USER MANUAL

DSL-2750B

VERSION 3.0

D-Link®

BROADBAND

TABLE OF CONTENTS

PACKAGE CONTENTS

- Wireless N300 ADSL2+ Modem Router + USB (DSL-2750B)
- CD-ROM with Installation Wizard and User Manual
- Quick Installation Guide
- Ethernet Cable
- Phone Cable
- ADSL2+ Microfilter / Splitter
- Power Adapter

Note: Using a power supply with a different voltage rating than the one included With the DSL-2750B will cause damage and void the warranty for this product.

SYSTEM REQUIREMENTS

1. ADSL Internet service
   Computer with:
   - 200MHz Processor
   - 64MB Memory
   - Ethernet Adapter with TCP/IP Protocol Installed
   - Windows 8/7/Vista/XP/2000
   - MAC OS
   - Internet Explorer v6 or later, FireFox v1.5

2. D-Link Click's Connect Utility
   Computer with:
   - Windows 8/7/Vista/XP/2000
   - CD-ROM Drive

INTRODUCTION

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

HIGH-PERFORMANCE WIRELESS
Embedded 802.11n technology for high-speed wireless connection, complete compatibility with 802.11b/g wireless devices

TOTAL SECURITY
Firewall protection from Internet attacks, user access control, WPA/WPA2 wireless security.

ULTIMATE INTERNET CONNECTION
The DSL-2750B is a versatile, high-performance remote router for home and the small office. With integrated ADSL2/2+ supporting up to 24Mbps download speed, firewall protection, Quality of Service (QoS), 802.11n wireless LAN and 4 Ethernet switch ports, this router provides all the functions that a home or small office needs to establish a secure and high-speed remote link to the outside world.

ULTIMATE WIRELESS CONNECTION WITH MAXIMUM SECURITY
This router provides maximize wireless performance by connecting this router to computer interfaces and stay connected from virtually anywhere at home and in the office. The router can be used with 802.11b/g/n wireless networks to enable significantly improved reception. It supports WPA/WPA2 and WEP for flexible user access security and data encryption methods.

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

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

FEATURES

- **Faster Wireless Networking** - The DSL-2750B provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Compatible with 802.11b and 802.11g Devices** - The DSL-2750B is still fully compatible with the IEEE 802.11b and g standards, so it can connect with existing 802.11b and g PCI, USB and Cardbus adapters.

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

- **Network Address Translation (NAT)** - For small office environments, the DSL-2750B allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user. NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.

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

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

- **Full Network Management** - The DSL-2750B incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via Telnet connection.

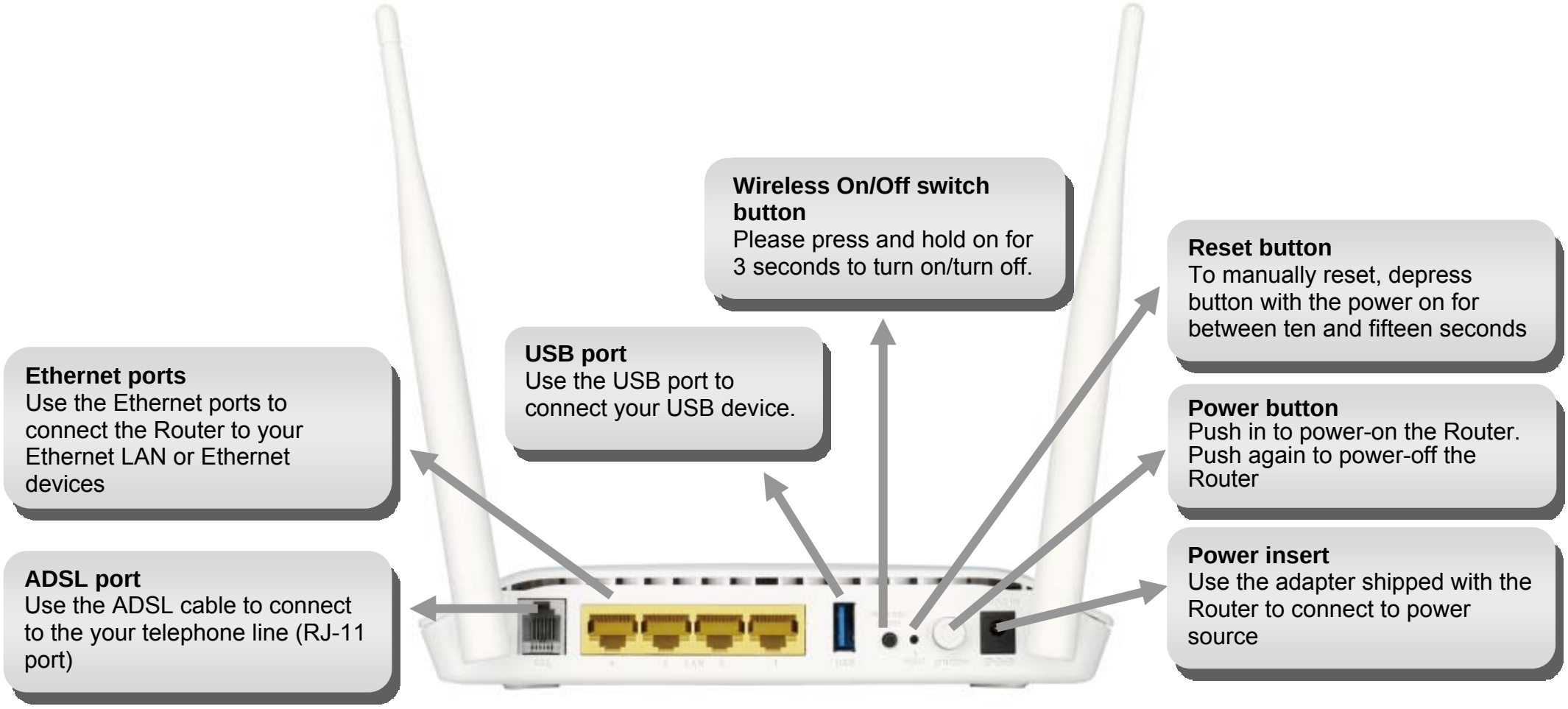
- **Easy Installation** - The DSL-2750B uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.

- **USB Support**- The DSL-2750B provides USB port for easy sharing files and printers. The DSL-2750B supports USB storage device sharing files through SAMBA file server, FTP server, Web file server and in addition also supports sharing USB printers to network members.

- **IPv6 Connection Support** – For IPv6 connection, the DSL-2750B provide several connection type: Link-local, Static IPv6, DHCPv6, Stateless Auto-configuration, PPPoE, and IPv6 in IPv4.

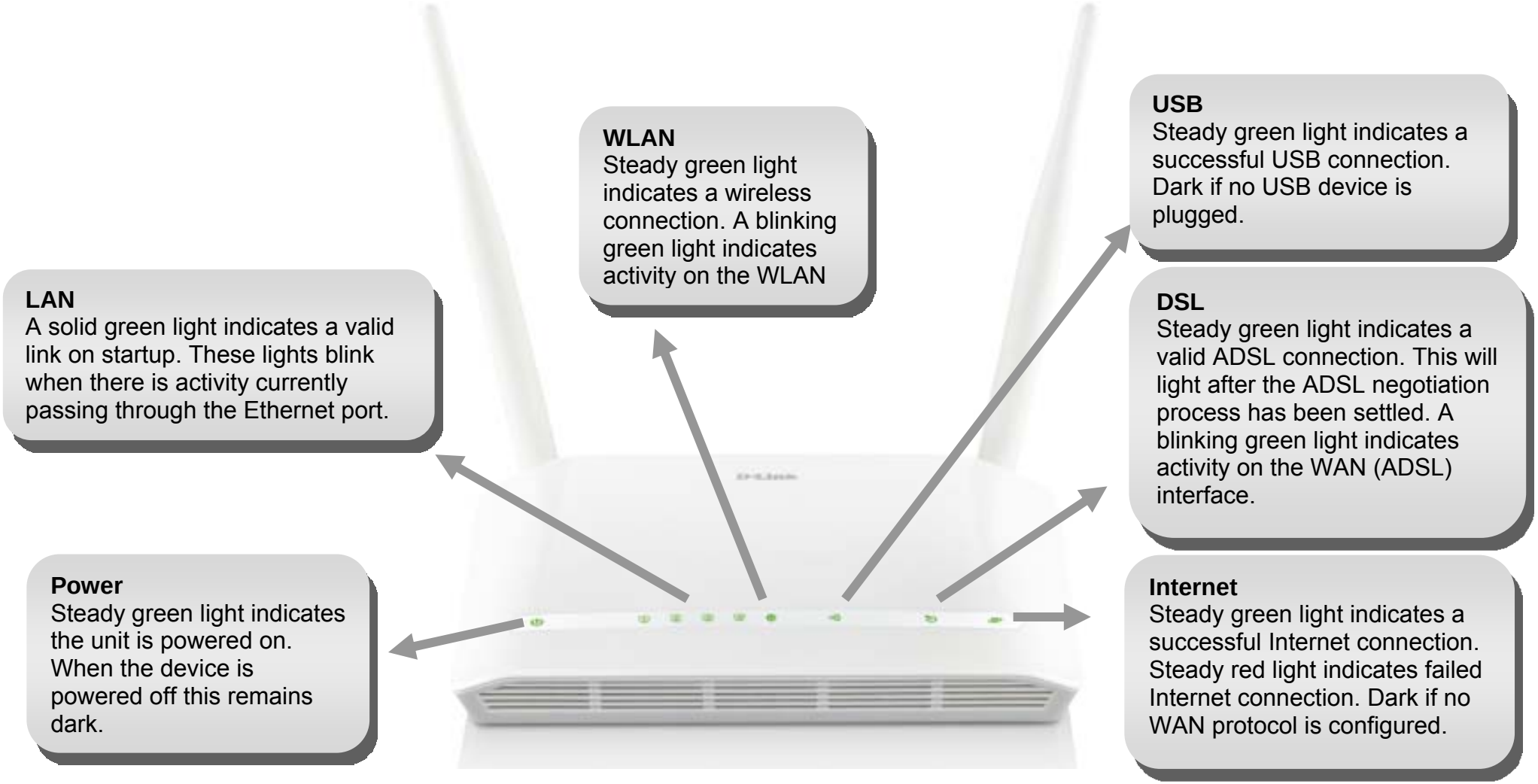
*Maximum wireless signal rate derived from IEEE standard 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental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

HARDWARE OVERVIEW
CONNECTIONS



HARDWARE OVERVIEW

LEDs



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 (Usern ame and Password) is required. For others, various parameters that control and defi ne 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 ha ve a hard copy of a ll the information needed to setup the Router . If it is necessary to reconfigure the device, all the nec essary 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-2750B 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, Windows 7 and Windows 8.

Web Browser

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

Ethernet Port (NIC Adapter)

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

802.11 Wireless LAN Configuration

All the 802.11 wireless LAN settings may be configured on a single page using the web-based manager. For basic wireless communication you need to decide what channel to use and what SSID to assign. These two settings must be the same for any wireless workstations or other wireless access point that communicate with the DSL-2750B through the wireless interface.

Security for wireless communication can be accomplished in a number of ways. The DSL-2750B supports WPA (Wi-Fi Protected Access), WPA2, and mixed WPA/WPA2. Wireless access can also be controlled by selecting MAC addresses that are allowed to associate with the device. Please read the section on Wireless Configuration.

Additional Software

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

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

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

Information You Will Need From Your ADSL Service Provider

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

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

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

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

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

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.

Note: Australian users will most likely be using a VPI of 8 and a VCI of 35.
New Zealand users will most likely be using a VPI of 0 and a VCI of 100.

Information You Will Need About DSL-2750B

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."

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-2750B
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-2750B
This is the subnet mask used by the DSL-2750B, 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-2750B to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2750B to connect to other computer or Ethernet devices.

DHCP Client status
Your DSL-2750B 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-2750B 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-2750B Wireless N300 ADSL2+ Modem Router + USB.

WIRELESS INSTALLATION CONSIDERATIONS

The DSL-2750B lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

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

2. Be aware of the direct line between network devices. A wall that is 0.5 metres, at a 45-degree angle appears to be almost 1 metre thick. At a 2-degree angle it looks over 14 metres thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

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

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

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

DEVICE INSTALLATION

The DSL-2750B Wireless ADSL Router maintains three separate interfaces, an Ethernet LAN, a wireless LAN and an ADSL Internet (WAN) connection. Carefully consider the Router's location suitable for connectivity for your Ethernet and wireless devices. You must have a functioning broadband connection via a bridge device such as a Cable or ADSL modem in order to use the Router's WAN function.

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

POWER ON ROUTER

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

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

FACTORY RESET BUTTON

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

1. Press and hold the reset button while the device is powered on.
2. Wait for 10 seconds and then release the reset button.

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

NETWORK CONNECTIONS

Connect ADSL Line

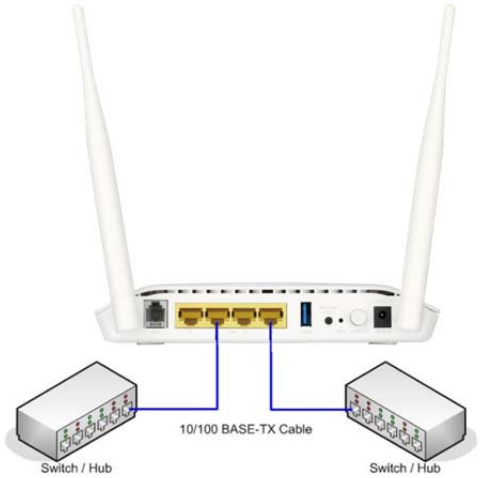
Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 connector) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the 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 Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port. Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch. The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

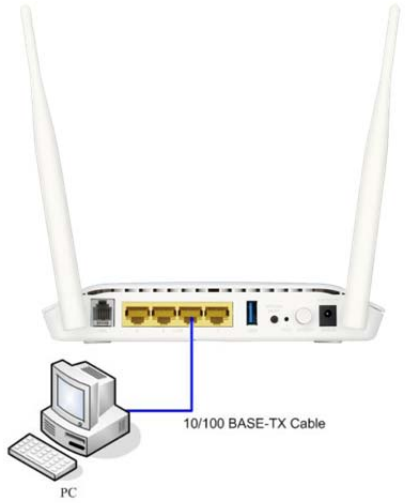
Hub or Switch to Router Connection

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



Computer to Router Connection

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



CONFIGURATION

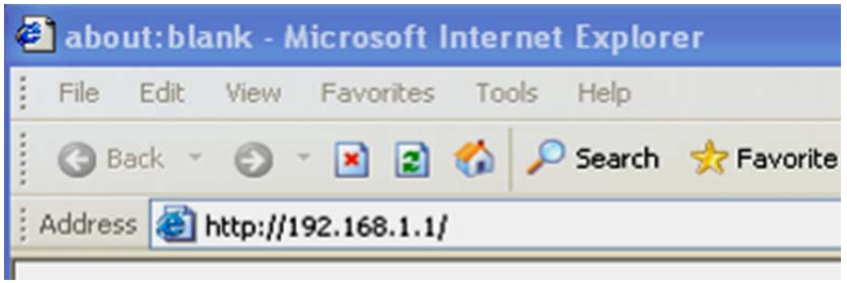
This section will show you how to configure your new D-Link Wireless Router using the web-based configuration utility.

WEB-BASED CONFIGURATION UTILITY

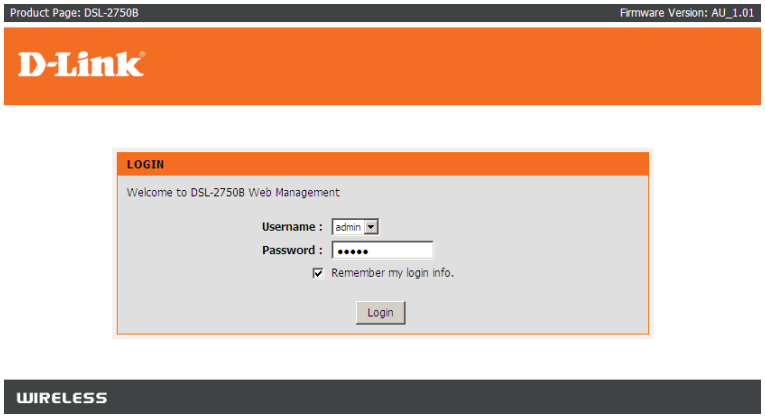
Connect to the Router

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

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



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



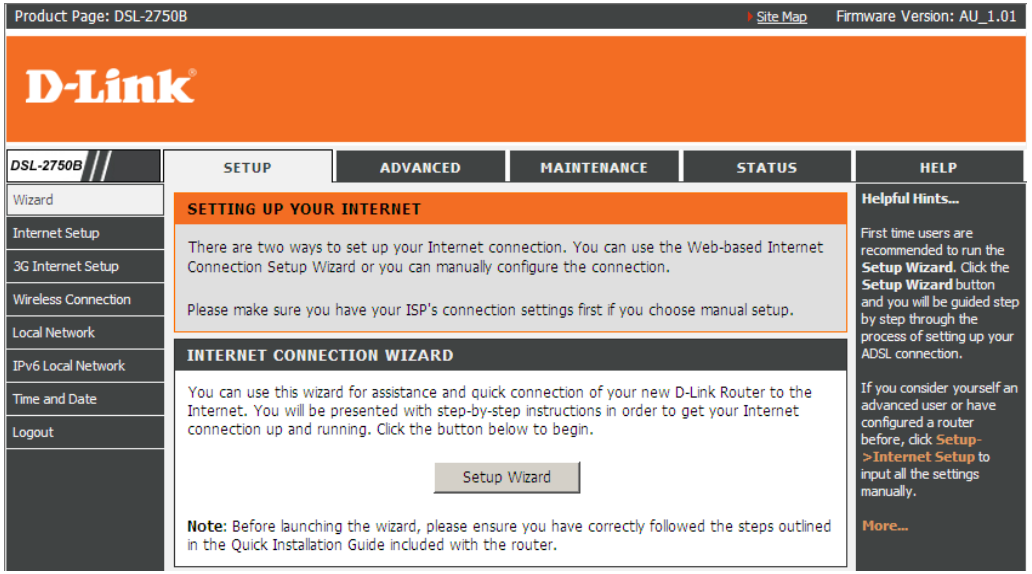
SETUP

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

WIZARD

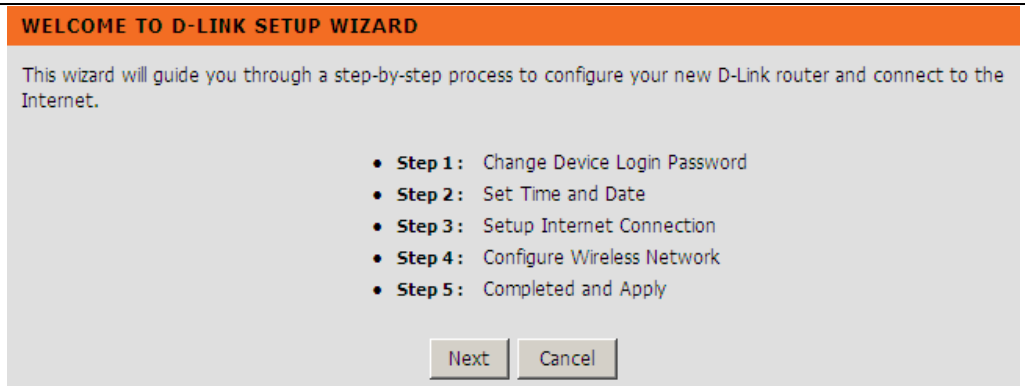
INTERNET CONNECTION WIZARD

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



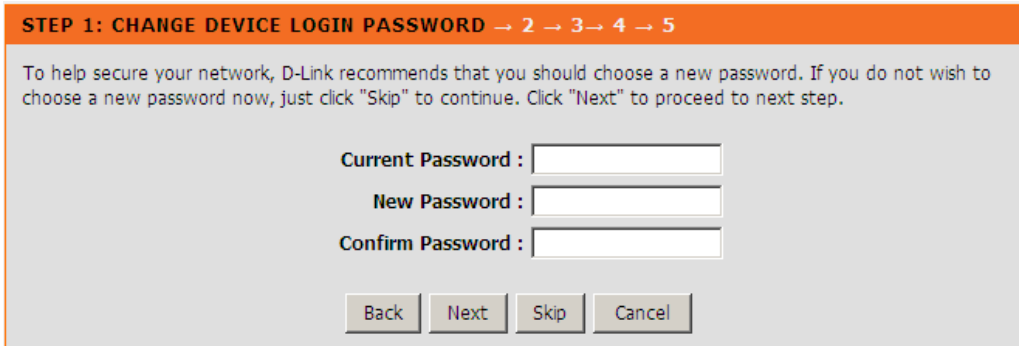
WELCOME TO D-LINK SETUP WIZARD

There are five steps to configuring your router. Click on the **Next** button to continue.



STEP 1: CHANGE DEVICE LOGIN PASSWORD

The default password is "**admin**", in order to secure your network, please modify the password. Note: Confirm Password must be same as "**New Password**". Of course, you can click on the **Skip** to ignore the step.



STEP 2: SET TIME AND DATE

TIME SETTINGS:

Please enable the **Automatically synchronize with Internet time servers** if you want to use time server.

You can use the default time server web site or type any web server name you want on the **First NTP time server** and the **Second NTP time server**.

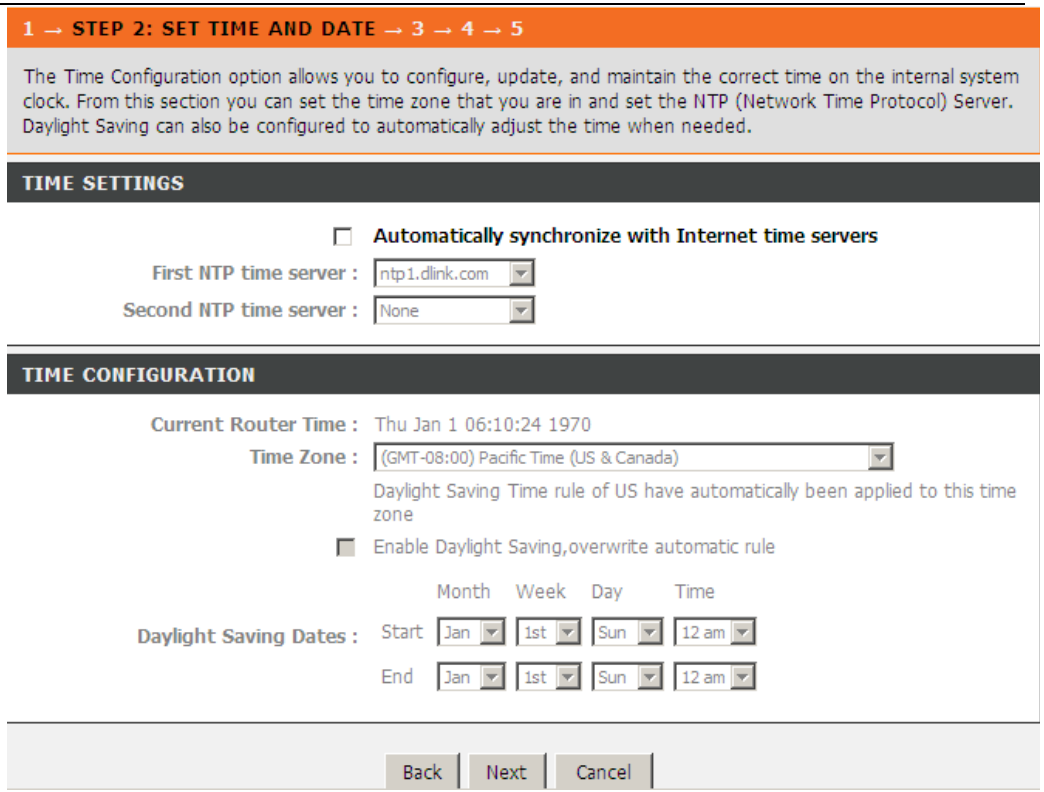
Please select the time zone of your country on the **Time Zone** option.

If you need to use the daylight saving, just choose the **Enable Daylight Saving**. Daylight saving is a period from late Spring to early Fall.

Set how many hours to change the time for Daylight saving Offset.

Configure Daylight Saving Dates, Daylight Saving time starts in the most parts of **Australia** on the first Sunday of October. Each time zone starts Daylight Saving time at 2 A.M. Thus, in Australia you must use October, **First**, **Sunday**, at **2:00 A.M.**

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



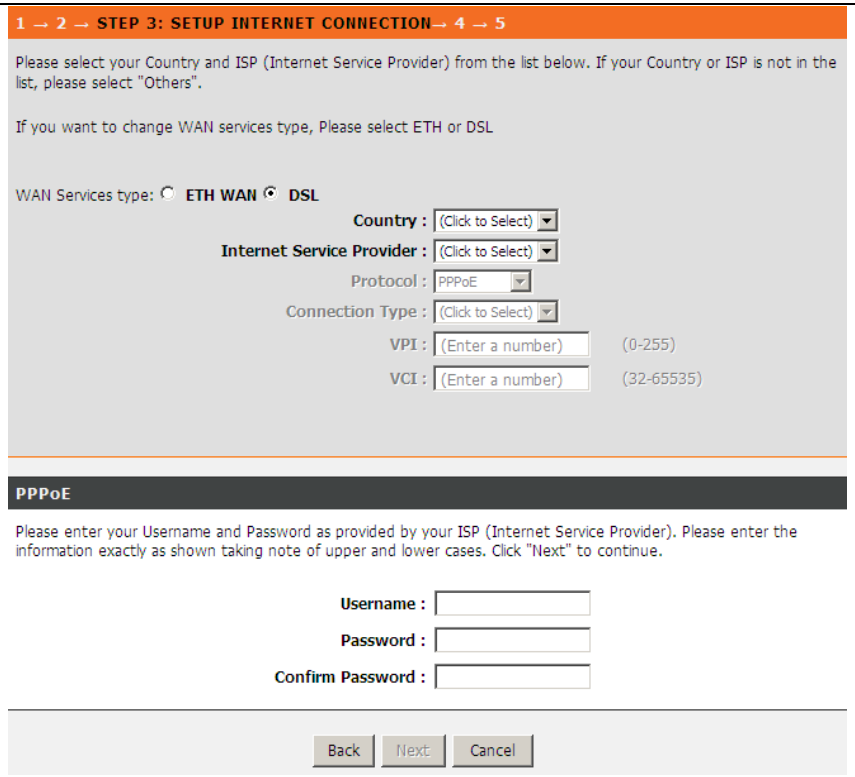
STEP 3: SETUP INTERNET CONNECTION

Please select your **Country** and **ISP Provider**, then the **Protocol**, **VPI/VCI**, and **Connection Type** will auto input the correct information.

If you cannot find the country and ISP in the list below; you can select **Others**, and then input the **Protocol**, **VPI/VCI** and **Connection Type**.

Please enter the **VPI/VCI** numbers if they are different and you have been instructed to do so by the ISP.

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

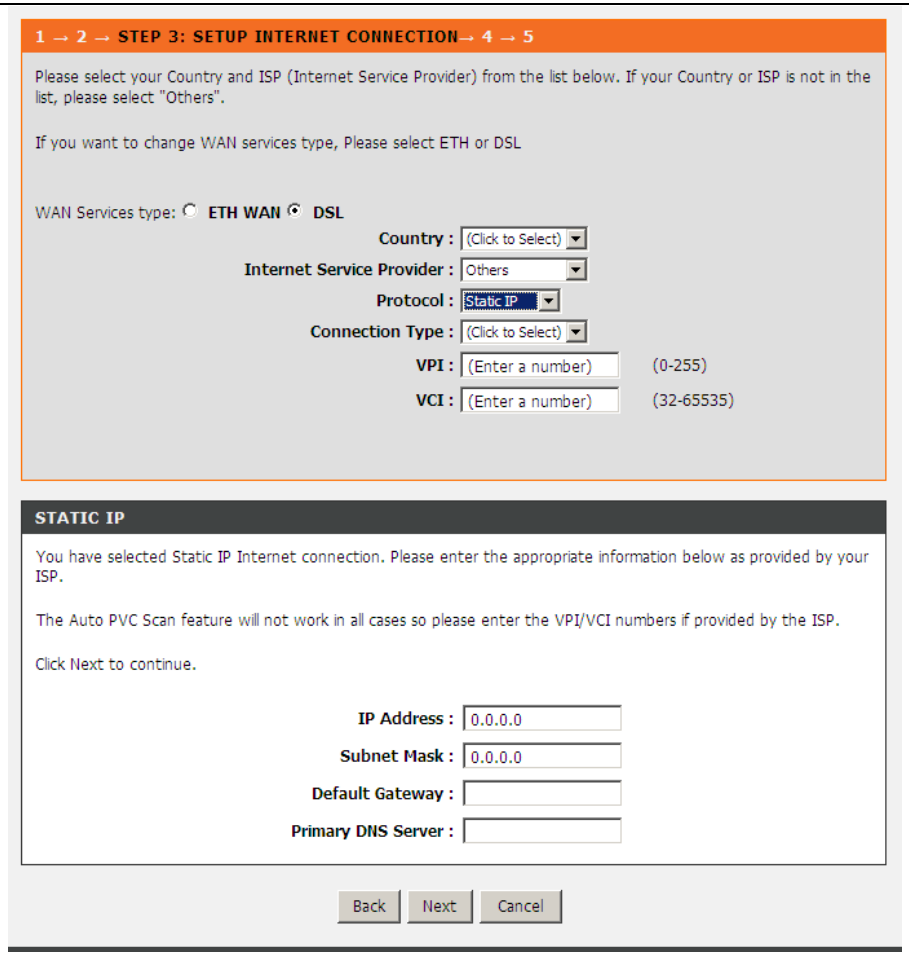


If your Protocol selects **PPPoE** or **PPPoA**, you need to enter your **Username** and **Password** as provided by your ISP

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

If your Protocol is selected as **Static IP**, you will need to enter the **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS server** as provided by your ISP.

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



STEP 4: CONFIGURE WIRELESS NETWORK

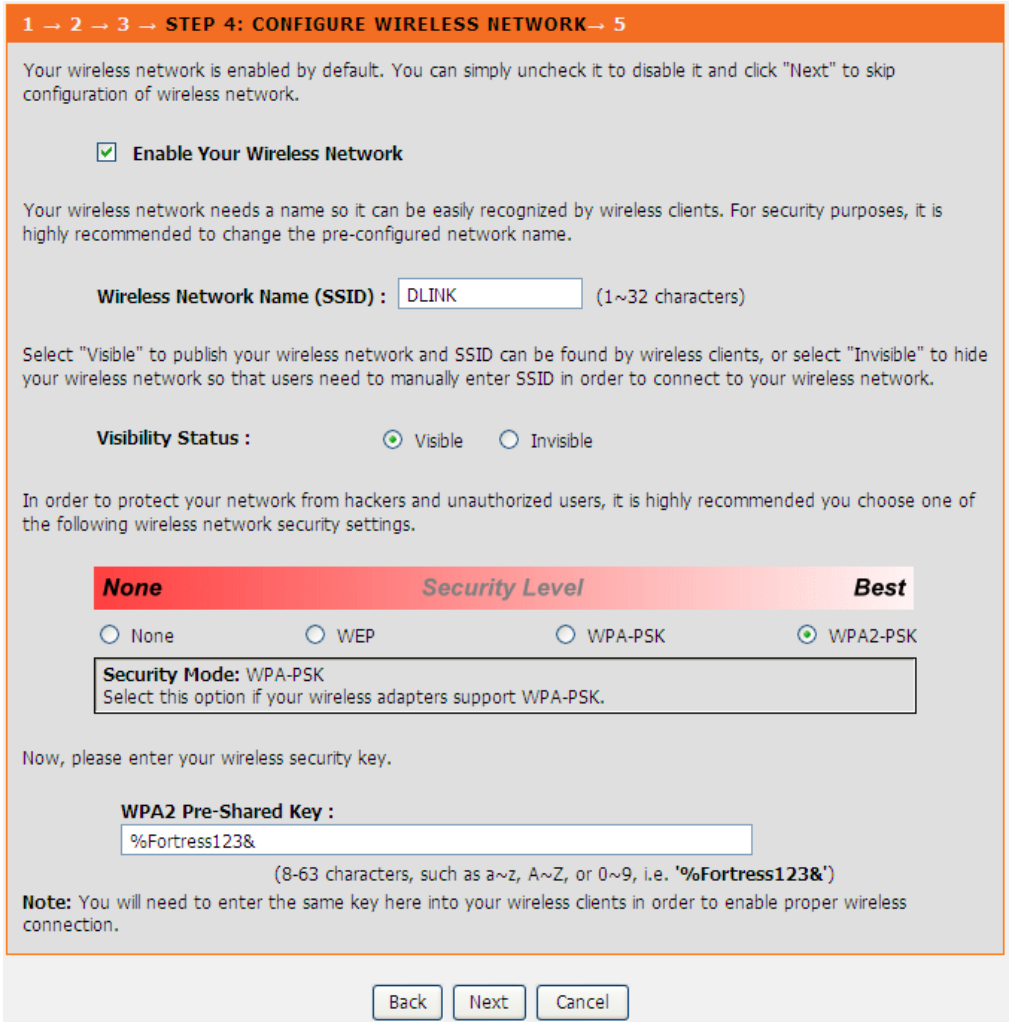
Please check **Enable Your Wireless Network** box to enable your wireless network.

Enter **Wireless Network Name (SSID)** to identify your wireless network.

Visibility Status selects **Visible** can be found by wireless clients, **Invisible** to hide your wireless network

Choose one wireless encryption mode for your wireless network. The **Security Level** from low to high as below:
None < WEP < WPA-PSK < WPA2-PSK

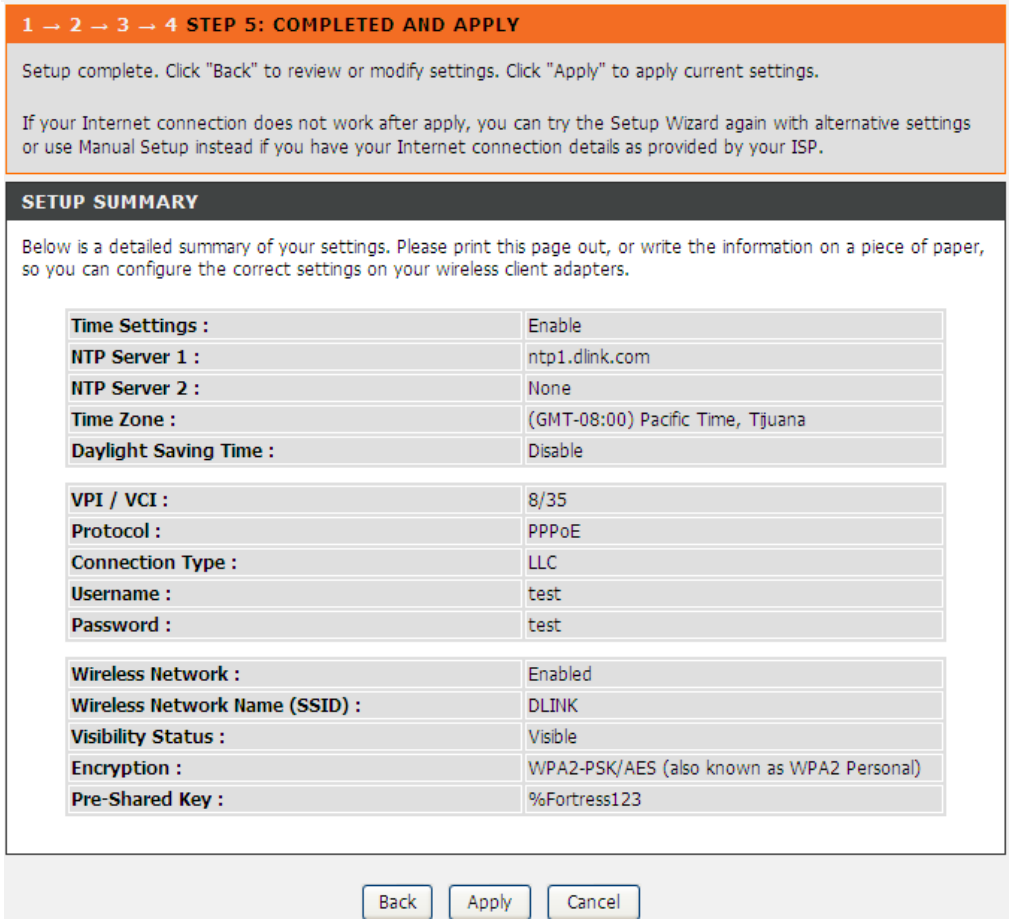
Click on the **Next** button to go to the next **Setup Wizard** window.



STEP 5: COMPLETED AND APPLY

Click **Apply** to complete current settings and finished the setup of the DSL-2750B router. Click **Back** to review or modify settings.

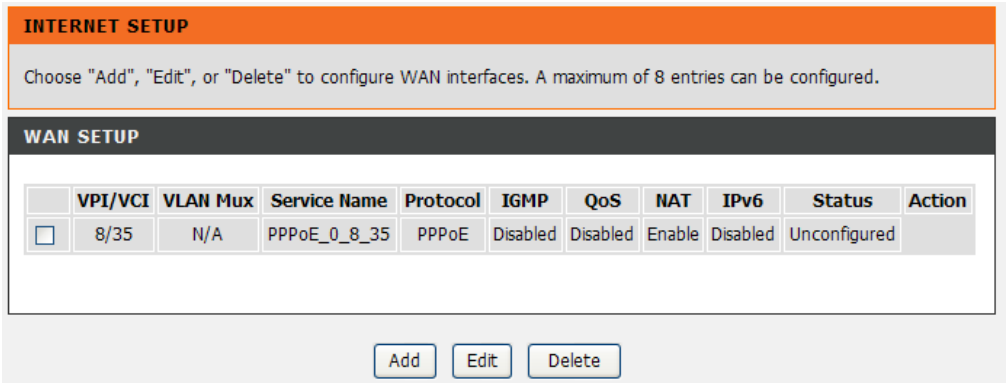
Note: In each step of the Wizard page, you can click **Back** to review or modify the previous settings. Click **Cancel** to exit the wizard page.



INTERNET SETUP

To access the settings page, click on the **Internet Setup** button in the **SETUP** section on this page:

Click **Add/Edit/Delete** to configure the settings.



INTERNET SETUP

ATM PVC CONFIGURATION

Set **VPI/VCI**, **Service Category** and input **Peak Cell Rate, Sustainable Cell Rate,** and **Maximum Burst Size.** This information was provided by your ISP, if they do not provide these details leave them as their default value.

IP QOS SCHEDULER ALGORITHM

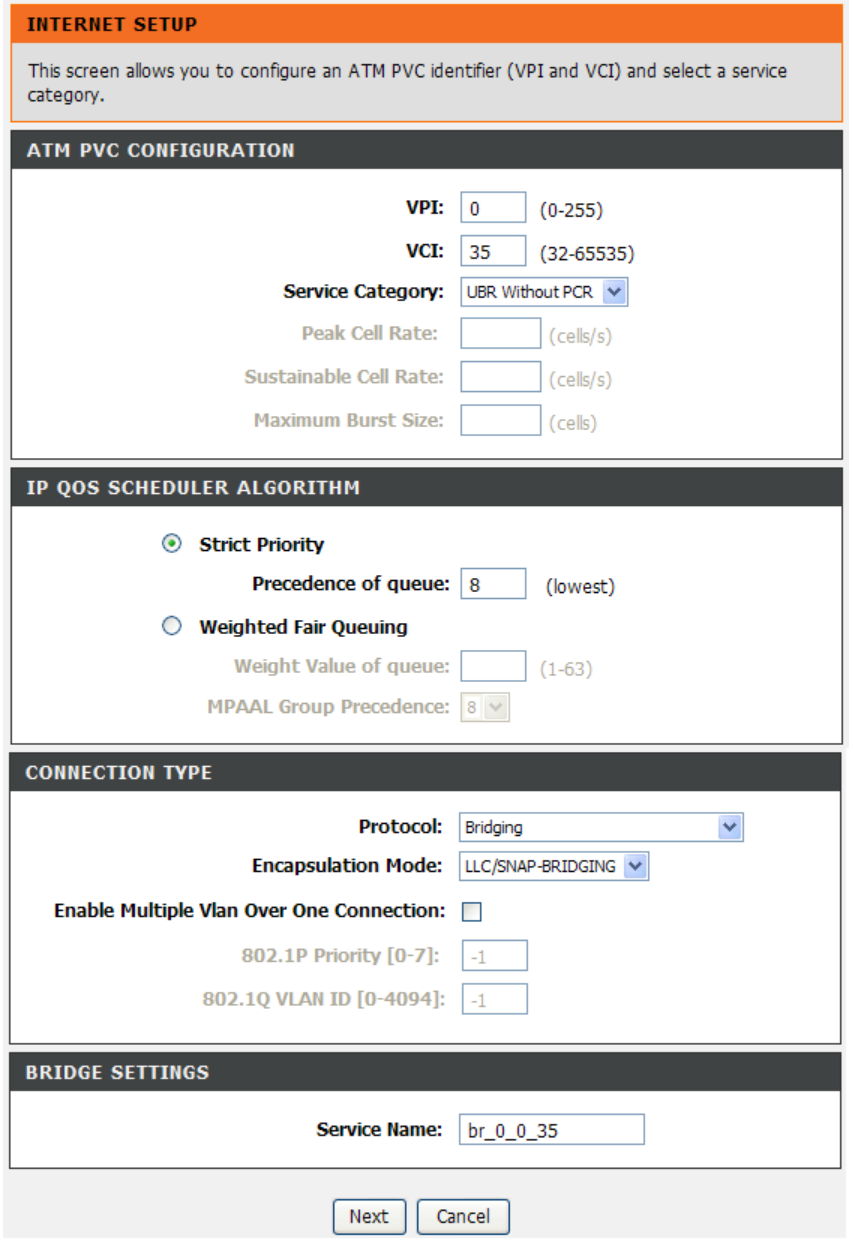
Select **Strict Priority** or **Weighted Fair Queuing**

CONNECTION TYPE

Protocol
Select DSL link type, **PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), MAC Encapsulation Routing (MER), IP over ATM (IPoA),** or **Bridging** from the drop-down list.

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

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



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

Click **Next** button to apply configuration.

For PPPoE/PPPoA CONNECTION

Select **Protocol** and **Encapsulation Mode** from the drop-down list.

Type in **PPP Username** and **PPP Password** and **Confirm PPP Password** which are provided by your ISP.

Authentication Method
The value can be **AUTO, PAP, CHAP, or MSCHAP**. Usually, you can select **AUTO**.

Dial on demand (with idle timeout timer): Check the box to enable the function, users need to enter the idle timeout time. The modem stops the PPPoE connection when detecting no continuous flow from the user. Once detecting the flow (like access to a webpage), the modem restarts the PPPoE dialup.

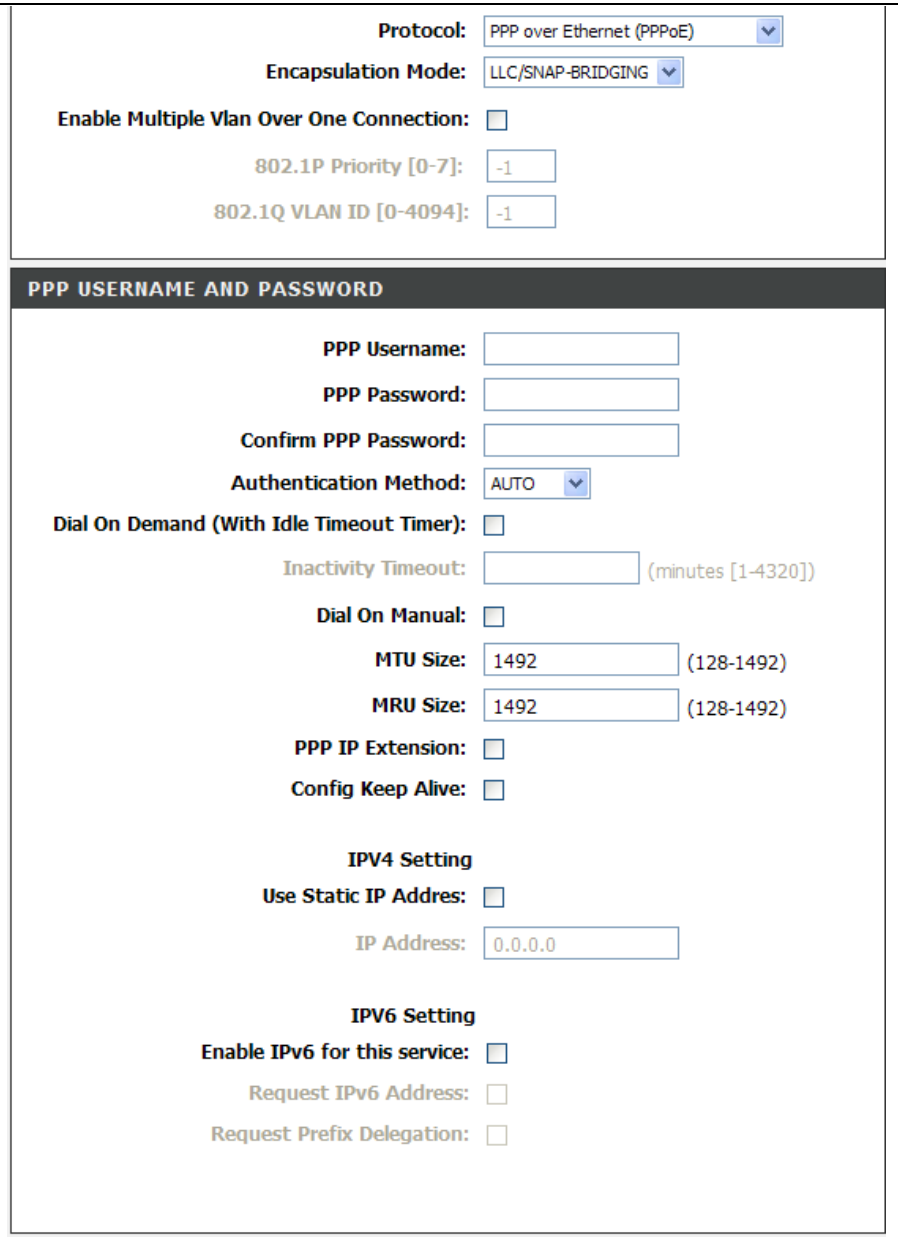
If this function is disabled, the modem performs PPPoE dial-up all the time, only if the modem is powered off or DSLAM/Uplink equipment behaves abnormal.

MTU (Maximum Transmission Unit)**/ MRU** (Maximum Receive Unit) **Size**
Set **MTU/MRU Size** between 128 - 1492.

PPP IP Extension:
Check the **PPP IP Extension**, the router passes the obtained IP address to the local PC and acts as a bridge only modem.

Config Keep Alive: Check the box to let the PPPoE dial-up keep alive

Use Static IP Address: If this function is disabled, the modem obtains an IP address assigned by an uplink equipment such as BAS, through PPPoE dial-up. If this function is enabled, the modem uses this IP address as the WAN IP address.

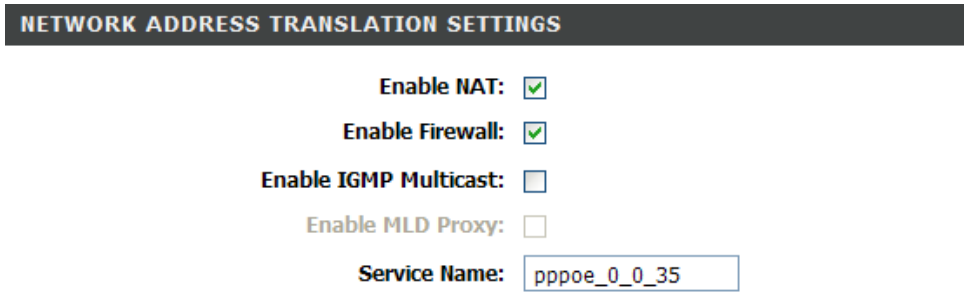


Enable IPv6 for this service
Check the box to support IPv6 service.

Request IPv6 Address
The modem will obtain a WAN IPv6 address automatically.

Request Prefix Delegation
The modem will request Prefix Delegation for local network.

NETWORK ADDRESS TRANSLATION SETTINGS



Enable NAT
Check the box to enable the NAT functions of the modem. If you do not want to enable NAT and wish the modem user to access the Internet normally, you must add a route on the uplink equipment. Otherwise, the access to the Internet fails. Normally, NAT should be enabled.

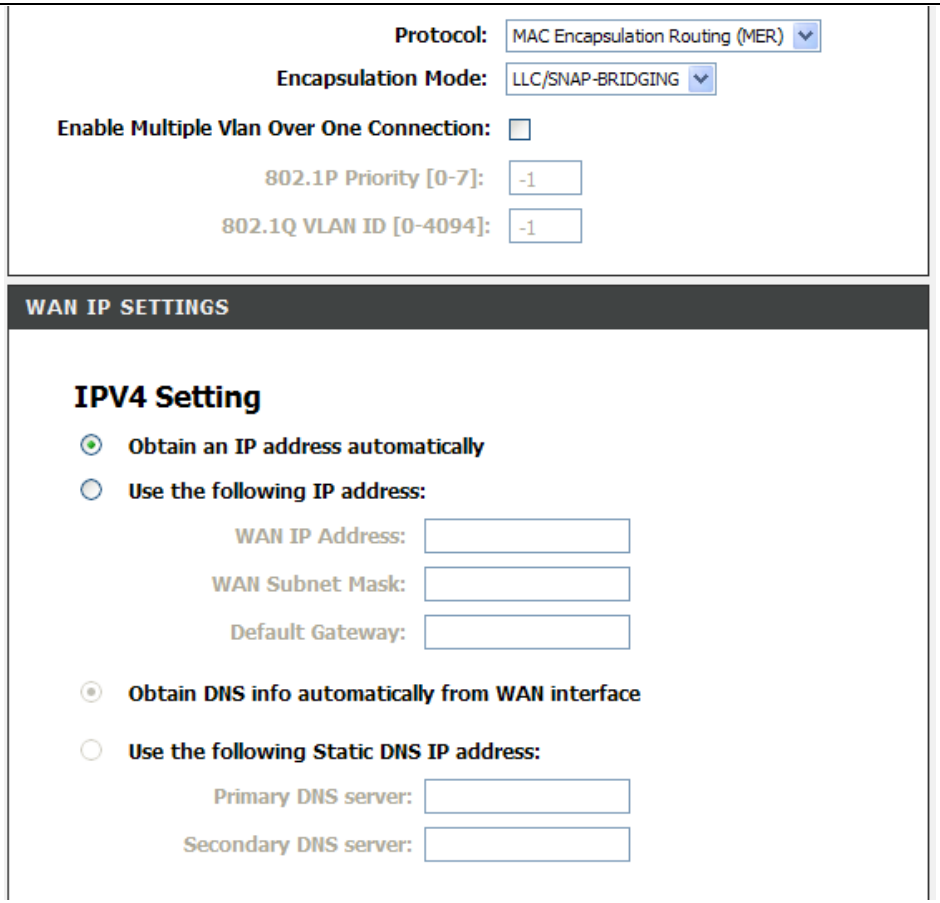
Enable Firewall
Enable or disable IP filtering.

Enable IGMP Multicast
IGMP proxy. Enable this function if you would like it supports IPTV in PPPoE mode.

Enable MLD Proxy
MLD Proxy can be used to support IPv6 multicast data.

For MAC Encapsulation Routing (MER) CONNECTION

Select **Protocol** and **Encapsulation Mode** from the drop-down list.



WAN IP SETTINGS

IPV4 Setting

Obtain an IP address automatically: The function enables DHCP client functions.

Use the following IP address: Select the function if you would like to enter the WAN IP address manually.

WAN IP Address: Enter the IP address of the WAN interface provided by your ISP.

WAN Subnet Mask: Enter the subnet mask concerned to the IP address of the WAN interface provided by your ISP.

Default Gateway: Enter the default gateway.

Obtain DNS info automatically from WAN interface: User can get DNS server information from the selected WAN interface

Use the following Static DNS IP address: Select it if you would like to enter the IP address of the DNS server manually.

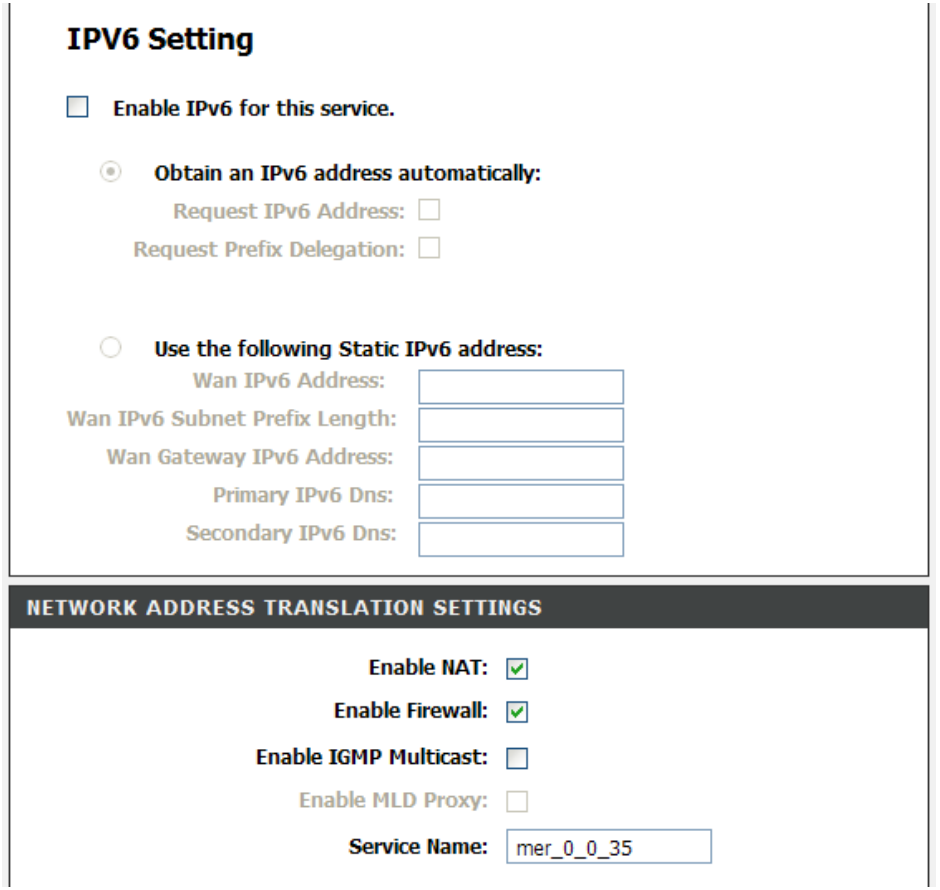
Primary DNS server: Enter the IP address of the primary DNS server.

Secondary DNS server: Enter the IP address of the secondary DNS server provided by your ISP.

Obtain an IPv6 address automatically: Select **Obtain an IPv6 address automatically**, DHCPv6 Client will be enabled on this WAN interface.

Use the following Static IPv6 address: Select **Use the following Static IPv6 address**, entering information provided by your ISP to configure the WAN IPv6 settings.

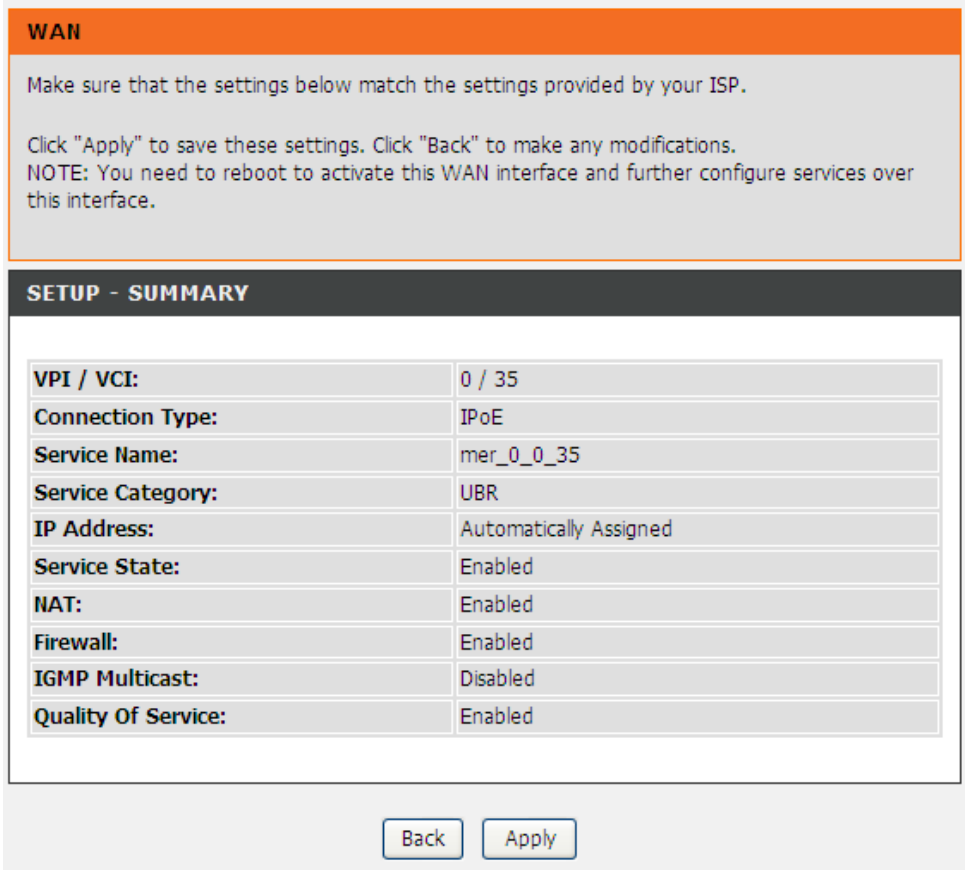
After proper settings, click **Next.**



SETUP-SUMMARY

Check your Internet setting.

Click on the **Apply** to apply your setting.



WIRELESS CONNECTION

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 onto your wireless clients and PC.

To access the **WIRELESS** (WLAN) settings window, click on the **Wireless Connection** button in the **SETUP** tab.

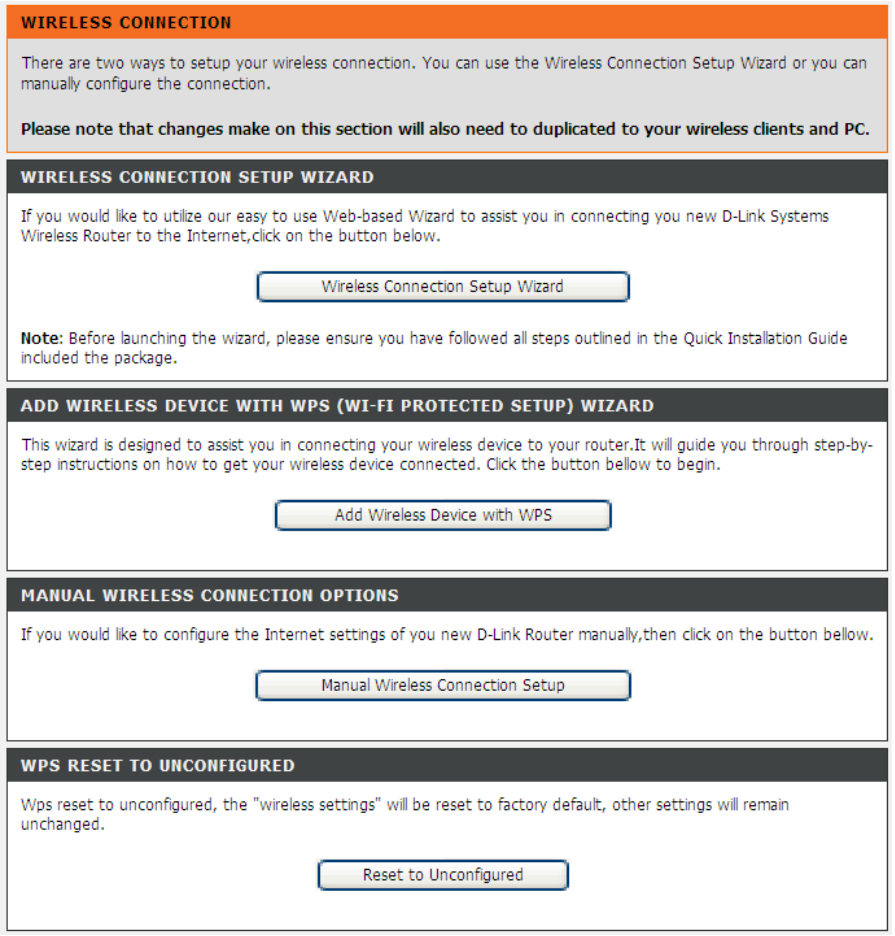
WIRELESS CONNECTION

Click on the **Wireless Connection Setup Wizard** button to setup the wireless connection in an easy way. It will use Web-based Wizard to assist you in connecting to your new D-Link Systems Wireless Router.

Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

Click on the **Add Wireless Device with WPS** button. This wizard is designed to assist you in connecting your wireless device to your router with WPS. It will guide you through step-by-step instructions on how to get your wireless device connected.

If you would like to configure the Wireless settings of your new D-Link Router manually, then click on the **Manual Wireless Connection Setup** button.



WIRELESS CONNECTION SETUP WIZARD

WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

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

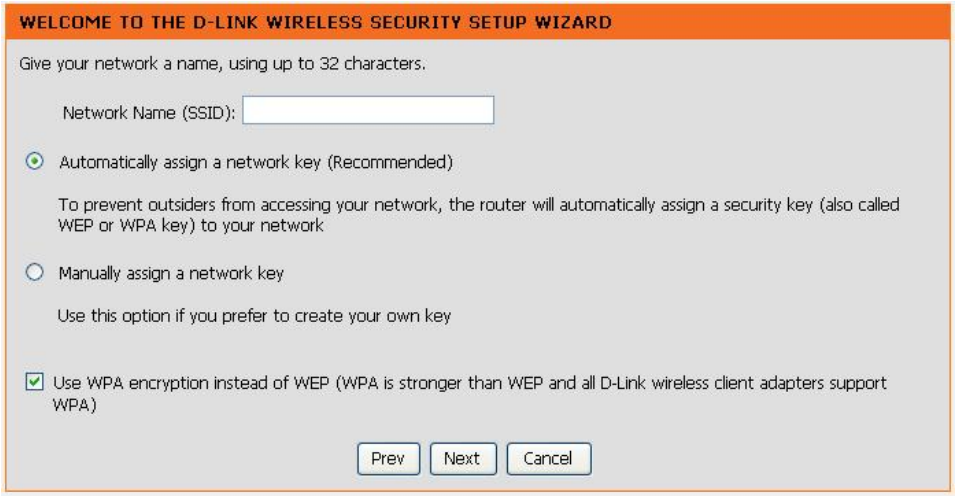
Automatically assign a network key (Recommended) In order to protect your network from hackers and unauthorized users; we adapt Auto (WPA or WPA2) for your wireless security mode. We provide user a random pre-shared key by automatically.

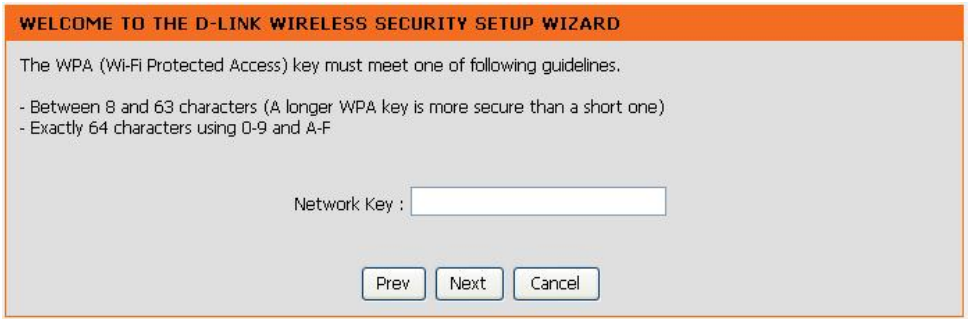
Manually assign a network key You can also set it manually if you do not prefer the key we generate. Type a string (Between 8-63 characters, or Exactly 64 characters using 0-9 and A-F) on the **Network Key**.

Click **Next** button to go to the next page.
Click **Cancel** button to return to the main menu of Wireless Setup page.

Check your wireless network setting.

Click **Save** button to apply your setting.
Click **Prev** button to pre-page to modify your setting.
Click **Cancel** button to cancel your setting.



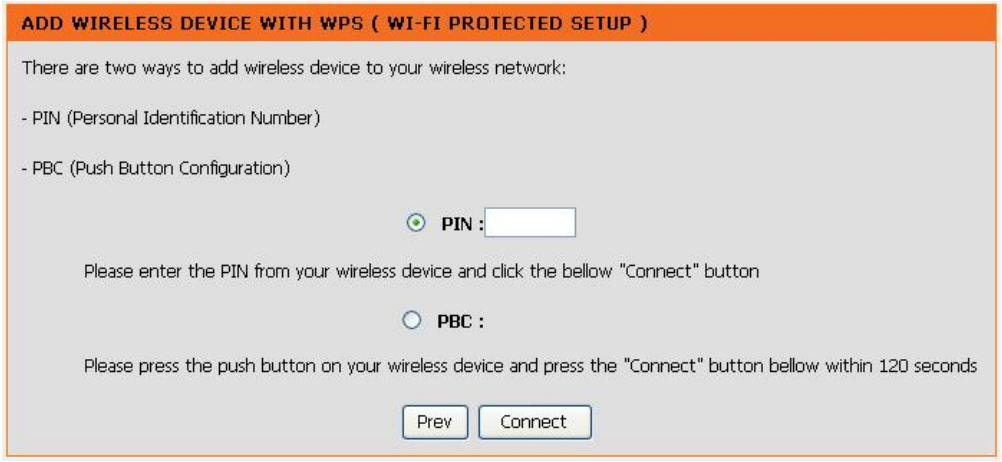


ADD WIRELESS DEVICE WITH WPS

The wizard shows the option to setup WPS by **Auto** or **Manual**.
Auto -- Select this option if your wireless device supports WPS(Wi-Fi Protected Setup)
Manual -- Select this option to display the current wireless settings for you to configure the wireless device manually.

Click **Next** button to go to the next page.
Click **Cancel** button to return to the main menu of Wireless Setup page.

ADD WIRELESS DEVICE WITH WPS (Auto)



This page allows you to select PIN or PBC to use WPS method.

PIN - Enter the PIN code from your wireless device and click the below **Connect** button to start the handshaking.

PBC - Please press the push button and hold on for 3 seconds on your wireless device and presses the **Connect** button below within 120 seconds to start the handshaking.

Click **Prev** to go back to previous page.

ADD WIRELESS DEVICE WITH WPS (Manual)

This section shows the information of the SSID, Wireless Security Mode, the Network key, allowing you to modify the setting. If you select **Auto** in the previous page, you won't see this page and please refer to next column.

Please type network name on the **Network Name SSID.**

Please type network key on the **Network Key**

Click **OK** button to process the next page.

Add Wireless Device with WPS (WI-FI PROTECTED SETUP)
Finally it will show all the configurations. You can check if it is exact, please click the **Next** button.

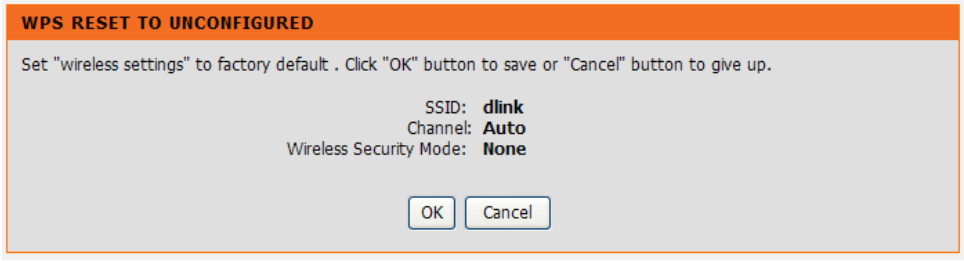
Manual Wireless Connection Setup

If you want to configure the wireless settings manually, click **Manual Wireless Connection Setup**. It will redirect to ADVANCED WIRELESS.

Reset to Unconfigured

Once the “**Reset to Unconfigured**” button is clicked, the “wireless settings” will be reset to factory default, other settings will remain unchanged.
Please type network key on the **Network Key**

Click **OK** button to process the next page.



LOCAL NETWORK

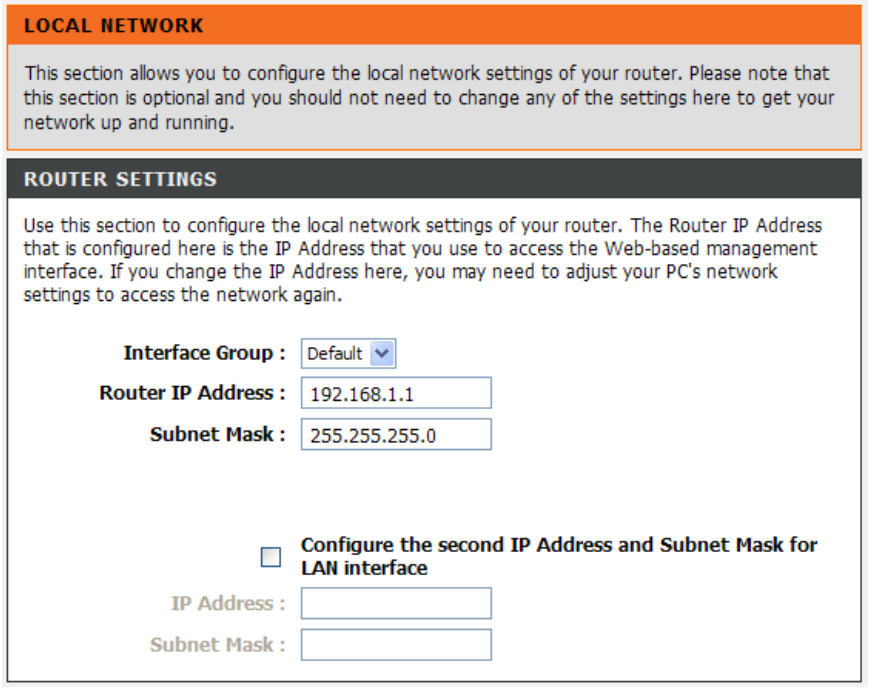
You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP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

To access the **Local Network** setting window, click on the **Local Network** button in the **SETUP** tab.

ROUTER SETTINGS
To change the **Router IP Address** or **Subnet Mask**, type in the desired values.

DHCP SERVER SETTINGS (OPTIONAL)
The **Enable DHCP Server** is selected by default for the Router's Ethernet LAN interface.

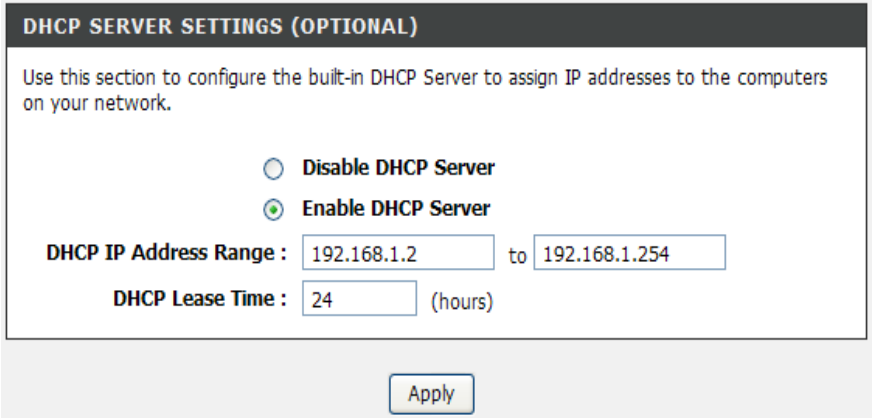
Set the **DHCP IP Address Range** and the default is from **192.168.1.2** to **192.168.1.254**. The IP address pool can be up to 253 IP addresses.



DHCP SERVER SETTINGS (OPTIONAL)

Set the value hours on the **DHCP Lease Time**

If you don't want DSL-2750B to be the DHCP server, you can disable.



DHCP RESERVATION LIST

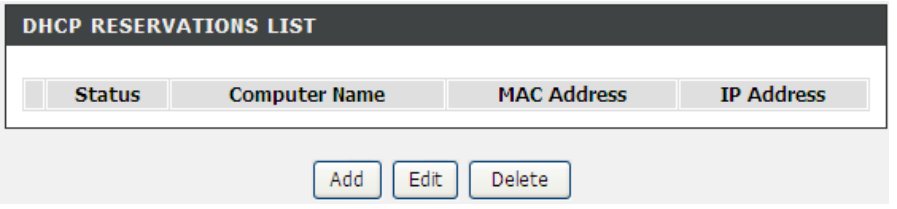
Click **Add/Edit/Delete** to configure the settings

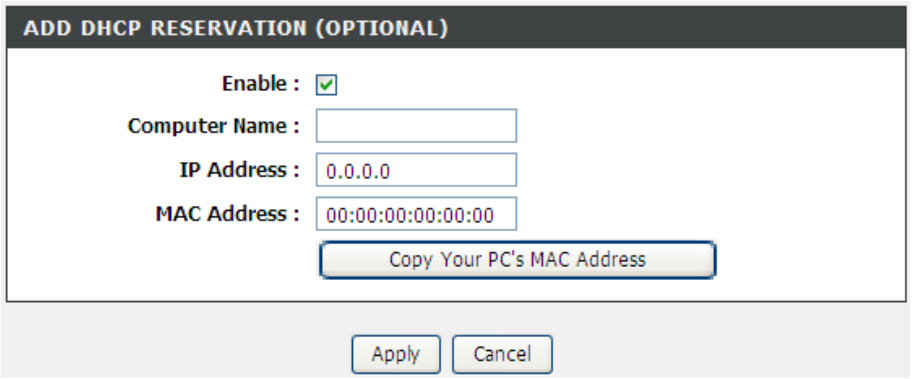
Select the **Enable** to let you reserve the **IP Address** for the designated PC with the configured **MAC Address**.

The **Computer Name** can help you recognize the PC with the **MAC Address**, such as "Dad's Laptop".

Clicking on the **Copy Your PC's MAC Address** button to help you get the MAC address from the PC you are using now browsing this web page.

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





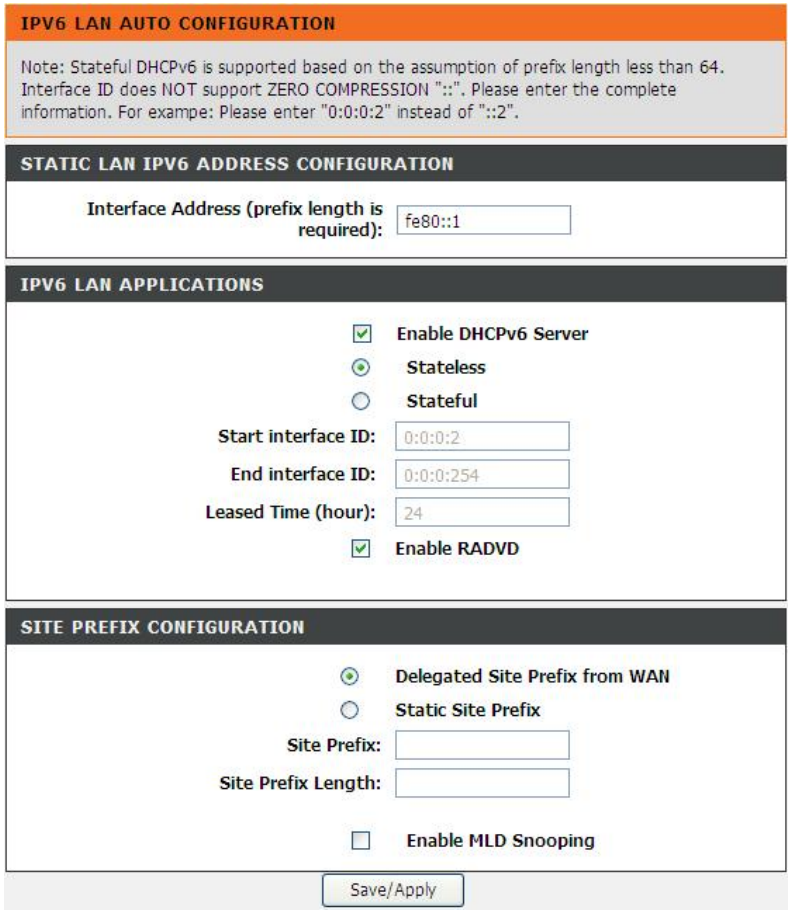
IPv6 Local Network

The **IPv6 Local Network** configuration option allows you configure IPv6 internet connection. You can configure follow **STATIC LAN IPV6 ADDRESS CONFIGURATION, IPV6 LAN APPLICATIONS** or **SITE PREFIX CONFIGURATION**.

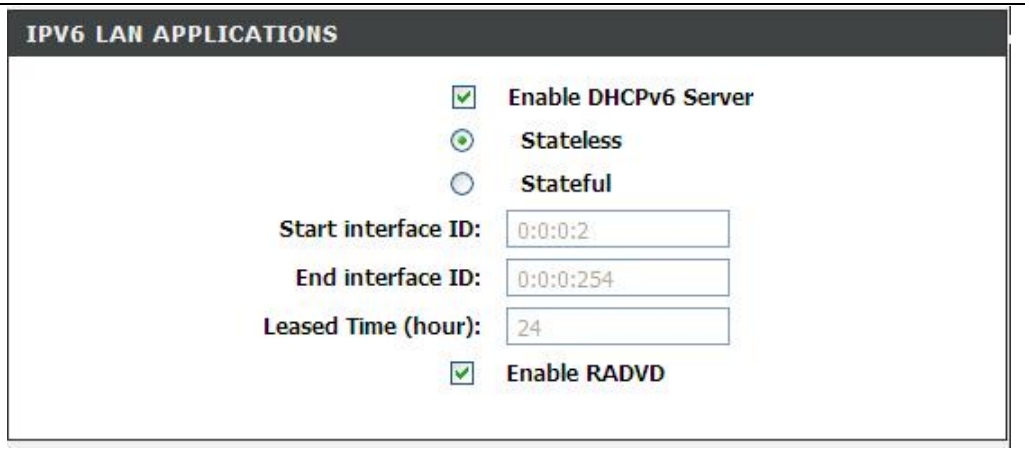
To access the **IPv6** setting window, click on the **IPv6 Local Network** button in the **SETUP tab**

IPV6 LAN AUTO CONFIGURATION

In the section, you can set an IP address for the DSL IPv6 router, enable the **DHCPv6 Server**, **Enable RADVD** and **Enable the MLD Snooping** function.



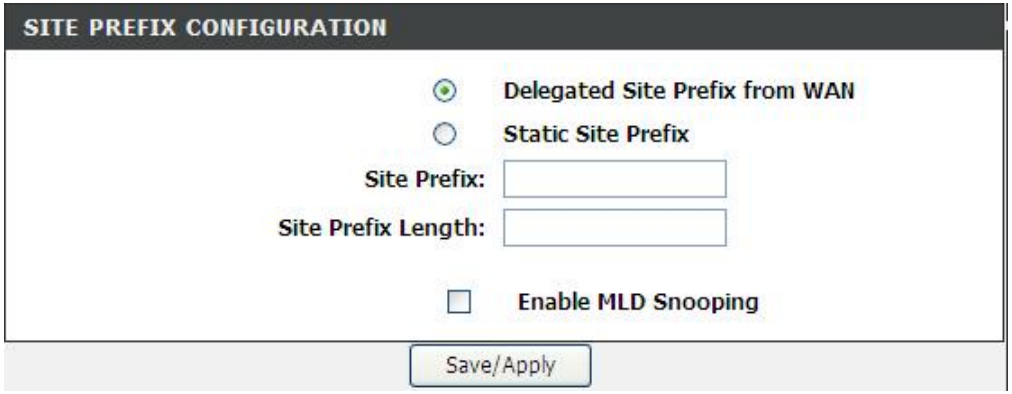
IPV6 LAN APPLICATIONS



Enable DHCPv6 Server
WIDE-DHCPv6 is an open-source implementation of dynamic host configuration protocol for IPv6 (DHCPv6) originally developed by the KAME project. The implementation mainly complies with the following standards: RFC3315, RFC3319, RFC3633, RFC3646, RFC4075, RFC 4272 etc.

Enable RADVD: The router advertisement daemon (RADVD) is run by Linux or BSD systems acting as IPv6 routers. It sends router advertisement messages, specified by RFC2461, to a local Ethernet LAN periodically and when requested by a node sending a router solicitation message. These messages are required for IPv6 stateless auto-configuration.

SITE PREFIX CONFIGURATION



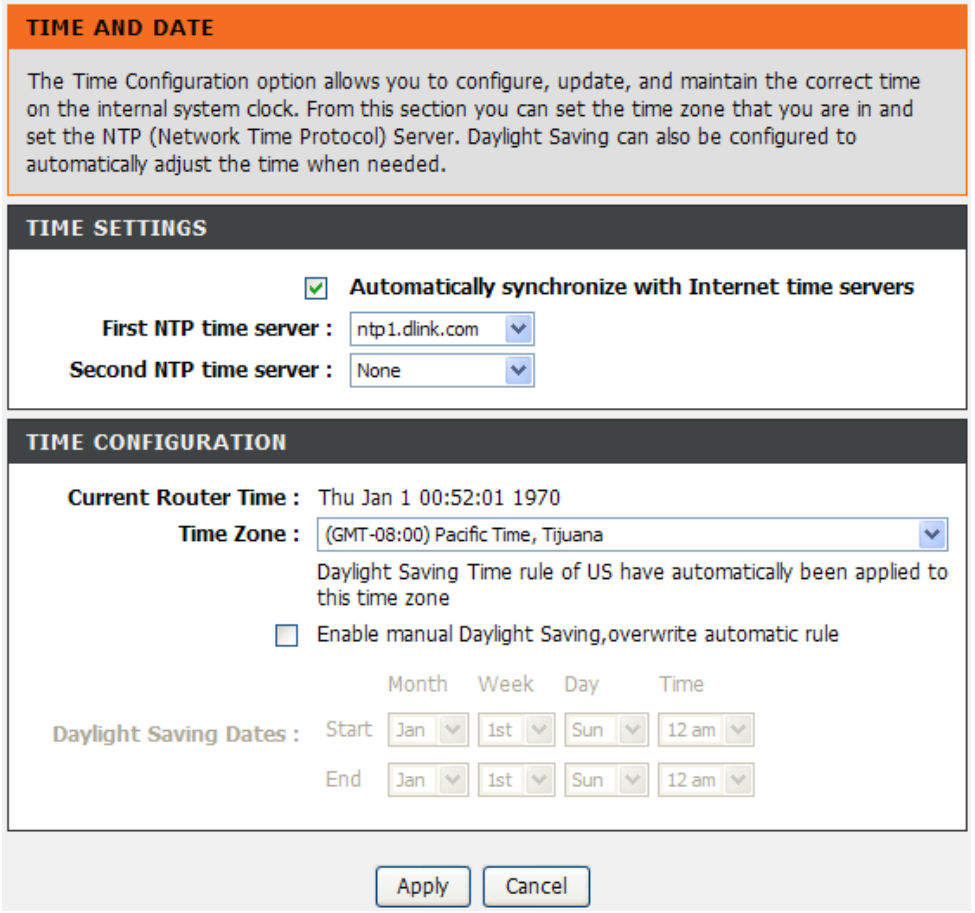
Enable MLD Snooping: Multicast Listener Discovery Snooping (MLD Snooping) is an IPv6 multicast constraining mechanism that runs on Layer 2 devices to manage and control IPv6 multicast groups. By analyzing received MLD messages, a Layer 2 device running MLD Snooping establishes mappings between ports and multicast MAC addresses and forwards IPv6 multicast data based on these mappings.

After finishing setting, click the **Save/Apply** button to apply the settings.

TIME AND DATE

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

To access the **TIME** setting window, click on the **Time and Date** button in the **SETUP tab**



TIME SETTING:

Check the **Automatically synchronize with Internet time servers**

Select specific time server to use from the **First NTP time server and Second NTP time server** specific NTP server name.

TIME CONFIGURATION:

Select your operating time zone from the **Time Zone** drop-down menu.

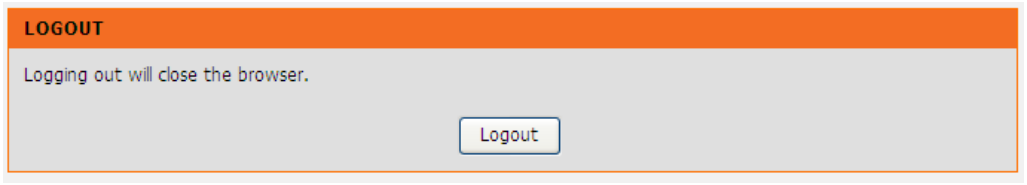
If you need to use the daylight saving, just choose the **Enable manual Daylight Saving, overwrite automatic rule**. Daylight saving is a period from late Spring to early Fall.

Configure Daylight Saving Dates, Daylight Saving time starts in the most parts of **Australia** on the first Sunday of October. Each time zone starts Daylight Saving time at 2 A.M. Thus, in Australia you must use October, **First**, **Sunday**, at **2:00 A.M.**

Please click the **Apply** button to save the configuration.

LOGOUT

The **LOGOUT** page enables you to logout of your router configuration and closes the browser. To access the **LOGOUT** setting window, click on the **Logout** button in the **ADVANCED** tab



LOGOUT

Click on the **Logout** button to logout of the router configuration settings and close the browser.

ADVANCED

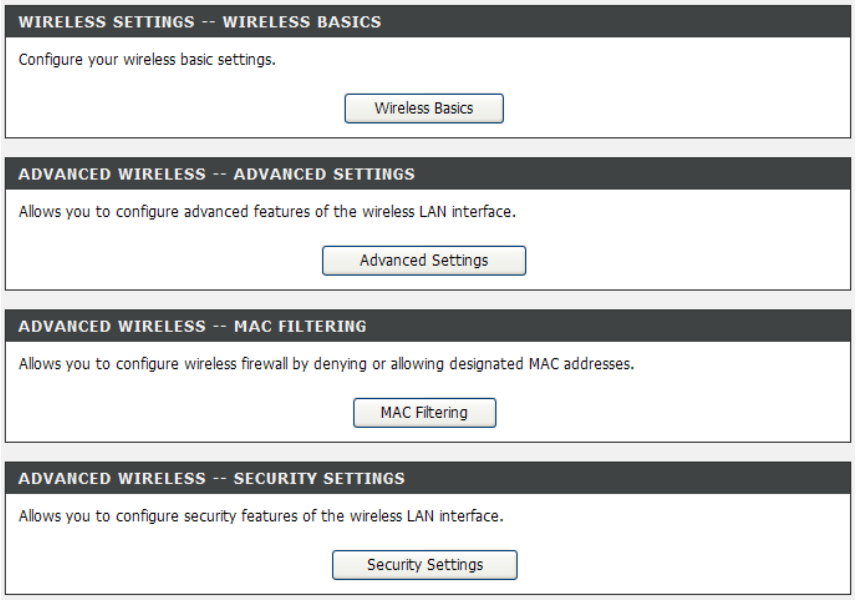
This chapter includes the more advanced features used for network management and security as well as administrative tools to manage the router, view status and other information used to examine performance and for troubleshooting.

ADVANCED WIRELESS

These options are for users that wish to change the behavior of their wireless radio from the standard setting. D-Link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

To access the setting window, click on the **Wireless Settings** button in the **ADVANCED** tab.

ADVANCED WIRELESS divided to **WIRELESS BASICS**, **ADVANCED SETTINGS**, **MAC FILTERING**, and **SECURITY SETTINGS.**



WIRELESS BASICS

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

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

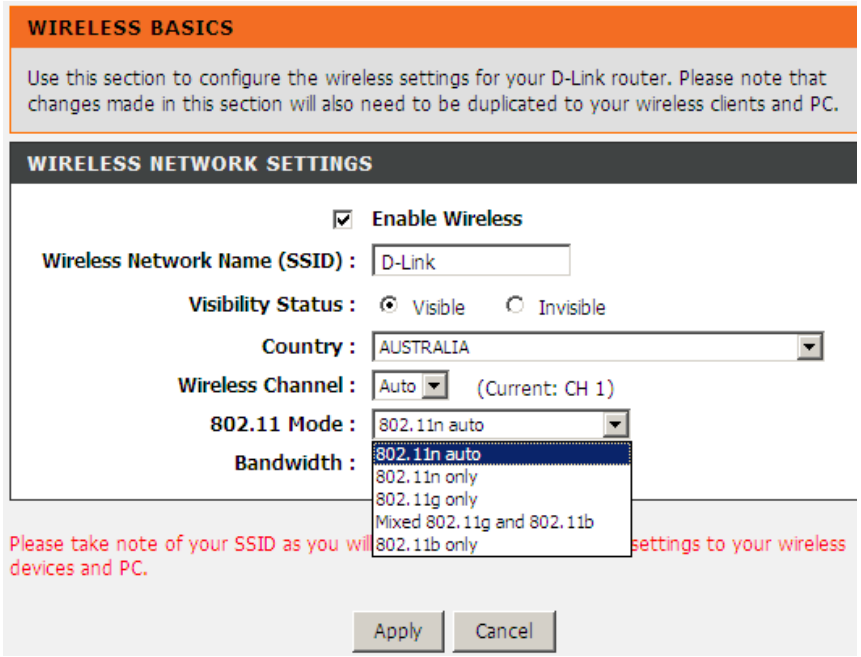
Click on the **Visible** or **Invisible** to decide if you want to show its SSID.

The **Wireless Channel** can let you select the channel of your access point. Channel availability is different for different countries due to their regulation.

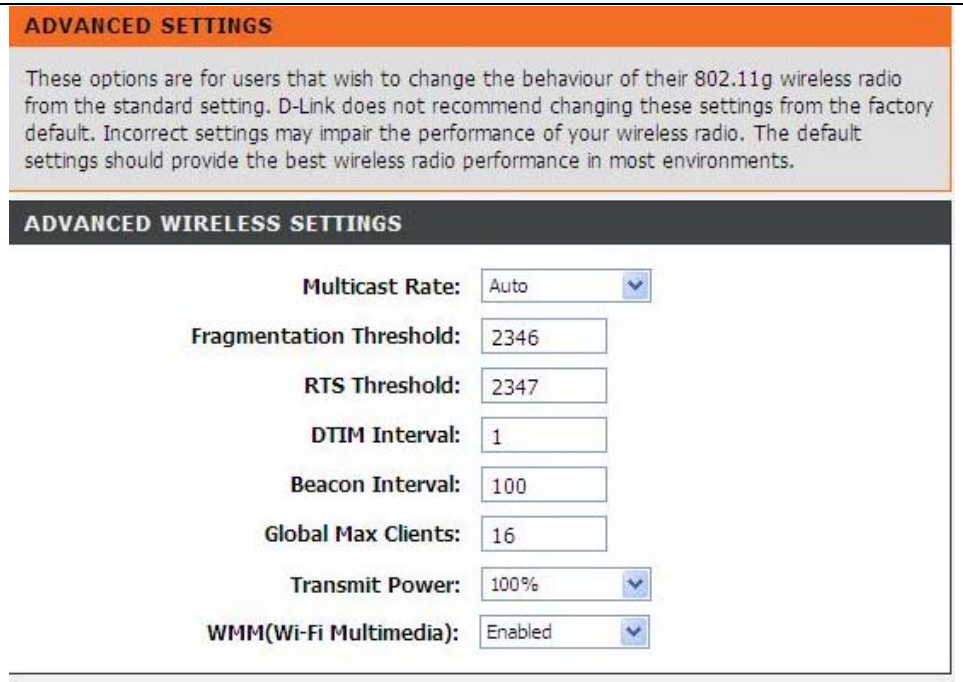
Select **802.11 auto** mode to operate in b/g/n mode. Or select specified mode to use. **802.11b only**, **802.11g only**, **802.11n only**. **Mixed 802.11g and 802.11b** which means DSL-2750B will detect the clients to use 802.11g or 802.11b to synchronize.

You can select **20MHz, 40MHz Upper band** or **40MHz Lower band** in **Bandwidth** to decide the transmission rate.

Click **Apply** to save the settings.



ADVANCED SETTINGS



Most about wireless setting was referred in **WIRELESS** chapter, if you need to change the other default setting,

The default value of **Multicast Rate** is **Auto**. The rate of data transmission should be set depending on the speed of your wireless network. You can select from a range of transmission speeds, or you can select **Auto** to have the Router automatically use the fastest possible data rate and enable the Auto-Fallback feature. Auto-Fallback will negotiate the best possible connection speed between the Router and a wireless client.

Packets that are larger than this threshold are fragmented into multiple packets. Try to increase the **Fragmentation Threshold** if you encounter high packet error rates. Do not set the threshold too low, since this can result in reduced networking performance.

This value of **RTS Threshold** should remain at its default setting as 2347.Should you encounter inconsistent data flow, only minor reductions are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The Router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission.

Input the value 1 to 255 into the **DTIM Interval.** A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast and multicast messages.

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

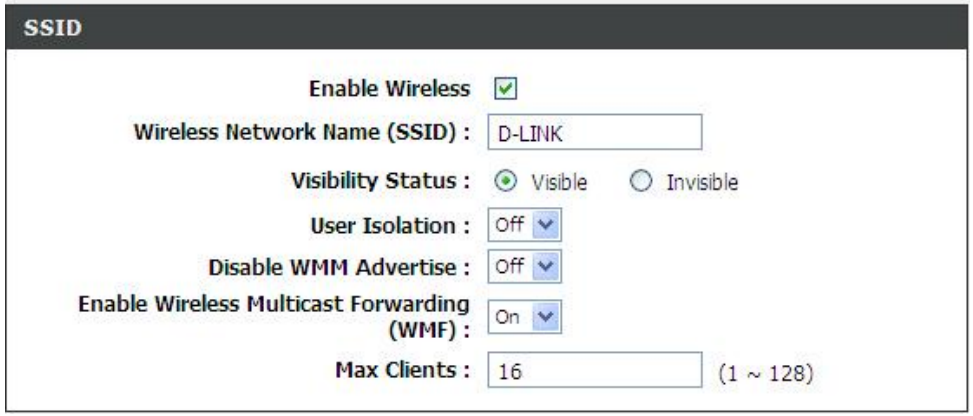
(ms). Default (100) is recommended.

Adjust the **Transmit Power** here. This tool can be helpful for security purposes if you wish to limit the transmission range.

Select whether **WMM** is enable or disabled. Before you disable WMM, you should understand that all QoS queues or traffic classes relate to wireless do not take effects.

SSID

Select **Enable Wireles** to turn Wi-Fi on and off.



The **Wireless Network Name (SSID)** is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

Visibility Status selects **Visible** can be found by wireless clients, **Invisible** to hide your wireless network

Select the **User Isolation** be ON so that users connect to the same access point cannot connect to each other's device via the access point.

Enable **Disable WMM Advertise**, the transmission performance multimedia of the voice and video data can be improved.

Enable **Enable Wireless Multicast Forwarding (WMF)**, the transmission quality of video service such as IPTV can be improved.

Clients exceed the value specified in the **Max Clients** will be refused to be linked up with access point.

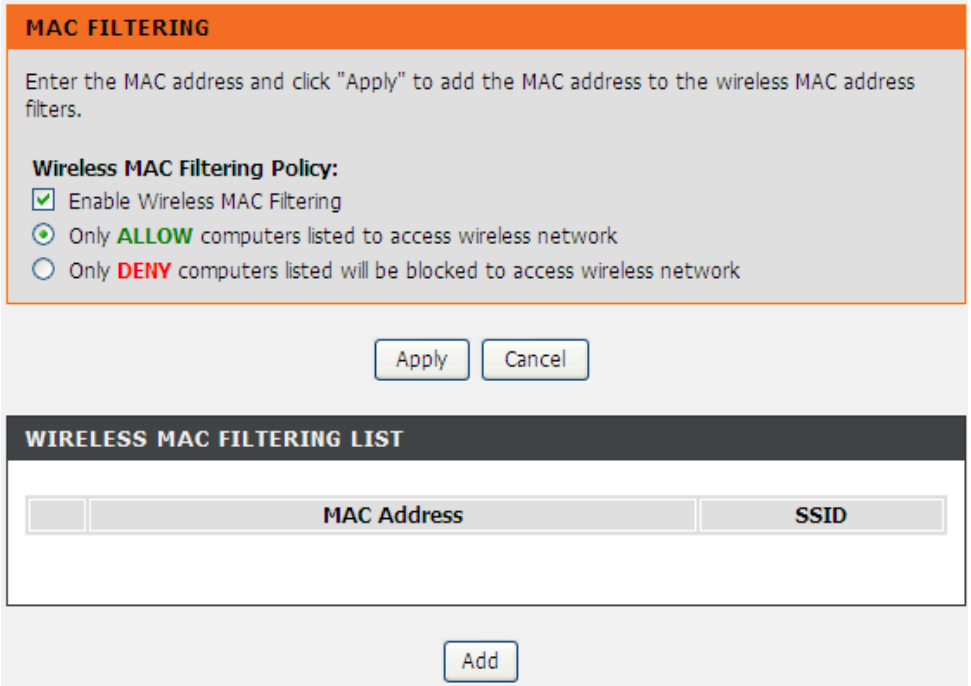
MAC FILTERING

Do not check the **Enable Wireless MAC Filtering** if you don't want to use the feature.

Enable **Wireless** MAC Filtering and select one of the two options,

ALLOW: Support WLAN devices make connection, except the mac address which is added in the filter table.
DENY: Support deny all WLAN devices make connection, except the mac address which is added in the filter table.

Press **Apply** button to **ADD** the MAC Filter in the list



SECURITY SETTINGS

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: **WEP**, **WPA**, **WPA2**, Auto(WPA or WPA2). WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Select SSID and configure **WIRELESS SECURITY MODE**

Open System

Anyone can access the network (no encryption). The default is a disabled WEP encryption setting. It allows users to select enabled WEP.

Shared Key

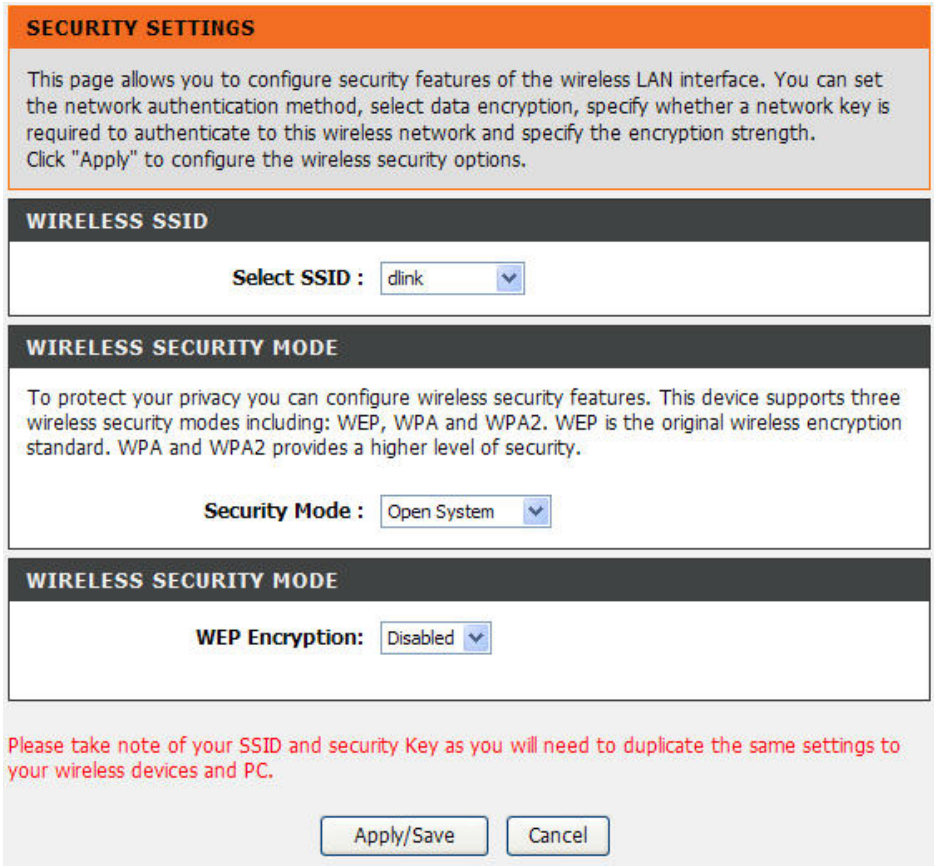
If you choose Shared Key as your security mode, please go to 'manage wireless networks' on the accessing PC to check the WEP encryption type. You should make sure the WEP encryption type on the accessing PC is shared. Because such encryption type is matching the Router's and it's more secure.

WPA-Personal

It include WPA only (WPA-PSK), WPA2 only (WPA2-PSK) and Auto **(WPA or WPA2) (WPA-PSK/WPA2-PSK-Mixed) WPA Mode.**

WPA-Enterprise

it includes WPA only, WPA2 only and Auto (WPA or WPA2) (WPA/WPA2-Mixed) WPA Mode.



Shared Key

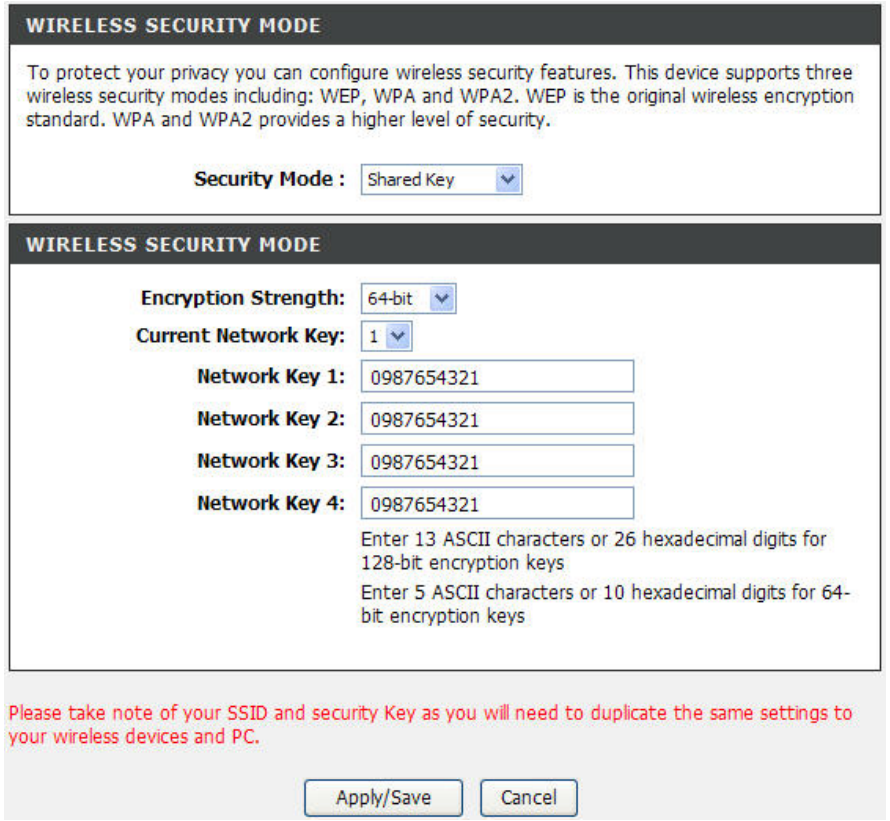
Shared Key (WEP) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys.

The router offers 64- or 128-bit encryption with four **Network Key** available.

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

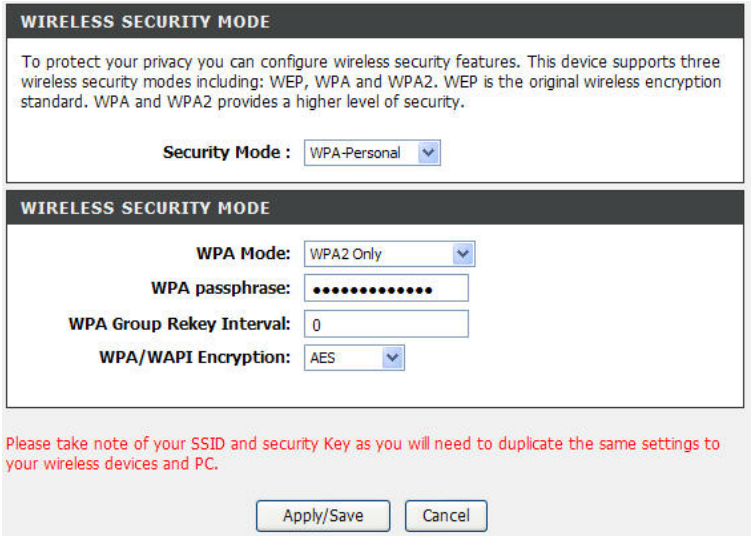
Enter the key into the **Network Key** field 1~4. (Key length is outlined at the bottom of the window.)

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



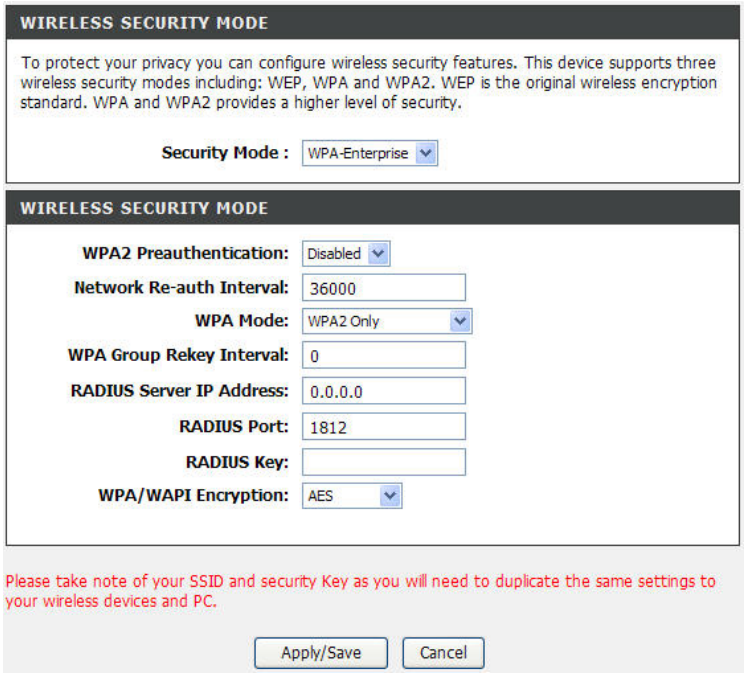
WIRELESS SECURITY MODE:
WPA-Personal

WPA only (WPA-PSK) configuration is similar to WEP. The key length is between 8 to 63 ASCII characters or 64 hexadecimal digits.



WIRELESS SECURITY MODE:
WPA-Enterprise

You can only use **WPA-Enterprise** if you have set up RADIUS server. This is the WPA/WPA2 authentication with RADIUS server instead of pre-shared key,



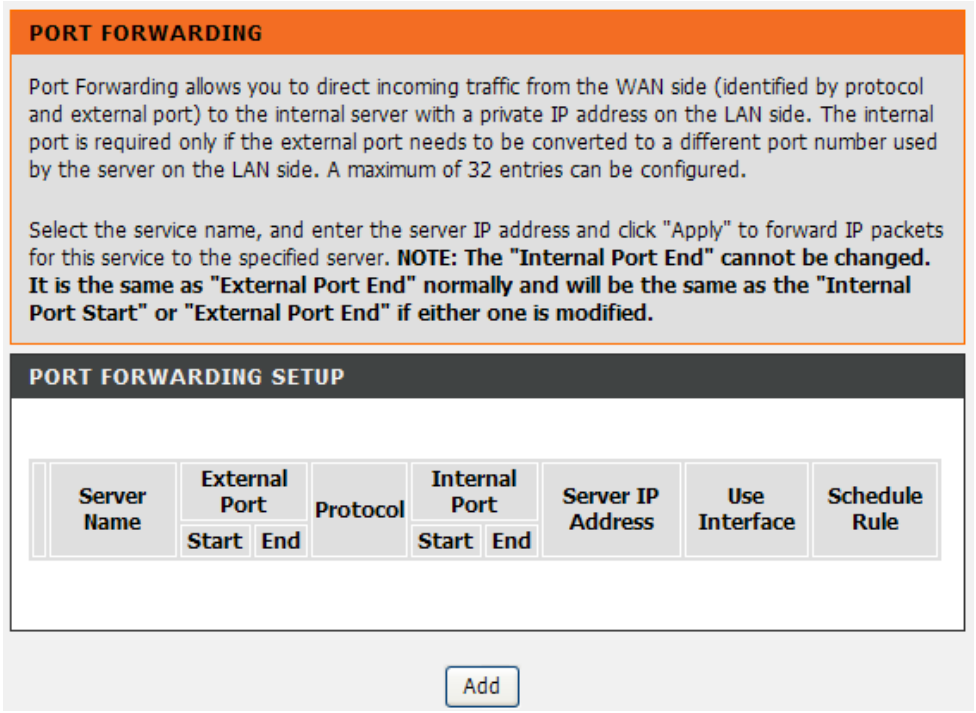
PORT FORWARDING

Use the **PORT FORWARDING** window to open ports in your router and re-direct data through those ports to a single PC on your network (WAN-to-LAN traffic). The Port Forwarding function allows remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DSL-2750B will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the LAN IP address you specify. Remember that the specified Private IP Address must be within the useable range of the subnet occupied by the Router.

To access the **PORT FORWARDING** settings window, click on the **PORT FORWARDING** button in the **ADVANCED** tab

PORT FORWARDING SETUP

Press **Add** button to add port forwarding rule.

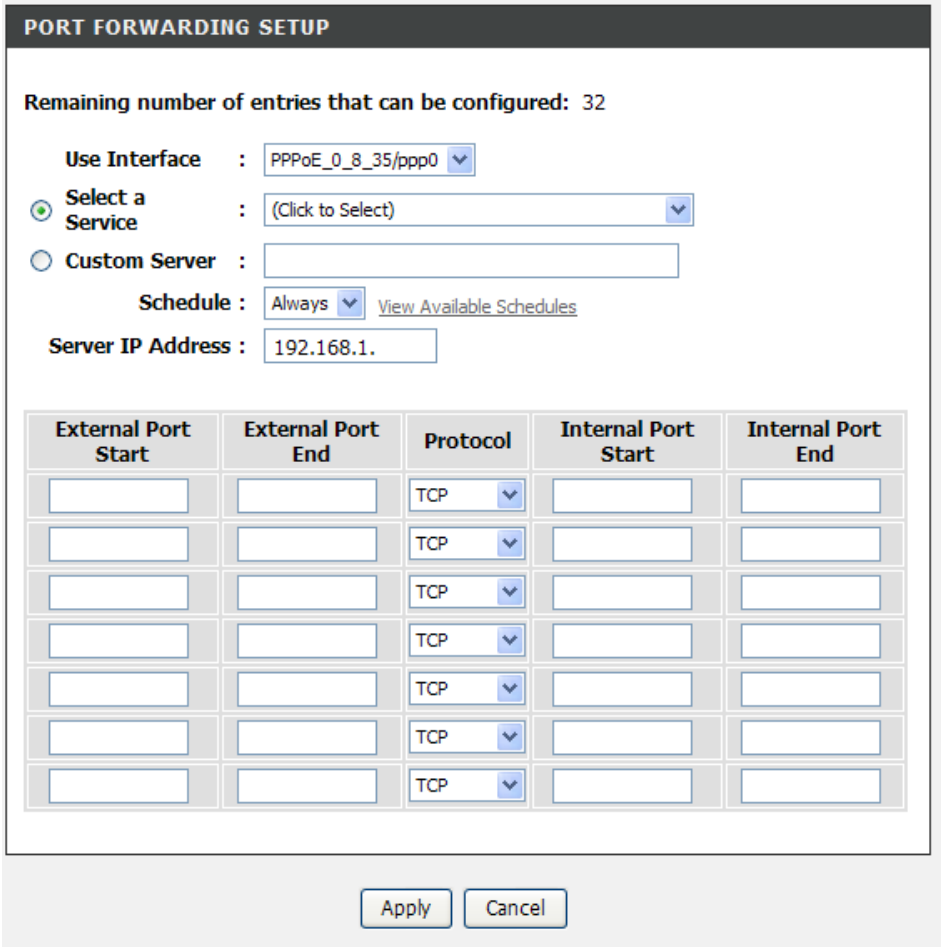


Select a Service drop-down menu for a pre-configured application or select **Custom Server** type a name input box to define your own application.

The **External Port** shows the ports opened for remote users in the WAN side of the router. The **TCP/UDP** means the protocol type of the opened ports.

The **Internal Port** shows the ports opened in the PC with the appointed IP Address. The **TCP/UDP** means the protocol type of the opened ports.

Please click the **Apply** button to save the configuration.



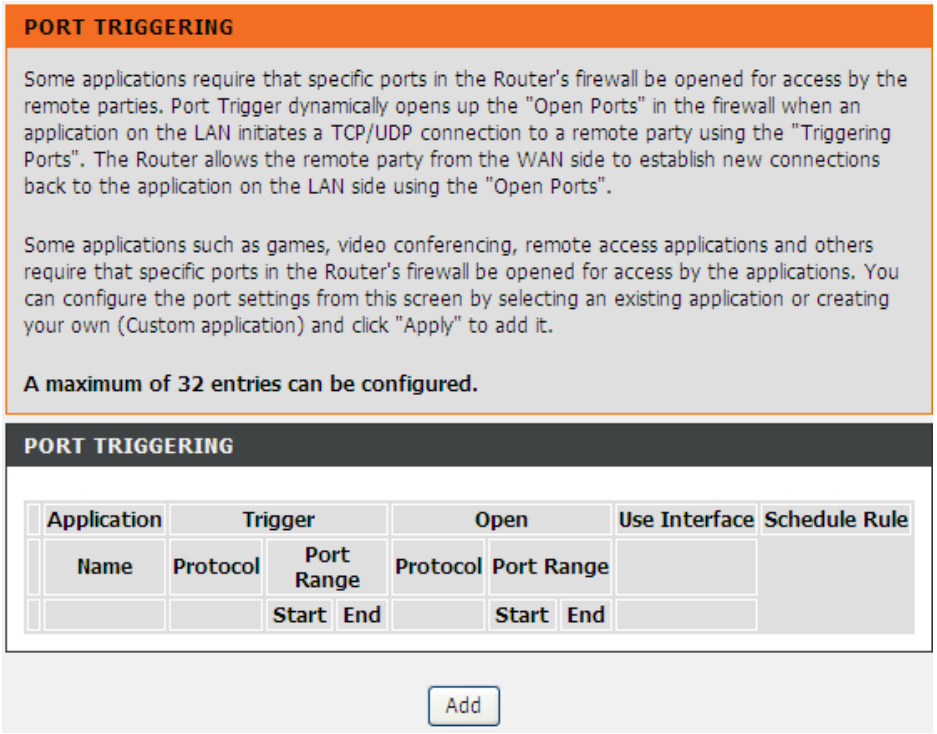
PORT TRIGGERING

Some applications such as games, video conferencing, remote access applications and others require that specific ports in the Router's firewall be opened for access by the applications.

To access **PORT TRIGGERING** setting windows, click on the PORT TRIGGERING button in the **ADVANCED left menu** directory

PORT TRIGGERING

Press **Add** button to add port forwarding.

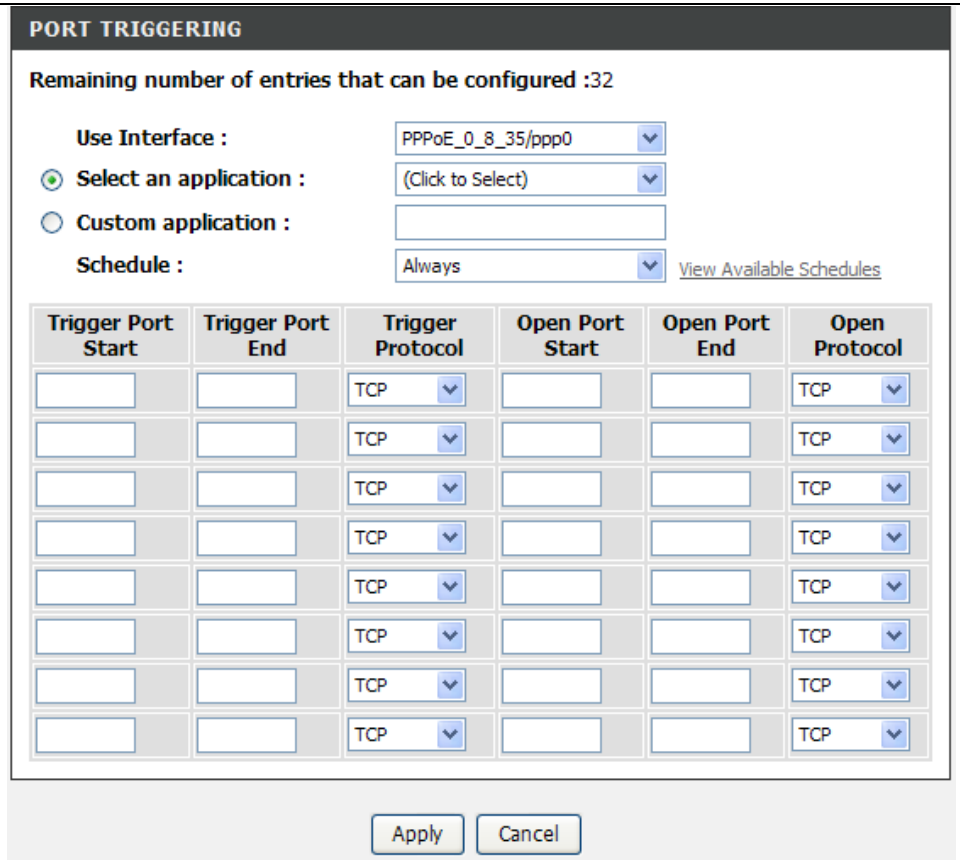


Select an application drop-down menu or **Custom application** type a name input box to choose the application you want to setup for port triggering.

The **Trigger Port** shows the ports opened for remote users in the WAN side of the router. The **TCP/UDP** means the protocol type of the opened ports.

The **Open Port** shows the ports opened in the PC with the appointed IP Address. The **TCP/UDP** means the protocol type of the opened ports.

Please click the **Apply** button to save the configuration.



DMZ

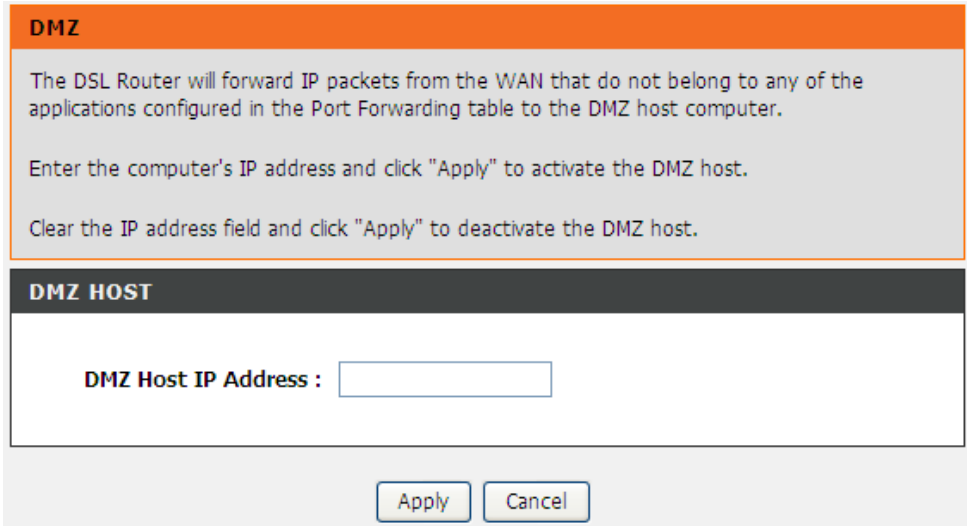
The DSL-2750B will forward IP packets from the WAN that do not belong to any of the applications configured in the Port Forwarding table to the DMZ host computer

To access setting window, click on the **DMZ** button in the **ADVANCED** tab

DMZ

Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible to agents on the Internet with the correct type of software. Note that any client PC in the DMZ is 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 DMZ.

Click **Apply** to save the settings.

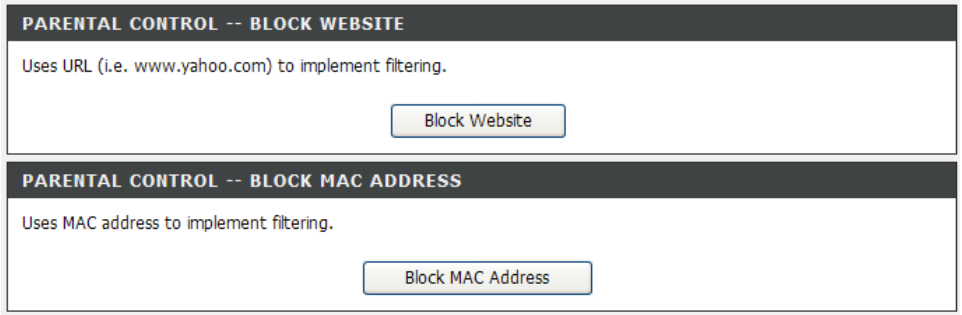


PARENTAL CONTROL

Parental Control provides the restricting Internet access. Block Websites allows you to quickly create a list of all web sites that you wish to stop users from accessing. Block MAC Address restrictions Client or PCs connected to Router to access the Internet. Trusted Computers allowed exclude a range of IP not restricted by Block Website

To access **PARENTAL CONTROL** setting windows, click on the **PARENTAL CONTROL** button in the **ADVANCED** tab

PARENTAL CONTROL divided into **BLOCK WEBSITE** and **BLOCK MAC ADDRESS**.

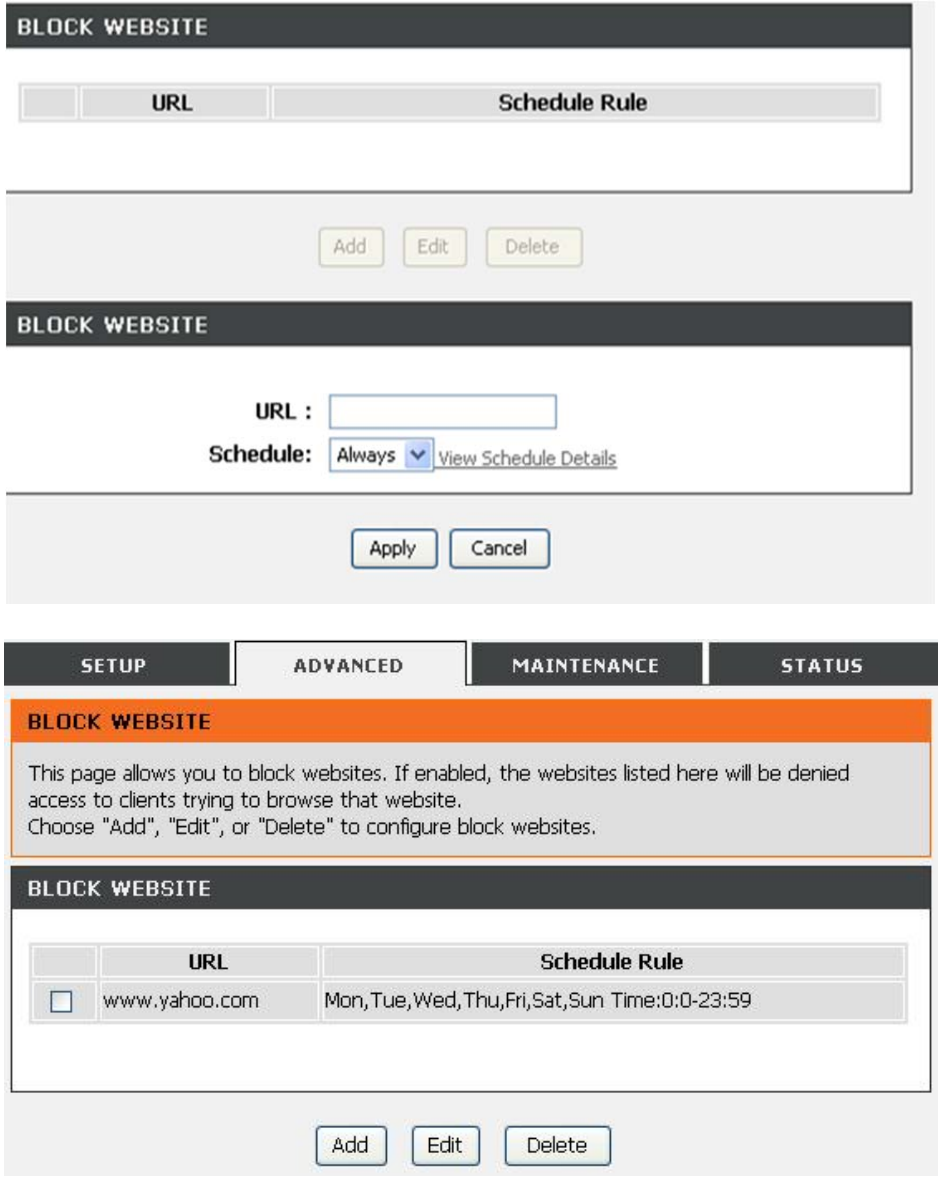


BLOCK WEBSITE

Press **Add** button and type the website URL which you want to block on the Website.

Schedule set the day and time to block.

After setting, click **Apply** button and then it will show in list.

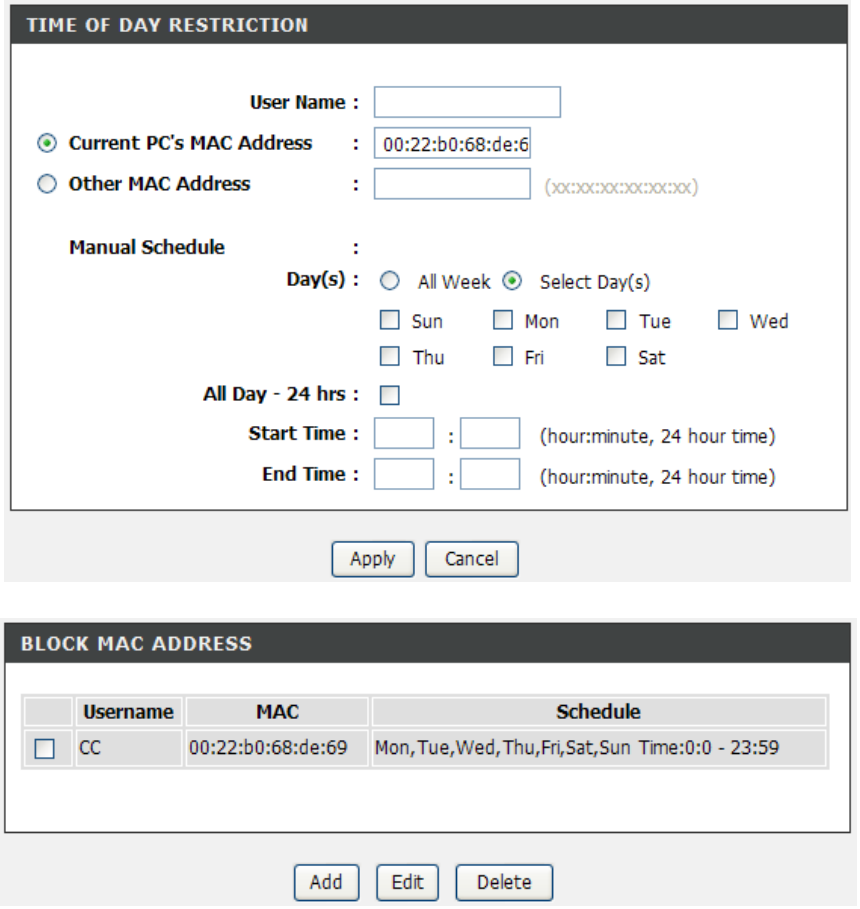


BLOCK MAC ADDRESS

Press **Add** button and type the MAC Addre ss of LAN device which you want to block

Schedule set the day and time to block.

After setting, please click **Apply** button and then it will show in list.

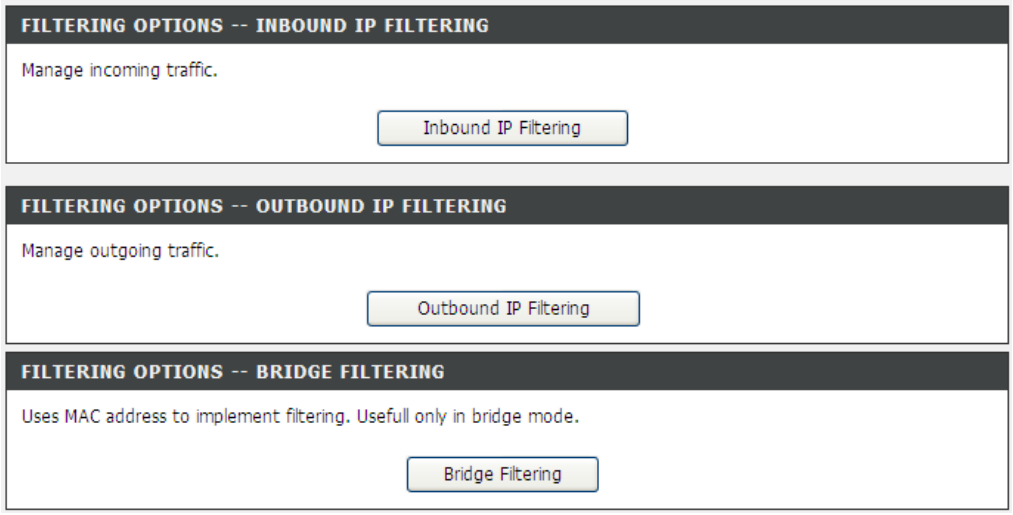


FILTERING OPTIONS

By default, all outgoing IP traffic from the LAN is allowed. The Inbound Filter allows you to create a filter rule to filter incoming IP traffic by specifying a filter name and at least one condition below. 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 below. All of the specified conditions in this filter rule must be satisfied for the rule to take effect.

To access Filter Option setting windows, click on the **Filtering Options** button in the **ADVANCED** tab

FILTERING OPTIONS divided into **INBOUND IP FILTERING**, **OUTBOUND IP FILTERING** and **BRIDGE FILTERING**.



INBOUND IP FILTER

Press **Add** button to active inbound filter

Enter the **Filter Name** and specify at least one of the following criteria: **Protocol, Source/Destination IP address, Source/Destination Subnet Mask**, and **Source/Destination Port.**

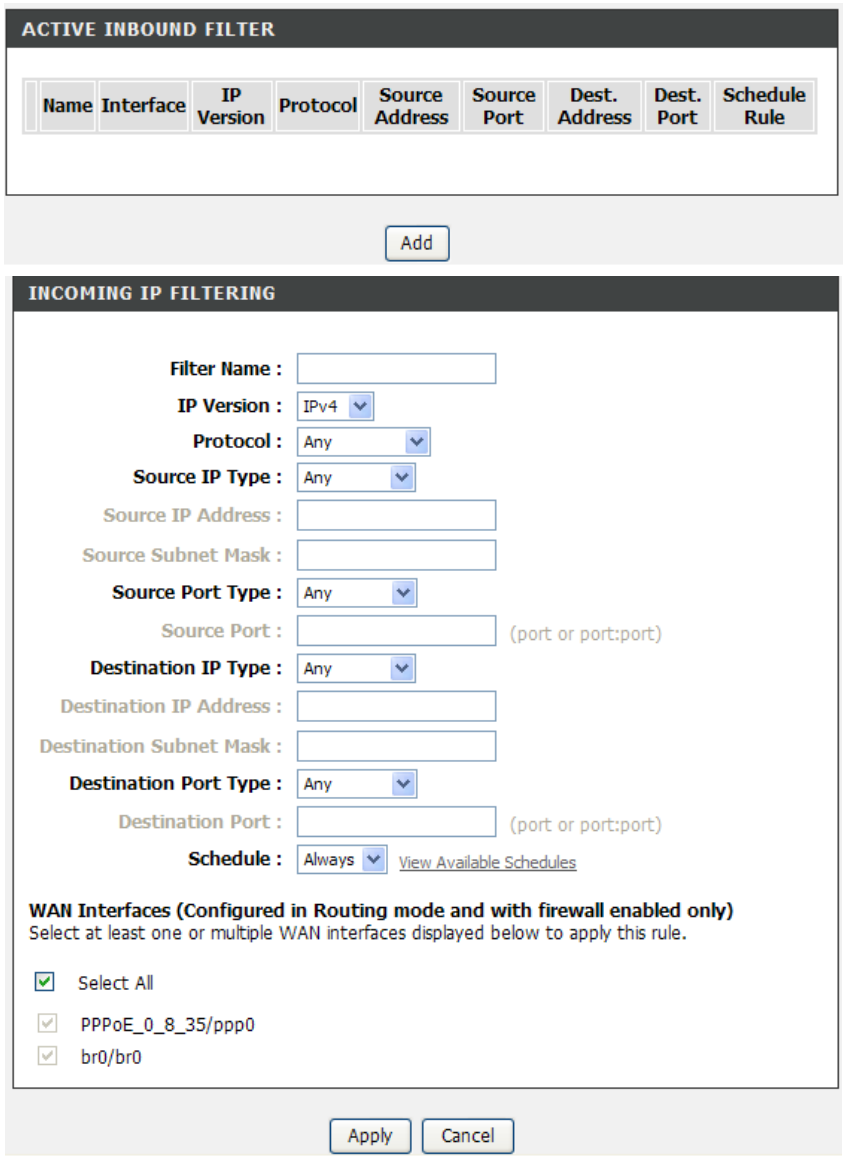
Type **Source IP address**, **Source Subnet Mask** and **Source Port**(port or port::port means from which port to which port)

Type **Destination IP address**, **Destination Subnet Mask** and **Destination Port**(port or port::port means from which port to which port)

Set the **Schedule**: Always, Never, or View Available Schedules

Click **Apply** to save the settings.

Note: The setting can be applied when the firewall is enabled.



OUTBOUND IP FILTER

Press **Add** button to active outbound filter

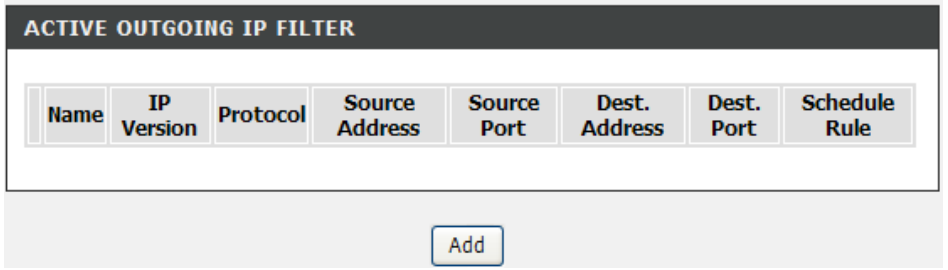
Enter the **Filter Name** and specify at least one of the following criteria: **Protocol, Source/Destination IP address, Source/Destination Subnet Mask**, and **Source/Destination Port.**

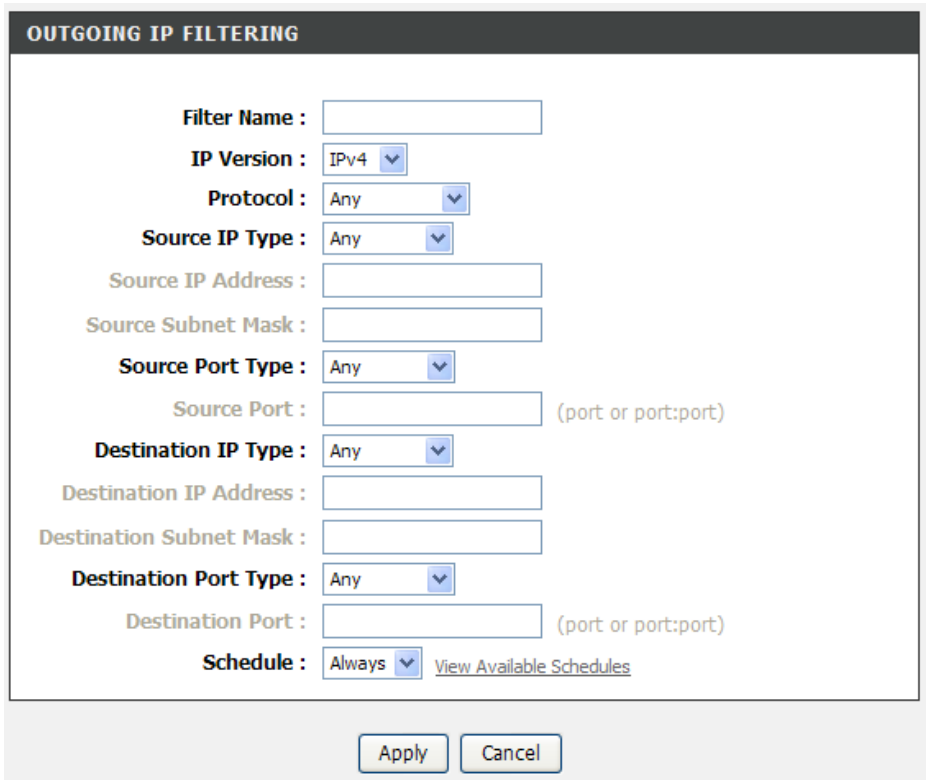
Type **Source IP address**, **Source Subnet Mask** and **Source Port**(port or port::port means from which port to which port)

Type **Destination IP address**, **Destination Subnet Mask** and **Destination Port**(port or port::port means from which port to which port)

Set the **Schedule**: Always, Never, or View Available Schedules

Click **Apply** to save the settings.





BRIDGE FILTERING

Press **Add** button to active **BRIDGE FILTER SETUP**

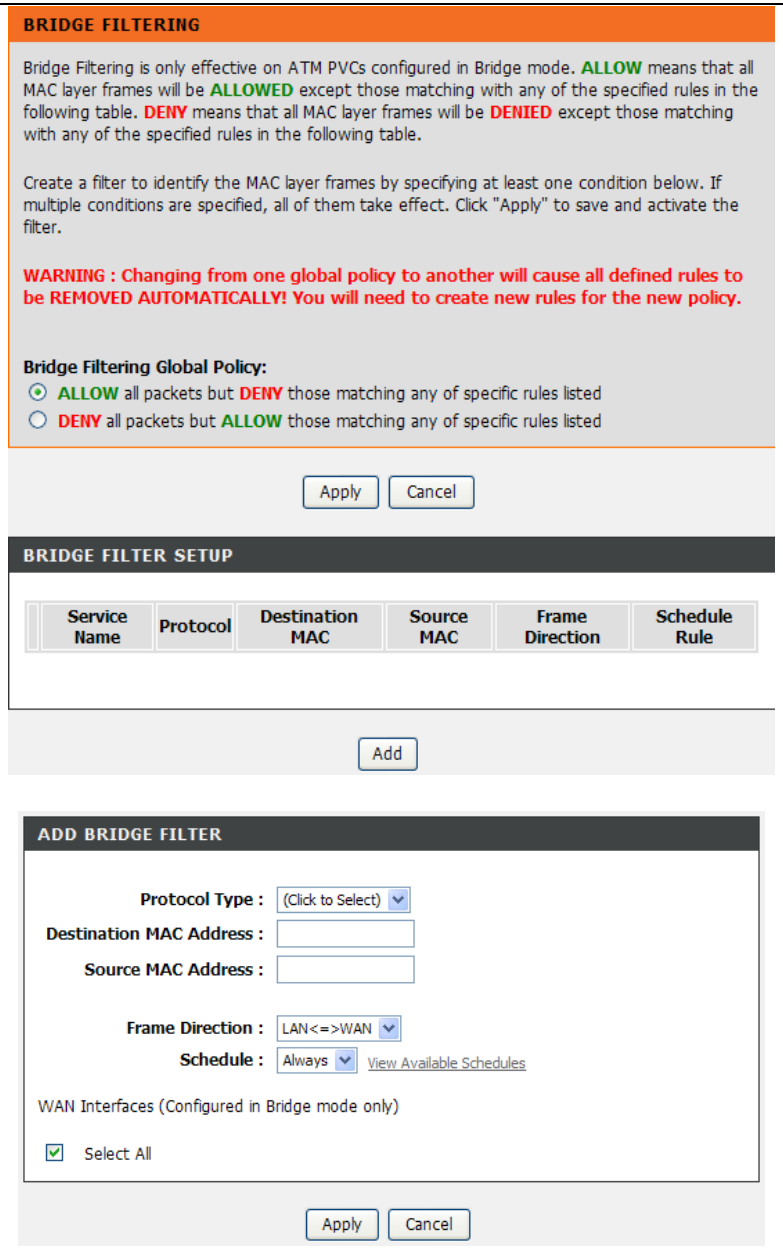
Select **Protocol Type.**

Input **Destination MAC Address** and **Source MAC address**,

Select Frame Direction, LAN <=>WAN or WAN => LAN or LAN => WAN

Set the **Schedule**: Always, Never, or View Available Schedules

Click **Apply** button to add the policy in the list.



DNS SETUP

DNS (Domain Name System) is used to translate the domain name to IP addresses. You can type it in or get it automatically.

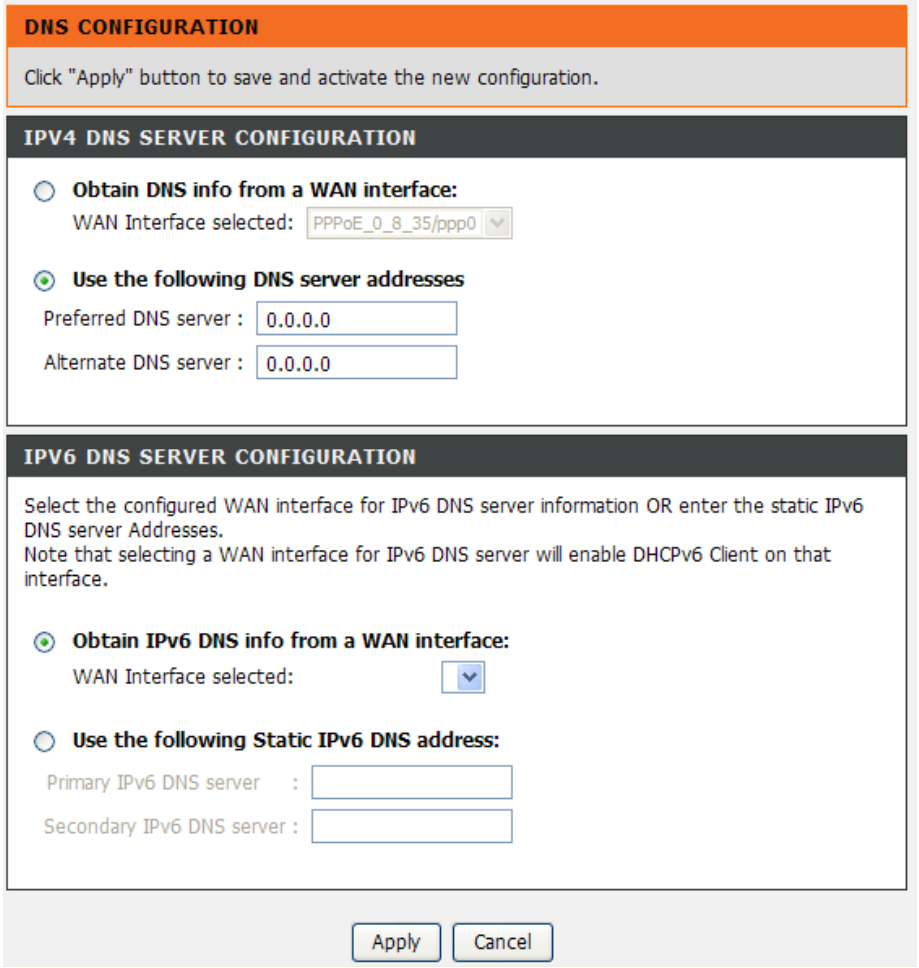
To access the **DNS** setting window, click on the **DNS** button under the **ADVANCED** tab.

DNS SERVER CONFIGURATION

The DNS is divided into **IPv4** and **IPv6 DNS SERVER CONFIGURATION**

If you are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network, check **Obtain DNS info from a WAN interface** box.

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



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 (for example: 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 and your friends don't mind what your IP address is, and then just type the DDNS name to reach. You can use the D-Link DDNS server, https://www.dlinkddns.com to have a free DDNS.

To set up, click on the **Dynamic DNS** button under the **ADVANCED** tab.

DDNS CONFIGURATION

Press **Add** / **Edit** / **Delete** button to modify your D-DNS list.

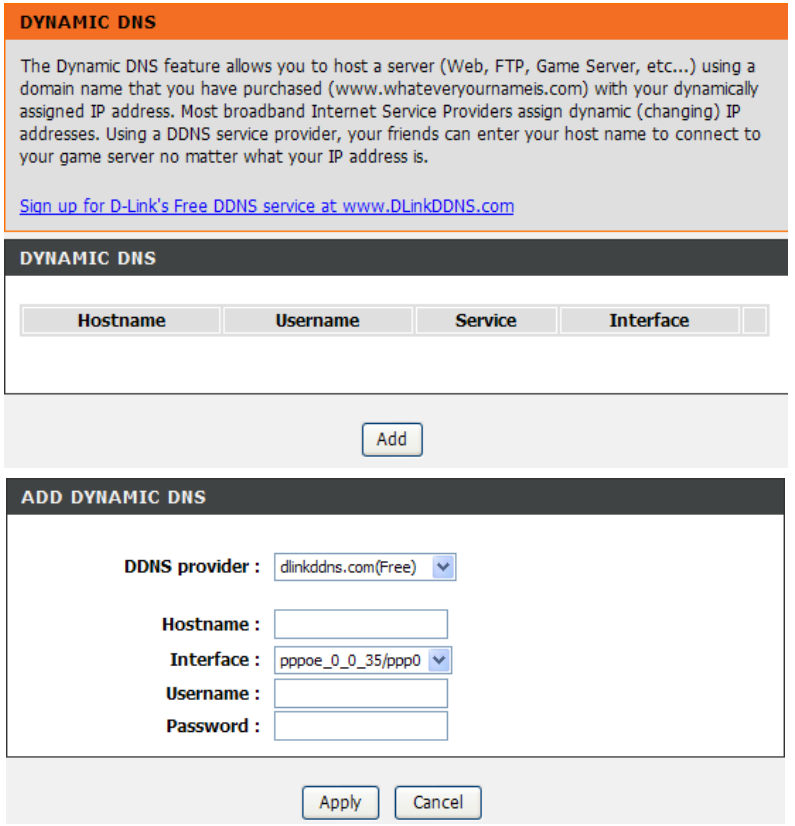
Select one of the **DDNS provider** from the down-list drop.

Enter the **Hostname** which you registered with your DDNS service provider.

Select the **Interface** you would like to use.

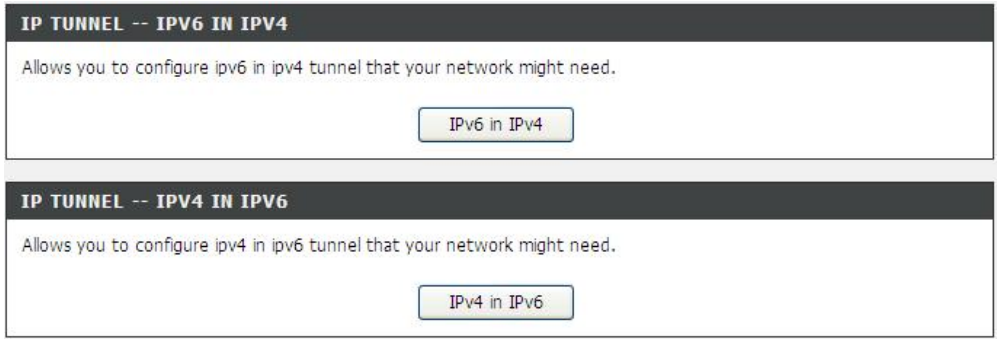
Enter the **Username/Password** for your DDNS account.

After configure the DNS settings as desired, click on the **Apply** button to apply settings.



IP TUNNEL

You can configure **IPv6 in IPv4** or **IPv4 in IPv6** in **IP Tunnel**. To set up, click on the **IP Tunnel** button under the **ADVANCED** tab.



IPV6 IN IPV4

This function allows you to configure a 6IN4 tunnel, in which IPv6 host can access IPv6 network via IPv4 network.

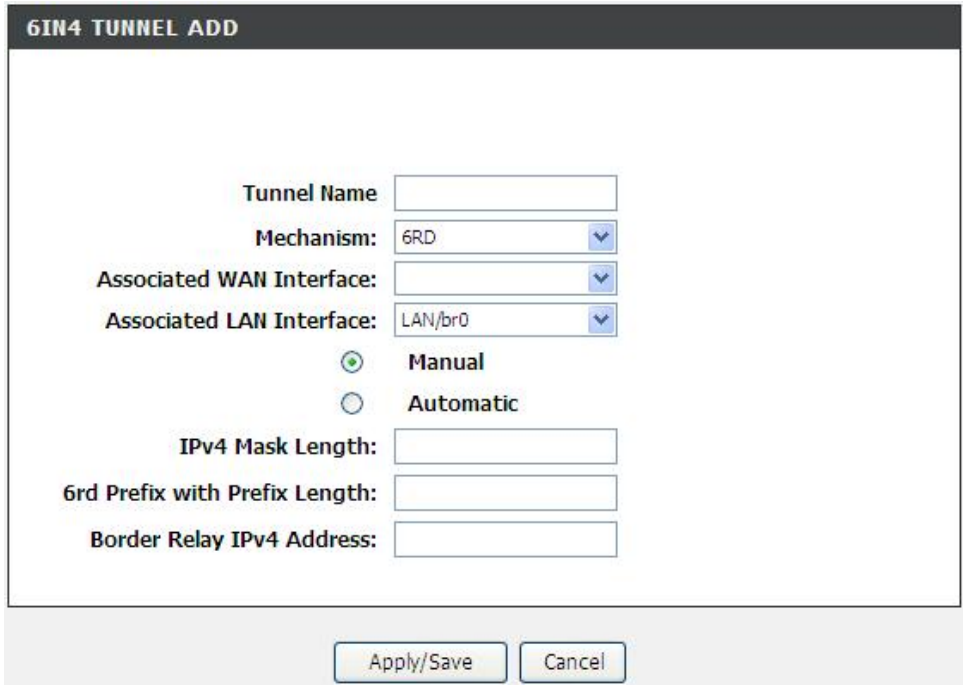
Note: Only 6RD is supported now.

Click **Add** to create a Tunnel, in which IPv6 packets are encapsulated in IPv4.

Tunnel Name: Enter a name of the tunnel
Mechanism: Only 6rd is supported now.
Associated WAN Interface: It is the connection that you want to apply to create the tunnel.

Notice: The WAN connection must support IPv6 service.

Associated LAN Interface: The tunnel that serves LAN sides. It must be fully IPv6 enabled.
Manual/Automatic: It determines how to get 6rd configure elements. Automatic means the elements got from DHCP option.
IPv4 Mask Length: The number of high-order bits that are identical across all CE IPv4 addresses within a given 6rd domain. For example, if there are no identical bits, IPv4 MaskLen is 0 and the entire CE IPv4 address is used to create the 6rd delegated prefix. If there are 8 identical bits (e.g., the Private IPv4 address range 10.0.0.0/8 is being used), IPv4MaskLen is equal to 8 and IPv4MaskLen RFC high-order bits are stripped from the IPv4 address before constructing the corresponding 6rd delegated prefix.
6rd Prefix with Prefix Length: The 6rd IPv6 prefix for the given 6rd domain.
Border Relay IPv4 Address: The IPv4 address of the 6rd Border Relay for a given 6rd domain.



IPV4 IN IPV6

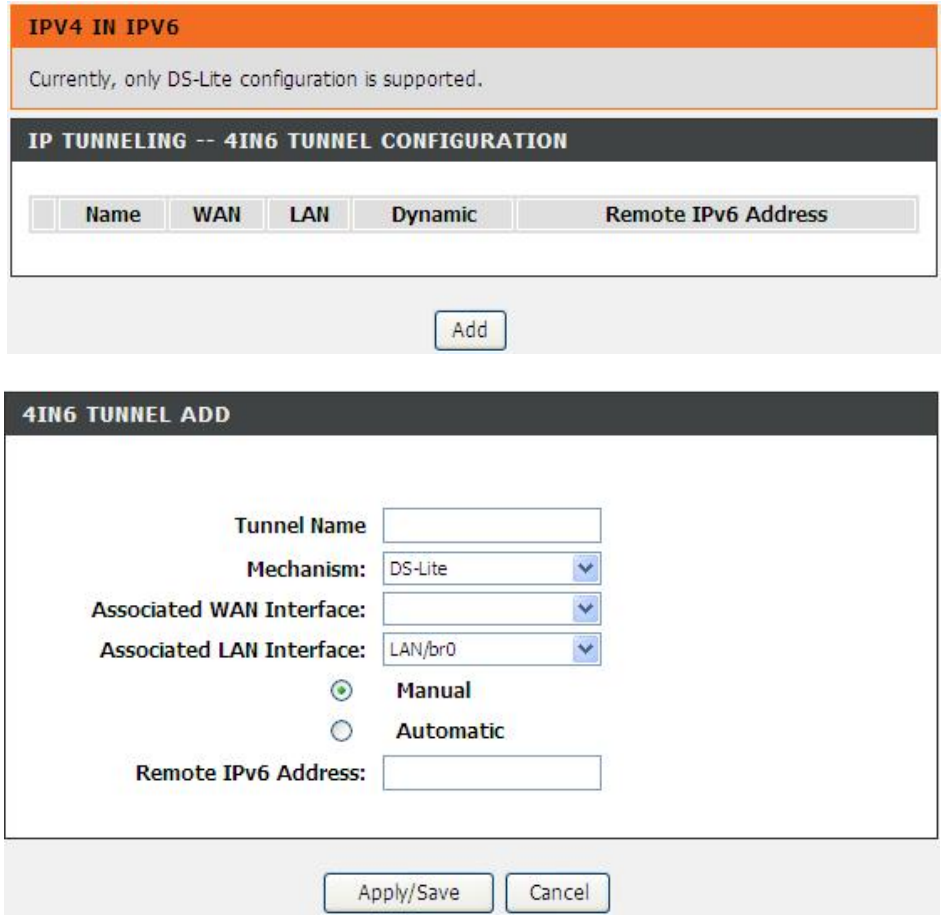
This function allows you to configure a 4IN6 tunnel, in which IPv4 host can access IPv4 network via IPv6 network.

Click **Add** to create a Tunnel, in which IPv4 packets are encapsulated in IPv6.

Note: Only DS Lite is supported now.

Tunnel Name: The name of the tunnel that you want to create.
Mechanism: Only DS Lite is supported now.
Associated WAN Interface: It is the WAN connection that you want to apply to create the tunnel. **Notice**: The WAN connection must support IPv6 service.
Associated LAN Interface: The tunnel that serves LAN sides, not used yet.
Manual/Automatic: Determines how to get AFTR's IPv6 address.
Automatic means the address got from DHCPv6 option.
Remote IPv6 Address: AFTR's IPv6 address.

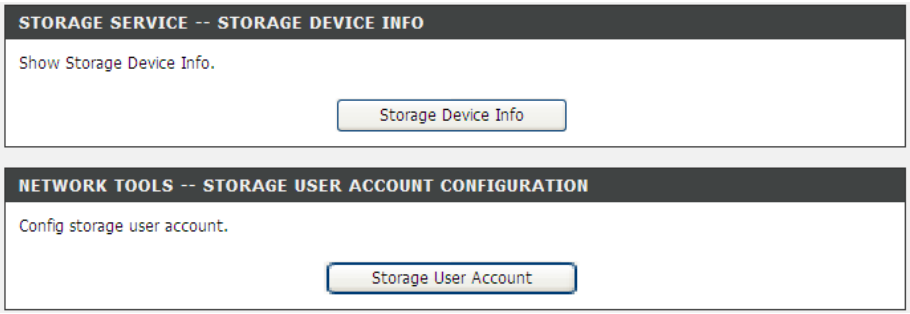
Click the **Apply/Save** button to apply settings.



STORAGE SERVICE

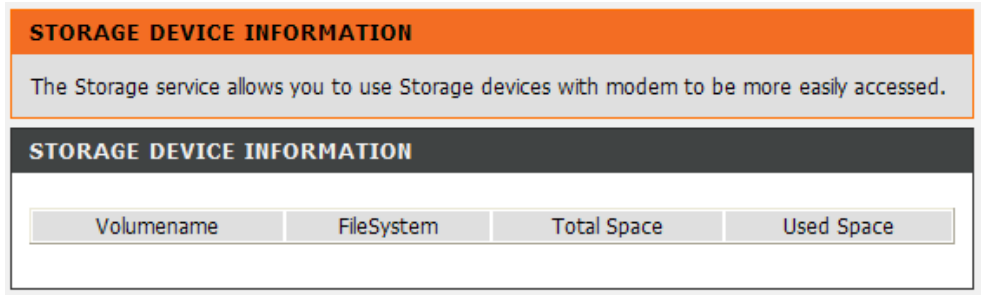
To set up, click on the **Storage Service** button under the **ADVANCED** tab.

STORAGE SERVICE is divided into **STORAGE DEVICE INFO** and **STORAGE USER ACCOUNT CONFIGURATION.**



STORAGE DEVICE INFORMATION

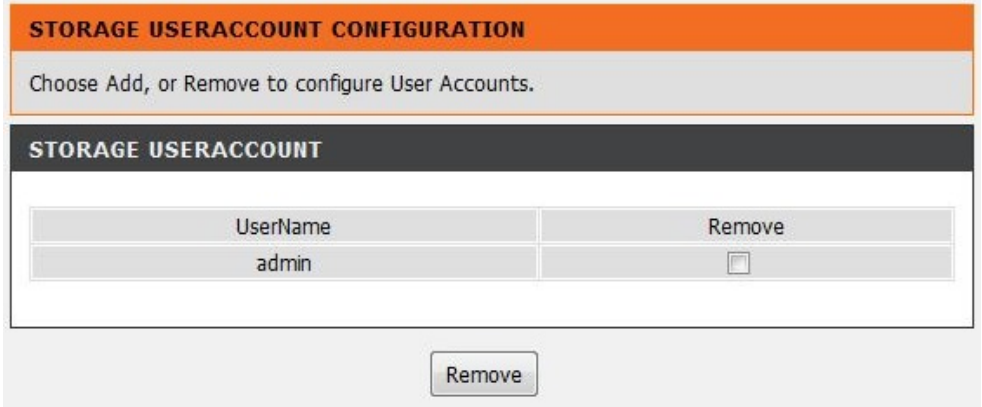
First connect your USB Storage device to the USB port, this page will be shown, the information including **File System, Total Space** and **Used Space.**

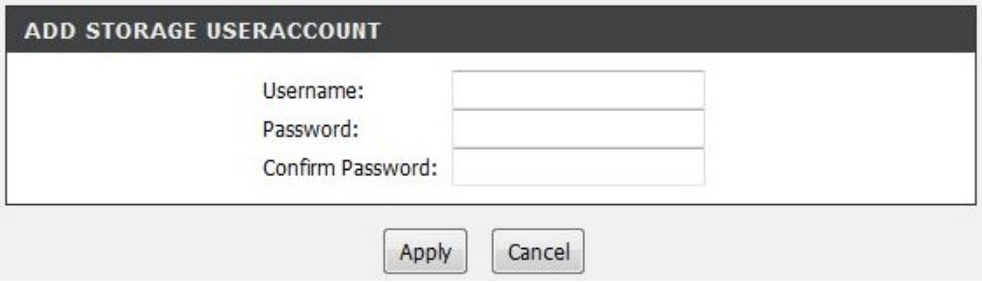


STORAGE USER ACCOUNT CONFIGURATION

Click **Add** to add a new user . Set a valid **Username** that access CPE' s samba server. Enter **Password** and **Confirm Password**.

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

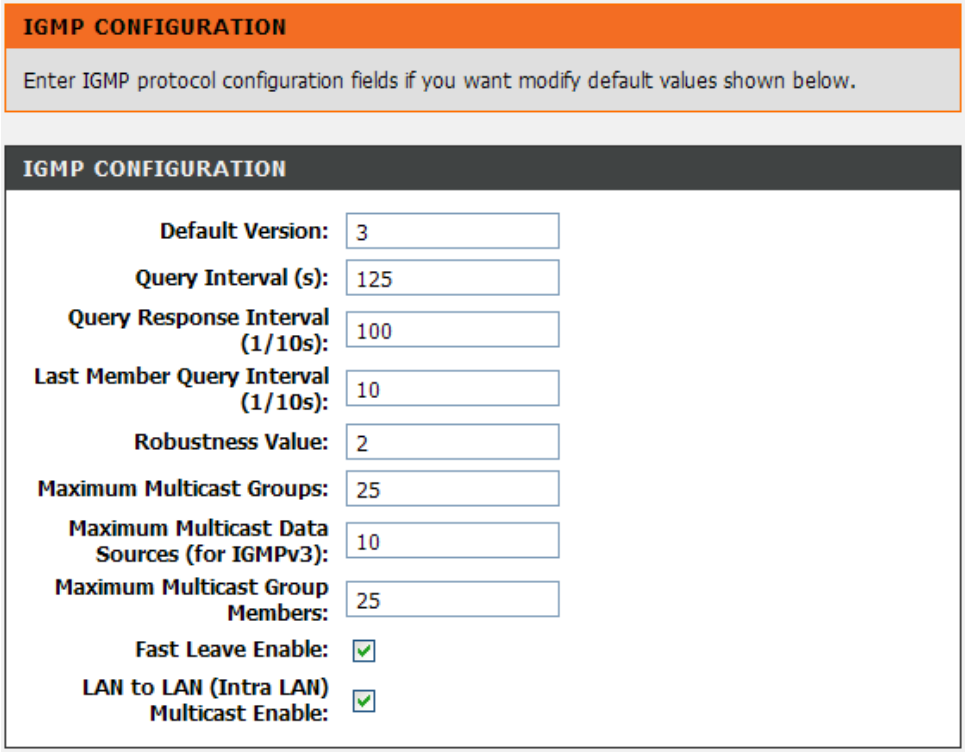




MULTICAST

IGMP CONFIGURATION

Default Version: IGMP version
Query Interval(s):The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet)
Query Response Interval (1/10s): The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval
Last Member Query Interval (1/10s): The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages.
Robustness Value: The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets.
Maximum Multicast Groups: max multicast groups
Maximum Multicast Data Sources (for IGMPv3): max group data sources that want to receive.
Maximum Multicast Group Members: max member in one group
Fast Leave Enable: Enable or disable fast leave feature.
LAN to LAN (Intra LAN) Multicast Enable: Enable or disable LAN to LAN multicast.



NETWORK TOOL

The **NETWORK TOOL** feature allows you to configure **PORT MAPPING, IGMP, QUALITY OF SERVICE, QUEUE CONFIG, QOS CLASSIFICATION, UPNP, ADSL, PACKET FLOW, TR-069,** and **CERTIFICATIONS**

To access the **NETWORK TOOL** setting window, click on the **NETWORK TOOL** button under the **ADVANCED** tab.

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

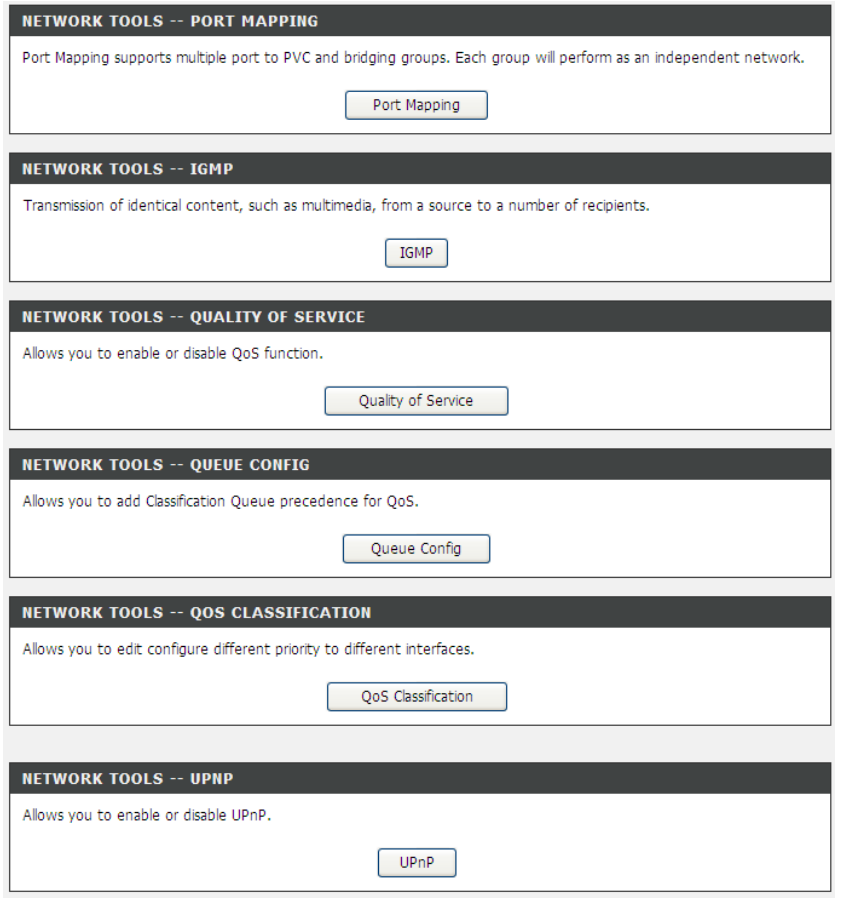
IGMP
Transmission of identical content, such as multimedia, from a source to a number of recipients.

QUALITY OF SERVICE
Allows you to manually configure spec ial routes that your network might need.

QUEUE CONFIG
Allows you to configure queuing for QoS.

QOS CLASSIFICATION
Allows you to edit QoS priority to different interfaces.

UPNP
Allows you to configure UPnP.

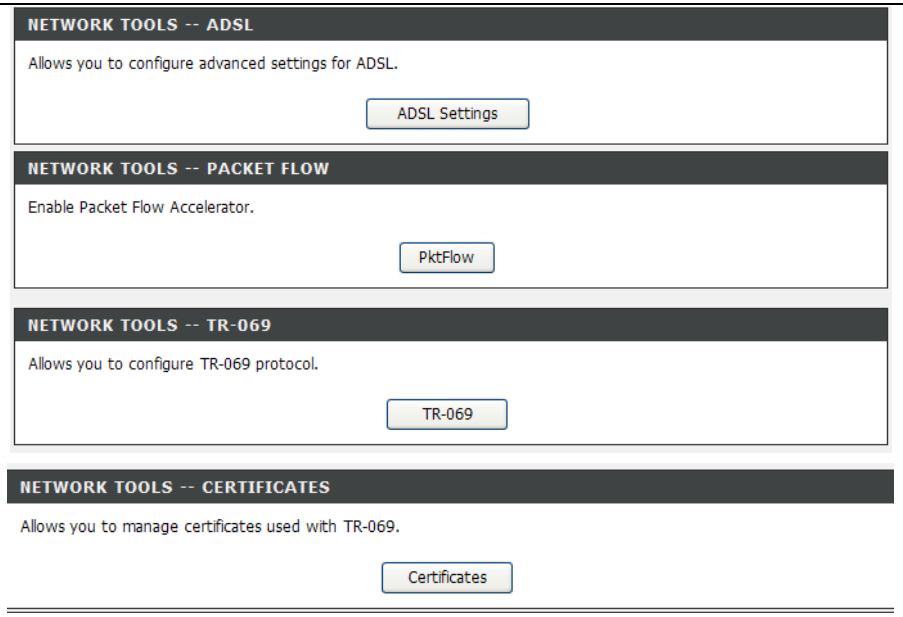


ADSL
Allows you to configure Default Gateway used by WAN Interface.

PACKET FLOW
Allows you to enable packet flow accelerator.

TR-069
Allows you to configure TR-069 protocol.

CERTIFICATIONS
Allows you to manage certification with TR-069.



PORT MAPPING

Port Mapping supports multiple ports to PVC and br idging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appr opriate LAN and W AN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group. Only the default group has IP interface.

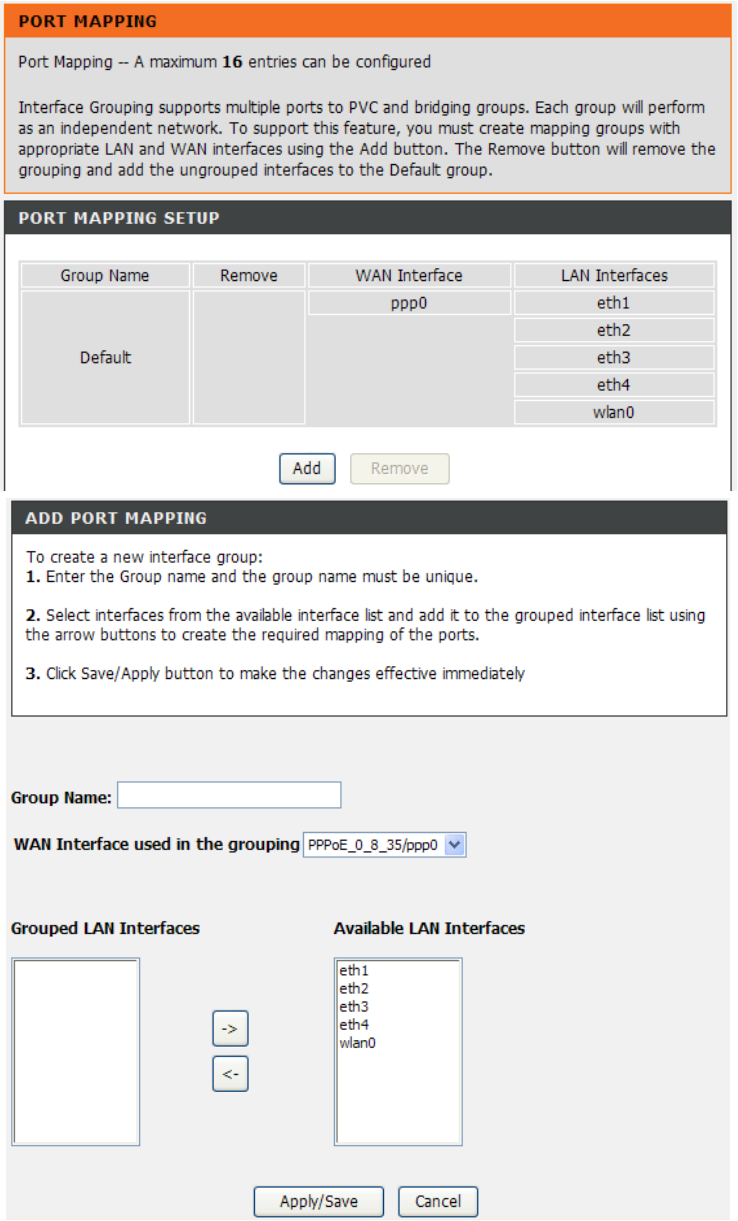
Click **Add** button to add port mapping configuration

In **ADD PORT MAPPING** page, please input the **Group Name** which you want to assign in the GROUP Name.

Select WAN interface you want to use in the **WAN Interface used in the grouping**

Select LAN Interface you want to use to join the group in the **Grouped LAN Interfaces** from the **Available LAN Interfaces**. The group name must be unique.

Click on the **Apply/Save** button to save settings.

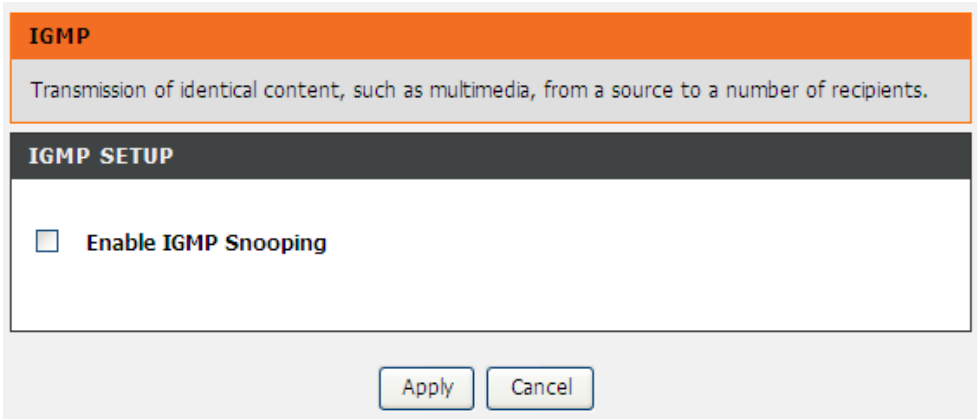


IGMP

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

Check the box to **Enable IGMP Snooping**

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

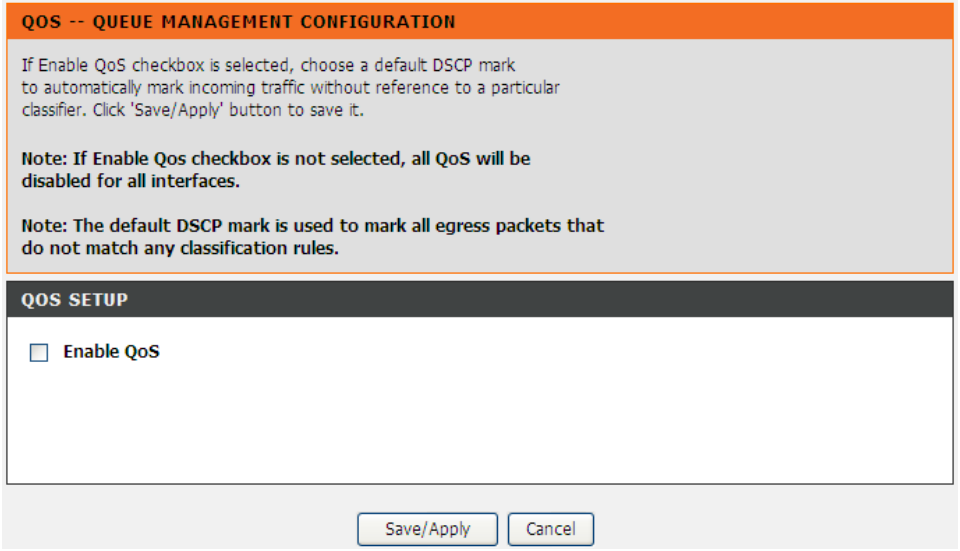


QoS

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

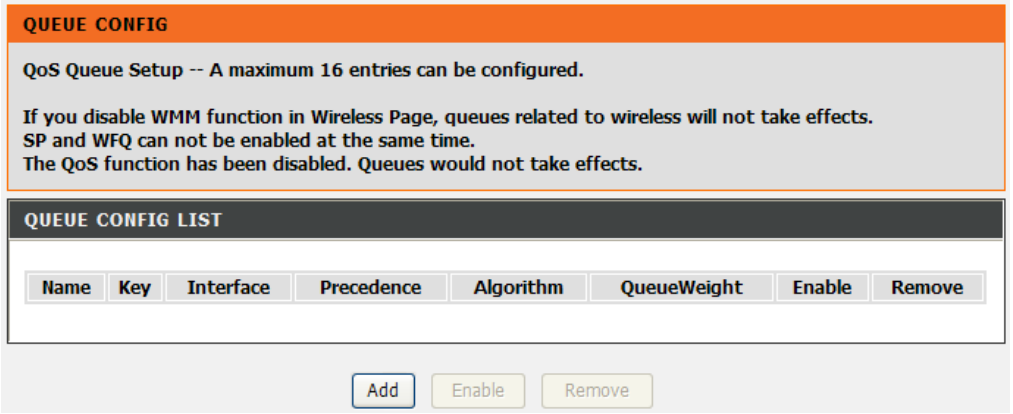
Check the box to enable/disable the QoS.

Click **Save/Apply** to take the setting effect.



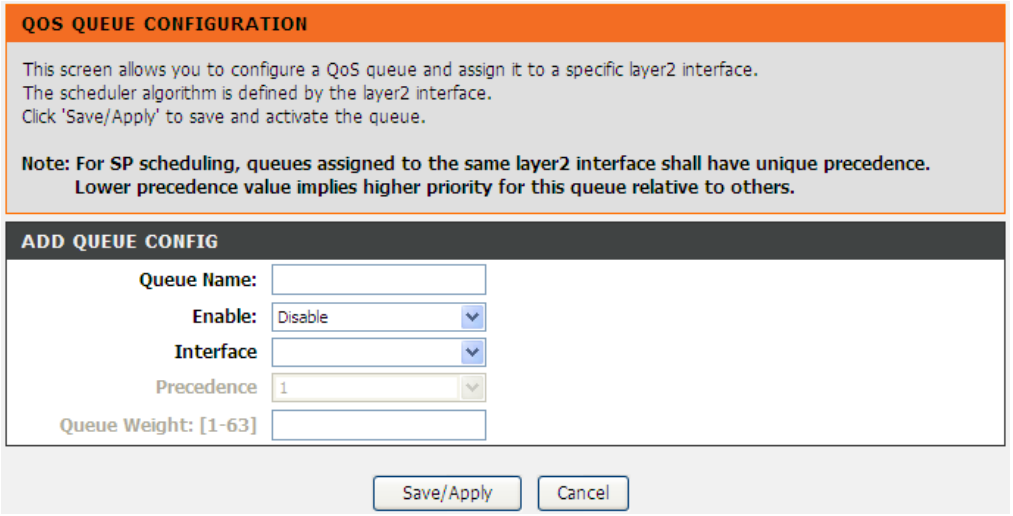
QUEUE CONFIG

Click **Add** button to proceed the **QOS QUEUE CONFIGURATION**



In **QOS QUEUE CONFIGURATION** page, type the **Queue Name**, select **Enable** and **Interface** in drop-down menu.

Click on the **Save/Apply** button to save settings.



QOS CLASSIFICATION

Click **Add** button to proceed the **QOS CLASSIFICATION**

In **QUALITY OF SERVICE** page, type the traffic class name in the **Traffic Class Name**.

If added more than one rules, you can select priority in the **Rule Order**.

Enable or Disable the rule in the **Rule Status**.

SPECIFY CLASSIFICATION CRITERIA

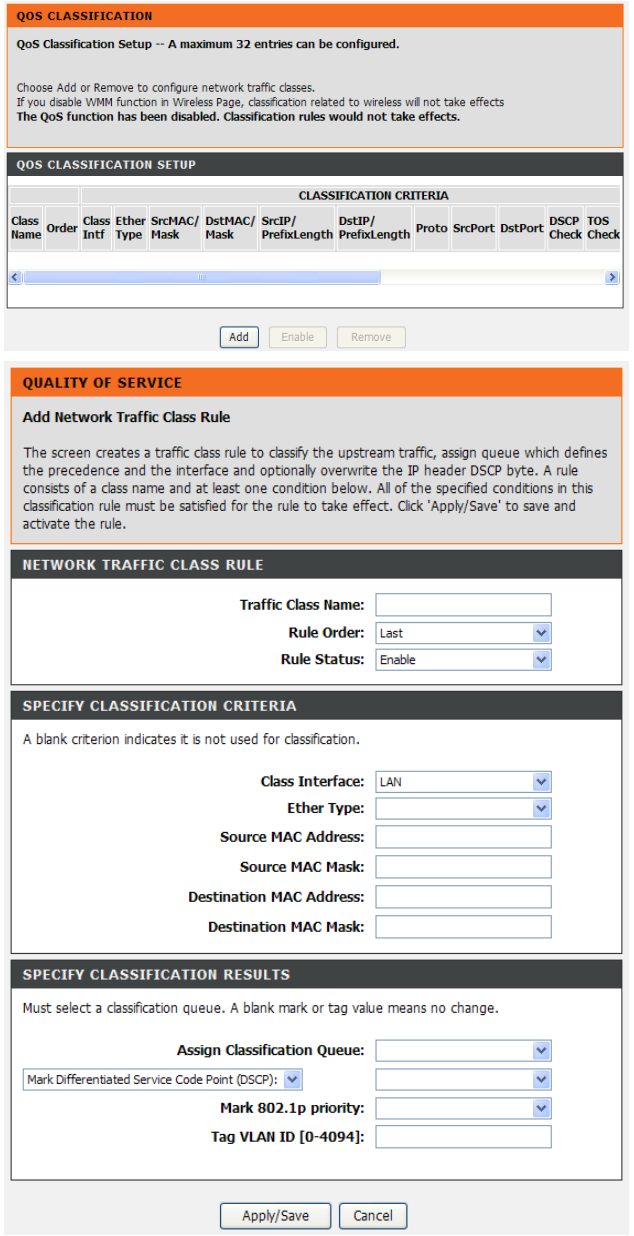
Select **Class Interface** and **Ether Type** in the drop-down menu.

Input the **Source MAC Address**, **Source MAC Mask**, **Destination MAC Address** and **Destination MAC Mask**.

SPECIFY CLASSIFICATION RESULTS

Select **Assign Classification Queue**, **Mark Differentiated Service Code Point (DSCP) and Mark 802.1p priority** in the drop-down menu. Type the **Tag VLAN ID [0-4094]**.

Click on the **Apply/Save** button to save settings.

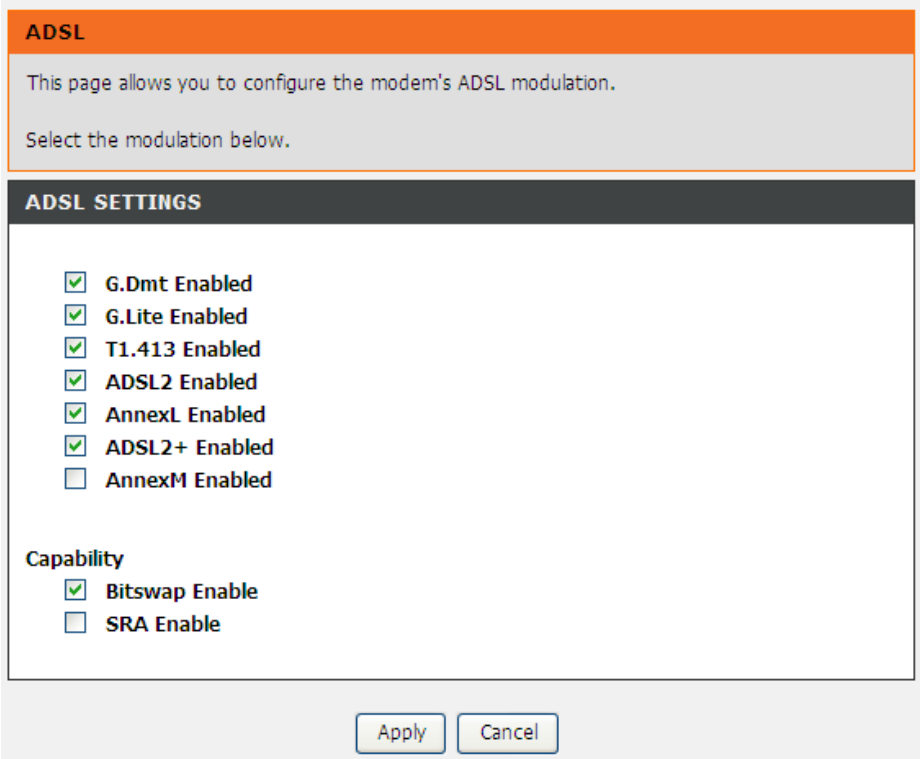


UPNP

Choose to Enable/Disable UPnP Configuration

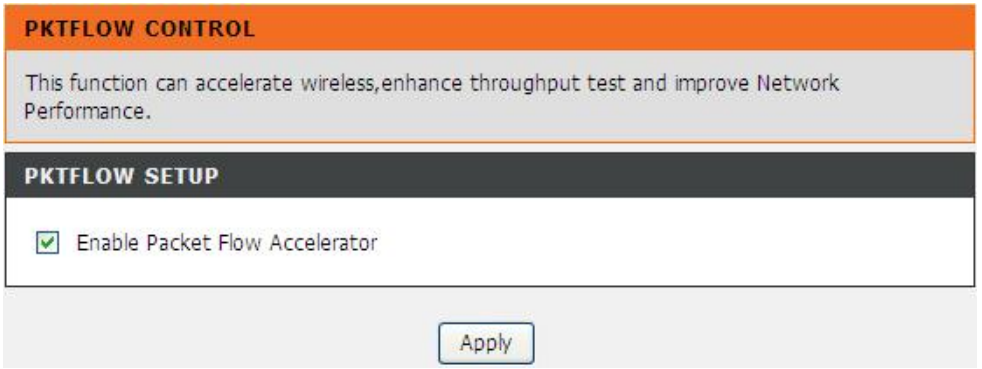
DSL Settings

The DSL settings page contains a modulation and capability section to be specified by your ISP. Consult your ISP to select the correct settings for each. Then click on Apply if you finish or click on Advanced Settings if you want to configure more



PKTFLOW CONTROL

Check the box to accelerate wireless, enhance throughput test and improve Network Performance.

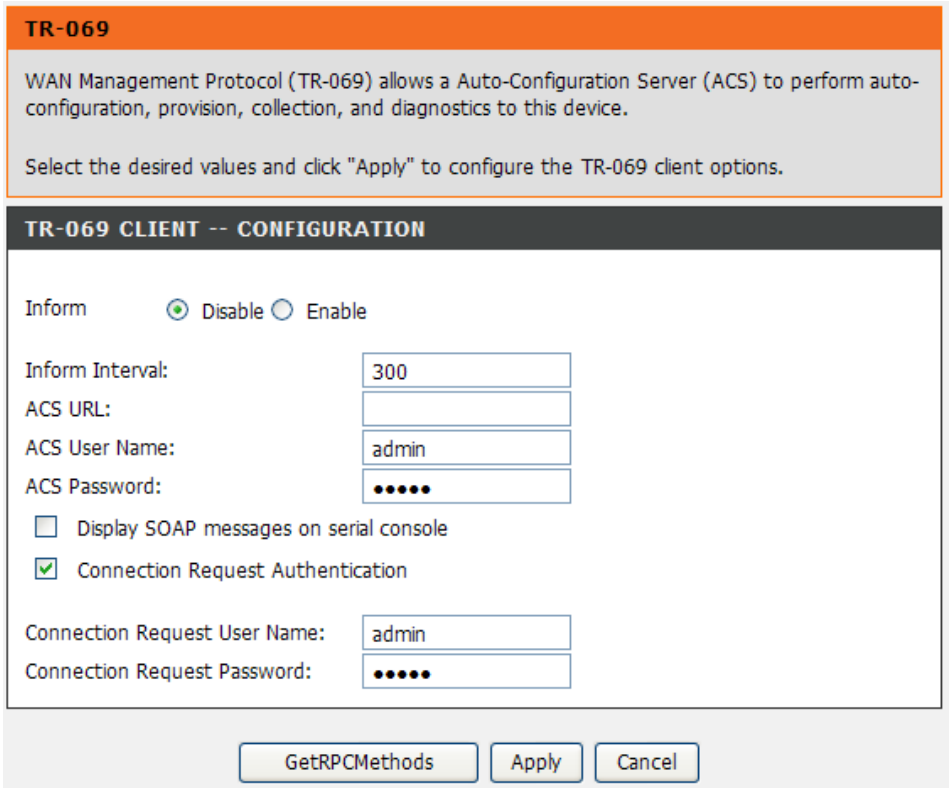


TR-069

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

In this page, you may configure the parameters such as the ACS URL, ACS password, and connection request user name.

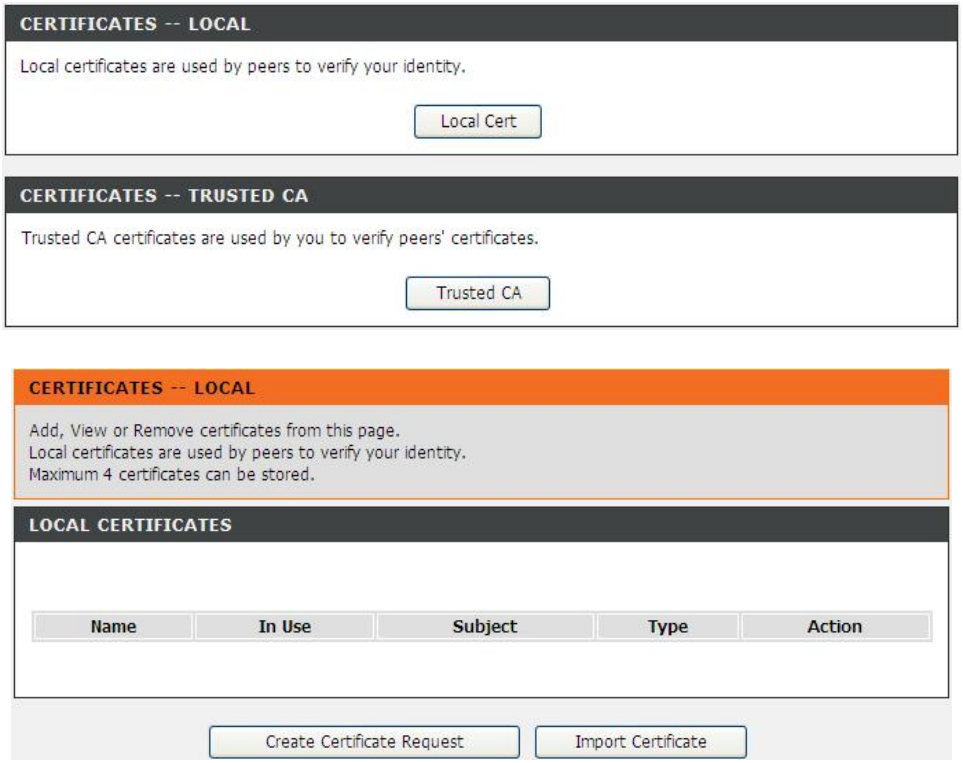
After finishing setting, click **Apply** to save and apply the settings.



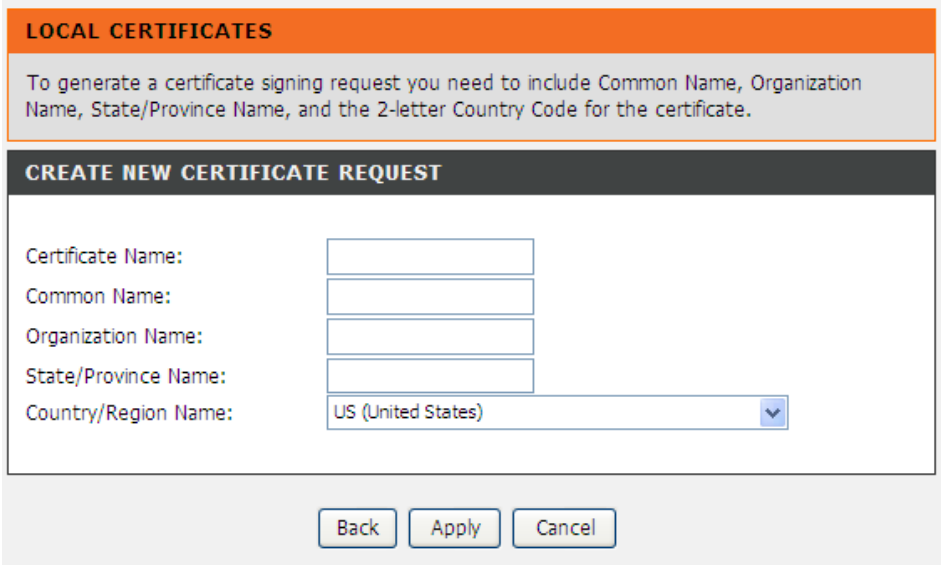
CERTIFICATIONS

Click **Local Cert** to import local certificates that are used by peers to verity your identity.

In **CERTIFICATES – LOCAL** page, you can acquire the local certificate by clicking Create Certificate Request or Import Certificate. You may also create or remove a certificate.



CREATE NEW CERTIFICATE REQUEST



Set the **Certificate Name** and input the **Common Name**, which is the "fully qualified domain name," (or FQDN) used for DNS lookups of your server (for example, www.mydomain.com). Browsers use this information to identify your Web site. Some browsers will refuse to establish a secure connection with your site if the server name does not match the common name in the certificate. Please do not include the protocol symbol "http://" or any port numbers or pathnames in the common name. Do not use wildcard characters such as “*” or “?”, and do not use an IP address.

Input **Organization Name.** The name of the organization to which the entity belongs (such as the name of a company).

Input **State/Province Name.** This is the name of the state or province where your organization's head office is located. Enter the full name of the state or province.

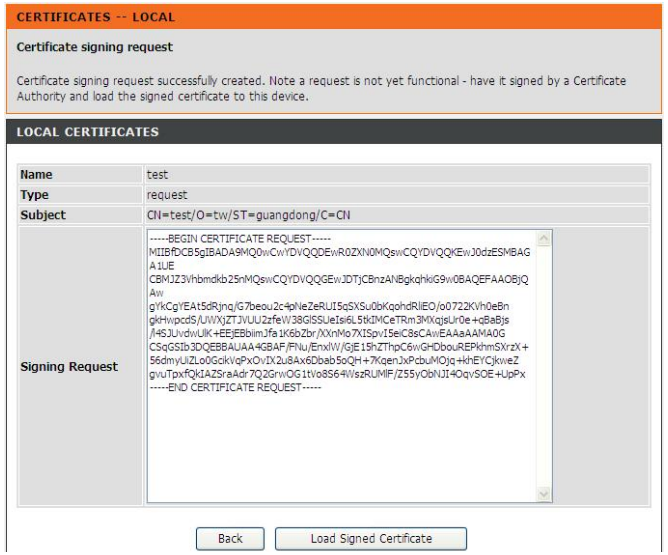
Select **Country/Region Name.** This is the two-letter ISO abbreviation for your country (for example, AU for Australia).

After finishing setting, click **Apply** to apply the settings.

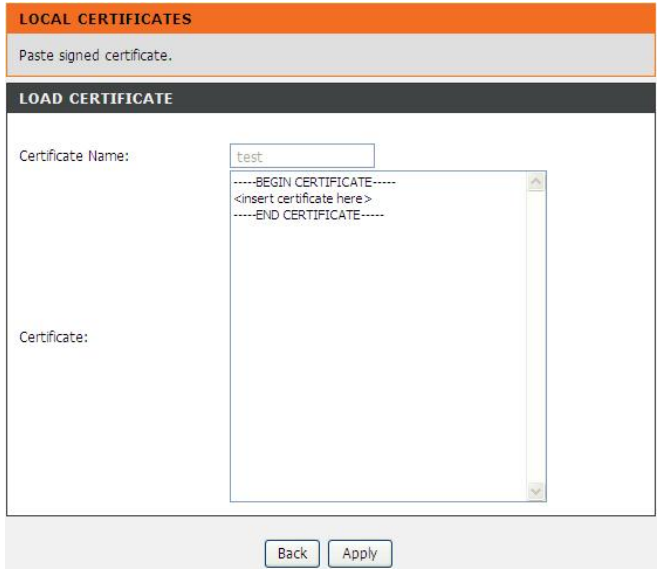
LOCAL CERTIFICATES

The certificate request needs to be submitted to a certificate authority, which will sign the request. Then the signed certificate needs to be loaded to the DSL router.

Click **Load Signed Certificate** to go to next setting.



In **LOAD CERTIFICATE**, paste the signed certificate, and click the **Apply** button. A new certificate is created then.

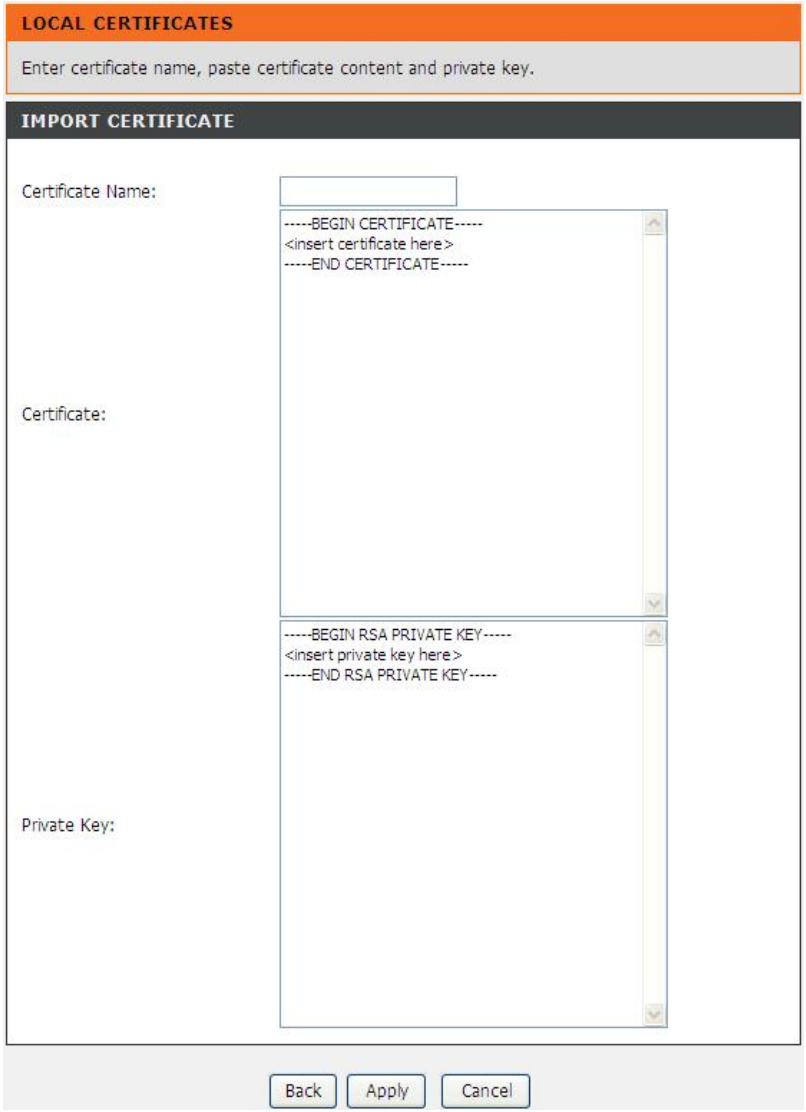


IMPORT CERTIFICATE

To import an existing certificate, click the **Import Certificate.**

Paste the certificate and the private key.

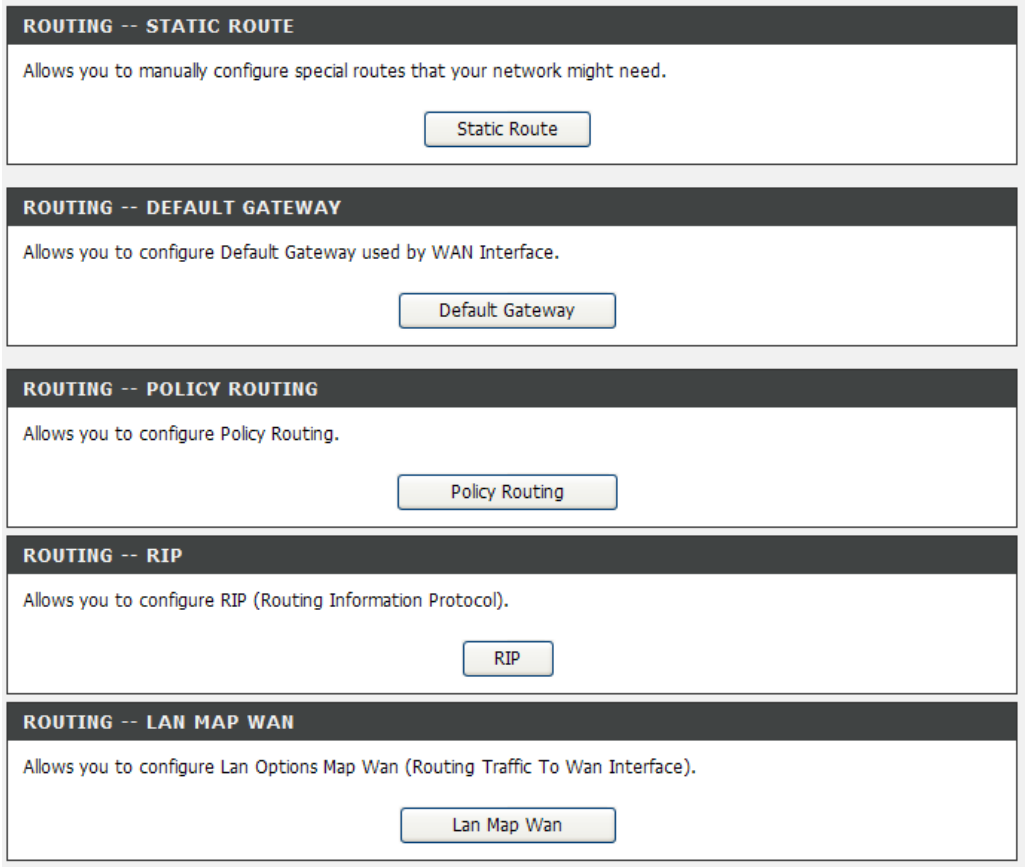
Click the **Apply** button to import the certificate.



ROUTING SETUP

To access the **Routing** setting window, click on the **Routing** button under the **ADVANCED** tab.

Routing Setup is divide into **STATIC ROUTE**, **DEFAULT GATEWAY, POLICY ROUTING**, **RIP** and **LAN MAP WAN.**



STATIC ROUTE

Click the **Add** to set a static routing policy in the list.

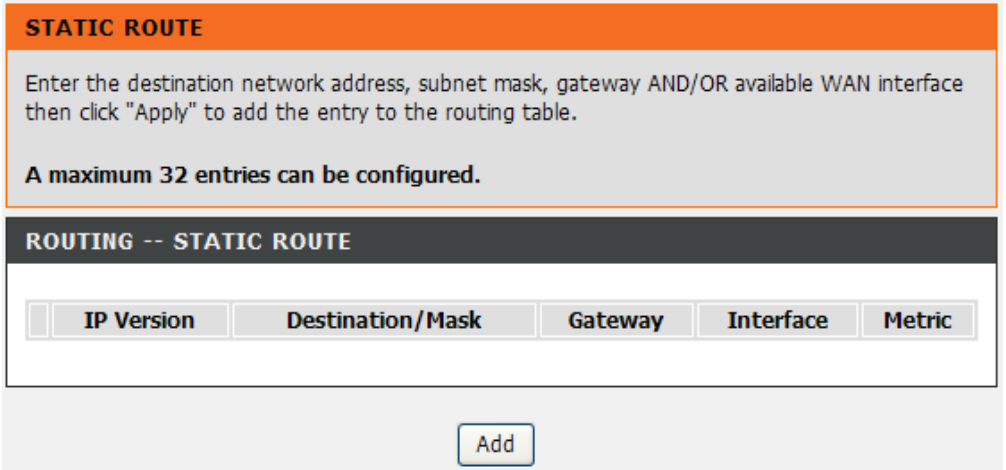
Select **IP Version** to be IPv4 or IPv6.

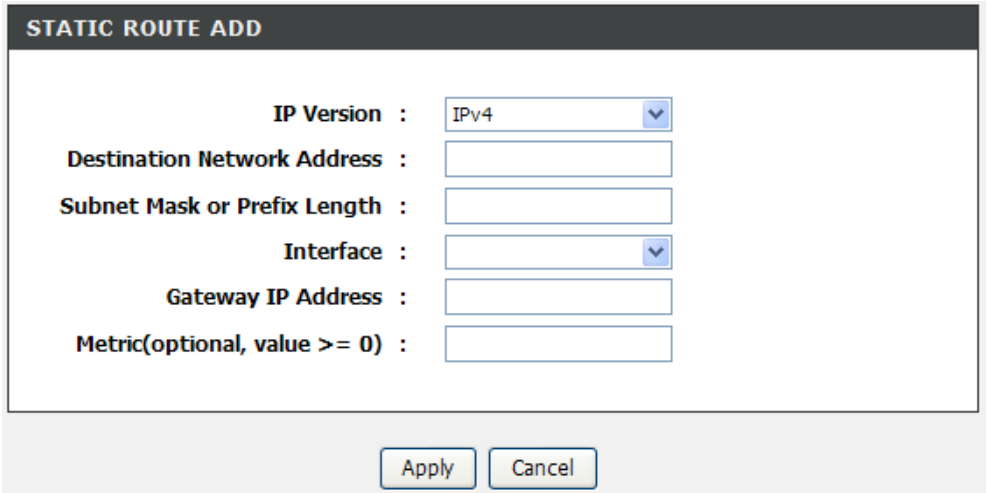
Type the **Destination Network Address** and **Subnet Mask or Prefix Length.**

Select the proper **Interface** or type the Gateway IP Address to be the routing interface.

Enter the metric value of routing in **Metric**

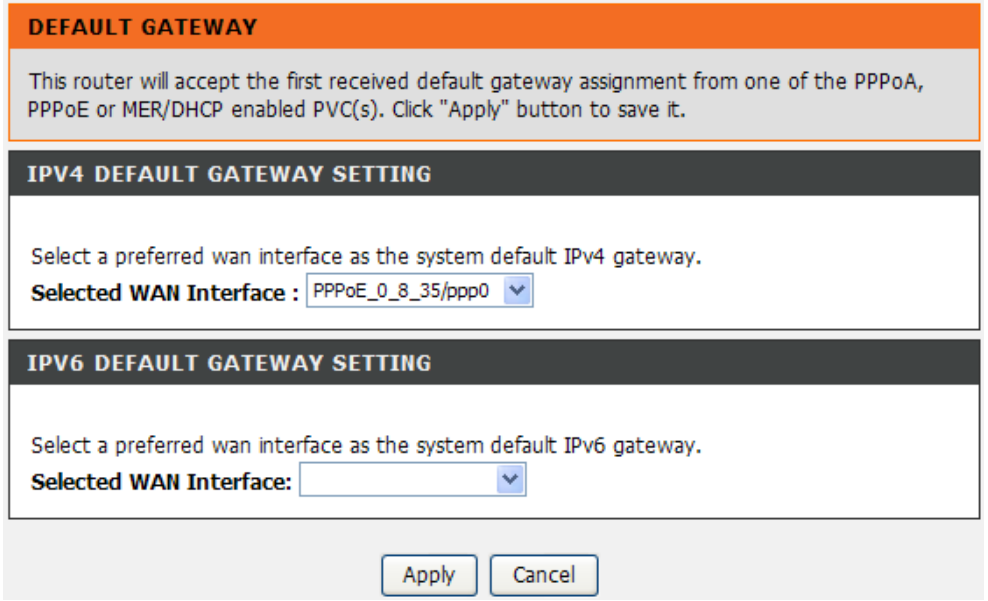
Click the **Apply** the button to save the configuration.





DEFAULT GATEWAY

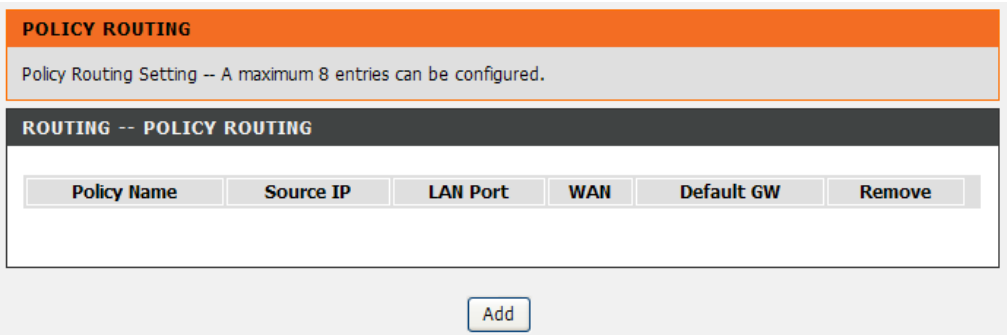
Select the **WAN Interface** as your default gateway. Click **Apply** to save the settings.



POLICY ROUTING`

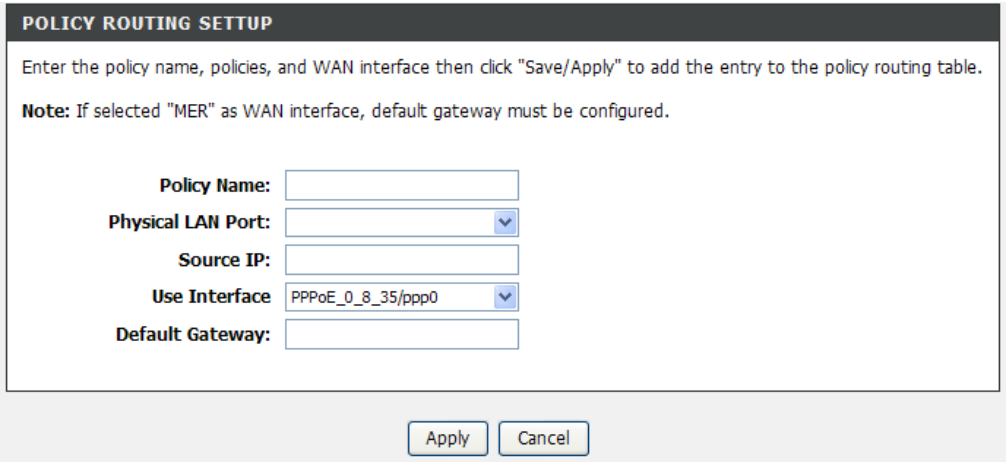
The **POLICY ROUTING** binds one WAN connection and one LAN interface

Click Add to the **POLICY ROUTING SETUP** page.



Enter the **Policy Name, Source IP and Default Gateway,** and select the **Physical LAN Port** and **Use Interface**.

Click **Apply** to save the settings.



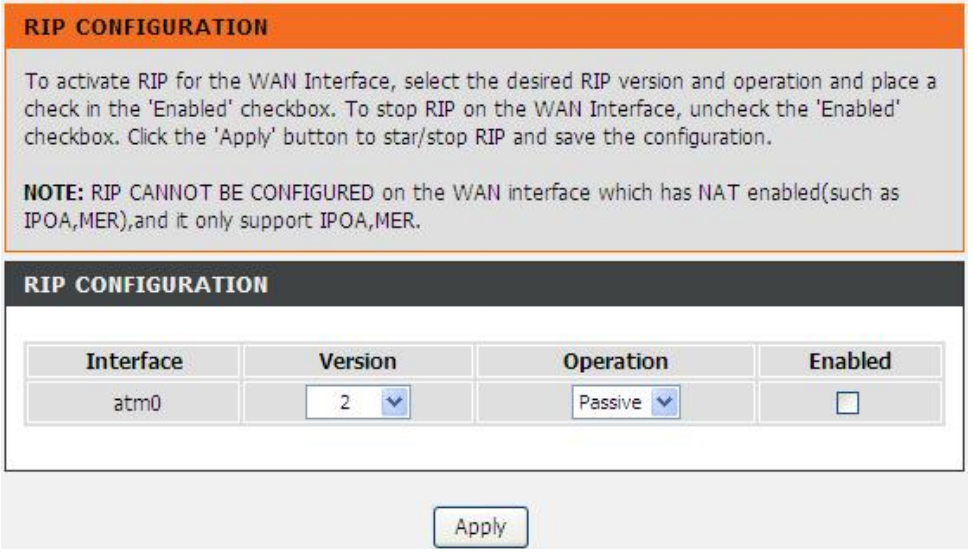
RIP Configuration

In this page, user can select the interfaces on your device that use RIP and the version of the protocol used.

Select the **Version** and **Operation**, and then decide to Enable or not.

RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled and un-ipoe.

Click **Apply** to save the settings.



LAN MAP WAN

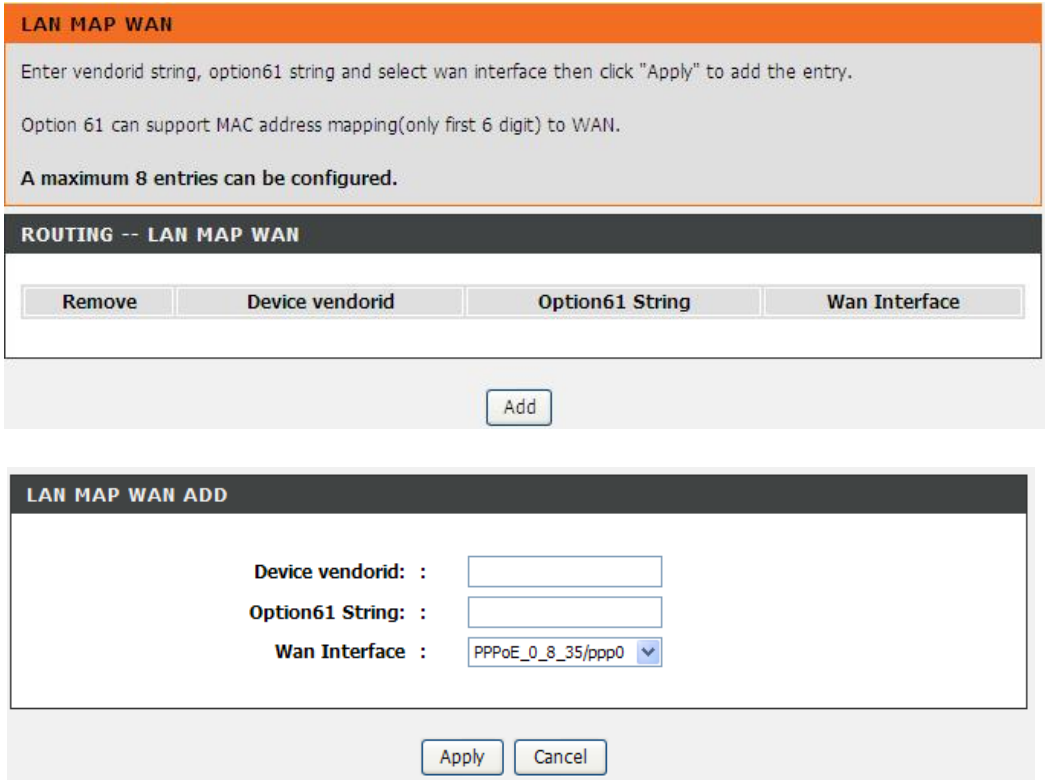
This function can support to get Vendor Class ID (option 60) or support to get first 6 digit MAC address from client device and map it with WAN interface.

We deployed such concept by connecting IP phone on it and let device learn from DHCP request (Option 60 or Option 61), then map it to the correct PVC. Such IP phone can map to the voice PVC (1/33 as our vendor ID mapping configuration) and register at the SIP server. The traffic of the specific IP phone can only pass through the mapped WAN interface and cannot flow to or from other WAN interface.

Click **Add** to start the settings.

Device vendorid: DHCP Option 60 ID, such as MSFT 5.0.
Option61 String: DHCP Option 61 ID, it can support MAC address mapping (only first 6 digits) to WAN, such as 02:10:18.

Click **Apply** to save the settings

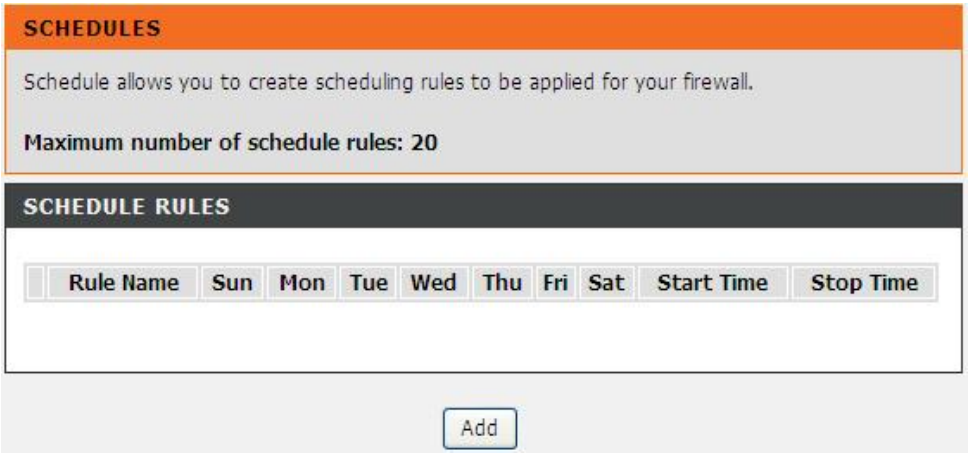


SCHEDULES

SCHEDULES allow you to create scheduling rules to be applied for your firewall. Maximum of 16 entries supported.

To access the **SCHEDULE** window, click on the **Schedules** button under the **ADVANCED** tab.

Press **Add** button to modify your **ADD SCHEDULE RULES** list.



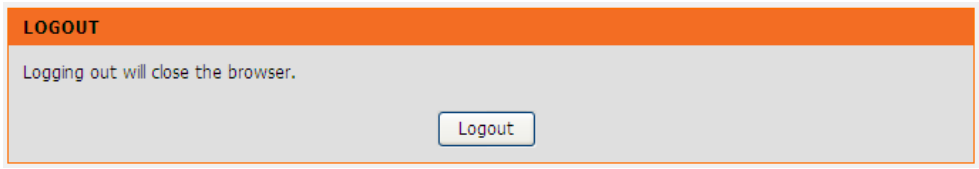
ADD SCHEDULE RULES

Type **Name** of this rule.

Select **Day(s)** or **ALL Day-24hrs** to active your firewall and type **Start Time** to **End Time**.

LOGOUT

Click **Logout** to log out of the configuration page.



MAINTENANCE

Click on the **MAINTENANCE** tab to reveal the window buttons for various functions located in this directory.

SYSTEM

To access the **SYSTEM** setting window, click on the **System** button under the **MAINTENANCE** tab

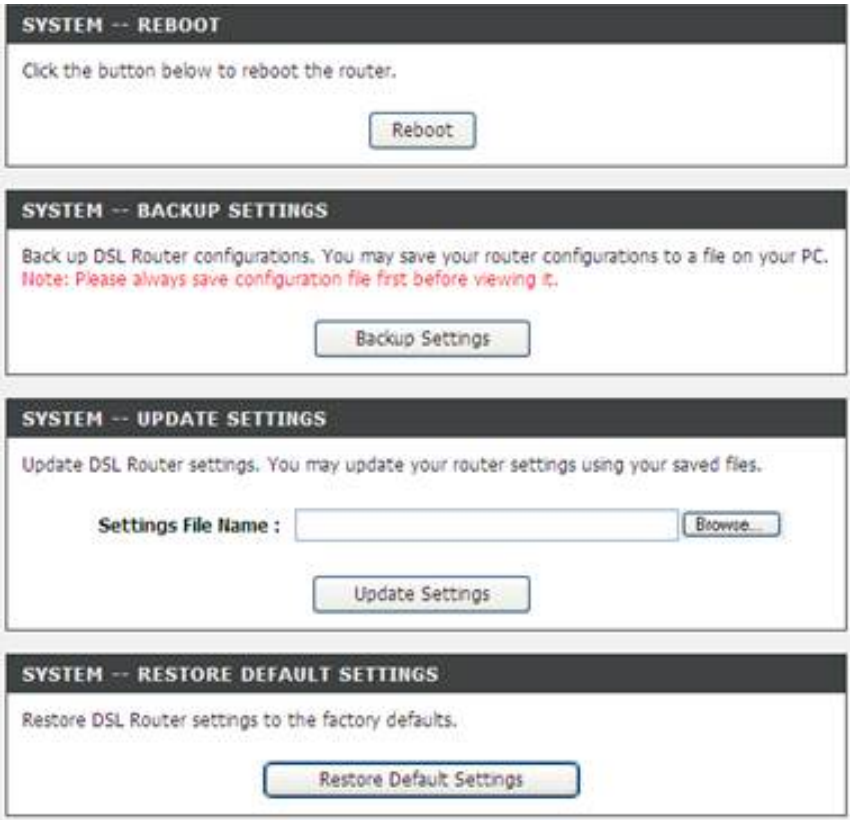
REBOOT: click **Reboot** button to reboot the router

BACKUP SETTINGS: click **Backup Settings** button to backup now setting of router.

UPDATE SETTINGS: click **Update Settings** and select a *.conf file which pre backup setting

RESTORE DEFAULT SETTING: If necessary, please click the **Restore Default Setting** button to have the default settings.

Note: Do not turn off your device or press the **Reset** button while an operation in this page is in progress.



FIRMWARE UPDATE

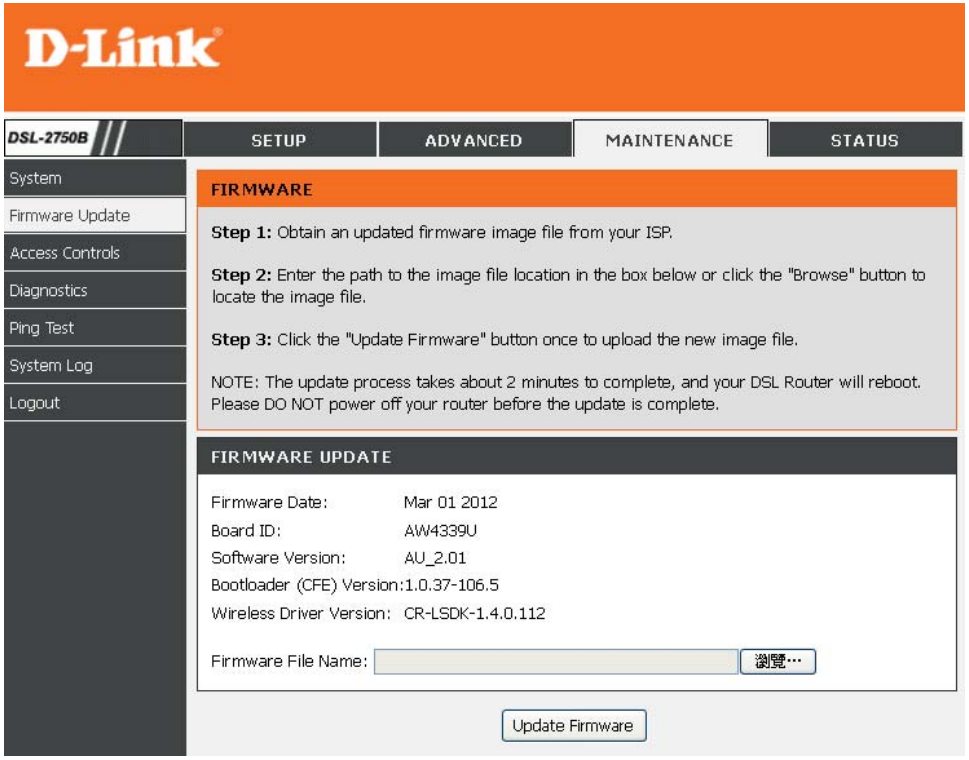
Use the **FIRMWARE UPGRADE** window to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you first save the configuration settings with the **SAVE/RESTORE SETTINGS** window described above.

To access the **FIRMWARE UPGRADE** setting window, click on the **Firmware Update** button under the **MAINTENANCE** tab.

FIRMWARE UPDATE

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

Note: Do not turn of f your device or press the reset button while this procedure is in progress.



ACCESS CONTROLS

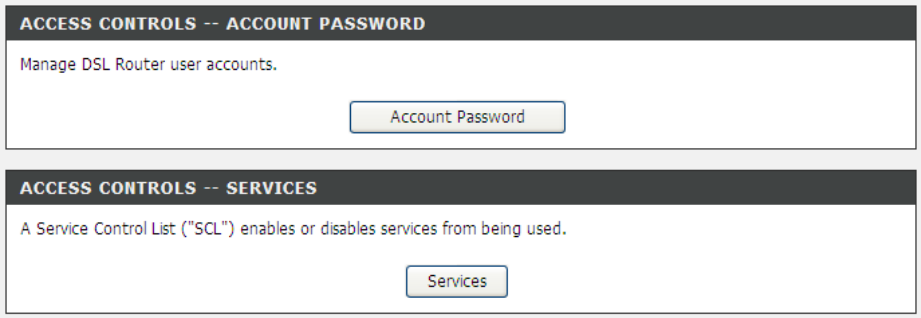
To access the **ACCESS CONTROL** setting window, click on the **Access Control** button in the **MAINTENANCE** directory.

ACCOUNT PASSWORD

Manage DSL Router user accounts, click **Account Password** button to set up.

SERVICES

A Service Control Lis t ("SCL") enables or disables services from being used. Click **Services** button to access **Services** page.



ACCOUNT PASSWORD

The Admin option is used to set a password for access to the Web-based management.

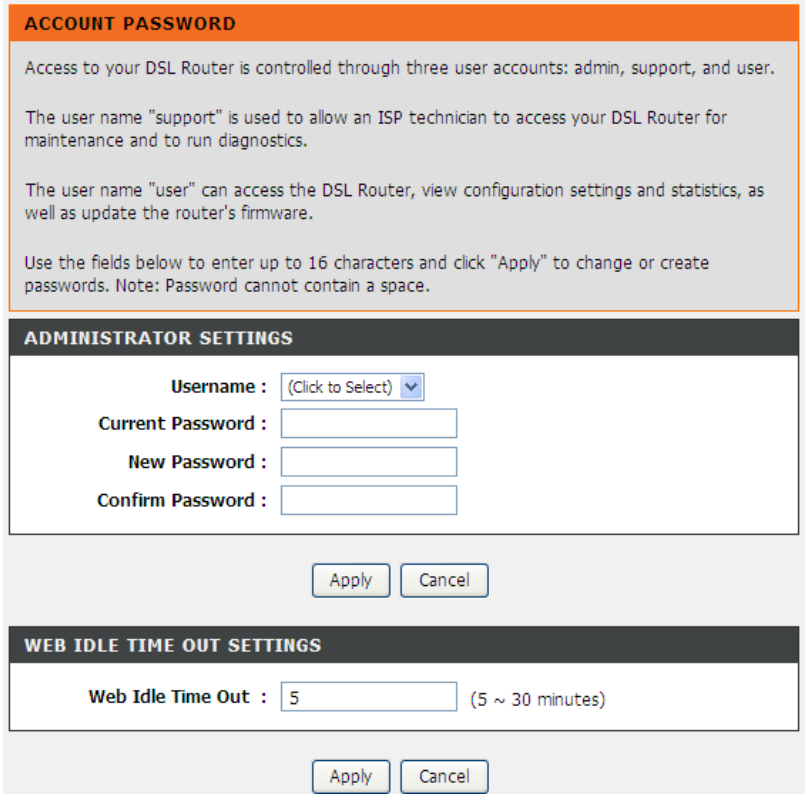
ADMINISTRATION SETTINGS

Select the **Username** from the drop-down list. You can select **admin**, **support**, or **user**. Enter the **Current Password** and **New Password** and confirm the new password, to change the password.

Click **Apply** to apply the settings.

WEB IDLE TIME OUT SETTINGS

Allows an ISP technician to access your DSL Router for maintenance and to run diagnostics.



SERVICES

Select **IPv4** or **IPv6** from the **SELECT IP VERSION** drop list.

LOCAL ACCESS CONTROL – SERVICES

Enable or disable the services that are used by the local host. For example, if telnet service is enabled and port is 23, the remote host can access the device by telnet through port 23. Normally, you need not change the settings.

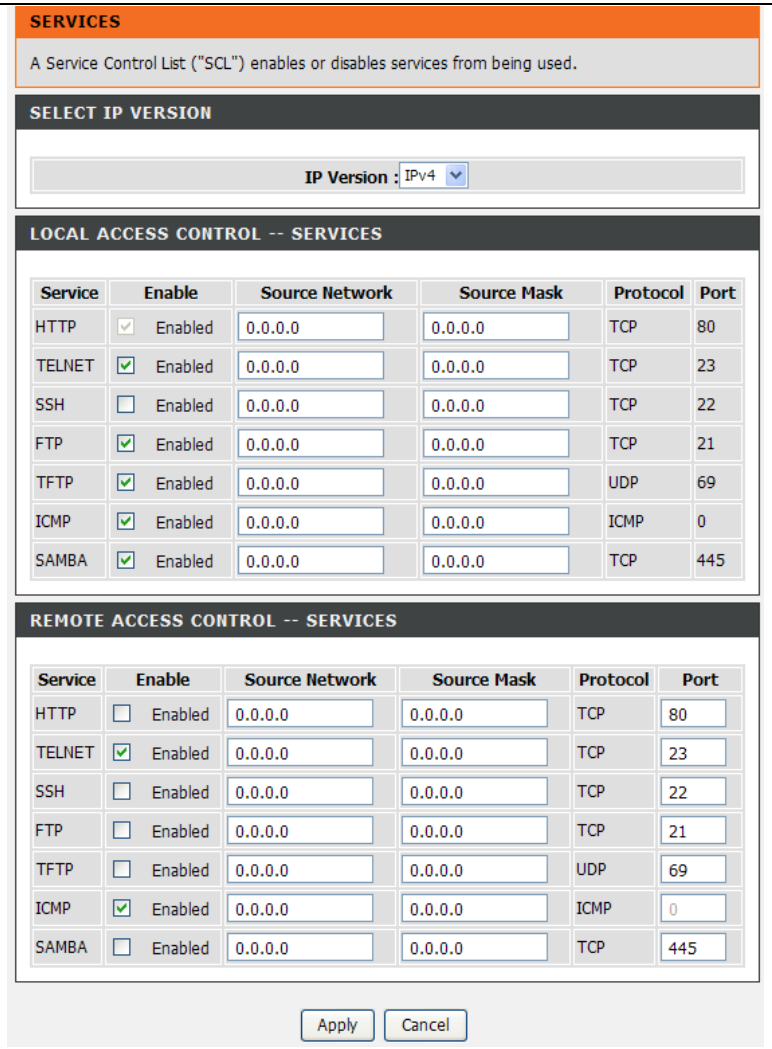
Select the management services that you want to enable or disable on the LAN or WAN interface.

REMOTE ACCESS CONTROL -- SERVICES

Allows access to the router via HTTP, TELNET, SSH, FTP, TFTP, ICMP, and SAMBA.

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

Note: If you disable the HTTP service, you cannot access the configuration page of the device any more.

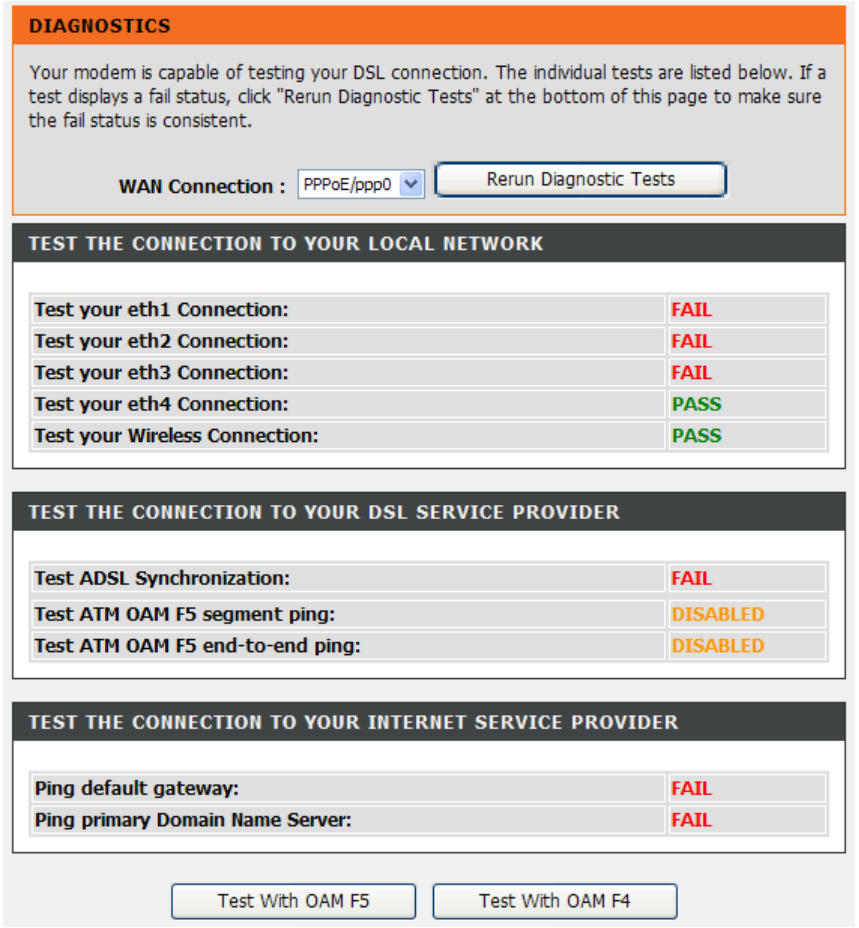


DIAGNOSTICS

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

To access the **Diagnostics** setting window, click on the **Diagnostics** button under the **MAINTENANCE** tab.

WAN Connection
Select a WAN interface and click **Rerun Diagnostics Tests**.



SYSTEM LOG

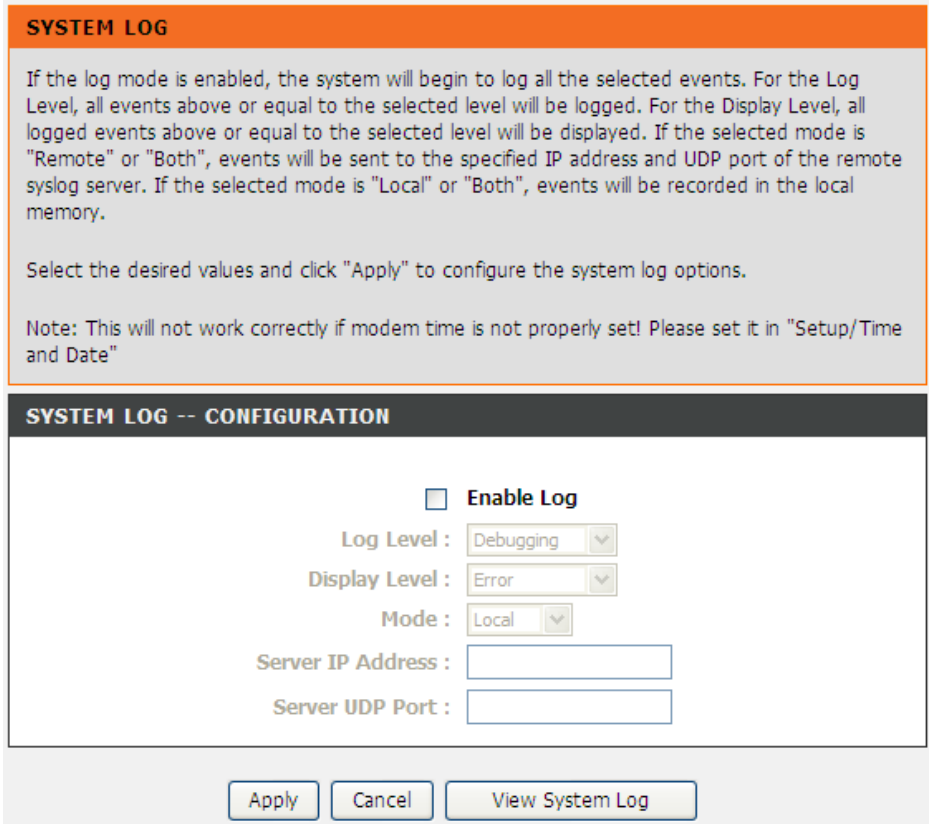
The System Log allows you to configure local, remote and email logging, and to view the logs that have been created.

To access the **SYSTEM LOG** setting window, click on the **System Log** button under the **MAINTENANCE** tab.

You can click **View System Log** button to view the system log if you enabled **Log**.

Select **Enable** and then set **Log Level**, **Display Level** and **Mode**.

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.



STATUS

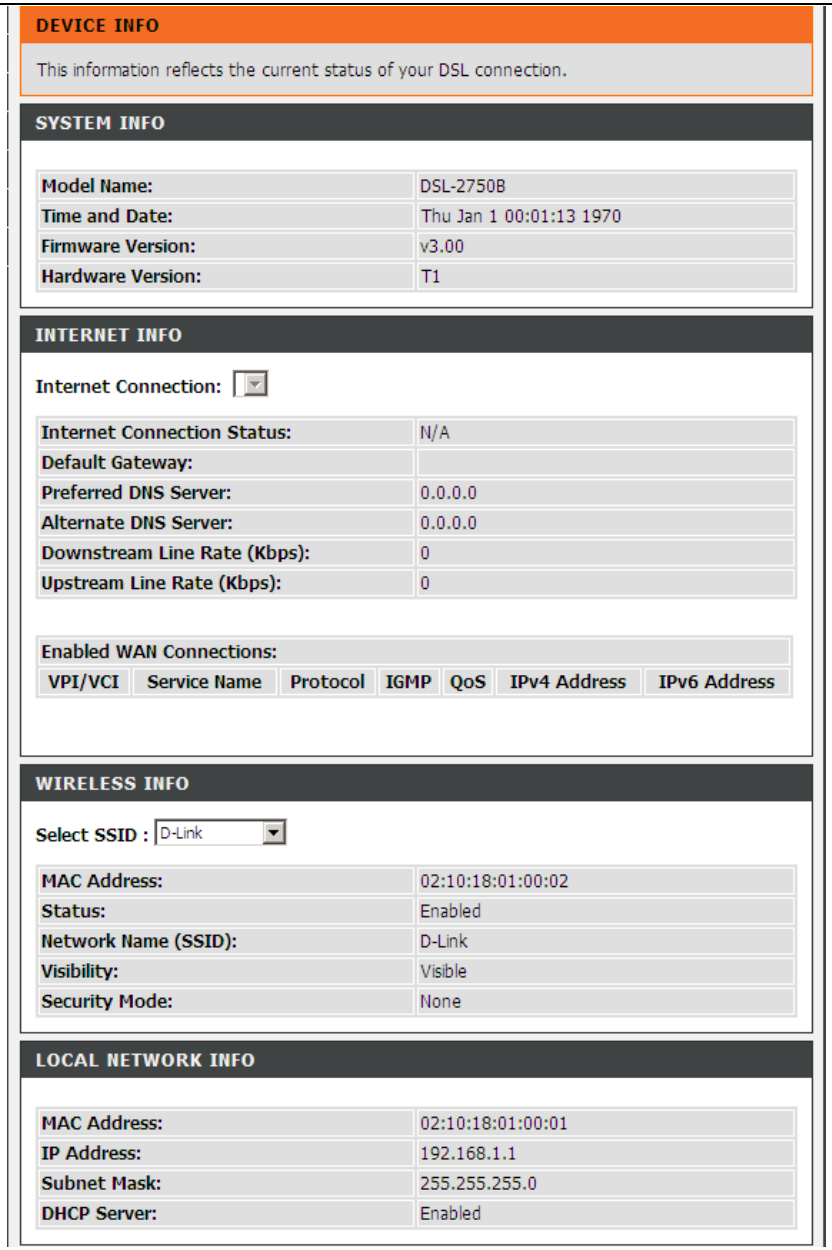
Click on the **STATUS** tab to reveal the window buttons for various functions located in this directory. The **DEVICE STATUS** window is the first item in the **STATUS** directory. Use these windows to view system information and monitor performance.

DEVICE INFO

The **Device Info** page displays a summary overview of your router status, including: Device software version and summary of your Internet configuration (both wireless and Ethernet status).

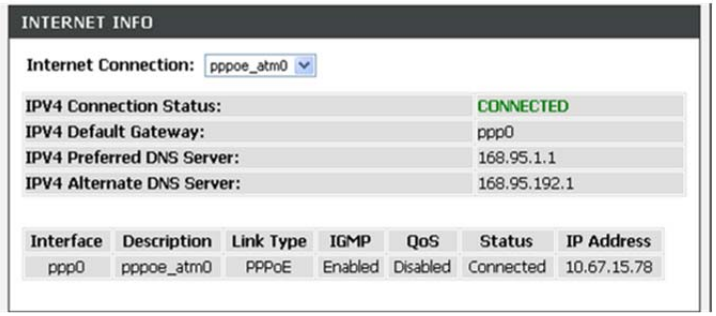
To access the **DEVICE INFO** setting window, click on the **Device Info** button in the **STATUS** tab.

This window displays current summary of **SYSTEM INFO**, **INTERNET INFO**, **WIRELESS INFO** and **LOCAL NETWORK INFO**.

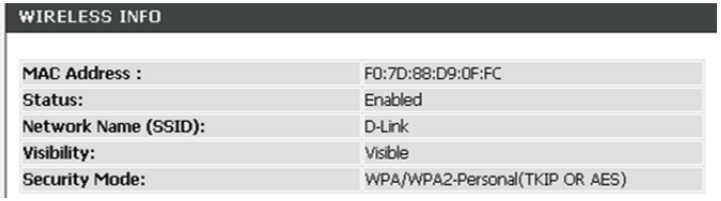


SYSTEM INFO
This window displays system information include Model Name, Time and Date, Firmware Version, Release Date.

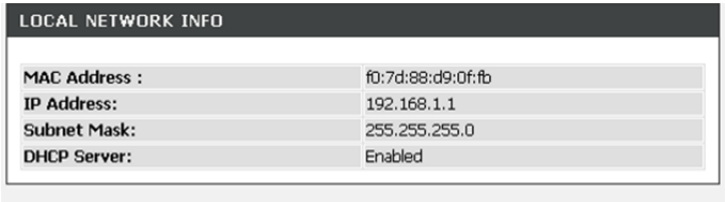
INTERNET INFO
This window displays WAN information including IP address, Mask, Default Gateway, Primary/Secondary DNS Server.



WIRELESS INFO
This window displays authenticated wireless stations and their status.



LOCAL NETWORK INFO
This window displays LAN information including MAC, IP address, Mask, and DHCP Server.

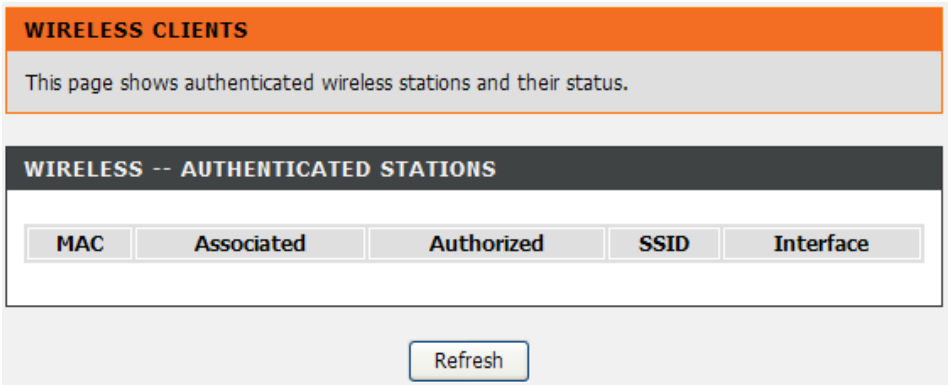


WIRELESS CLIENTS

This feature shows all the currently connected wireless and LAN computers or PCs.

To access the Wireless clients setting window, click on the **Wireless Clients** button in the **STATUS** tab.

WIRELESS – AUTHENTICATED STATIONS
This window displays authenticated wireless stations and their status.



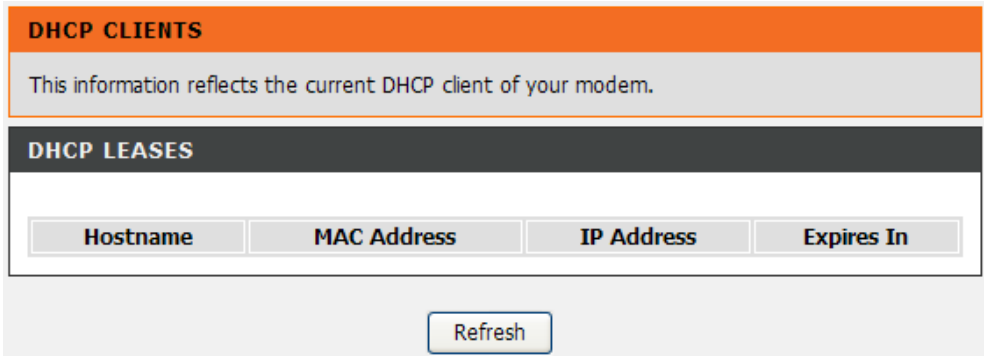
DHCP CLIENT

This feature shows all the currently connected LAN computers or PCs.

To access the DHCP clients setting window, click on the **DHCP Clients** button in the **STATUS** tab.

DHCP CLIENTS

This window displays all the entities which link to the LAN interface successfully.



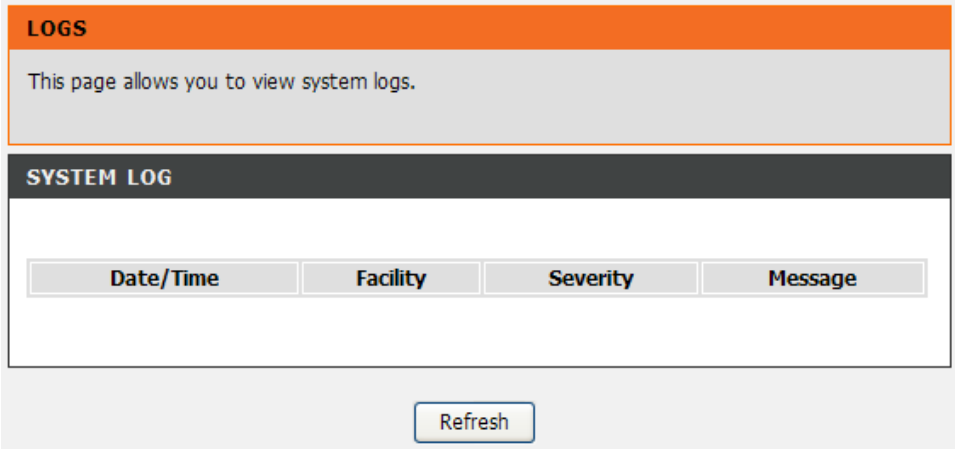
LOGS

This feature shows all the system logs.

To access the **LOGS** window, click on the Logs button in the **STATUS** tab.

LOGS

This window displays all the Logs. Click **Refresh** button to update new log.



STATISTICS

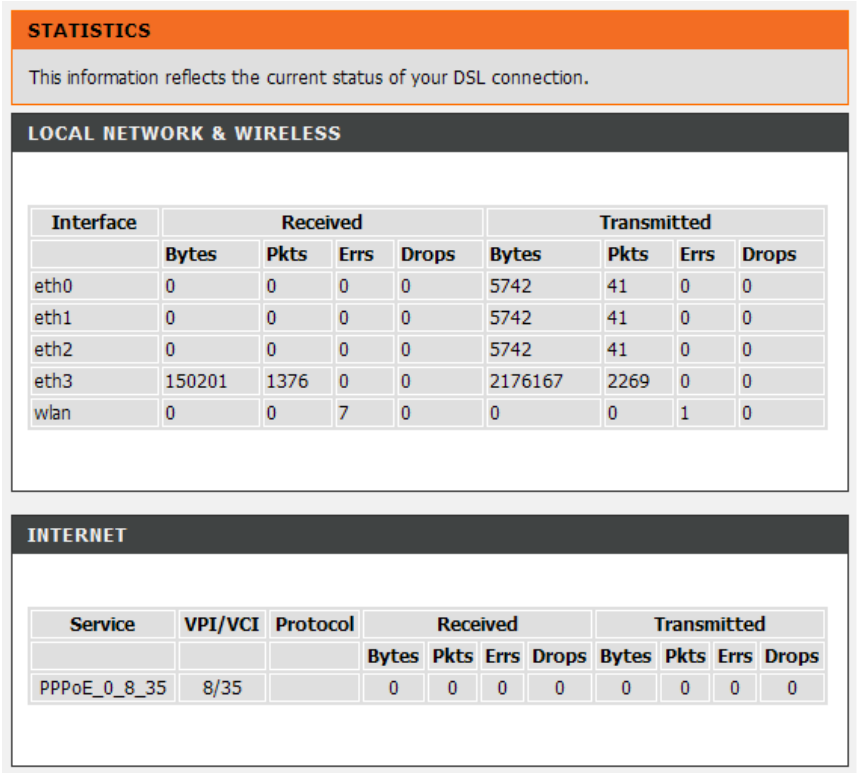
This information reflects the current status of your router. To access the **STATISICS** window, click on the **Statistics** button in the **STATUS** tab.

LOCAL NETWORK & WIRELESS

This window displays all the **Received** and **Transmitted** packet status on the LAN interface.

INTERNET

This window displays all the **Received** and **Transmitted** packet status on the WAN interface.



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	0	0	0	0	5742	41	0	0
eth1	0	0	0	0	5742	41	0	0
eth2	0	0	0	0	5742	41	0	0
eth3	150201	1376	0	0	2176167	2269	0	0
wlan	0	0	7	0	0	0	1	0

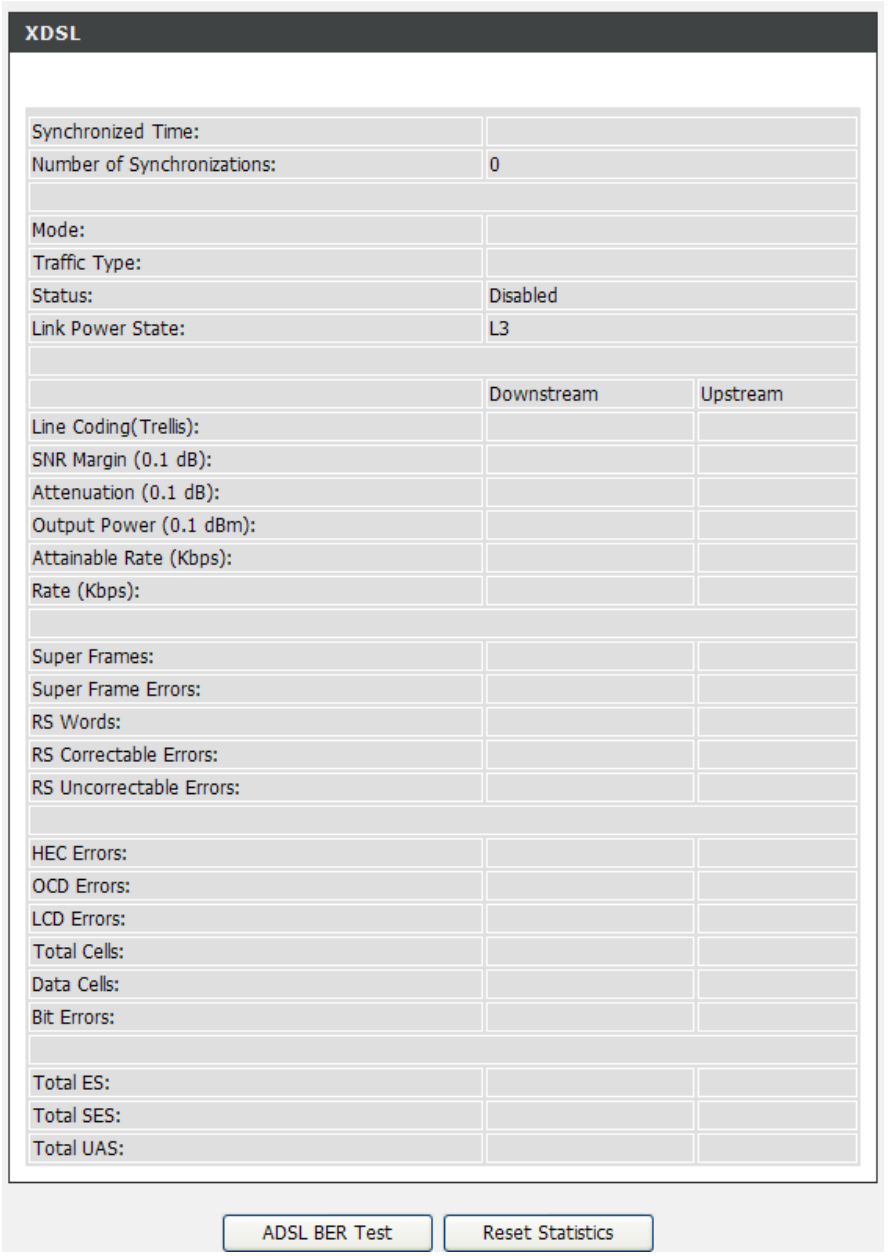
INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
PPPoE_0_8_35	8/35		0	0	0	0	0	0	0	0

xDSL

This window displays all the **ADSL status**

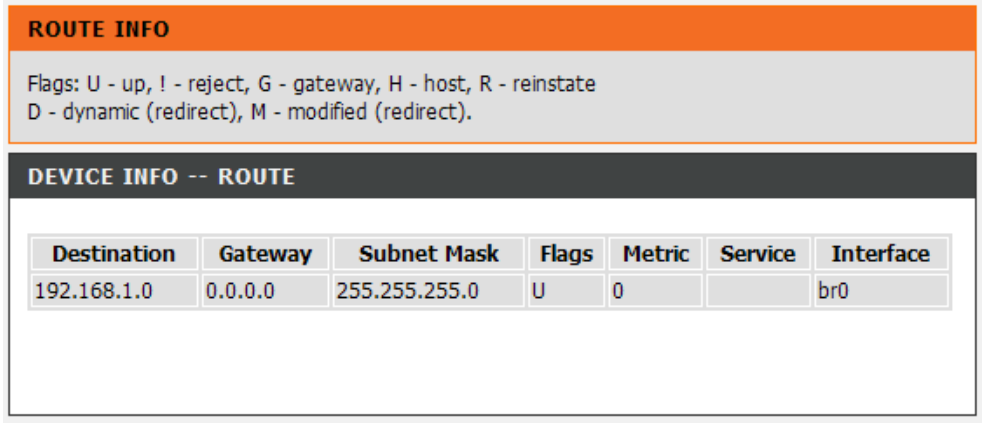
You can click the **ADSL BER Test** button to test the ADSL connection or to click the **Reset Statistics** button to set all statistics to recount.



ROUTE INFO

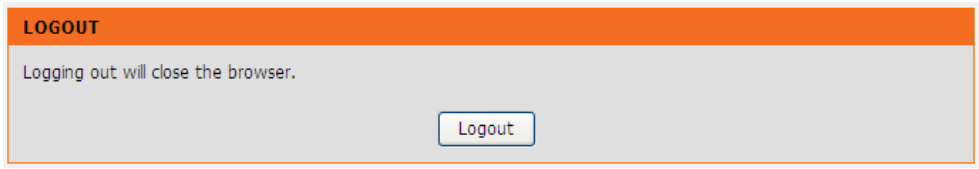
To access the **ROUTE INFO** setting window, click on the **ROUTE INFO** button under the **STATUS** tab.

The **ROUTE INFO** section displays route information showing the IP addresses of the destination, gateway, and subnet mask as well as other route information



LOGOUT

Click **Logout** to log out of the configuration page.



TROUBLESHOOTING

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-2750B. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 6.0 or higher
  - Firefox 1.5 or higher

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

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

- Configure your Internet settings:
  - Go to **Start > Settings > Control Panel**. Double-click on the **Internet Options** Icon. From the **Security** tab, click on the button to restore the settings to their defaults.
  - Click on the **Connection** tab and set the dial-up option to Never Dial a Connection. Click on the LAN Settings button. Make sure nothing is checked. Click on the **OK**.
  - Go to the **Advanced** tab and click on the button to restore these settings to their defaults. Click on the **OK** button three times.
  - Close your web browser (if open) and open it.

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

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

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

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

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process.

Wait about 30 seconds to access the router. The default IP address is 192.168.1.1. When logging in, type in the default User Name “admin,” and the default Password “admin” then click on the OK button to access the web-based manager.

APPENDIX

WIRELESS BASICS

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

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

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

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

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

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

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

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

Wireless Personal Area Network (WPAN)
Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away. Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

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

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

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

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

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

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

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

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

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

NETWORKING BASICS

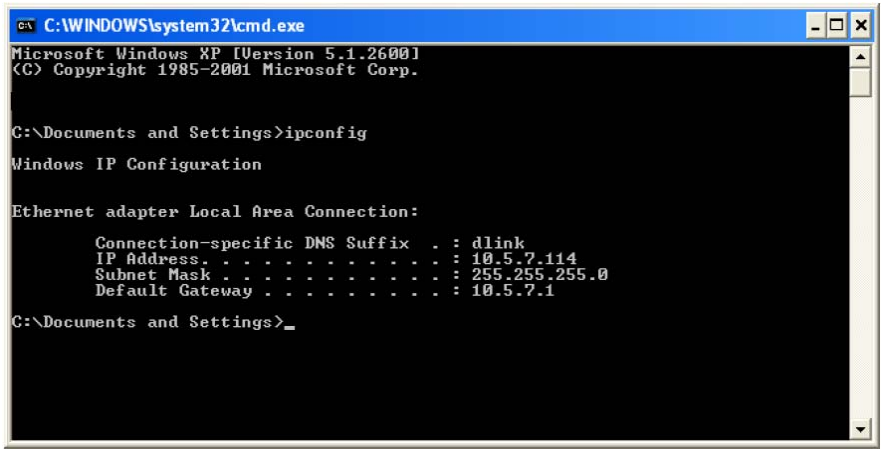
Check your IP address

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

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

Statically Assign an IP address

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

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

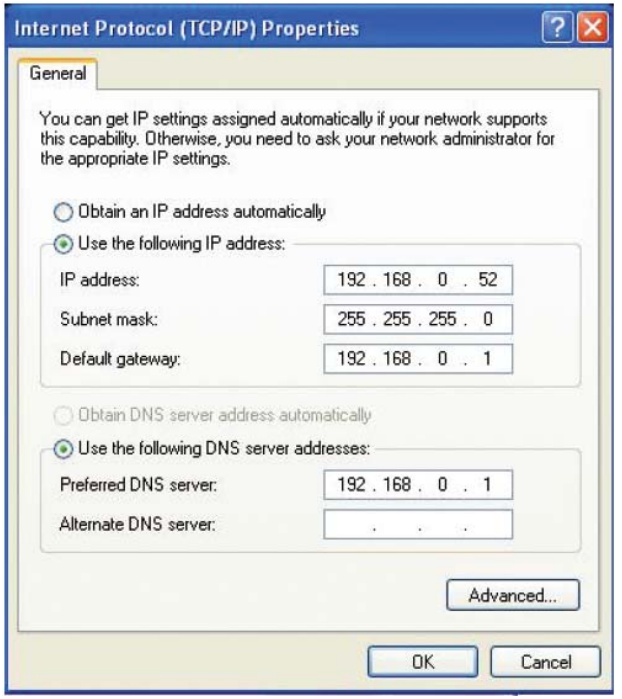
Step 2
Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.

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

Step 4
Click on the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.
Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

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

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



FCC CAUTION

Statement：

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Class B:

FEDERAL COMMUNICATIONS COMMISSION INTERFERENCE STATEMENT This equipment has been tested and found to comply with the limits for a Class B digital dev ice, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable prot ection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However , there is no guarante e that interference will not occur in a Particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment of f and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.

-Increase the separation between the equipment and receiver.

-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/ TV technician for help.

CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

CONTACTING TECHNICAL SUPPORT

You can find software updates and user documentation on the D-Link websites.

If you require product support, we encourage you to browse our FAQ section on the Support Web Site before contacting the Support line.

We have many FAQ's which we hope will provide you a speedy resolution for your problem.

For Customers within Australia:

Tel: 1300-766-868

24/7 Technical Support

Web: http://www.dlink.com.au

E-mail: support@dlink.com.au

For Customers within New Zealand:

Tel: 0800-900-900

24/7 Technical Support

Web: http://www.dlink.co.nz

E-mail: support@dlink.co.nz

D-Link SharePort™

Introduction

The D-Link SharePort™ allows you to share USB devices such as external storage drives and multifunction printers with other users across your network by simply connecting the device to select D-Link routers. This allows you to use an external storage drive or printer located across your network as if it were connected to your local PC.

System Requirements

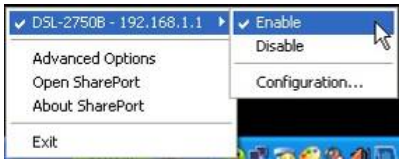
- Windows
- 2000 / 2003 / XP / Vista / 7 32-bit / 64-bit
- Pentium 3 800MHz or better
- 256MB RAM or higher
- CD-ROM drive
- A compatible D-Link router

Installation

1. Insert the CD-ROM into your computer.
2. Follow the on-screen instructions.
3. The  icon should appear in the System Tray at the lower-right corner on the desktop.

Set up the D-Link Router

1. Connect the D-Link Router to the network.
2. Power on the D-Link Router.
3. Double-click on the icon to open the D-Link SharePort.
4. Right-click on in the System Tray at the lower-right corner on your Windows Desktop. A window pops up to display the D-Link Router.



Enable Network USB on the D-Link Router

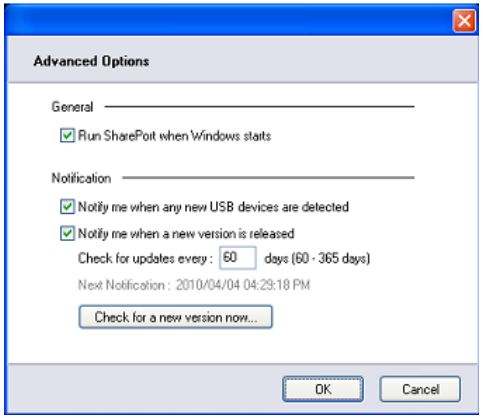
1. Click on the D-Link Router.
2. Click on **Enable**.
3. The icon in the Windows System Tray should change to a icon.

Connect USB Devices to the D-Link Router

The D-Link SharePort automatically detects for each connected USB device. A window will pop up for each detected USB device.

1. Right-click on the  icon.
2. Click on Open SharePort.
3. The D-Link SharePort displays the connected USB devices on the network.

4. Advanced Options can be set by clicking on Advanced Options.

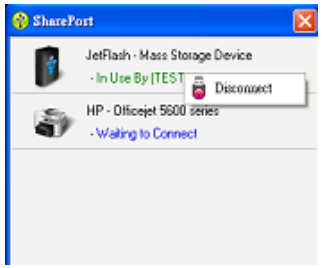


● Virtually Connect and Disconnect a USB Device

1. Move the cursor to Waiting to Connect and click on **Connect** to virtually connect a USB device.

2. The D-Link SharePort displays which user is virtually connecting this USB device.

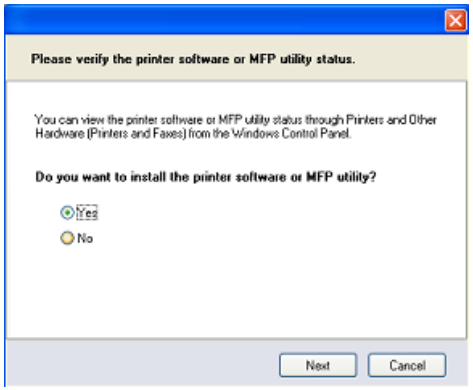
3. Move the cursor to In Use By (Owner) and click on **Disconnect** to virtually disconnect the USB device.



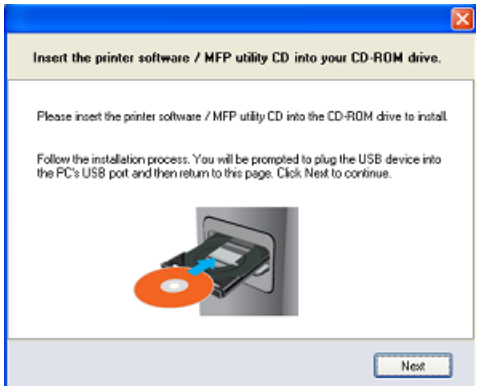
● When the USB Device is a Multifunction Printer

1. Move the cursor to Waiting to Connect and click on **Manage Device**.

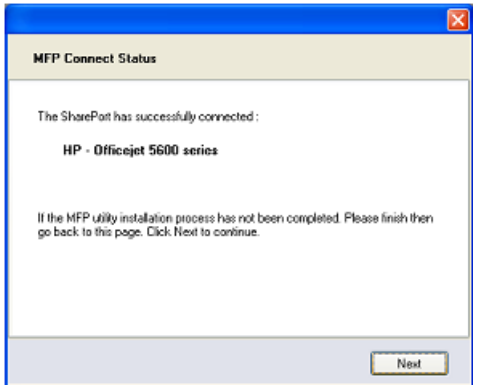
2. Click **Yes** on the question “Do you want to install the printer software or MFP utility?”



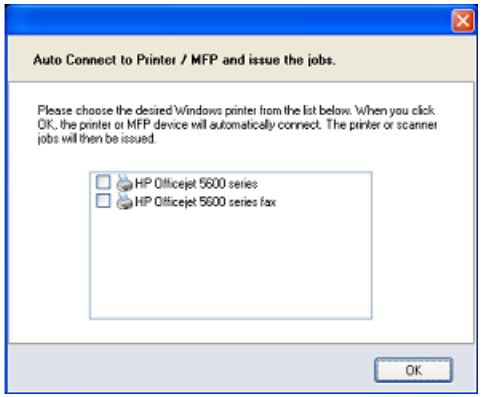
3. Insert the CD-ROM of the multifunction printer and follow the instructions to install the multifunction printer’s driver. When the installation process prompts you to connect the multifunction printer to your PC, click **Next**.



4. The D-Link SharePort virtually connects to this multifunction printer. Click **Next**



5. Choose the printer driver that you want D-Link SharePort to auto-connect when you print.



When You Want to Scan

1. Move the cursor to Available for Use and click on **Scan** Now.

TECHNICAL SPECIFICATIONS

ADSL Standards

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

ADSL2 Standards

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

ADSL2+ Standards

- ITU G.992.5 Annex A

Protocols

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

Data Transfer Rate

ADSL

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

ADSL2

- G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 1 Mbps

ADSL 2+

- Full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps

Media Interface

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

WIRELESS LAN

- 802.11b/g/n standards
- Wireless speed: up to 300Mbps (802.11n)
- Frequency range: 2.4 GHz to 2.484G Hz
- Antennas: 2 non-detachable dipole antennas.
- WEP data encryption
- WPA/WPA2 (Wi-Fi Protected Access) security
- Multiple SSID
- 802.11e Wireless QoS (WMM/WME)
- MAC address-based access control