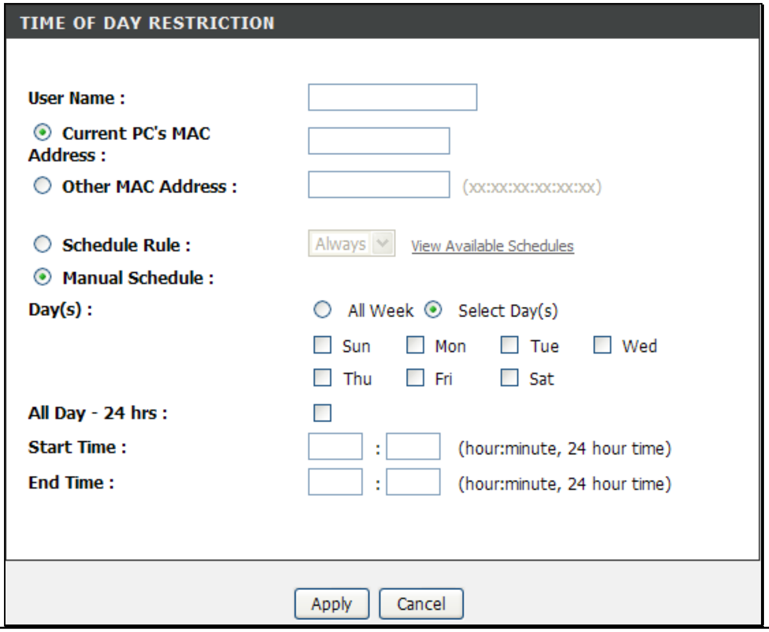
BLOCK MAC ADDRESS

Access Time Restriction -- A maximum 16 entries can be configured.

This page adds time of day restriction to a special LAN device connected to the Router. The ' PC's MAC Address ' automatically displays the MAC address of the LAN device where the browser is running. To restrict other LAN device, click the "Other MAC Address" button and enter the MAC address of the other LAN device. To find out the MAC address of a Windows based PC, go to command window and type "ipconfig /all".

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 : □

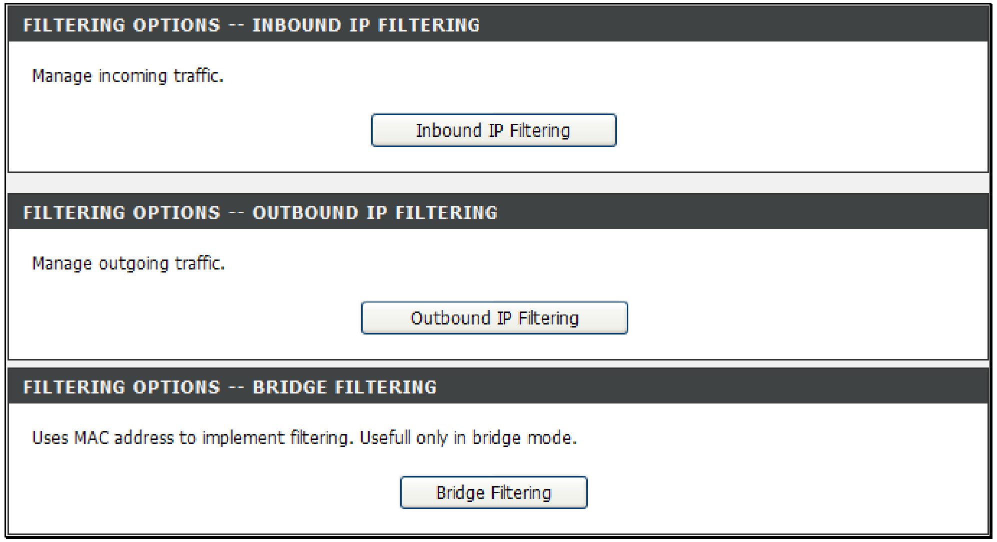
Start Time : : (hour:minute, 24 hour time)

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

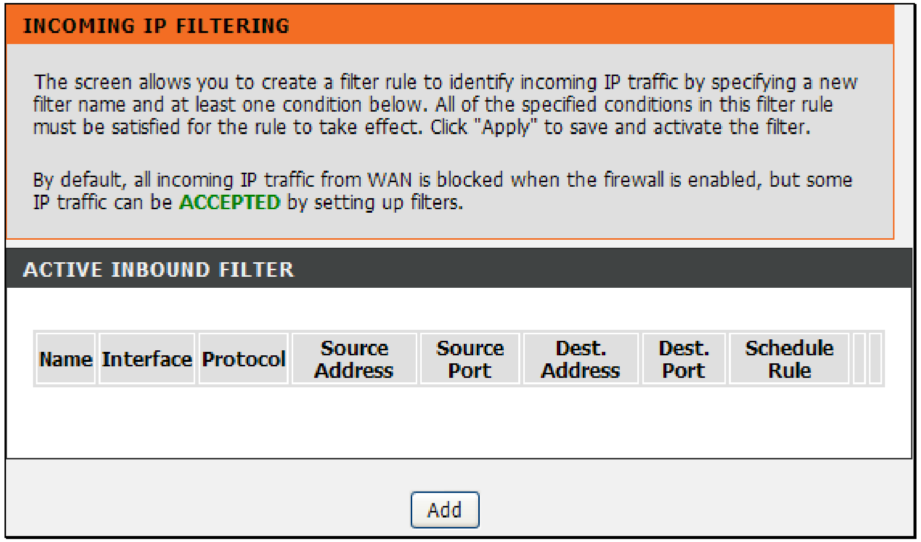
Uses MAC address to implement filtering. Usefull only in bridge mode.

Inbound Filtering

To access Inbound Filtering, point to the **Filtering Options** on the left window and click **Inbound IP Filtering** submenu, or click the **Inbound IP Filtering** 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 Add Inbound 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, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 button, make the desired changes, and then click the **Apply** button.



INCOMING IP FILTERING

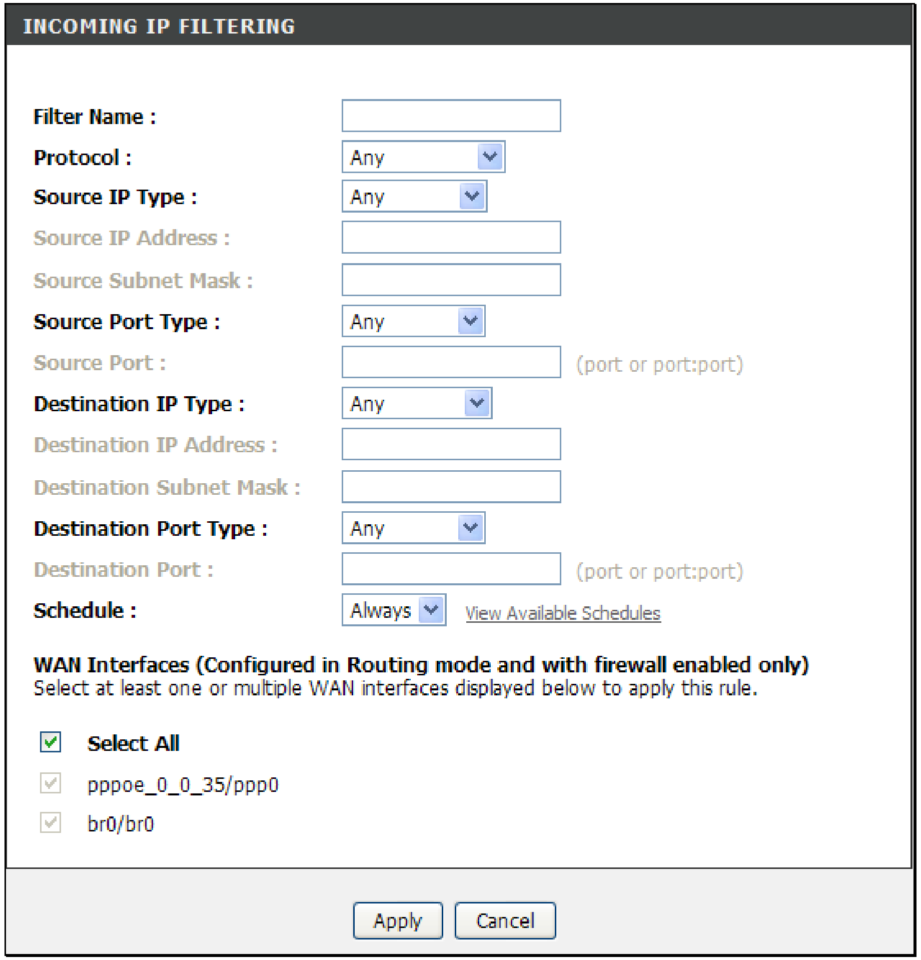
The screen allows you to create a filter rule to identify incoming IP traffic by specifying a new filter name and at least one condition below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect. Click "Apply" to save and activate the filter.

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.	
Source/ Destination IP Type	Select either **Single IP, Network IP** or **IP Range** to show different items.	
	Source/Destination IP Address	This is the single IP address which you are creating the filter rule.
	Source/Destination IP Address & Source/Destination Subnet Mask	This is the Network IP address and its associated subnet for which you are creating the filter rule.
	Start/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	The Source/Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule.	
WAN Interface	Select the WAN interfaces you want to apply for this rule.	



INCOMING IP FILTERING

Filter Name :		
Protocol :	Any	
Source IP Type :	Any	
Source IP Address :		
Source Subnet Mask :		
Source Port Type :	Any	
Source Port :		(port or port:port)
Destination IP Type :	Any	
Destination IP Address :		
Destination Subnet Mask :		
Destination Port Type :	Any	
Destination Port :		(port or port:port)
Schedule :	Always	View Available Schedules

WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.

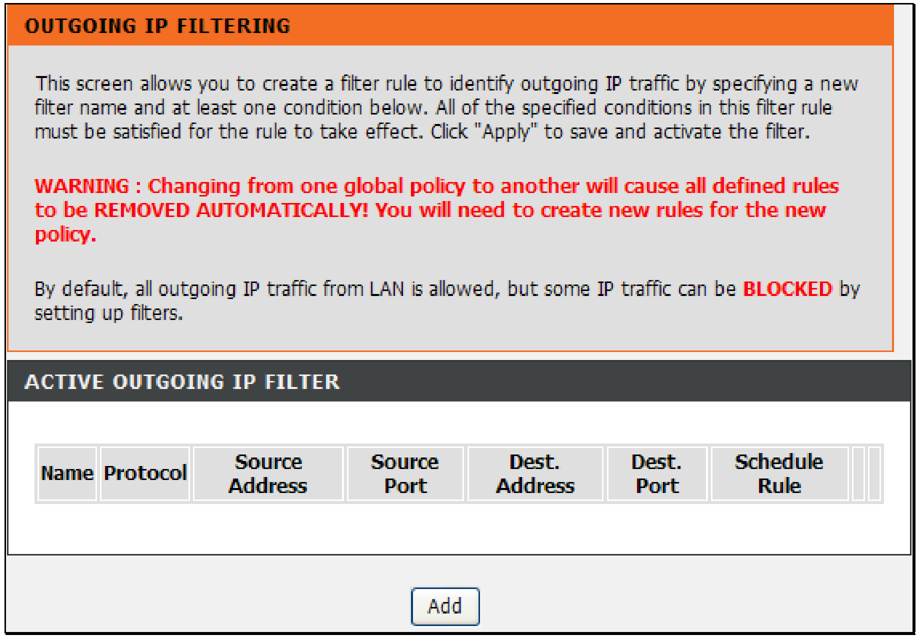
☑ **Select All**
☑ pppoe_0_0_35/ppp0
☑ br0/br0

Outbound Filtering

To access Outbound Filtering, point to the **Filtering Options** on the left window and click **Outbound IP Filtering** submenu, or click the **Outbound IP Filtering** 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 Add Outbound 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, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 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.

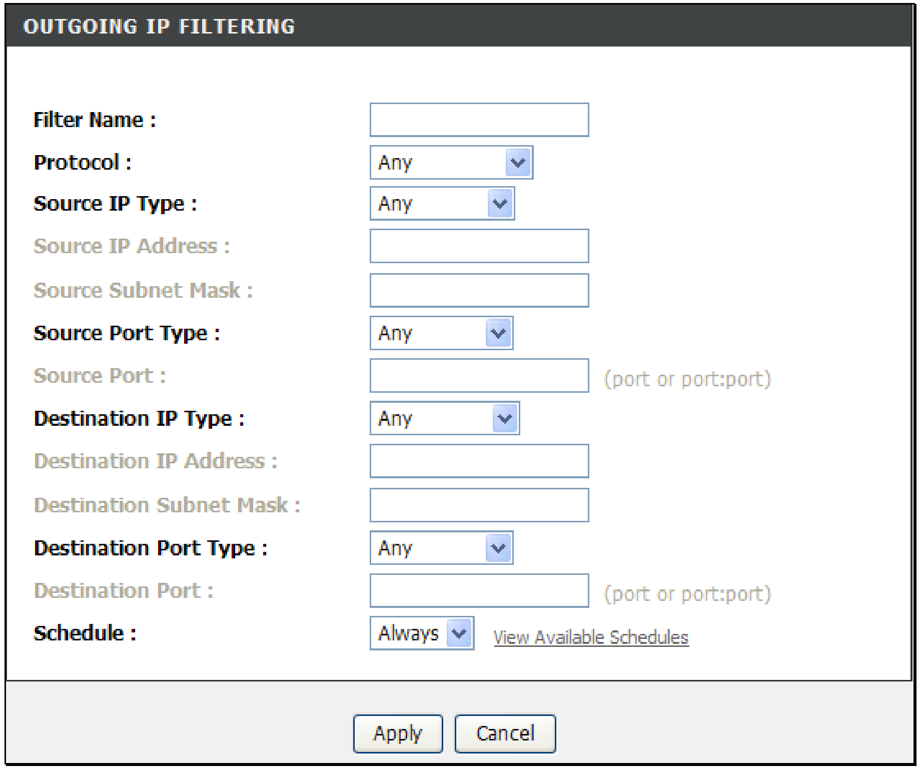
WARNING : Changing from one global policy to another will cause all defined rules to be REMOVED AUTOMATICALLY! You will need to create new rules for the new policy.

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.	
Source/ Destination IP Type	Select either **Single IP, Network IP** or **IP Range** to show different items.	
	Source/Destination IP Address	This is the single IP address which you are creating the filter rule.
	Source/Destination IP Address & Source/Destination Subnet Mask	This is the Network IP address and its associated subnet for which you are creating the filter rule.
	Start/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	The Source/Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule.	
WAN Interface	Select the WAN interfaces you want to apply for this rule.	



OUTGOING IP FILTERING

Filter Name :

Protocol : Any

Source IP Type : Any

Source IP Address :

Source Subnet Mask :

Source Port Type : Any

Source Port : (port or port:port)

Destination IP Type : Any

Destination IP Address :

Destination Subnet Mask :

Destination Port Type : Any

Destination Port : (port or port:port)

Schedule : Always View Available Schedules

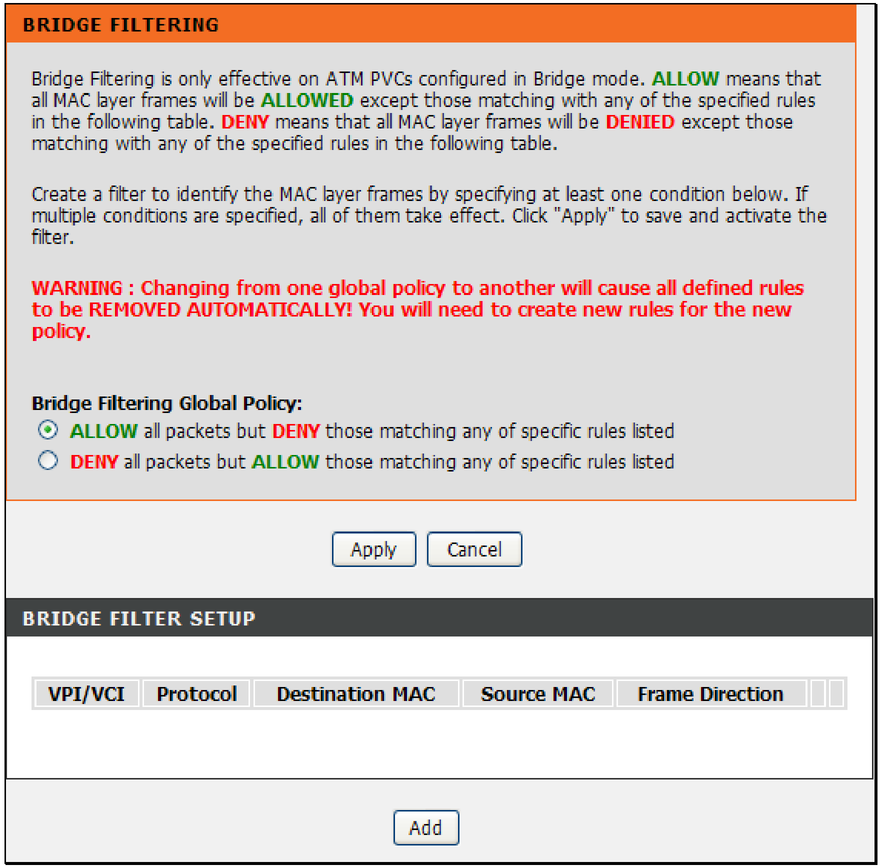
Bridge Filtering

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

To remove an entry in the table, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 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:

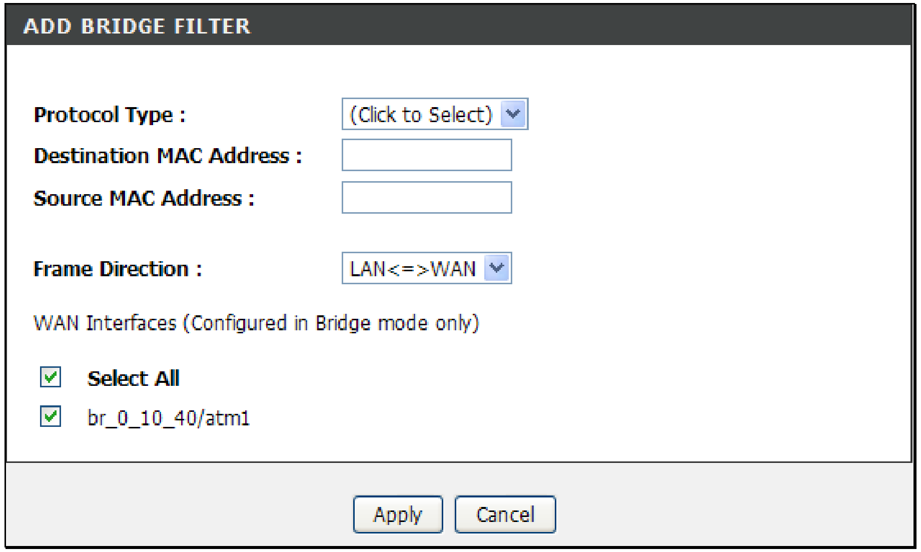
● ALLOW all packets but DENY those matching any of specific rules listed

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

BRIDGE FILTER SETUP

VPI/VCI	Protocol	Destination MAC	Source MAC	Frame Direction

Click the **Add** button to see the Add Bridge Filter section. Select a protocol (PPPoE, IPv4, IPv6, 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. Select the WAN interface you want to apply for this rule. Click the **Apply** button to add the entry in the Active Bridge Filters table.



ADD BRIDGE FILTER

Protocol Type : (Click to Select)

Destination MAC Address :

Source MAC Address :

Frame Direction : LAN<=>WAN

WAN Interfaces (Configured in Bridge mode only)

☑ Select All

☑ br_0_10_40/atm1

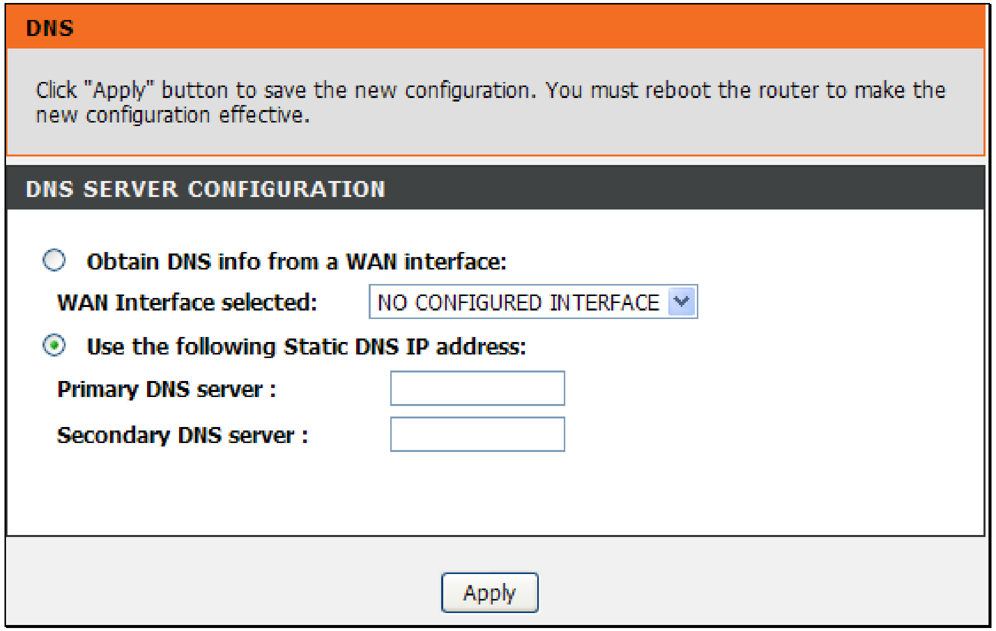
DNS Setup

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

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

If you have not been given specific DNS server IP addresses or if the Router is not pre-configured with DNS server information, select the **Obtain DNS server address automatically** option. Auto discovery DNS instructs the Router to automatically obtain the DNS IP address from the ISP through DHCP. If your WAN connection uses a Static IP address, auto discovery for DNS cannot be used.

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

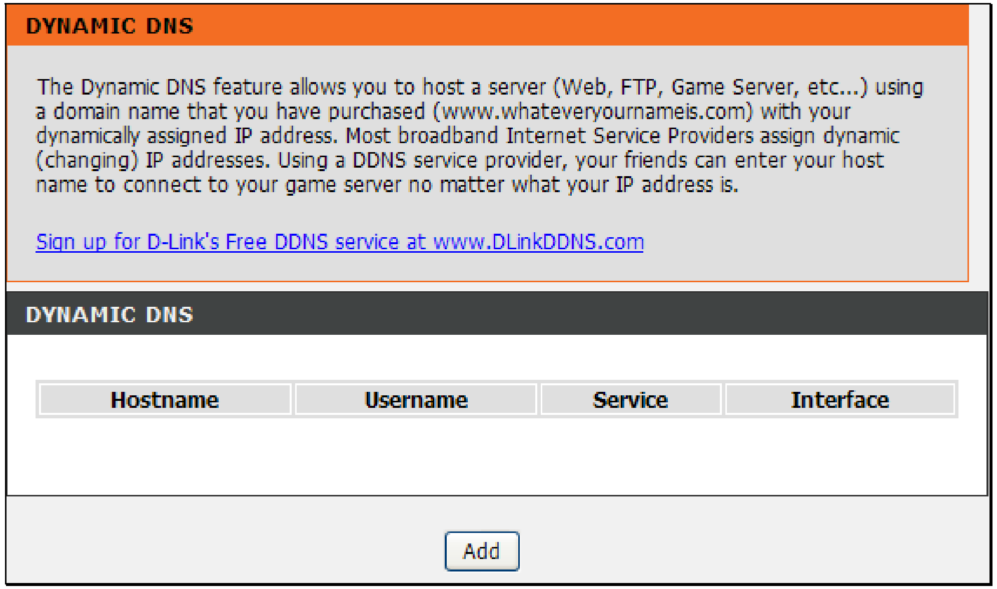
To access the Dynamic DNS window, click the **Dynamic DNS** button in the **Advanced** directory.

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

Click **Add** to see the Add Dynamic DNS section. Enter the required DDNS information, click the **Apply** button to see the entry in the Dynamic DNS table. To remove an entry in the table, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 button, make the desired changes, and then click the **Apply** button.

Note

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



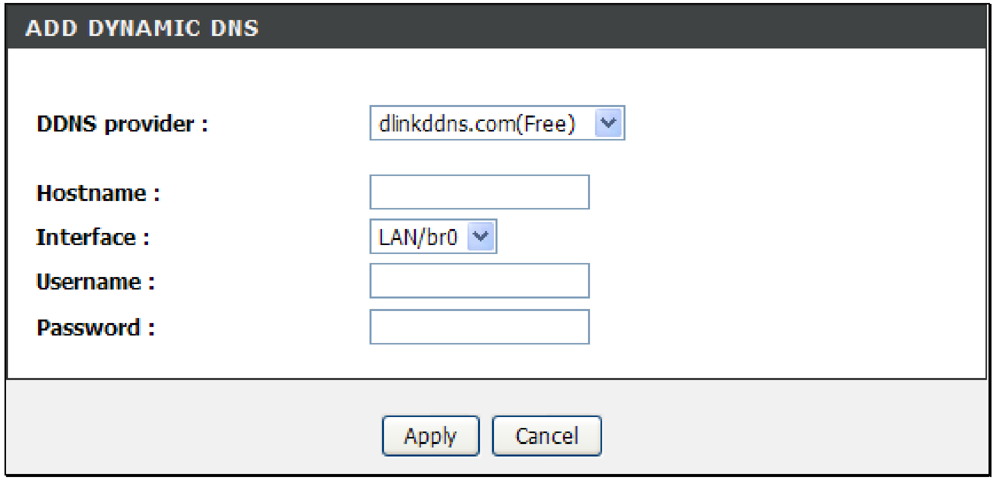
DYNAMIC DNS

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.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com

DYNAMIC DNS

Hostname	Username	Service	Interface



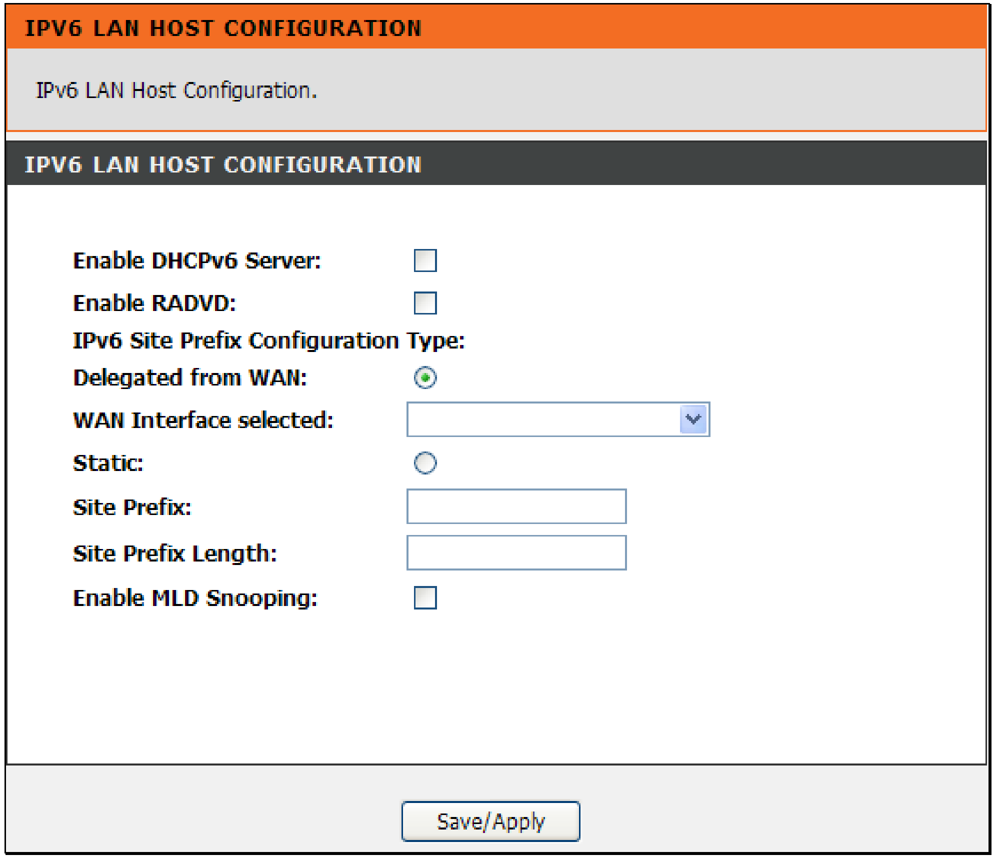
ADD DYNAMIC DNS

DDNS provider :	dlinkddns.com(Free)
Hostname :	
Interface :	LAN/br0
Username :	
Password :	

IPv6 LAN Config

To access the IPv6 LAN config window, click the **IPv6 LAN Config** button in the **Advanced** directory.

The Router supports to be IPv6 host.
Enable DHCPv6 Server: Tick the check box to enable the Router as DHCPv6 server.
Enable RADVD: RADVD advertises the IPv6 prefix to the local network, so that a new client can generate its own IP address.
IPv6 Site Prefix configuration Type: Select to get the prefix from WAN or add a static site prefix.
Delegated from WAN: Click this radio button to get the prefix from WAN.
WAN Interface selected: Select a WAN interface from the drop-down menu.
Static: Click the radio button to have a site prefix configured below.
Site Prefix: Enter the site prefix.
Site Prefix Length: Enter the site prefix length.
Enable MLD Snooping: Tick the check box to enable MLD snooping.



IPV6 LAN HOST CONFIGURATION

IPv6 LAN Host Configuration.

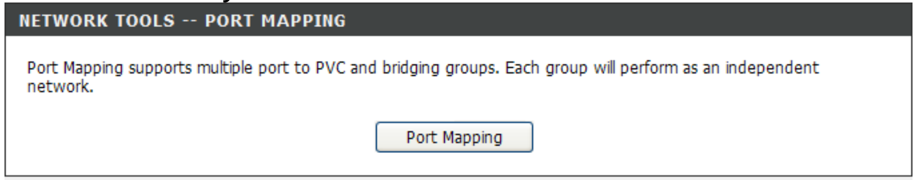
IPV6 LAN HOST CONFIGURATION

Enable DHCPv6 Server: □
Enable RADVD: □
IPv6 Site Prefix Configuration Type:
Delegated from WAN: ●
WAN Interface selected:
Static: ○
Site Prefix:
Site Prefix Length:
Enable MLD Snooping: □

Network Tools

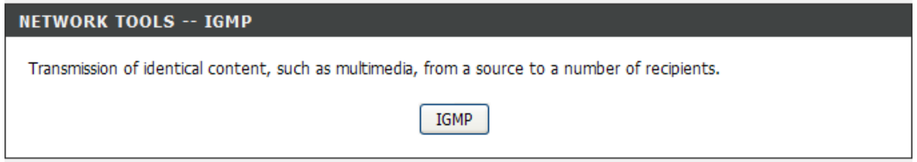
To access the Network Tools window, click the **Network Tools** button in the **Advanced** directory.

There are ten subcategories in Network Tools: **Port Mapping**, **IGMP**, **Quality of Service**, **Queue Config**, **QoS Classification**, **UPnP**, **DSL**, **SNMP**, **TR-069**, and **Certificates**. 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.



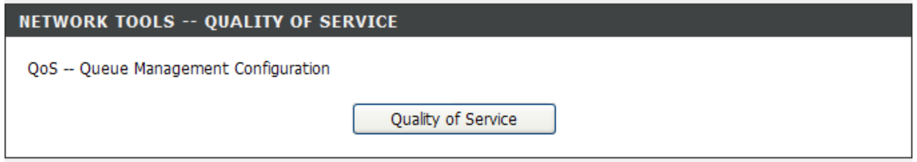
NETWORK TOOLS -- PORT MAPPING

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



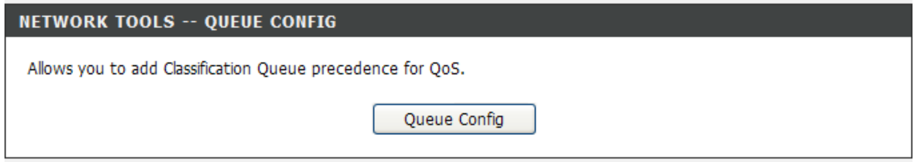
NETWORK TOOLS -- IGMP

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



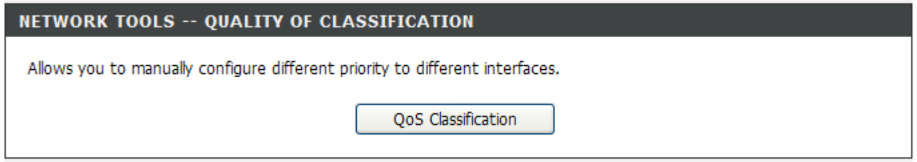
NETWORK TOOLS -- QUALITY OF SERVICE

QoS -- Queue Management Configuration



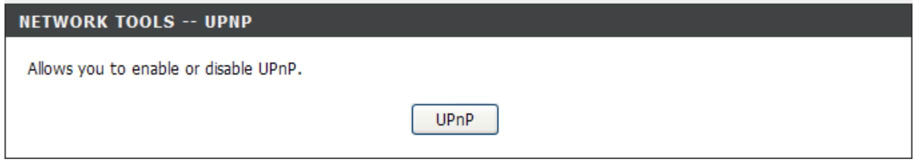
NETWORK TOOLS -- QUEUE CONFIG

Allows you to add Classification Queue precedence for QoS.



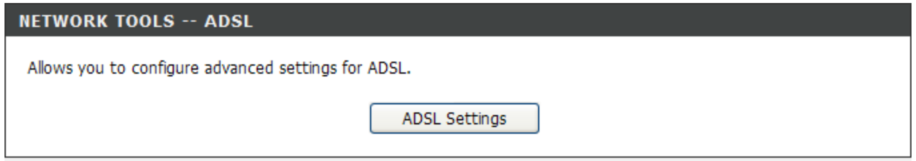
NETWORK TOOLS -- QUALITY OF CLASSIFICATION

Allows you to manually configure different priority to different interfaces.



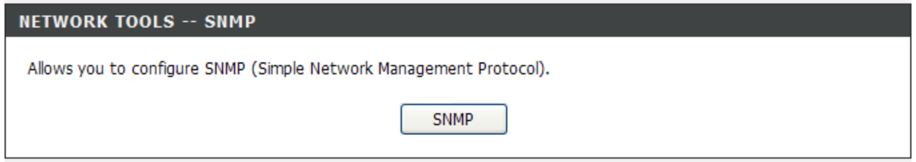
NETWORK TOOLS -- UPNP

Allows you to enable or disable UPnP.



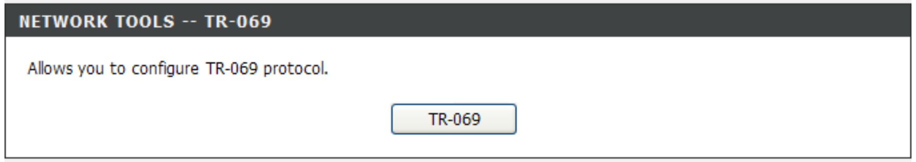
NETWORK TOOLS -- ADSL

Allows you to configure advanced settings for ADSL.



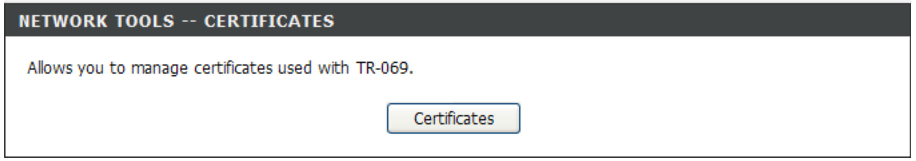
NETWORK TOOLS -- SNMP

Allows you to configure SNMP (Simple Network Management Protocol).



NETWORK TOOLS -- TR-069

Allows you to configure TR-069 protocol.



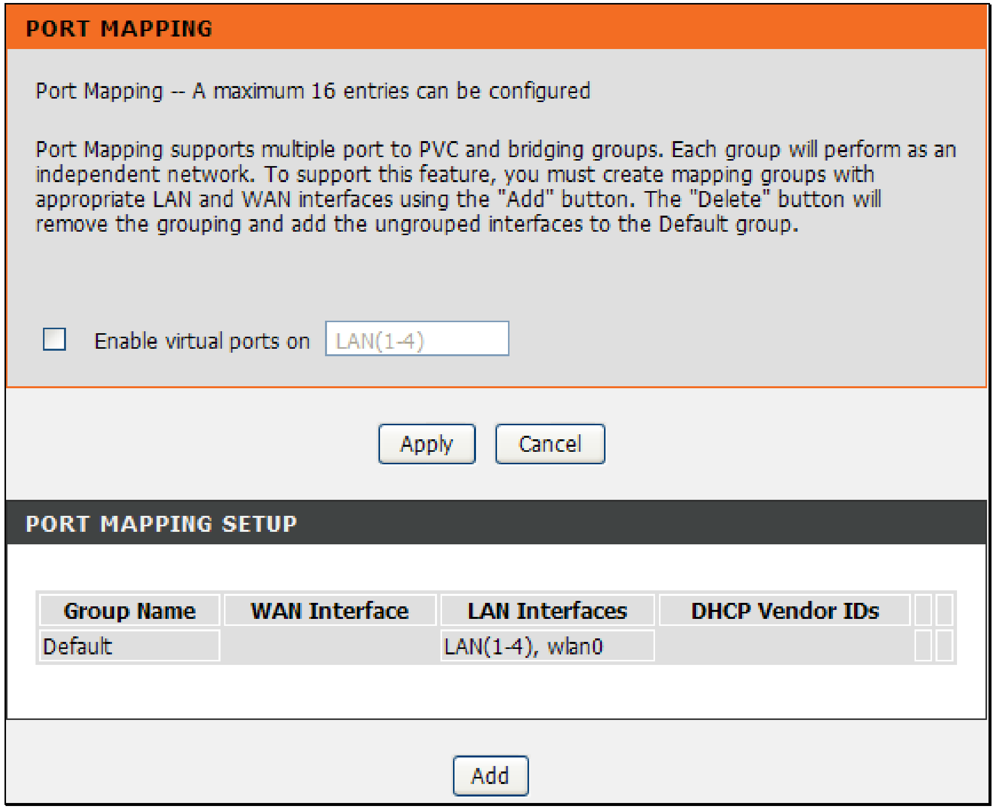
NETWORK TOOLS -- CERTIFICATES

Allows you to manage certificates used with TR-069.

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.

Tick the **Enable Virtual Ports on** check box and enter an interface to apply for. Click **Apply** to take effect.



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 LAN(1-4)

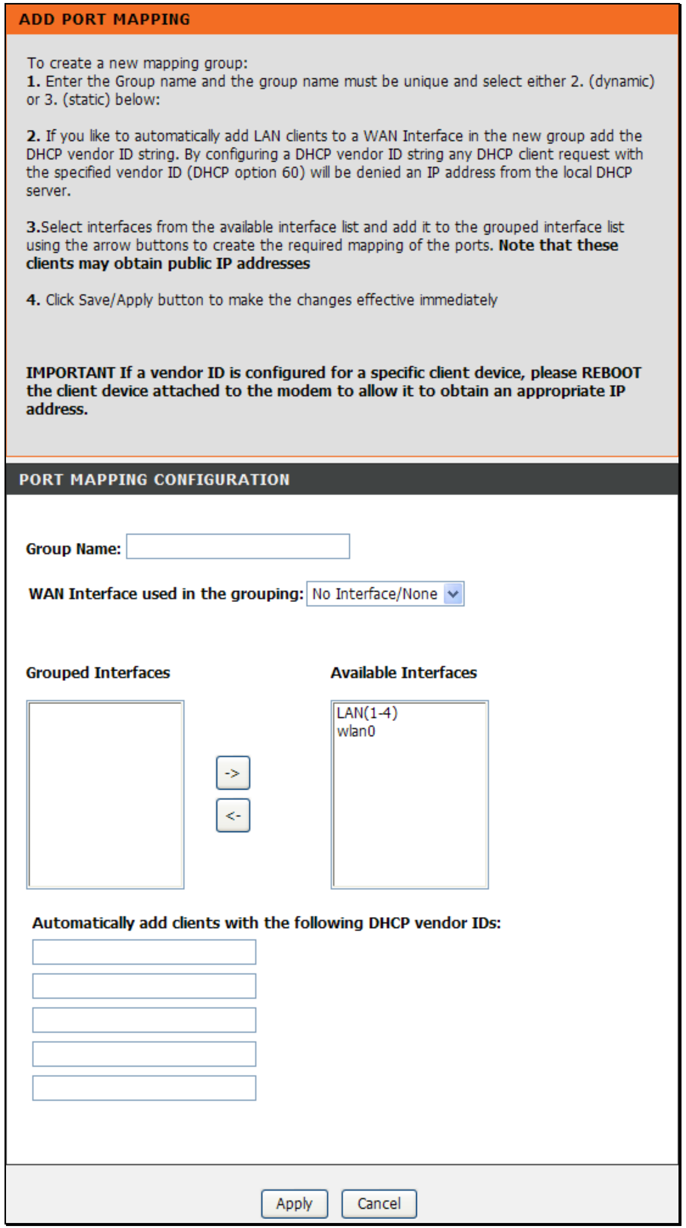
PORT MAPPING SETUP

Group Name	WAN Interface	LAN Interfaces	DHCP Vendor IDs		
Default		LAN(1-4), wlan0			

Click the **Add** button to see the Add Port Mapping section.

To create a new mapping group, enter **Group Name**, add interfaces to **Grouped Interfaces**.

Click the **Apply** button to save the changes.



ADD PORT MAPPING

To create a new mapping group:
1. Enter the Group name and the group name must be unique and select either 2. (dynamic) or 3. (static) below:

2. If you like to automatically add LAN clients to a WAN Interface in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.

3.Select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. **Note that these clients may obtain public IP addresses**

4. Click Save/Apply button to make the changes effective immediately

IMPORTANT If a vendor ID is configured for a specific client device, please REBOOT the client device attached to the modem to allow it to obtain an appropriate IP address.

PORT MAPPING CONFIGURATION

Group Name:

WAN Interface used in the grouping: No Interface/None

Grouped Interfaces

Available Interfaces: LAN(1-4), wlan0

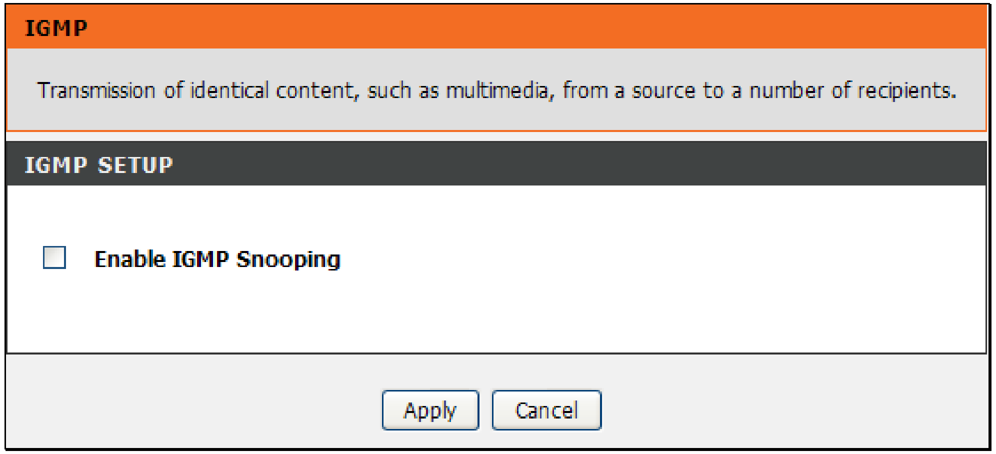
Automatically add clients with the following DHCP vendor IDs:

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 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.

Click the **Apply** button to take effect.



IGMP

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

IGMP SETUP

□ Enable IGMP Snooping

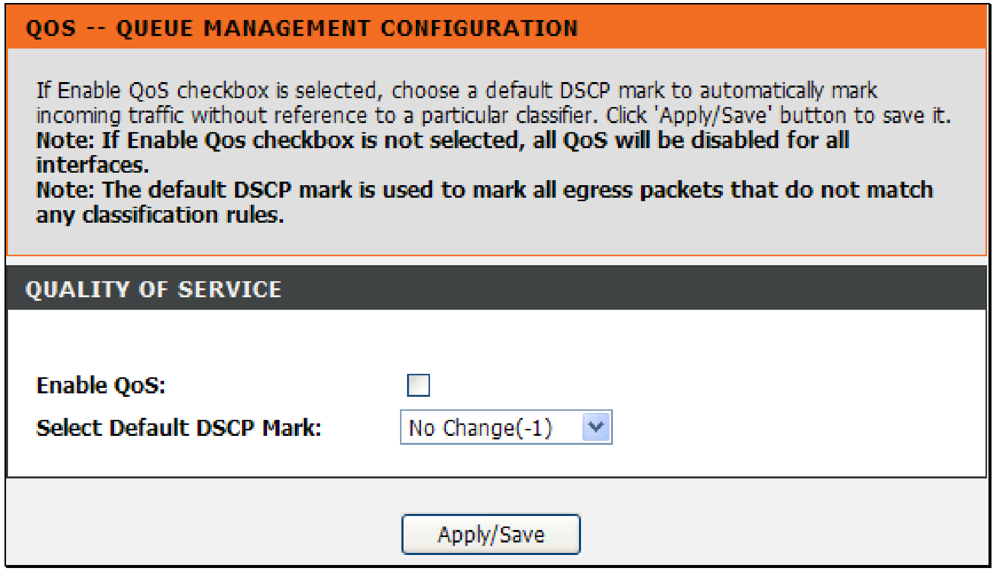
Quality of Service

To access QoS, 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.

QoS or Quality of Service allows your Router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs.

Tick the **Enable QoS** check box and select a default DSCP mark from the drop-down menu.

When you are finished, click **Apply/Save** to take the settings 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)

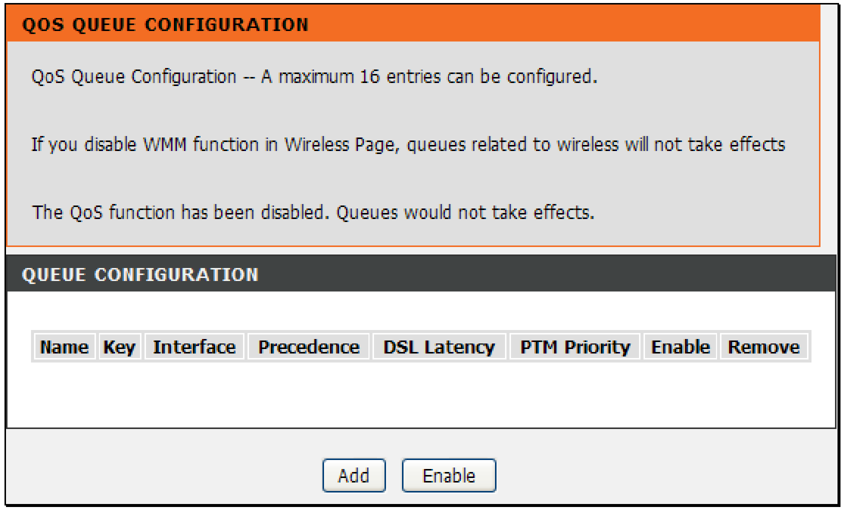
Queue Config

To access Queue Config, 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.

Click the **Add** button to add a Queue Configuration entry.

In the Add Queue Config section, enter the name and select from the **Enable**, **Interface**, and **Precedent** drop-down menu to configure the queue.

Click the **Apply/Save** button to save and activate this rule.



QOS QUEUE CONFIGURATION

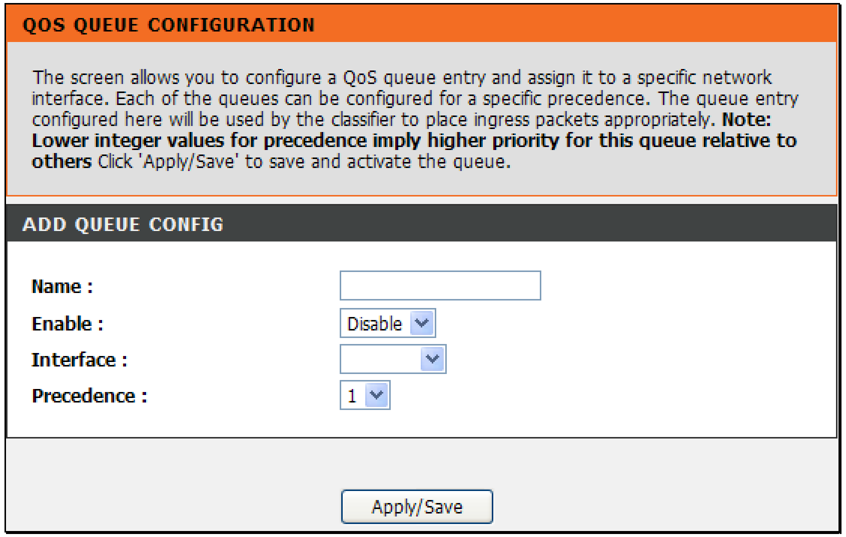
QoS Queue Configuration -- A maximum 16 entries can be configured.

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

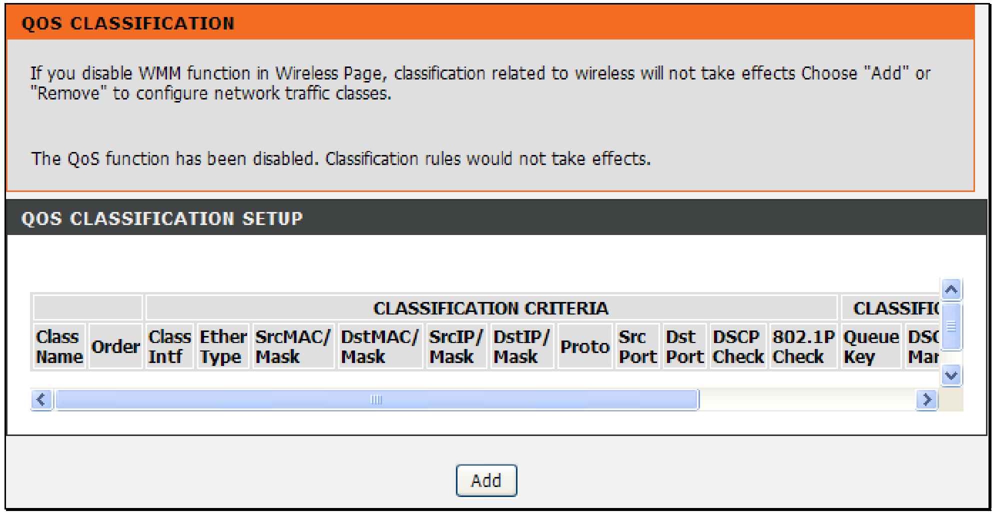
Name :
Enable : Disable
Interface :
Precedence : 1

Queue Classfication

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 on the **Add** button to add a new entry.



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.

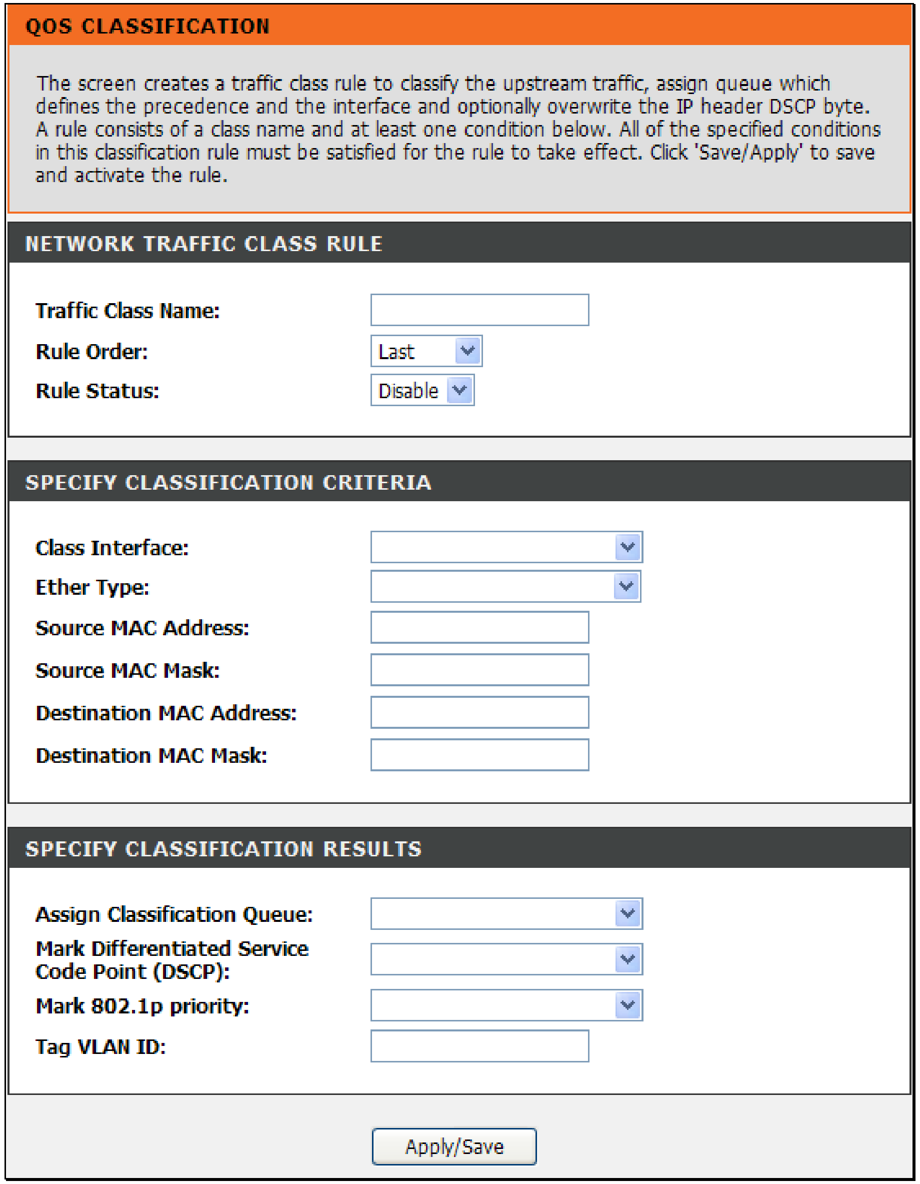
The QoS function has been disabled. Classification rules would not take effects.

QOS CLASSIFICATION SETUP

		CLASSIFICATION CRITERIA											CLASSIFI	
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	DSC Mar

Use this window to create a traffic class rule to classify the upstream traffic, assign a queue that 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. Please remember that all of the specified conditions on this window must be met for the rule to take effect.

Click the **Apply/Save** button to save and activate this 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

SPECIFY CLASSIFICATION CRITERIA

Class Interface:	
Ether Type:	
Source MAC Address:	
Source MAC Mask:	
Destination MAC Address:	
Destination MAC Mask:	

SPECIFY CLASSIFICATION RESULTS

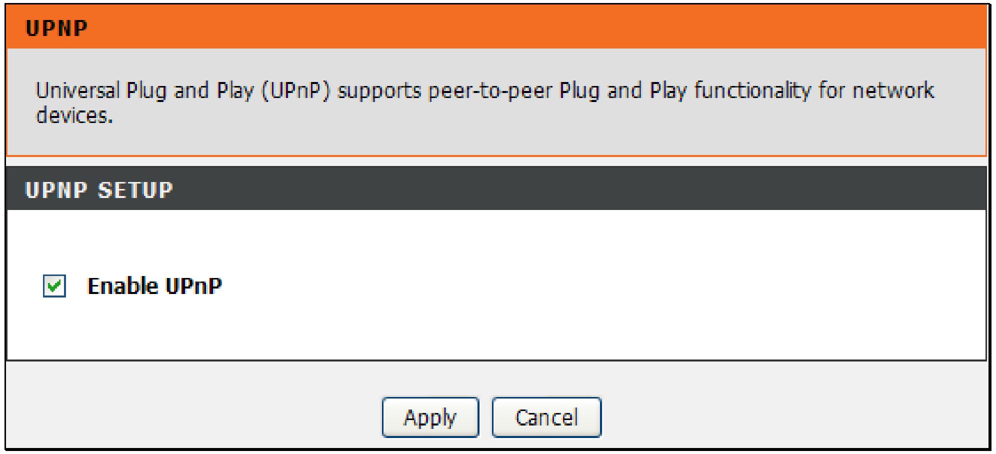
Assign Classification Queue:	
Mark Differentiated Service Code Point (DSCP):	
Mark 802.1p priority:	
Tag VLAN ID:	

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.

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



UPNP

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

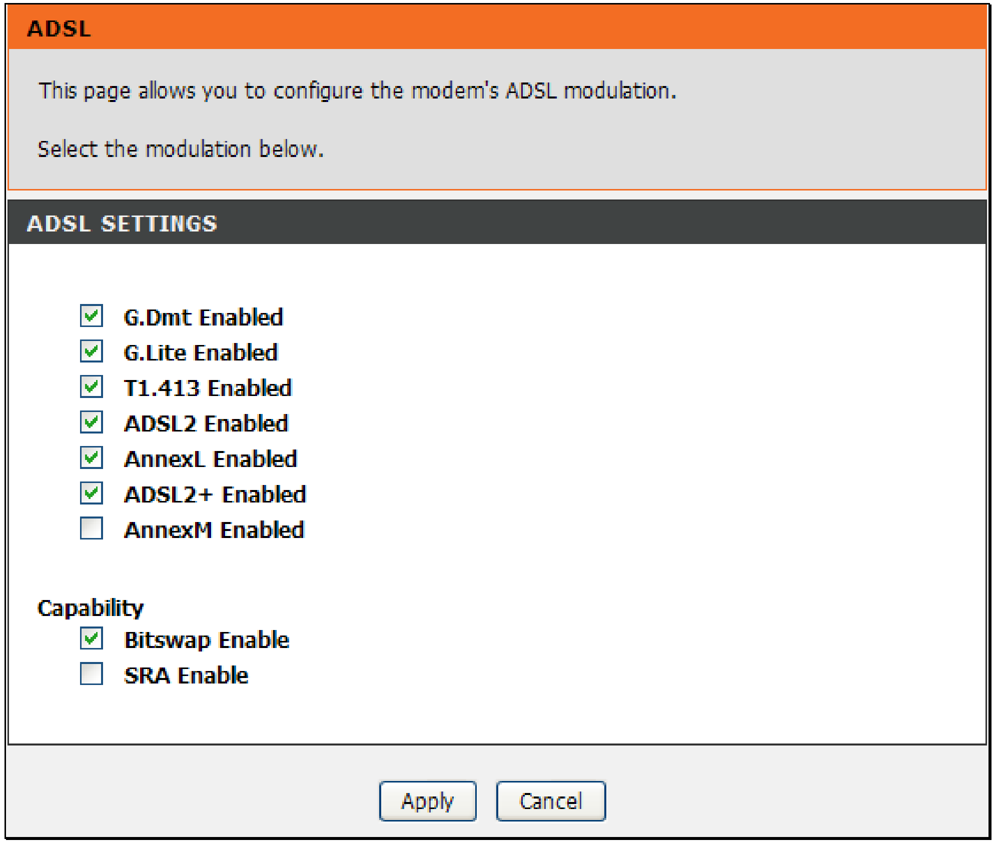
UPNP SETUP

☑ Enable UPnP

DSL

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

This window allows you to select the desired modulation, phone line pair, and capability. Click the **Apply** button when you are finished.



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

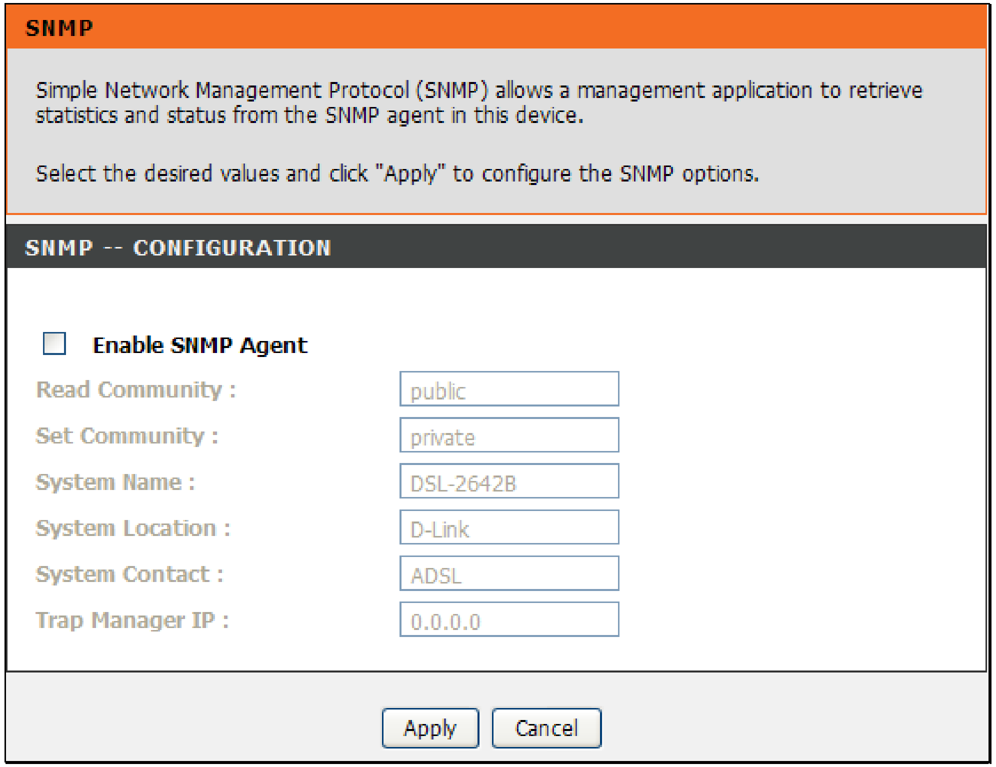
Capability
☑ Bitswap Enable
□ SRA Enable

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-2642B
System Location :	D-Link
System Contact :	ADSL
Trap Manager IP :	0.0.0.0

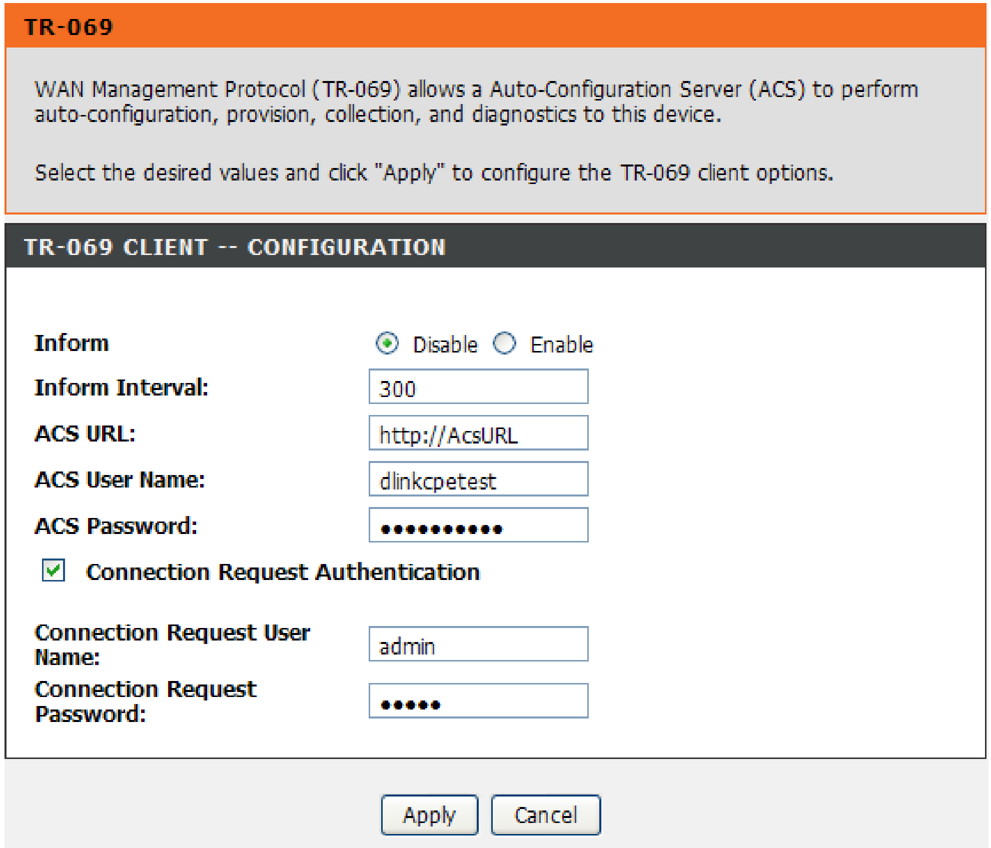
TR-069

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.

Inform: Select this option to enable the TR-069 feature on this device.
Inform Interval: Enter the Inform Interval used here.
ACS URL: Enter the ACS URL used here.
ACS User Name: Enter the ACS username used here.
ACS Password: Enter the ACS password used here.
Connection Request Authentication: Select this option to enable connection request authentication.
Connection Request User Name: Enter the connection request username used for this feature in here.
Connection Request Password: Enter the connection request password used for this feature in here.

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



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:	http://AcsURL
ACS User Name:	dlinkcpetest
ACS Password:	••••••••••

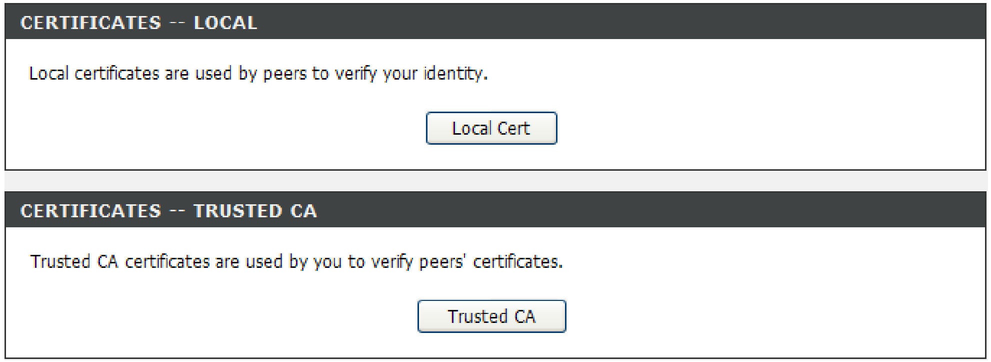
☑ Connection Request Authentication

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

Certificates

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

This is for TR-069 certification. There are two subcategories in Certificates: **Local Cert**, and **Trusted CA**. Click one of the buttons in the Certificates window.



CERTIFICATES -- LOCAL

Local certificates are used by peers to verify your identity.

CERTIFICATES -- TRUSTED CA

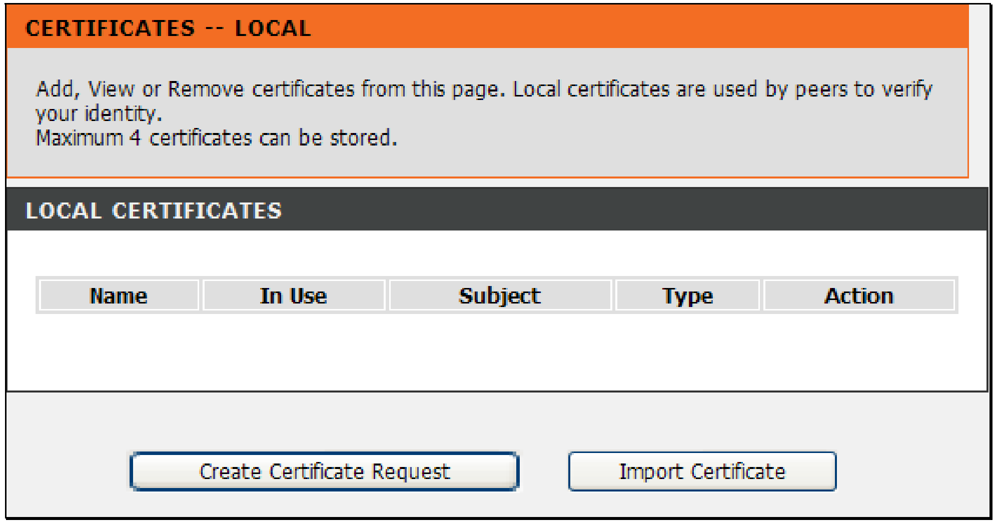
Trusted CA certificates are used by you to verify peers' certificates.

Certificates – Local Cert

This is for peers to verify your identity.

Click the **Create Certificate Request** button to add a local certificate entry.

Click **Import Certificate** button to paste certificate content and private key.



CERTIFICATES -- LOCAL

Add, View or Remove certificates from this page. Local certificates are used by peers to verify your identity.
Maximum 4 certificates can be stored.

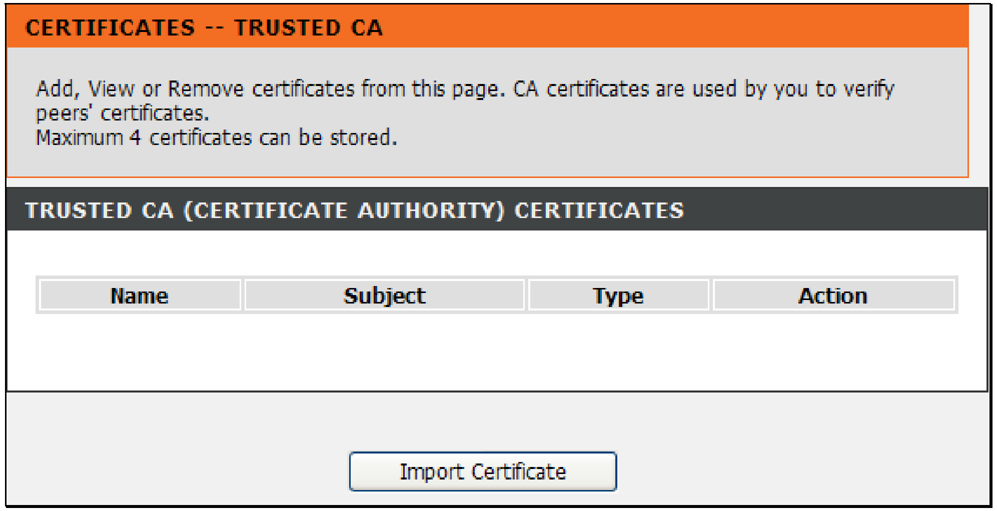
LOCAL CERTIFICATES

Name	In Use	Subject	Type	Action

Certificates – Trusted CA

This is for you to verify peers' certificates.

Click **Import Certificate** button to paste certificate content.



CERTIFICATES -- TRUSTED CA

Add, View or Remove certificates from this page. CA certificates are used by you to verify peers' certificates.
Maximum 4 certificates can be stored.

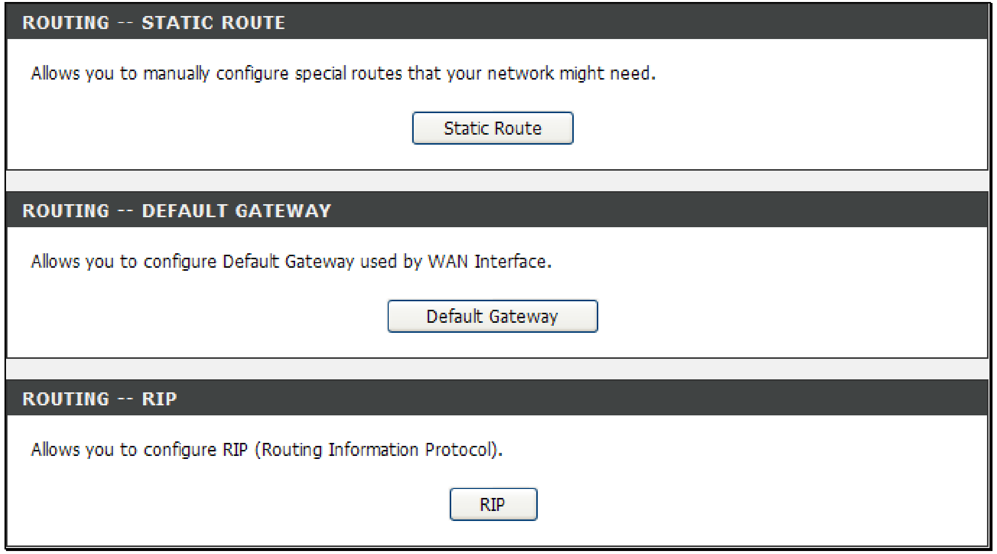
TRUSTED CA (CERTIFICATE AUTHORITY) CERTIFICATES

Name	Subject	Type	Action

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

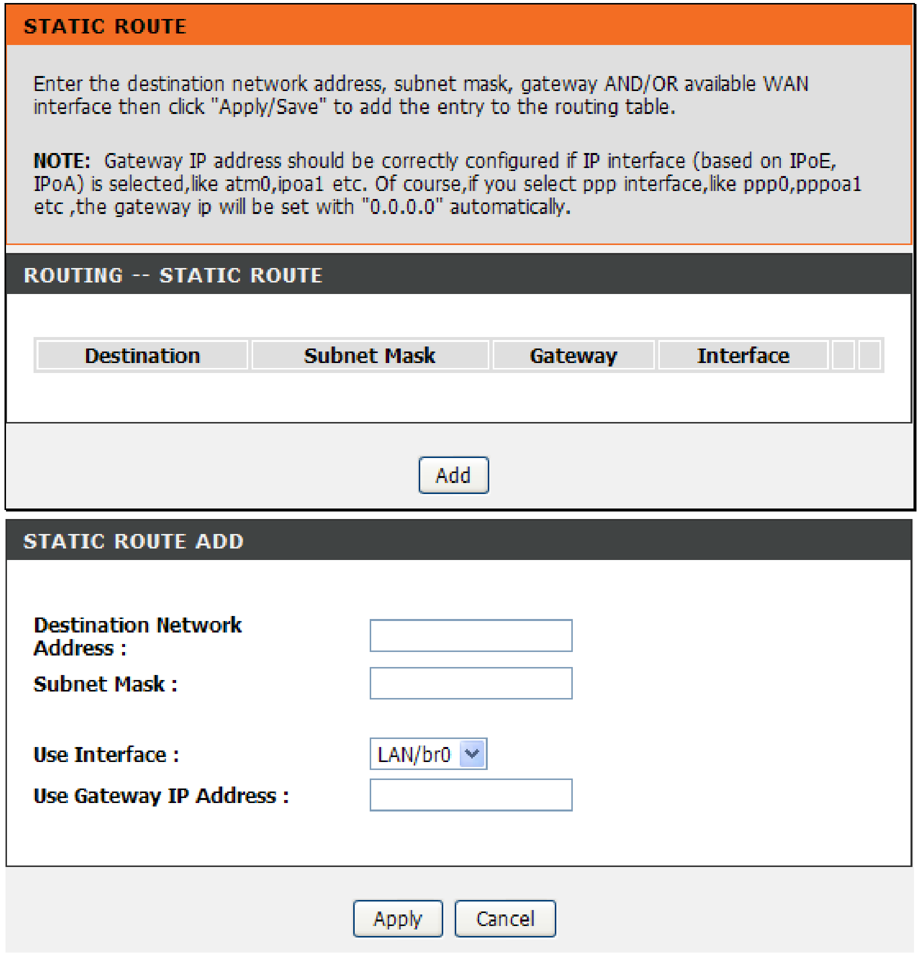
Allows you to configure RIP (Routing Information Protocol).

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, complete the fields in the Add Static Route section. 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 add a static route to a specific destination IP, click **Add** to see the Add Static Route section. Enter a **Destination** IP address, **Netmask** and Gateway's IP address. Select a PVC in the **Connection** drop-down list. Click **Apply** to see the entry in the Active Static Route table. To remove an entry in the table, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 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		

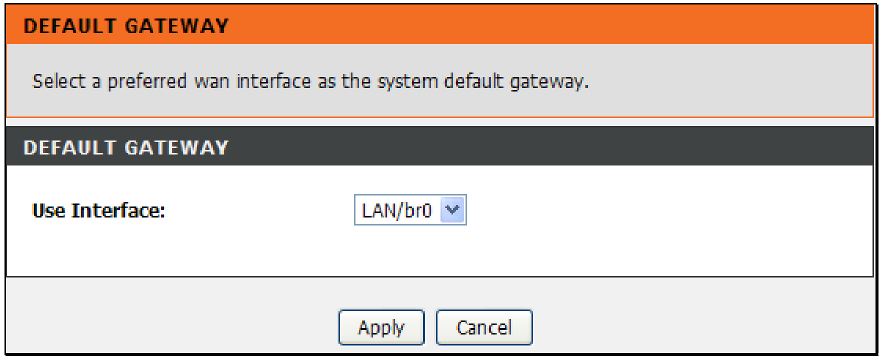
STATIC ROUTE ADD

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 either automatically assign a default gateway to the device or manually type in a default gateway or the device or interface. It is recommended to select **Enable Automatic Assigned Default Gateway** to automatically detect the Gateway IP address.



DEFAULT GATEWAY

Select a preferred wan interface as the system default gateway.

DEFAULT GATEWAY

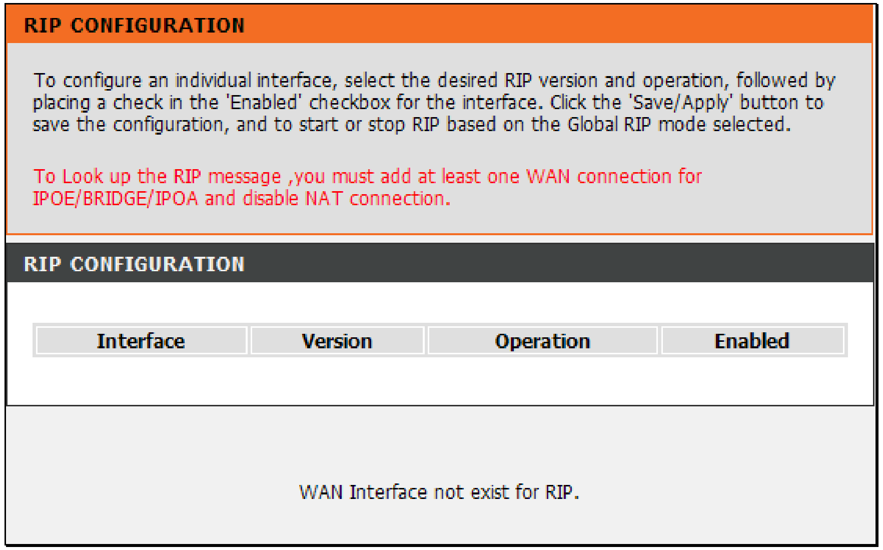
Use Interface: LAN/br0

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, tick the Enable check box of the interface you want to enable, 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/Save** button to 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

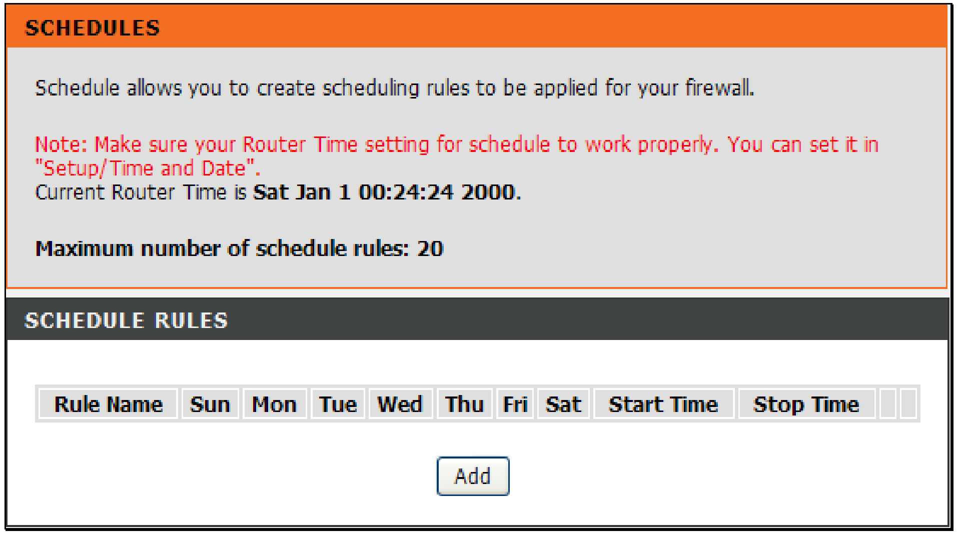
WAN Interface not exist for RIP.

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, click the corresponding 🗑 button. To modify a table entry, click the corresponding 📝 button, make the desired changes, and then click the **Apply** button.



SCHEDULES

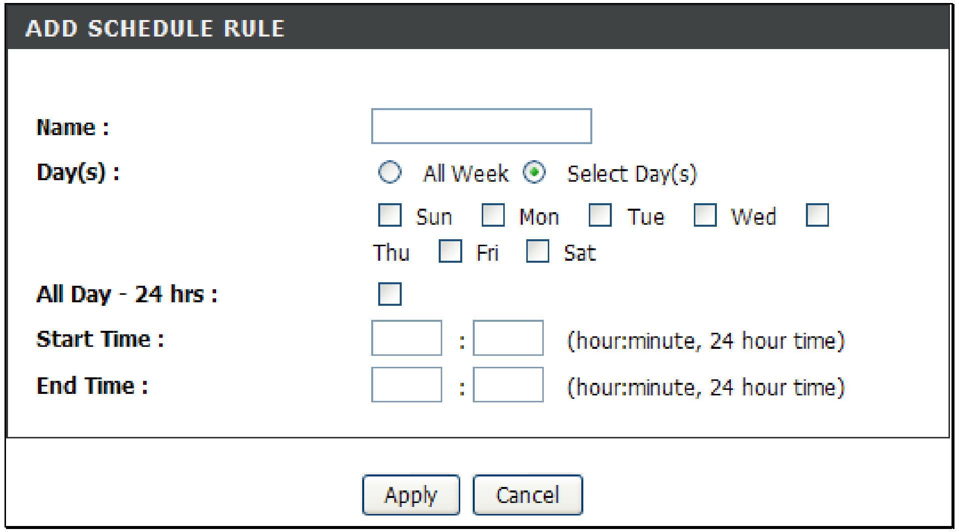
Schedule allows you to create scheduling rules to be applied for your firewall.

Note: Make sure your Router Time setting for schedule to work properly. You can set it in "Setup/Time and Date".
Current Router Time is **Sat Jan 1 00:24:24 2000.**

Maximum number of schedule rules: 20

SCHEDULE RULES

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



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)

Maintenance

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

System

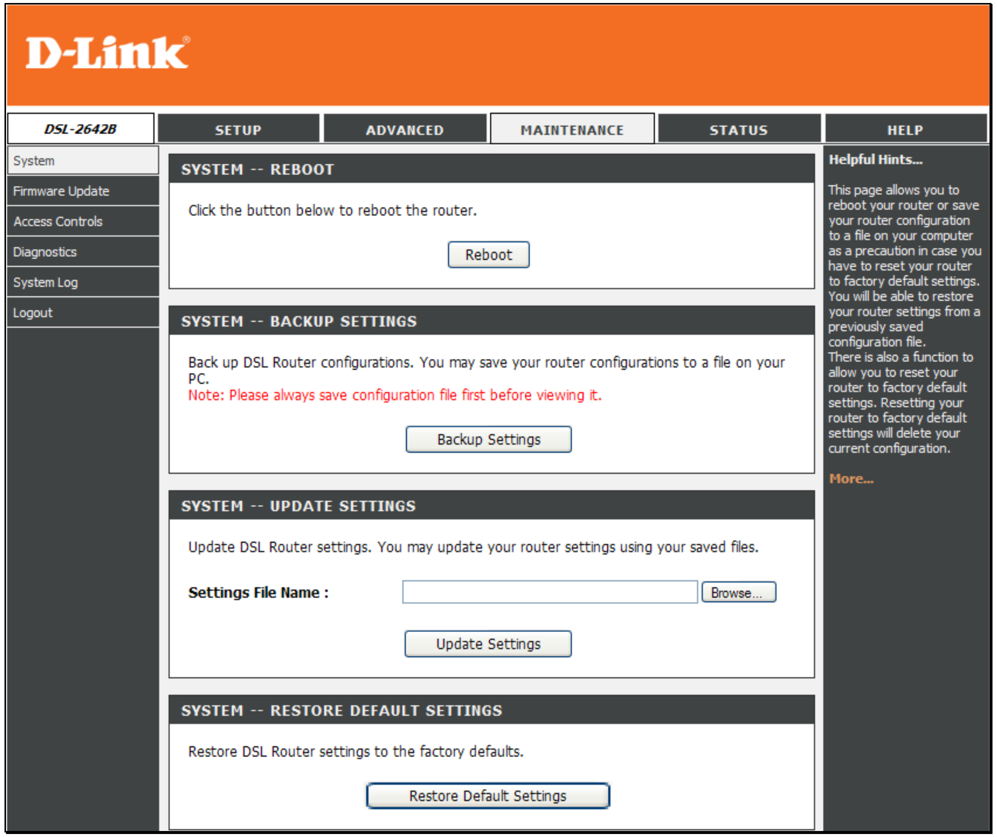
To access the System window, click the **System** button in the **Maintenance** directory.

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.

Helpful Hints...

This page allows you to reboot your router or save your router configuration to a file on your computer as a precaution in case you have to reset your router to factory default settings. You will be able to restore your router settings from a previously saved configuration file.
There is also a function to allow you to reset your router to factory default settings. Resetting your router to factory default settings will delete your current configuration.

Firmware Update

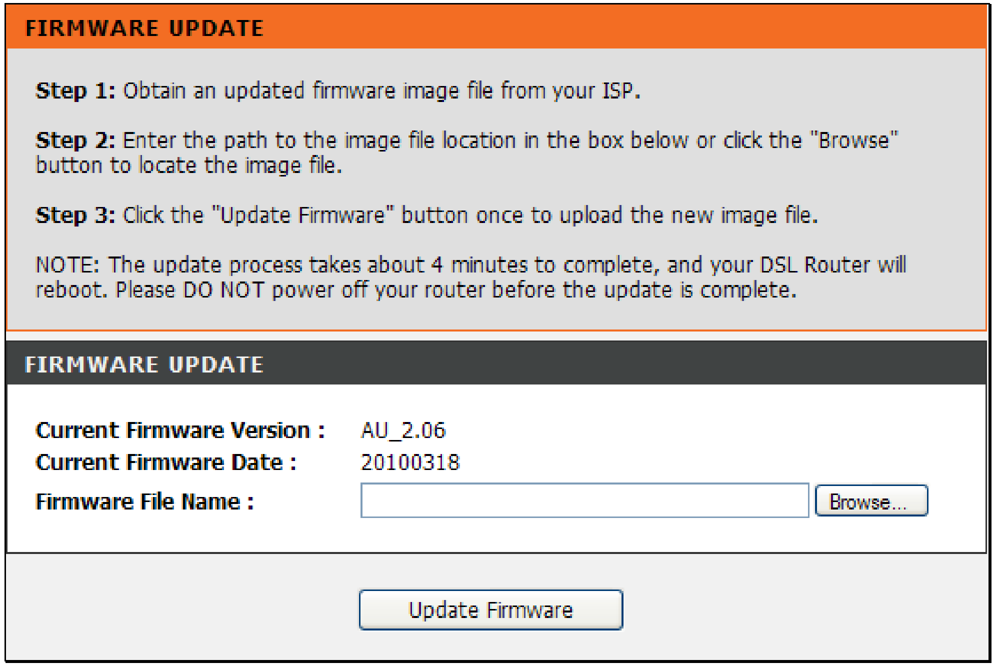
To access the **Firmware Update** window, click the **Firmware Update** button in the **Maintenance** directory.

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_2.06

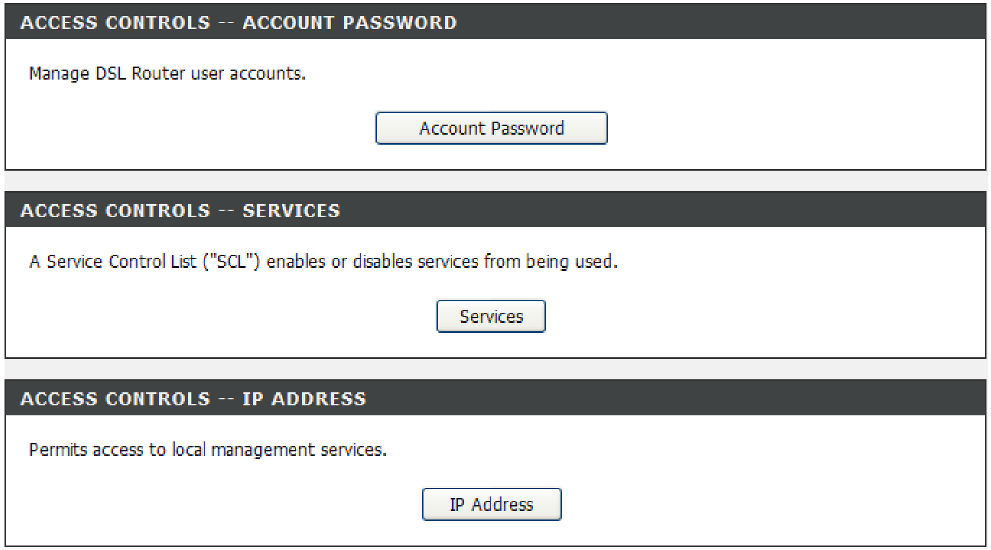
Current Firmware Date : 20100318

Firmware File Name :

Access Controls

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

There are three subcategories in Access Controls: **Account Password**, **Services**, and **IP Address**. You can Y either point to the **Access Controls** on the left window and click one of the submenus, or click one of the buttons in the Access Controls window.



ACCESS CONTROLS -- ACCOUNT PASSWORD

Manage DSL Router user accounts.

ACCESS CONTROLS -- SERVICES

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

ACCESS CONTROLS -- IP ADDRESS

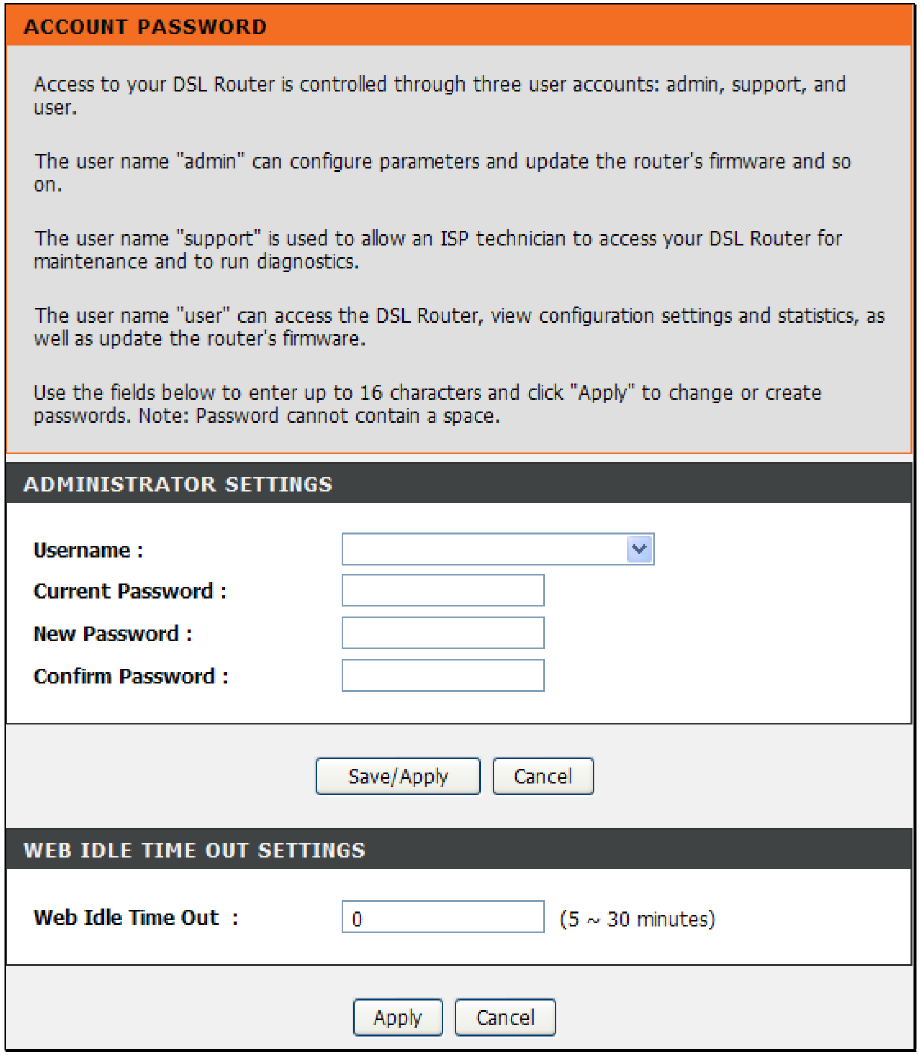
Permits access to local management services.

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, User or Support), 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.

You can configure the idle time between 5 and 30 minutes for the webpage asking you to logout.
Click the **Apply** button to save the changes.



ACCOUNT PASSWORD

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

The user name "admin" can configure parameters and update the router's firmware and so on.

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

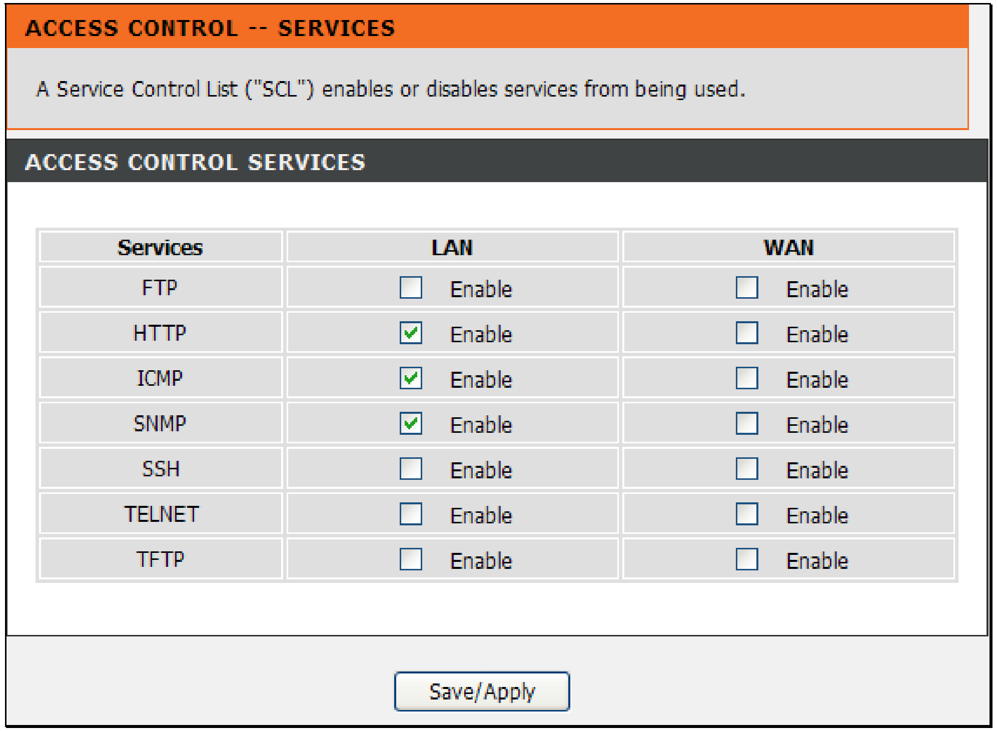
Web Idle Time Out : 0 (5 ~ 30 minutes)

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 FTP, HTTP, ICMP, SNMP, SSH, TELNET, and TFTP that can enable at LAN, WAN or both. Tick to enable the services, or deselect to disable them.

When you are finished, click **Apply/Save** to save the settings.



ACCESS CONTROL -- SERVICES

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

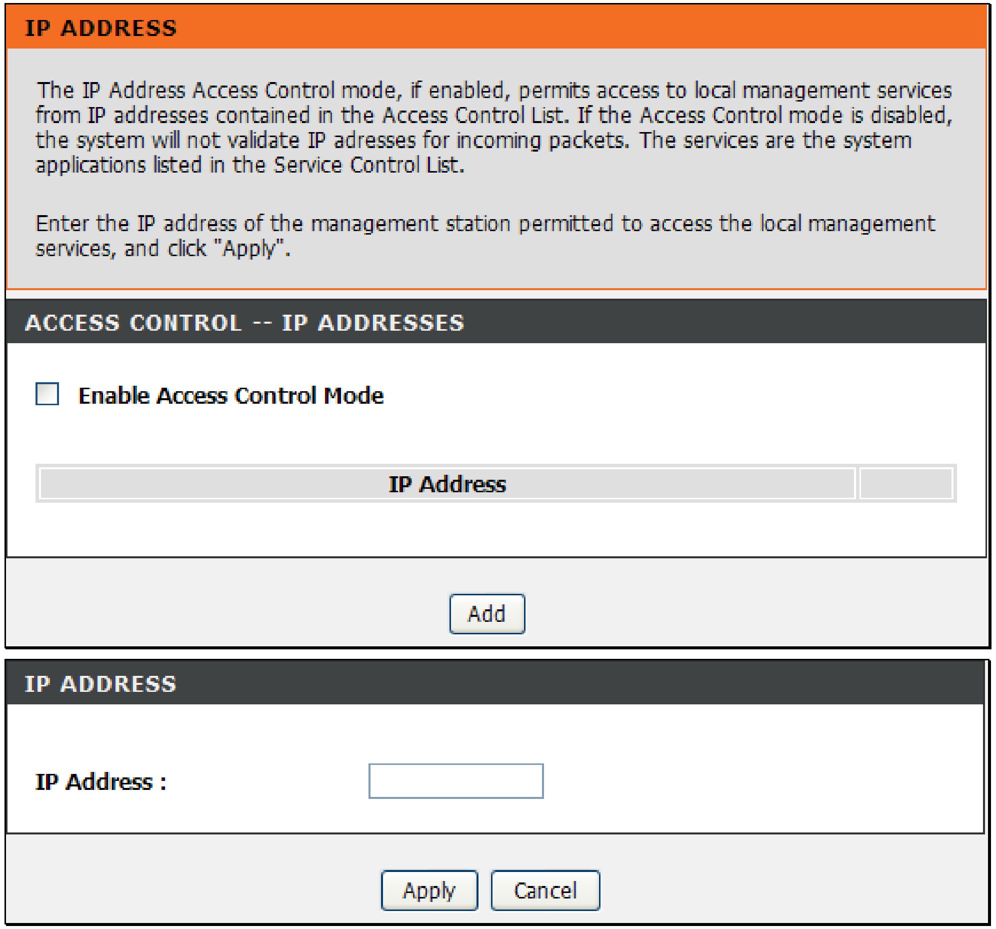
ACCESS CONTROL SERVICES

Services	LAN	WAN
FTP	□ Enable	□ Enable
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 and click **Apply** in this section 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	

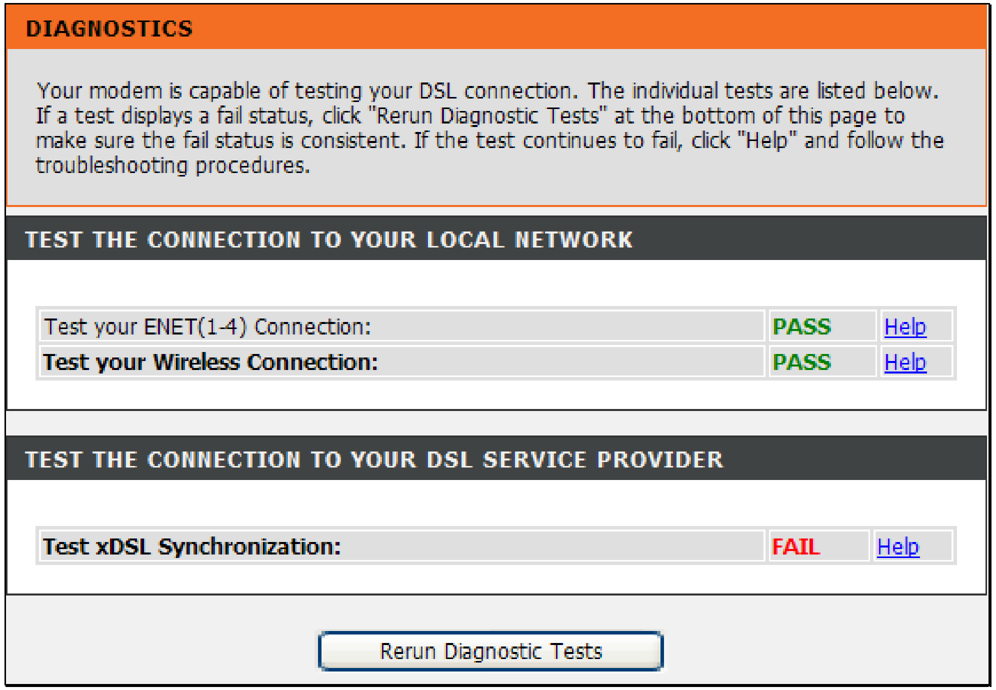
IP ADDRESS

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.



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 ENET(1-4) Connection:	PASS	Help
Test your Wireless Connection:	PASS	Help

TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER

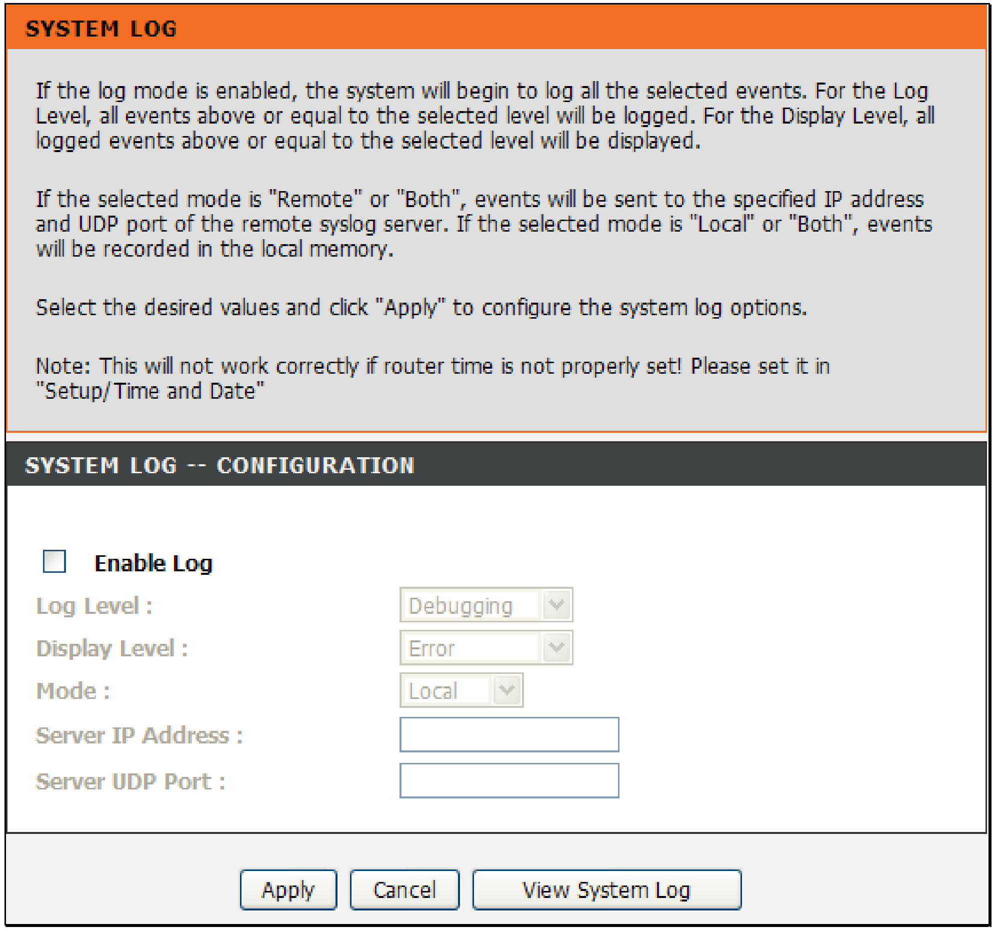
Test xDSL Synchronization:	FAIL	Help

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 Remote 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.



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 router 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 :	

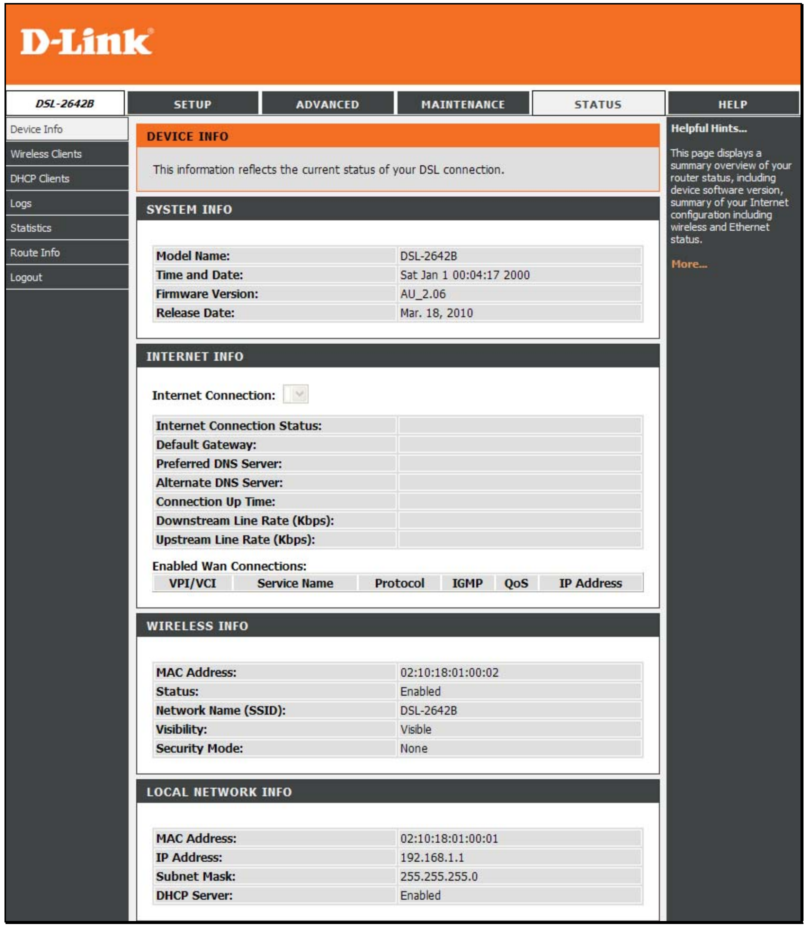
Status

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-2642B
Time and Date:	Sat Jan 1 00:04:17 2000
Firmware Version:	AU_2.06
Release Date:	Mar. 18, 2010

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:	02:10:18:01:00:02
Status:	Enabled
Network Name (SSID):	DSL-2642B
Visibility:	Visible
Security Mode:	None

LOCAL NETWORK INFO

MAC Address:	02:10:18:01:00:01
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enabled

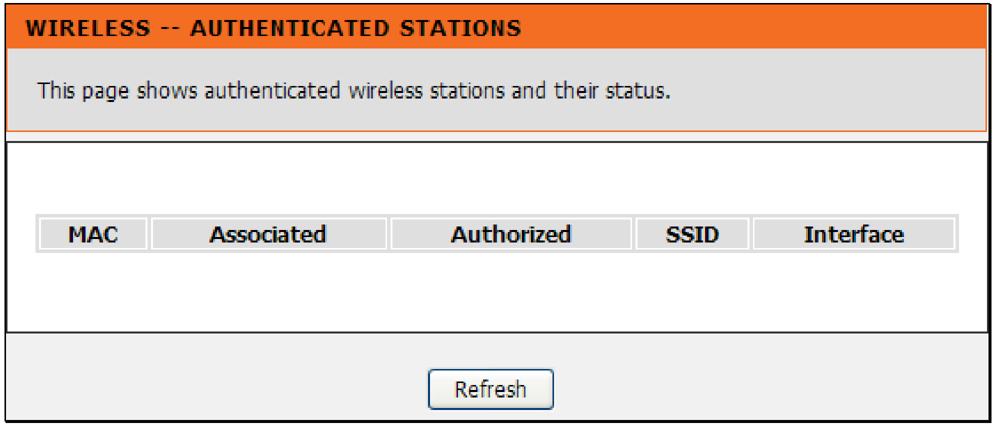
Helpful Hints...

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

Wireless Clients

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

The page displays the authenticated wireless stations and their status. Click the **Refresh** button to update the status.



WIRELESS -- AUTHENTICATED STATIONS

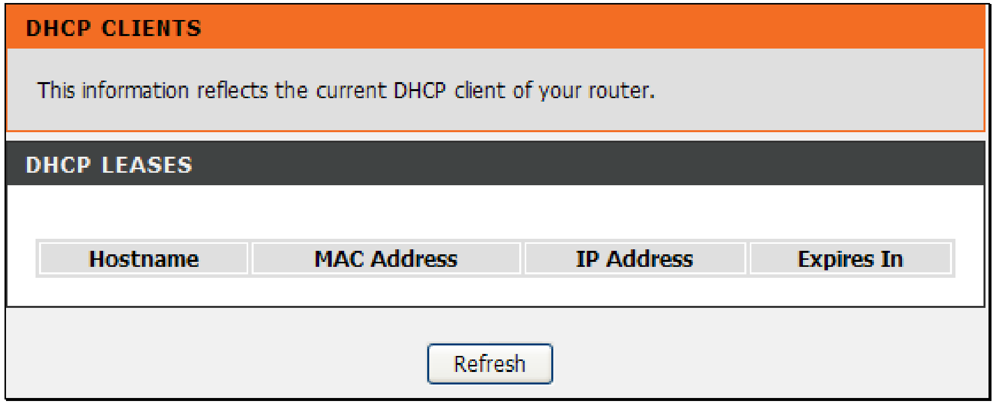
This page shows authenticated wireless stations and their status.

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. Click the **Refresh** button to update the status.



DHCP CLIENTS

This information reflects the current DHCP client of your router.

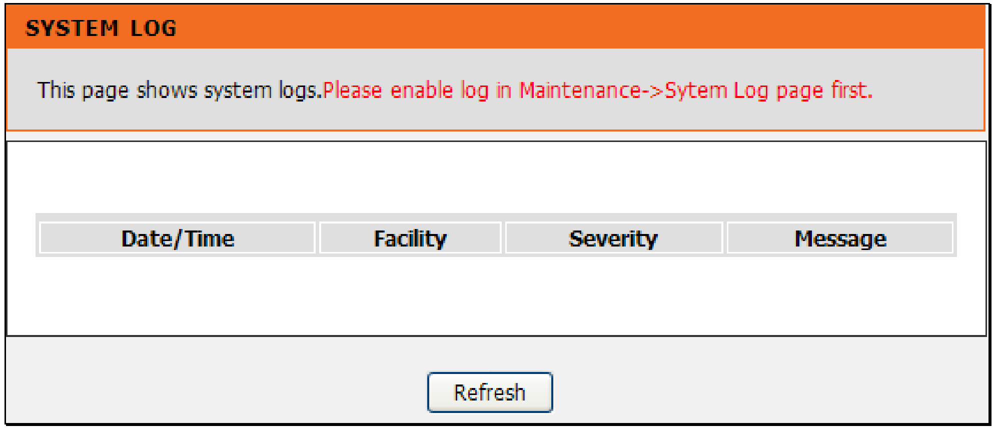
DHCP LEASES

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. Click the **Refresh** button to update the status.



SYSTEM LOG

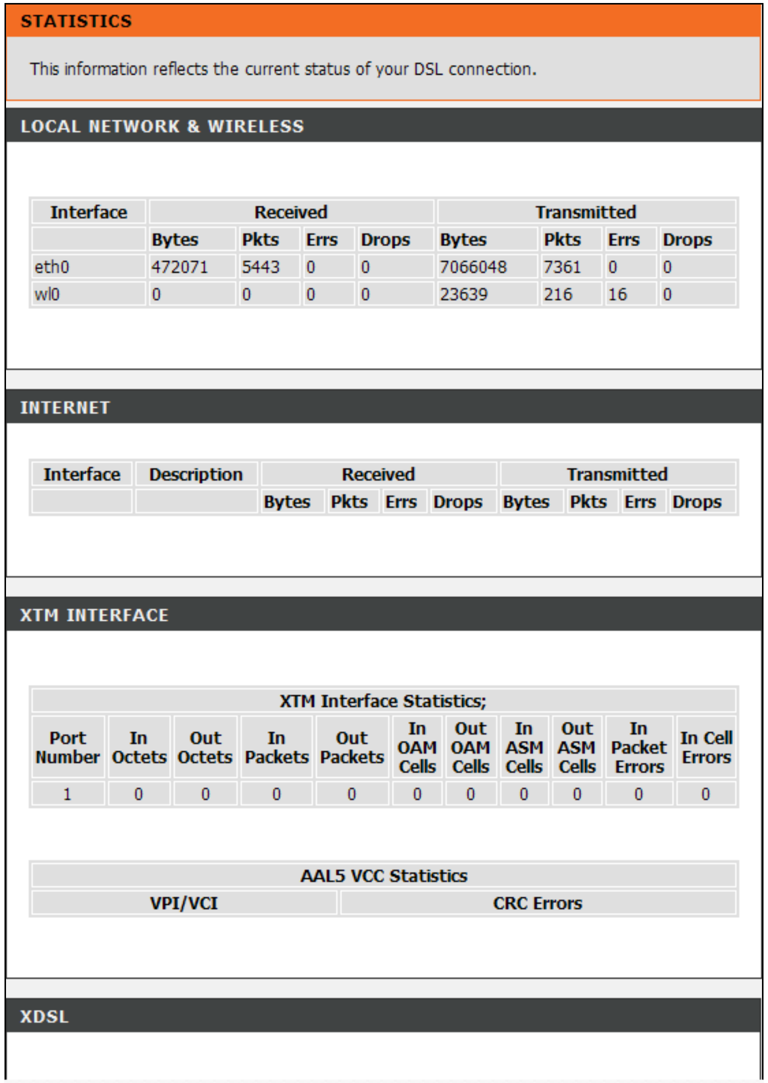
This page shows system logs.Please enable log in Maintenance->Sytem Log page first.

Date/Time	Facility	Severity	Message

Statistics

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

Use this window 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	472071	5443	0	0	7066048	7361	0	0
wl0	0	0	0	0	23639	216	16	0

INTERNET

Interface	Description	Received				Transmitted			
		Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops

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

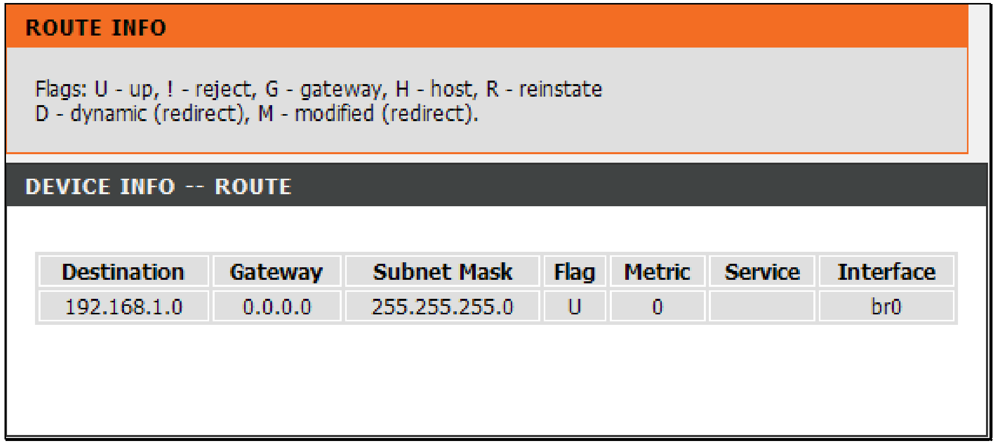
AAL5 VCC Statistics	
VPI/VCI	CRC Errors

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

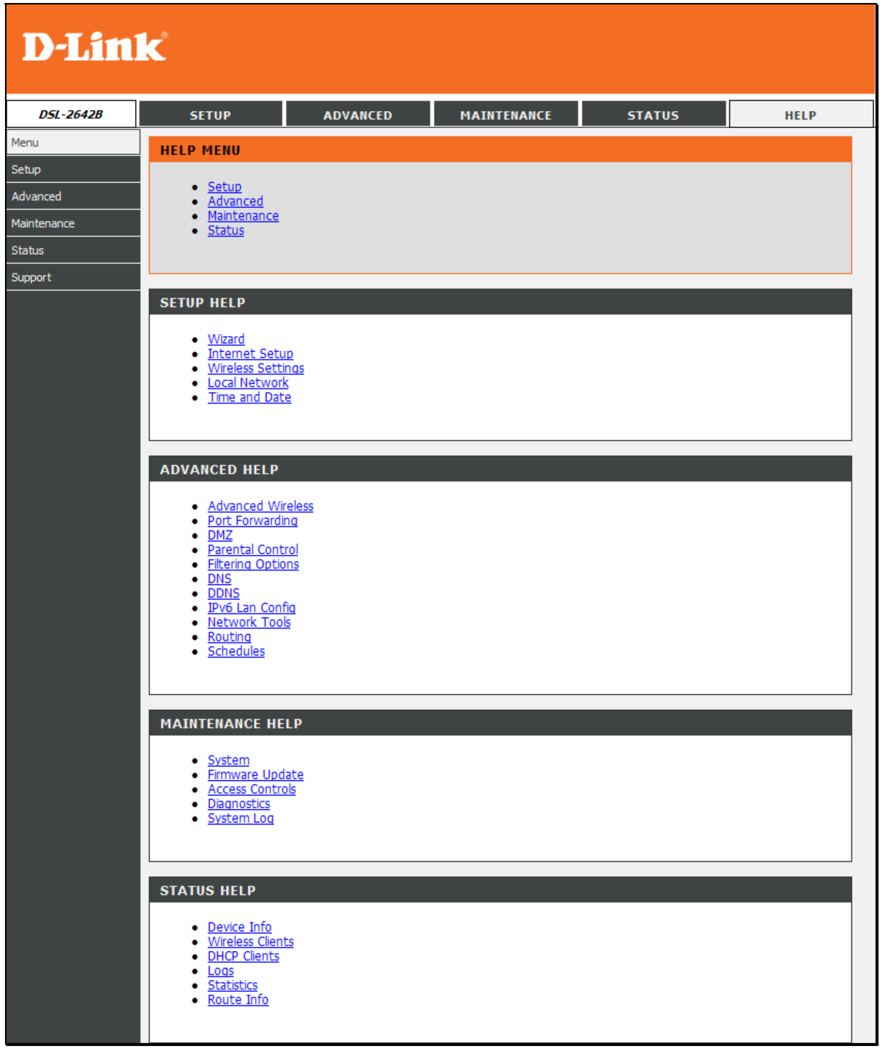
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate
D - dynamic (redirect), M - modified (redirect).

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
- IPv6 Lan Config
- 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-2642B. 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-2642B 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 5 to 8 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.

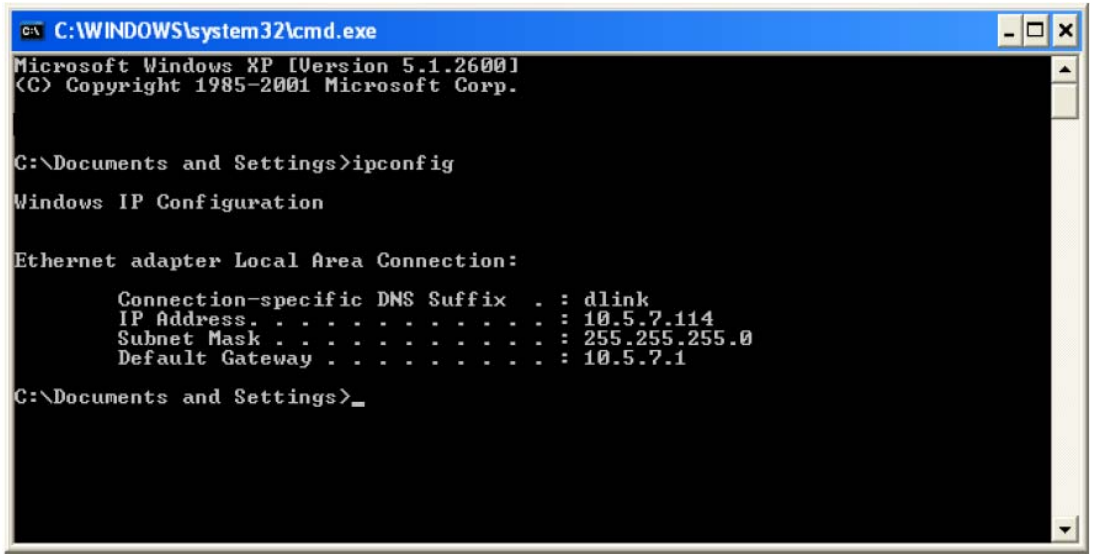
Click on **Start** > **Run**. In the run box type ***cmd*** and click on the **OK**.

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

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

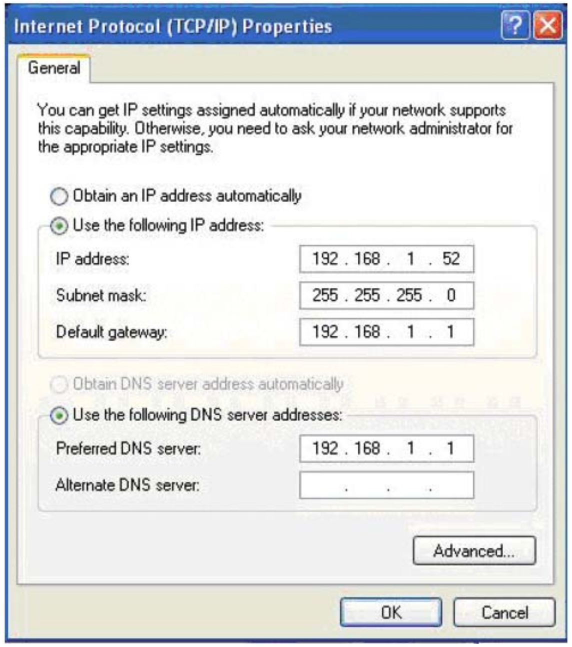
Step 3
Highlight **Internet Protocol (TCP/IP)** and click on the **Properties**.

Step 4
Click 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.

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



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: . . .

Technical Specifications

ADSL Standards

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

ADSL2 Standards

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

RE-ADSL2 (Reach Extended ADSL2)

- Annex L

ADSL2+ Standards

- ITU G.992.5 Annex A/M

Protocols

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

Data Transfer Rate

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

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