USER MANUAL
DSL-2640B

VERSION 1.0

D-Link® | **BROADBAND**

Table of Contents

Package Contents

- DSL-2640B Wireless N 150 ADSL2+ Router
- One non-detachable Antenna
- Power Adapter
- CD-ROM with User Manual and router firmware
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- One Quick Installation Guide

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

System Requirements

- ADSL Internet service
- Computer with:
    - 200MHz Processor
    - 64MB Memory
    - CD-ROM Drive
    - Ethernet Adapter with TCP/IP Protocol Installed
    - Windows win7/vista/XP/2000
    - MAC OS
    - Internet Explorer v6 or later, FireFox v1.5

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-2640B ADSL2+ router is a versatile, high-performance remote router for home and the small office. With integrated ADSL2/2+ supporting up to 24Mbps download speed, firewall protection, Quality of Service (QoS), 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.
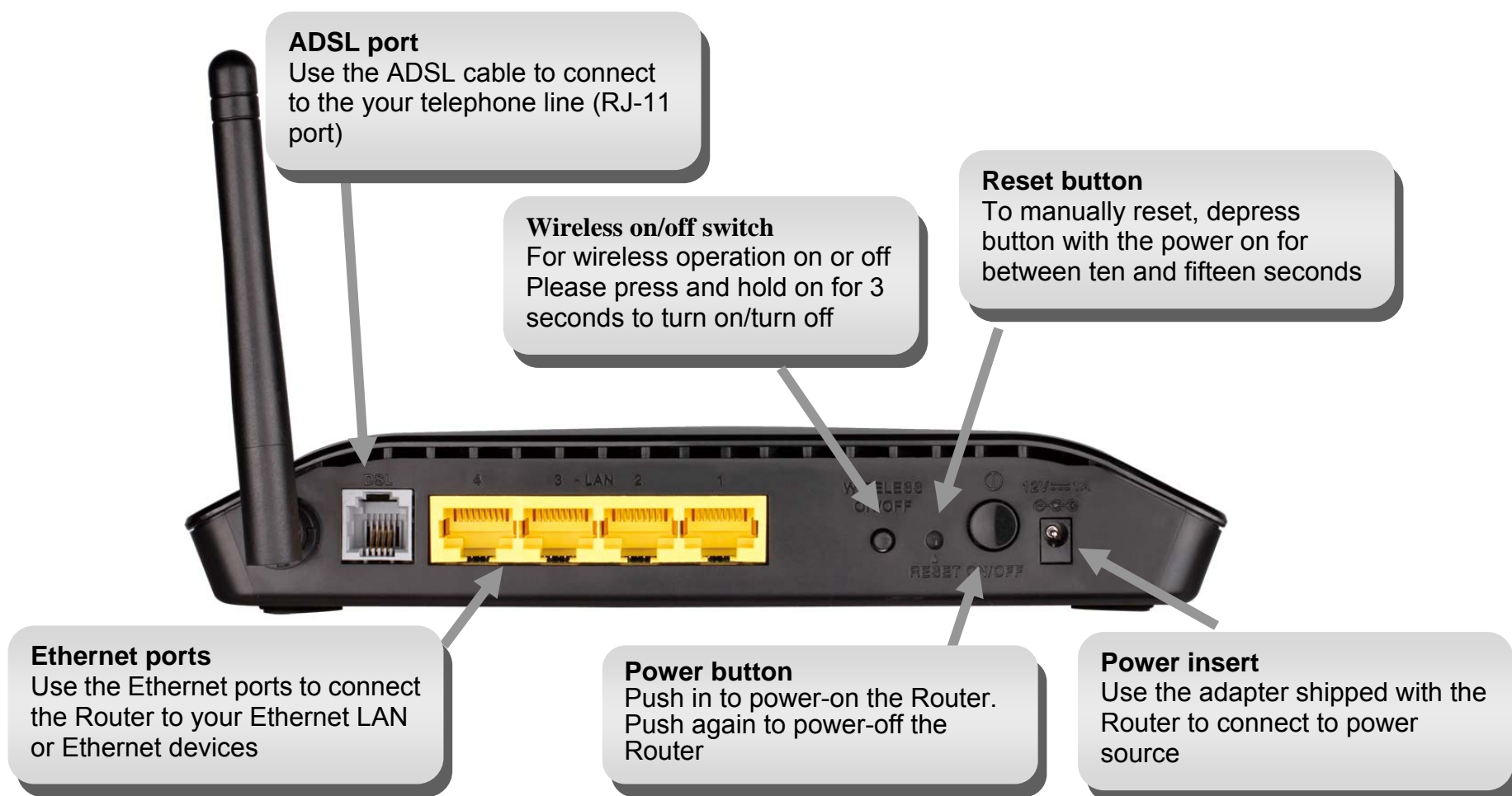
*Maximum wireless signal rate derived from IEEE standard 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Features

- **Faster Wireless Networking** - The DSL-2640B provides up to 150Mbps* 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-2640B 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-2640B 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.992.5 standard. (For ADSL2+)

- **Full Network Management** - The web-based management and text-based network management via Telnet connection.

- **Easy Installation** - The DSL-2640B uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.
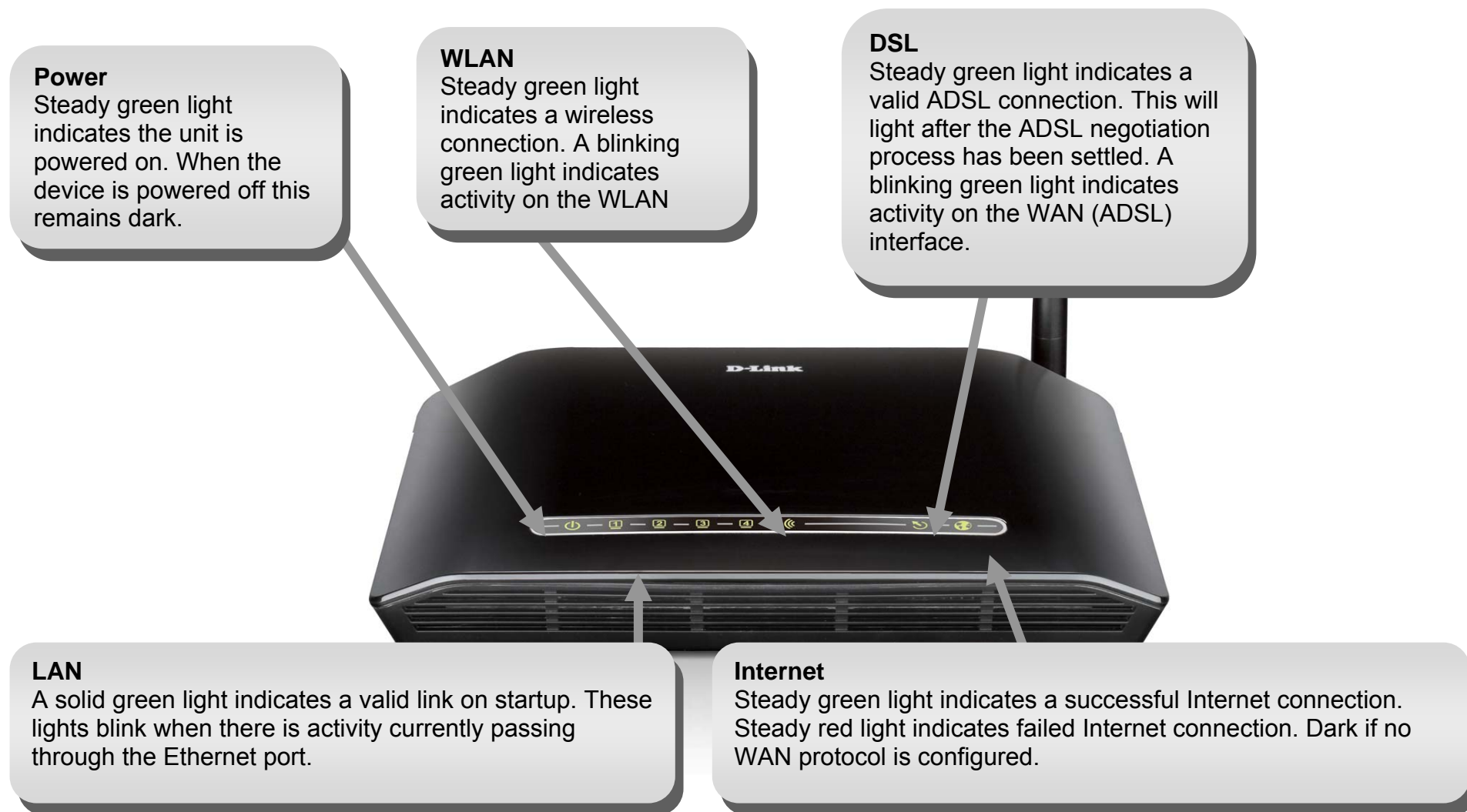
Hardware Overview

Connections

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

Reset button
To manually reset, depress button with the power on for between ten and fifteen seconds

Wireless on/off switch
For wireless operation on or off Please press and hold on for 3 seconds to turn on/turn off

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

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

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

Hardware Overview
LEDs

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

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

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

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

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

Installation

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

Before you Begin

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

Installation Notes

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

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

Operating Systems
The DSL-2640B uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, and Windows XP.

Web Browser
Any common web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Opera, Microsoft Internet Explorer® version 6.0, Mozilla Firefox 3.5, 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-2640B through the wireless interface.

Security for wireless communication can be accomplished in a number of ways. The DSL-2640B supports WPA (Wi-Fi Protected Access), WPA2, and mixed WPA/WPA2. Wireless access can also be controlled by selecting MAC addresses that are allowed to associate with the device. Please read the section on Wireless Configuration.

Additional Software

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

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

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

Information you will need from your ADSL service provider

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

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

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

- PPPoE/PPoA (PPPoE LLC, PPPoA LLC or PPPoE Vc-Mux, PPPoA VC-Mux)

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

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

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

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

Information you will need about DSL-2640B

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

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

LAN IP addresses for the DSL-2640B
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-2640B
This is the subnet mask used by the DSL-2640B, 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-2640B to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-2640B to connect to other computer or Ethernet devices.

DHCP Client status
Your DSL-2640B ADSL Router is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-2640B 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 collection 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-2640B Wireless ADSL Router.

Wireless Installation Considerations

DSL-2640B lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

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

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

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

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

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

Device Installation

The DSL-2640B Wireless ADSL Router maintains three separate interfaces, an Ethernet LAN, a wireless LAN and an ADSL Internet (WAN) connection. Carefully consider the Router's location suitable for connectivity for your Ethernet and wireless devices. You must have a functioning broadband connection via a bridge device such as a Cable or ADSL modem in order to use the Router's WAN function.

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

Power on Router

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

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

Factory Reset Button

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

1. Press and hold the reset button while the device is powered off.

2. Turn on the power.

3. Wait for 10~15 seconds and then release the reset button.

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

Network Connections

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

Connect Router to Ethernet
The Router may be connected to a single computer or Ethernet device through the 10/100BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds higher than 10/100Mbps, 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 auto adapting (MDI/MDI-X). 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 any port (MDI or MDI-X) on an Ethernet
hub or switch with a straight-through cable as shown in this
diagram.
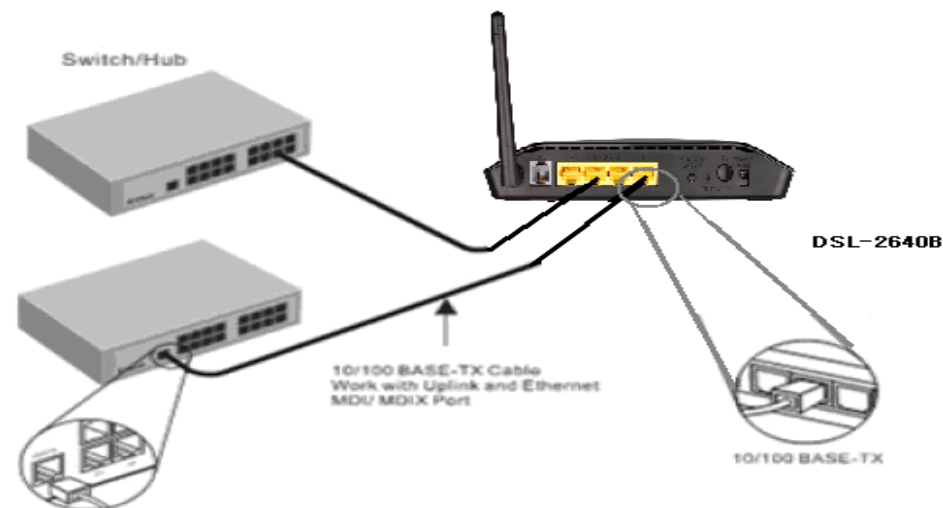
Computer to Router Connection
You can connect the Router directly to a 10/100BASE-TX
Ethernet adapter card (NIC) installed on a PC using the
Ethernet cable provided as shown in this diagram.
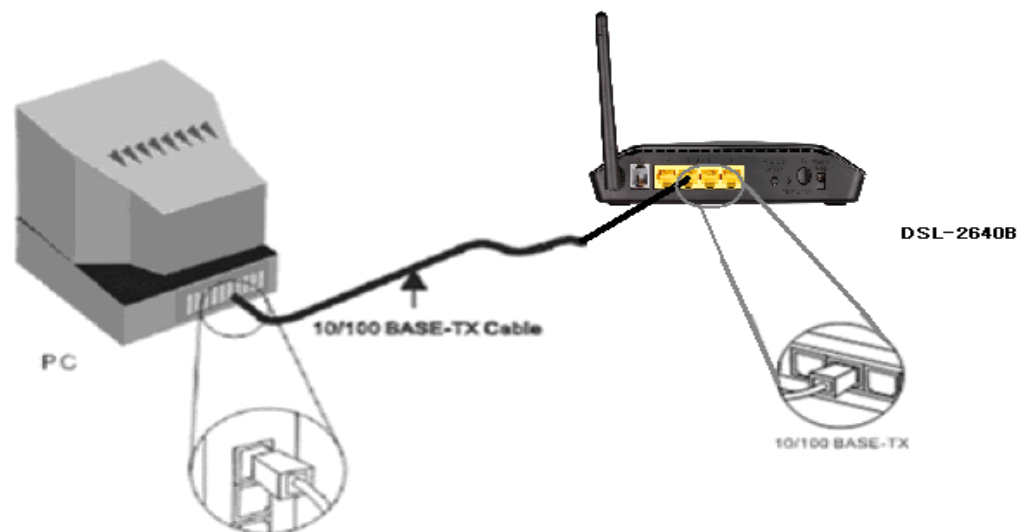
Configuration

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

Web-based Configuration Utility

Connect to the Router

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

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

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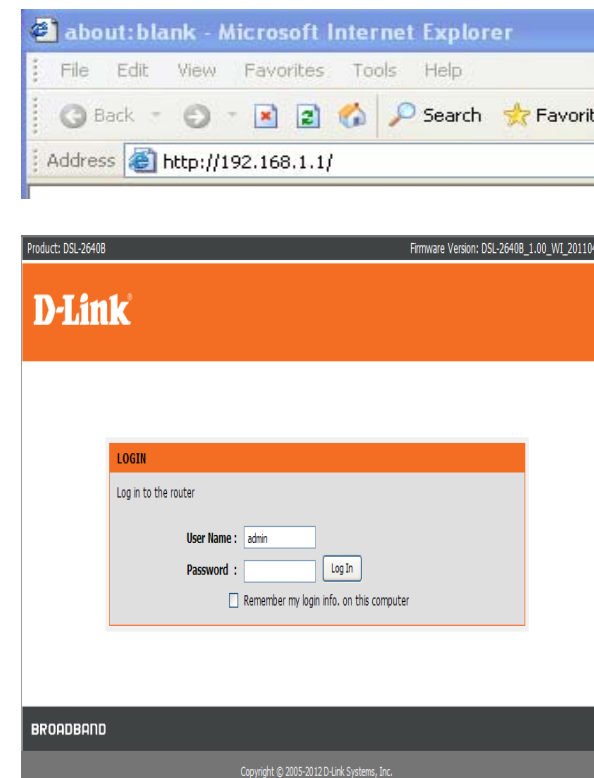
STATUS

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: **SYSTEM INFO**, **INTERNET INFO**, **WIRELESS INFO** and **LOCAL NETWORK INFO**.

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

SYSTEM INFO
This window displays **Model Name**, the **Time and Date** and the **Firmware Version**.

INTERNET INFO
This window displays WAN information including

Connection Status: You can know the connection is up or down now.

Internet Connection Up Time: Let you know how much time the connection has already been up for.

IP address/Default Gateway: They are from the ISP's distribution or you configure them manually.

Primary/Secondary DNS Server: They are from the ISP's distribution or you configure them manually.

Downstream Line Rate (Kbps): It shows the current Downstream speed.

Upstream Line Rate (Kbps): It shows the current Upstream Line speed.

INTERNET INFO

Connection Status:	CONNECTED
Internet Connection Up Time :	0 days 0 hours 0 minutes 21 seconds
Default Gateway:	ppp0_2
Preferred DNS Server:	168.95.1.1
Alternate DNS Server:	168.95.192.1
Downstream Line Rate (Kbps):	27471
Upstream Line Rate (Kbps):	1233

Interface	Description	Link Type	IGMP	QoS	Status	IP Address
ppp0_2	pppoe__1	PPPoE	Disabled	Disabled	Connected	10.0.0.148

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

WIRELESS INFO

MAC Address :	00:1A:2B:26:40:01
Status:	Enabled
Network Name (SSID):	D-Link DSL-2640B
Visibility:	Visible
Security Mode:	None

LOCAL NETWORK INFO

This window displays LAN information including MAC, IP address, Mask, and DHCP Server status.

LOCAL NETWORK INFO	
MAC Address :	00:1a:2b:26:40:00
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enabled

WIRELESS CLIENTS

This feature shows all the current connected wireless MACs.

CONNECTED WIRELESS CLIENTS
This window displays all the connected devices' MACs, Associated status, Authorized status, linked SSID and the connected wireless interface.

WIRELESS STATION INFO

This page shows authenticated wireless stations and their status, and will be refreshed every 30 seconds.

WIRELESS -- AUTHENTICATED STATIONS

MAC	Associated	Authorized	SSID	Interface
1c:af:f7:75:8e:1f	Yes	No	D-Link DSL-2640Bjackyyeh	ath0

DHCP CLIENTS

This feature shows the current status of all the DHCP leased devices.

DHCP CLIENTS

This window displays all the DHCP leased devices' hostname (ex. PC's name), MAC address, released IP and counting expires time.

DHCP CLIENTS

This information reflects the current DHCP client of your modem.

DHCP LEASES

Hostname	MAC Address	IP Address	Expires In
RQ-ALLEN-N	00:15:f2:ac:15:de	192.168.1.2	23 hours, 30 minutes, 33 seconds
RH-JASON-N3	1c:af:f7:75:8e:1f	192.168.1.3	23 hours, 55 minutes, 49 seconds

LOG

This feature is linked to the Maintenance/System Log/View System Log.

SYSTEM LOG

This window displays the level even log which is configured by the Maintenance/System Log/Configure System Log
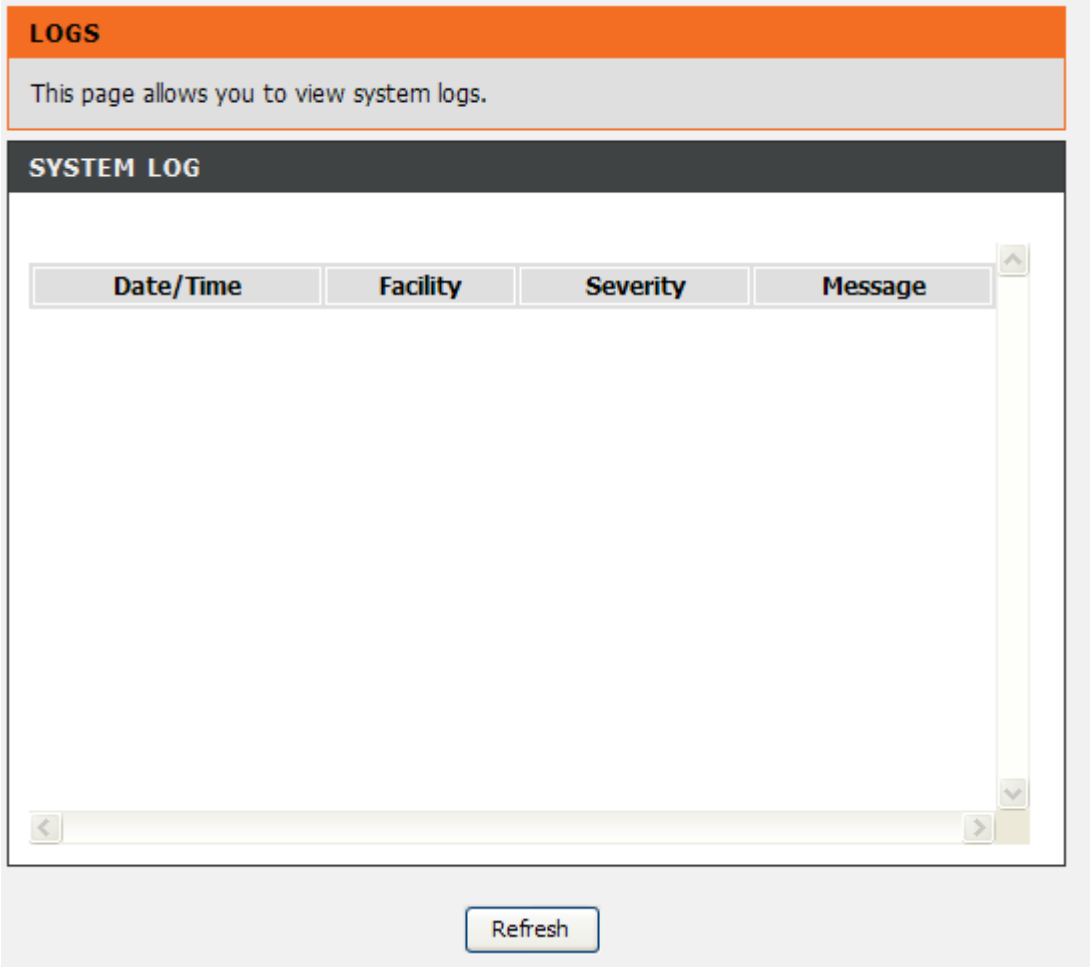
STATISTICS

This information shows the current statistics of all your available interfaces.

LAN

This window displays all the current **Receiver** and **Transmitted** Bytes and packets statistics on the LAN and wireless interfaces.

STATISTICS

This information reflects the current status of your DSL connection.

LAN

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
eth0	825541	7242	0	0	7829825	8994	0	0
eth1	0	0	0	0	0	0	0	0
eth2	0	0	0	0	0	0	0	0
eth3	0	0	0	0	0	0	0	0
ath0	37713	410	0	0	31856	261	0	0

WAN

This window displays all the current **Receiver** and **Transmitted** Bytes and packets statistics on the WAN interfaces.

WAN

Interface	PVC	Protocol	Service Name	Received				Transmitted			
				Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Dro
ppp0_2	0/33	EoA	pppoe__1	82581	89	0	0	9309	77	0	0

ADSL STATISTICS

This window displays the ADSL linking mode, Traffic type, linking status and linking power status.

● **ADSL linking line status:**

Line Coding(Trellis): trellis modulation (also known as trellis coded modulation, or simply TCM)

SNR Margin: Signal-to-noise ratio (often abbreviated SNR or S/N) is a measure used in science and engineering to quantify how much a signal has been corrupted by noise.

Attenuation: The signal levels to be lower relative to any local noise and attenuation. This will have the effect of reducing speeds or causing connection failures.

Output Power: Transmitting power.

Attainable Rate (Kbps): Line rate

Rate(kbps): Date rate.

ADSL STATISTICS

Mode:		ADSL_2plus
Traffic Type:		ATM
Status:		Up
Link Power State:		L0
	Downstream	Upstream
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	61	66
Attenuation (0.1 dB):	0	6
Output Power (0.1 dBm):	64	93
Attainable Rate (Kbps):	28216	1335
	Path 0	
	Downstream	Upstream
Rate (Kbps):	27471	1233
MSGc (# of bytes in overhead channel message):	51	14
B (# of bytes in Mux Data Frame):	244	13
M (# of Mux Data Frames in FEC Data Frame):	1	16
T (Mux Data Frames over sync bytes):	4	9
R (# of check bytes in FEC Data Frame):	0	8
S (ratio of FEC over PMD Data Frame length):	0.2850	5.7639
L (# of bits in PMD Data Frame):	6875	322
D (interleaver depth):	1	8
Delay (msec):	0.7	11.52

HEC: Header error control
OCD: Out of Cell Delineation
LCD: Loss of Cell Delineation

ES: Errored Second

Delay (msec):	0.7	11.60
INP (DMT symbol):	0.0	0.80
Super Frames:	0	0
Super Frame Errors:	0	0
RS Words:	0	3627648
RS Correctable Errors:	0	2
RS Uncorrectable Errors:	0	0
HEC Errors:	0	0
OCD Errors:	0	0
LCD Errors:	0	0
Total Cells:	341792072	15209727
Data Cells:	115134	10293
Bit Errors:	0	0
Total ES:	0	0
Total SES:	0	0
Total UAS:	21	21

You can click the **ADSL BER Test** button to test the ADSL connection.

You can click the **Reset Statistics** button to set all statistics to recount.

ADSL BER Test	Reset Statistics

ADSL BER Test - Result

The ADSL BER test completed successfully.

Test Time (sec):	20
Total Transferred Bits:	0x000000001DB5DB00
Total Error Bits:	0x0000000000000000
Error Ratio:	0.00e+00

Close
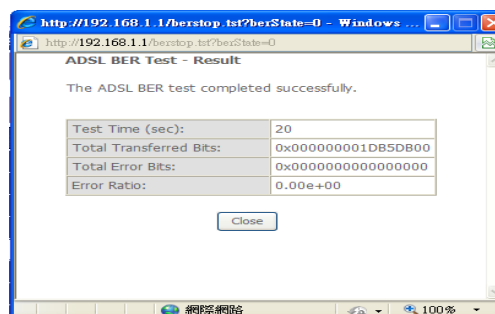
ROUTE INFO

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 segments of the destination, gateway, and subnet mask as well as other route information

ROUTING

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

DEVICE INFO -- ROUTE

Destination	Gateway	Subnet Mask	Flag	Metric	Service	Interface
168.95.98.254	0.0.0.0	255.255.255.255	UH	0	pppoe__1	ppp0_2
192.168.1.0	0.0.0.0	255.255.255.0	U	0		br0
0.0.0.0	0.0.0.0	0.0.0.0	U	0	pppoe__1	ppp0_2

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.

WIRELESS

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 Setup** button in the **SETUP** directory.

Wireless Network Setting

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.

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

Welcome to the D-Link Wireless Security Setup Wizard

Network Name (SSID) Accept the default name or change it to something else and the maximum is up to 32 characters. If the default SSID is changed, all other devices on the wireless network must also use the same SSID.

Automatically (Recommended)

In order to protect your network from hackers and unauthorized users,

we adapt Auto (WPA or WPA2-PSK) for your wireless security mode.

We provide user a random pre-shared key automatically.

Click **Next** button to go to the next page.
Click **Cancel** button to return to the main menu of Wireless Setup page.
Click **Prev** to go back to previous page.
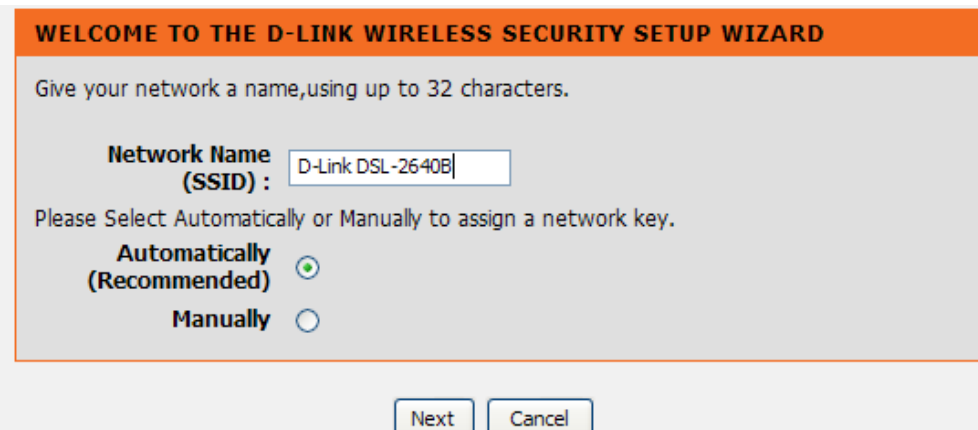
Click **Save** button to restore the configurations

Manually

You can select the **WPA (Recommended)** or **WEP.**

When you select the **WPA (Recommended)**, type a string (8-63 characters, such as A~Z, or 0~9.) on the **Network Key**.

When you select the **WEP**, type a string.

- Exactly 5 or 13 characters
- Exactly 10 or 26 characters using 0-9 and A-F

Manual WIRELESS Connection Setup SETTINGS
Click on the **Enable Wireless** box to allow the router to operate in the wireless environment. You can use the **New Schedule** button which links to the **Advanced/schedule** to set the schedule.

The **SSID** 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.

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

Select **802.11 Mode** to operate in b/g/n **Mixed** mode. Or select specified mode **802.11b only**, **802.11g only**, **802.11n only** to use.

Mixed 802.11g and 802.11b which means DSL-2640B will detect the clients to use 802.11g or 802.11b to synchronize.

Mixed 802.11n, 802.11g and 802.11b which means DSL-2640B will detect the clients to use 802.11n, 802.11g or 802.11b to synchronize.

Bandwidth, You can select **20MHz** or **Auto 20MHz/40MHz**. The maximum rate for **20 MHz** is 65 Mbps. The maximum rate for **40 MHz** is 150 Mbps (GI=1).

Transmission Rate, suggest keeping the Best (automatic) selection. This is related to Receive Sensitivity as follows, for example,

	MANRATE	HT20/GI=0	HT40/GI=0	HT40/GI=1
MCS 0	0x80	6.5Mbps	13.5Mbps	X
MCS 1	0x81	13Mbps	27Mbps	X
MCS 2	0x82	19.5Mbps	40.5Mbps	X

MCS 3	0x83	26Mbps	54Mbps	X
MCS 4	0x84	39Mbps	81Mbps	X
MCS 5	0x85	52Mbps	108Mbps	X
MCS 6	0X86	58.5Mbps	121.5Mbps	X
MCS7	0x87	65Mbps	135Mbps	150Mbps

Enable or Disable the **Hide wireless Network** to decide if you want to show the SSID.

WIRELESS SECURITY Mode

To protect your privacy you can configure wireless security features.

This device supports three wireless security modes including: **WEP, WPA, WPA2** and **Auto (WPA or WPA2).**

WEP is the original wireless encryption standard.

WPA (TKIP or AES)/WPA2 (AES) provide a higher level of security.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA, WPA2 and Auto.

The **WEP** mode is the original wireless encryption standard.WPA provides a higher level of security.

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

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

Security Mode : Auto (WPA or WPA2) ▾ (TKIP or AES)

WIRELESS SECURITY MODE - WEP

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

Select **WEP Key Length** from the drop-down menu. (**128 bit** is stronger than **64 bit**)

Type strings to define these 4 keys for each on **WEP Key 1/2/3/4**.

Choose which WEP key from 1 to 4 you want to use to link to clients on the **Default WEP Key**.

Select **Authentication** type from the drop-down menu. (**Shared** is better than **Open**)

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

WEP

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

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

WEP Key Length :	128 bit (13 characters or 26 hex digits) (length applies to all keys)
WEP Key 1 :	4ecc643252bdf
WEP Key 2 :	4ecc643252bdf
WEP Key 3 :	4ecc643252bdf
WEP Key 4 :	4ecc643252bdf
Default WEP Key :	WEP Key 1
Authentication :	Open

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

Apply Settings   Cancel

WIRELESS SECURITY MODE – WPA-Personal

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

According to the WiFi Alliance 11N specification, Wi-Fi Protected Setup is not full supported under WPA Only mode. We will disable your Wi-Fi Protected Setup if you use WPA Only mode.

Choose **Auto(WPA or WPA2) / WPA2 only / WPA only** on the **WPA Mode**

Type the value seconds on the **Group Key Update Interval.** The default value is 1800.

Type the string on the **Pre-Shared Key**

Click the **Apply Settings** button to save the configuration.
Choose the **Hide** or **Display** to decide if you want to show the SSID.

WIRELESS SECURITY MODE – WPA-Enterprise
802.1x

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

Enter your RADIUS server data: **IP Address, Port,** and **Secret Key**. The **Authentication Timeout** is 36000 seconds.

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

EAP (802.1X)

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

Authentication Timeout :	36000 (seconds)
RADIUS server IP Address :	0.0.0.0
RADIUS server Port :	1812
RADIUS server Shared Secret :	

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

Apply Settings   Cancel

INTERNET SETUP

To access the **INTERNET SETUP** (WAN) settings window, click on the **INTERNET Setup** button in the **SETUP** directory

INTERNET SETUP

Protocollo :

PPPoE/PPPoA Choose this option if your ISP uses PPPoE/PPPoA.(For most DSL users)

Incapsulamento : Please select the LLC or VC-Mux to match to your ISP's CO DSLAM's encapsulation.

Type **VPI/VCI** to match the exact channel.

Type **username/password** which your ISP provides to you when you apply the connection.

Press the **Apply** button to let the configurations take effect.

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** directory.

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

You also can enable the **second IP Address and subnet Mask for LAN Interface** to let LAN side has 2 different IP segments. For example, 192.168.1.0/24 (The default segment) and the 192.168.2.0/24 (The second segment).

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

Configure 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.

You can change the value hours on the **DHCP Lease Time** and the default is 24 hours.

Please press the **Saving Settings** button to take effect.
ADD/EDIT DHCP RESERVATION (OPTIONAL)

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 "Father's Laptop".

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

Press the **Apply** button to save the settings

DHCP SERVER SETTINGS (OPTIONAL)

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

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

Save Settings

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address

Add   Edit   Delete

ADD/EDIT DHCP RESERVATION (OPTIONAL)

Enable : ☑
Computer Name :
IP Address : 0.0.0.0
MAC Address : 00:00:00:00:00:00

Copy Your PC's MAC Address

Apply   Cancel

DHCP RESERVATIONS LIST

After saved the DHCP reservation, the **DHCP RESERVATIONS LIST** will list the configuration.

The **NUMBER OF DYNAMIC DHCP CLIENTS** shows how many DHCP clients (PC or Laptop) connected to the router currently.

Click on the **Save Settings** button. You will be asked to reboot by a pop-up window. Click on the **OK** to reboot the router.

DHCP RESERVATIONS LIST

	Enable	Computer Name	MAC Address	IP Address
☐	Enable	Father	00:18:8B:BF:5A:F4	192.168.1.5

Add   Edit   Delete

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Computer Name	MAC Address	IP Address	Expire Time
06967NBWINXP5P2	00:18:8B:BF:5A:F2	192.168.1.2	23 hours, 57 minutes, 7 seconds

TIME and DATE

The **TIME** configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. 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** directory

TIME

Enable the **Automatically synchronize with Internet time servers**.

Select specific time server to use from the **First/Second NTP Server** drop-down menu. Or, you can type the specific NTP server name.

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

If you need to use the daylight saving, just enable 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 the **United States** on the second Sunday of March. Each time zone in the United States starts Daylight Saving time at 2 A.M. Thus, in the United States you must use **March**, **Second**, **Sunday**, at **2:00 A.M.**

Daylight Saving time starts in the **European Union** on the last Sunday of March. Thus, in European Union, you must select **March**, **Last**, **Sunday**. The time must depend on your country's time zone. For example, In Germany you must type 2 because Germany's time zone is 1 hour ahead of GMT or UTC (GMT+1). Thus, in Germany you must use **March**, **Last**, **Sunday**, at **1:00 A.M.**

Daylight Saving time ends in the most parts of the United States on the First Sunday of November. Each time zone in the United States must use Daylight Saving time at 2:00 A.M. Thus, in the United States you must set **November**, **First**, **Sunday**, at **2:00 A.M**.

Daylight Saving time ends in the European Union on the Last Sunday of October. For instance, in Germany you must type 2 because Germany's time zone is 1 hour ahead of GMT (GMT+1). Thus, in Germany you must use **March**, **Last**, **Sunday**, at **1:00 A.M.**

SET THE DATE AND TIME MANAULLY

You can also use the **Copy Your Computer's Time Settings** to synchronize the Date and Time to your local PC. Or, you also can adjust **Year/Month/Day/Hour/Minute/Second** manually.

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

SET THE DATE AND TIME MANUALLY

Date And Time :

Year: 2005   Month: Jan   Day: 1

Hour: 1 am   Minute: 6   Second: 18

Copy Your Computer's Time Settings

Apply   Cancel

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 **SETUP** directory

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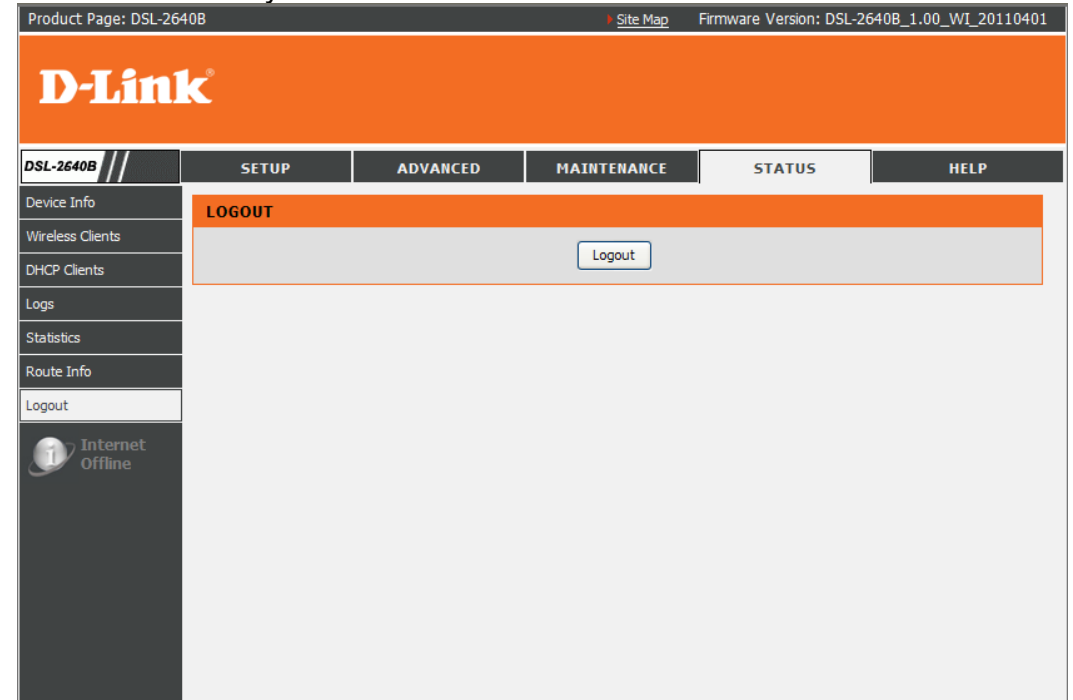
ADVANCED

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 INTERNET

The Multiple PVC Settings allow you to **Add**, **Delete** or **Edit** multiple PVCs connection for advanced ADSL service. The Advanced ADSL settings allow you to choose which ADSL modulation settings your modem router will support. D-Link do not recommend that you change these settings unless directed to do so by your ISP.

MULTIPLE PVC SETTINGS

Please click the **Add** button to add the multiple PVC

You can also press the **Edit** button to edit the configuration.

You can press the **Remove** button to delete the connection.

ADVANCED WIRELESS

These options are for users that wish to change the behavior of their 802.11g 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.

ADVANCED WIRELESS SETTINGS

To access the **ADVANCE WIRELESS** setting window, click on the **Advanced Wireless** button in the **ADVANCED** directory.

ADVANCED SETTINGS
Allows you to configure advanced features of the wireless LAN interface

MAC FILTER
Allows you to configure wireless firewall by denying or allowing

designated MAC addresses.

QOS (QUALITY OF SERVICE)

Allows you to configure wireless QoS.
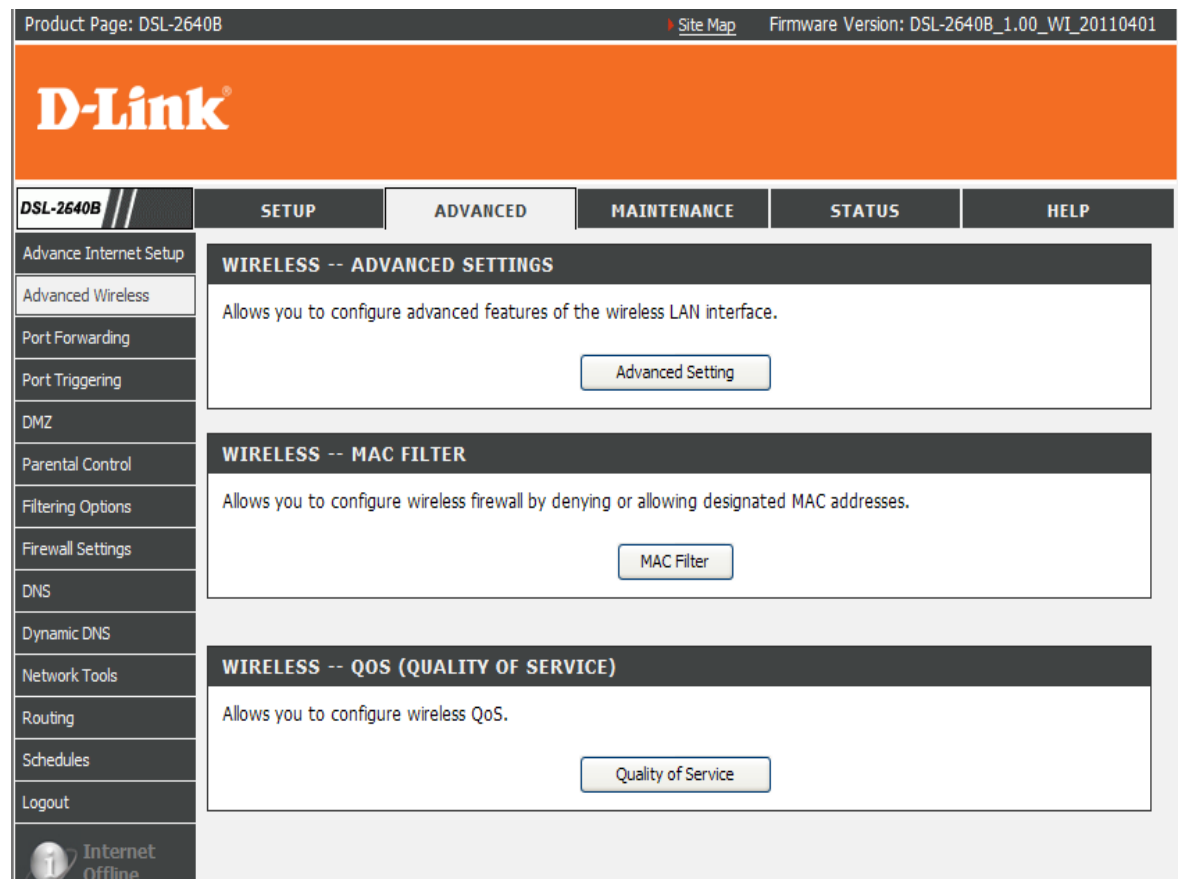
ADVANCE WIRELESS SETTINGS

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

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

RTS Threshold: If a network packet is smaller than the preset RTS threshold size, the RTS/CTS mechanism will not be enabled. The router sends Request to Send (RTS) frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a Clear to Send (CTS) frame to acknowledge the right to begin transmission. The range is **1~2347** bytes.

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

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

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

WIRELESS -- ADVANCED SETTINGS

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

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

ADVANCED SETTINGS

Band:	2.4GHz
Channel:	Auto Current: 6
Bandwidth:	20MHz
Support 802.11n Client Only:	Off
Basic Rate:	Default
Fragmentation Threshold(byte):	2346
RTS Threshold(byte):	2347
DTIM Interval(ms):	1
Beacon Interval(ms):	100
Transmit Power:	100%

The DLink DSL-2640B also provides the **Guest wireless** for your guests for security.

Please enable the **Enable Wireless Guest Network**.

If you want to change the default guest SSID, please edit it on the **Wireless Network Name.**

If you want to hide the SSID, please enable the **Hide Wireless Network**

If you want to isolate the guest wireless, you can select **on** in this **AP Isolation**

You can define the **Security mode** for the guest wireless by selecting WEP/WPA/WPA2/Auto

Please press the **Save/Apply** button to save the configurations.

ADD MAC FILTER
The default is **Disable**.

Select which wireless network you want to apply the filter from **SSID** drop down menu.

Select the **MAC Restrict Mode** as **Allow** to filter out all wireless MAC address besides the MAC addresses in the Wireless Mac Filter lists.

Select the **MAC Restrict Mode** as **Deny** to filter out all wireless MAC address in the Wireless Mac Filter lists

Enter the **Wireless MAC Address** and press the **Save/Apply** button to add in the wireless MAC filter list.

WIRELESS -- MAC FILTER

Sets wireless MAC filter.

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

WIRELESS -- MAC FILTER

Select SSID: InfostradaWiFi-264000

MAC Restrict Mode: ⦿ Disabled ○ Allow ○ Deny

MAC Address

Add   Remove

WIRELESS -- MAC FILTER

MAC Address:

Save/Apply

WIRELESS QOS

WMM is used to prioritize the data packets from to/from WLAN. It is very useful when transmitting delay-sensitive packets like VoIP.

You can select **Enabled** or **Disabled** to decide if you want to use WMM.

Please press the **Apply** button to take it effect.

WIRELESS -- QOS

This page lets you add, remove, enable and disable wireless QoS.

WMM(WI-FI MULTIMEDIA) SETTINGS

WMM(Wi-Fi Multimedia):   Enabled

Apply

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-2640B 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** directory

PORT FORWARDING RULES CONFIGURATION

Press the **Add** button to have a port forwarding policy now.

Select a WAN interface on the **Use Interface**.

Select a service name from the **Select a Service** drop-down menu for a pre-configured application or type a name in the **Customer Server** input box to define your own application.

You can choose the **Allow All** or **Deny All** on the **Inbound Filter** to decide if you need to open the service you configured or close the service. BTW, you don't have to delete the services to save time and you can keep the service to use next time.

Type an IP address in the **IP address** input box to appoint the PC to receive the forwarded packets.

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 server PC with the appointed **IP Address**. The **TCP/UDP** means the protocol type of the opened ports.

PORT FORWARDING SETUP

Remaining number of entries that can be configured:31

Use Interface : pppoe_atm0_1/ppp0_2

Server Name :

⦿ Select a Service : (Click to select)

○ Custom Server :

Inbound Filter : Allow All

Server IP Address : 192.168.1. [192.168.1.2 - 192.168.1.254]

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

Apply   Cancel

PORT TRIGGERING

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

To access the PORT TRIGGER **setting window, click on the** PORT TRIGGER **button in the** ADVANCED **directory.**

PORT TRIGGER RULES CONFIGURATION

Press the **Add** button to have a Port Triggering policy now.

Select a WAN interface on the **Use Interface**.

Select a service name from the **Select a application** drop-down menu for a pre-configured application or type a name in the **Customer application** input box to define your own application.

Type an IP address in the **IP address** input box to appoint the PC to receive the forwarded packets.

You also can select **Always** or **Never** on the **Schedule** or you can press the link to launch the **Advanced/Schedule** settings to configure a period time which you want.

Enter your **Trigger** and **Open** port(s), and select the **Traffic Type** if you select to type the application manually.

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

PORT TRIGGERING

Remaining number of entries that can be configured :32

Use Interface : pppoe_atm0_1/ppp0_2
Application Name :
Select an application : (Click to select)
Custom application :
Schedule : Always   *View Available Schedules*

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP
		TCP			TCP

Apply   Cancel

DMZ

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

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

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

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

Clear the IP address field and press "**Apply**" button to deactivate the DMZ host.

| Product Page: DSL-2640B | Site Map | Firmware Version: DSL-2640B_1.00_WI_20110401 |

D-Link

| DSL-2640B | SETUP | ADVANCED | MAINTENANCE | STATUS | HELP |

Advance Internet Setup
Advanced Wireless
Port Forwarding
Port Triggering
DMZ
Parental Control
Filtering Options
Firewall Settings
DNS
Dynamic DNS
Network Tools
Routing
Schedules
Logout

Internet Offline

DEMILITARIZED ZONE

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

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

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

DMZ HOST

DMZ Host IP Address : 192.168.1.   [192.168.1.2 - 192.168.1.254]

Apply   Cancel

Helpful Hints...

Enable the DMZ option only as a last resort. If you are having trouble using an application from a computer behind the router, first try opening ports associated with the application in the **Advanced -> Port Forwarding** section.

More...

PARENTAL CONTROL

The **PARENT CONTROL** provides two useful tools for restricting Internet access. **Block Websites** allows you to quickly create a list of all web sites that you wish to stop users from accessing. **Time Restrictions** allows you to control when clients or PCs connected to Router are allowed to access the Internet.

To access the **PARENT CONTROL** setting window, click on the **Parental Control** button in the **ADVANCED** directory

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

BLOCK MAC ADDRESS
Uses MAC address to implement filtering

TRUSTED COMPUTERS
Uses Trusted computers to avoid parental control.

BLOCKED WEBSITES SCHEDULING

Press the **Add** button to type the **Website URL** and select the corresponding schedule if you want to add the block website policy.

Press the **Apply** button to add to your blocked websites scheduling configuration.

Schedule

You also can select **Always** or **Never** on the **Schedule** or you can press the link to launch the **Advanced/Schedule** settings to configure a period time which you want.

Check the **checkbox** in the head of the row, and then click on the **Delete** button. The checked items will be deleted from the table.

BLOCK WEBSITE

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

BLOCK WEBSITE

	URL	Schedule Rule

Add   Edit   Delete

BLOCK WEBSITE

URL :

Schedule: Always ∨ View Schedule Details

Apply   Cancel

BLOCK MAC ADDRESS

In a home setting, parents can also restrict certain computers' accessibility to the internet for the time and day of the week.

Enter the **User name** and **MAC address** of the restricted PC.

Select the schedule for the rule to take effect in **Blocking on Schedule**.

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

BLOCK MAC ADDRESS

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

BLOCK MAC ADDRESS

	Username	MAC	Schedule Rule

Add   Edit

TIME OF DAY RESTRICTION

User Name: [   ]

⦿ Browser's MAC Address: 00:15:f2:ac:15:de

◯ Other MAC Address: [   ]
(xx:xx:xx:xx:xx:xx)

Blocking on Schedule: Always ▾ View Schedule Details

Apply   Cancel

TRUSTED COMPUTERS

Block website function will not block website for trusted computers.

But Trusted Computers function doesn't influence Block MAC Address, that is to say: if a PC MAC is restricted by Block MAC Address, even if the pc IP Address is in Trusted User IP Range, the pc can't connect to the route too.

Type **a range of IP address** which is not restricted by Block Website.

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

TRUSTED COMPUTERS

To exclude a range of IP which is not restricted by Block Website, the range of Ip is free to access any web site even if the site is blocked by Block Website. But Trusted Computers function don't influence Block MAC Address, that is to say: if a pc mac is restricted by Block MAC Address, even if the pc Ip Address is in Trusted User IP Range, the pc can't connect to the route too.

TRUSTED USER IP RANGE

From: 0.0.0.0

To: 0.0.0.0

Apply   Cancel

FILTERING OPTION

Use this section to configure the **FILTER OPTION** setting 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 **FILTER OPTION** settings window, click on the **FILTER OPTION** button in the **ADVANCED** directory.

INBOUND IP FILTER
Manage incoming traffic.

OUTBOUND IP FILTER
Manage outgoing traffic.

BRIDGE FILTER
Uses MAC address to implement filtering. Useful only in bridge mode.

ADD INBOUND IP FILTER

Press the **Add** button to set inbound IP filter Setup setting

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

The **source IP/PORT** means that the packet is from **WAN**.

You also can select **Always** or **Never** on the **Schedule** or you can press the link to launch the **Advanced/Schedule** settings to configure a period time which you want.

You also can choose which **WAN interface** you want to configure the Inbound IP filter policy.

Press the **Add/Apply** button to add and apply settings.

Note: This section only applies when the Firewall is enabled.

ADD OUTBOUND IP FILTER

Press the **Add** button to set outbound IP filter rule.

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

The **source IP/PORT** means that the packet is from **LAN**.

You also can select **Always** or **Never** on the **Schedule** or you can
press the link to launch the **Advanced/Schedule** settings to configure
a period time which you want.

Press the **Add/Apply** button to add and apply settings.

Note: This section only applies when the Firewall is enabled.

Bridge Filtering is only effective on ATM PVCs configured in Bridge mode.

BRIDGE FILTERING

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

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

BRIDGE FILTERING POLICY(CONFIGURED IN BRIDGE MODE ONLY)

Press the **Add** button to set Bridge filter setting

FORWARD:**ALLOW** all packets but **DENY** those matching any of specific rules listed

BLOCKED:**DENY** all packets but **ALLOW** those matching any of specific rules listed

	Bridge Interface	Policy

Click on the **Change Policy** button to alter the global policy setting.

[Change Policy] [Cancel]

BRIDGE FILTER SETUP

FOWARD: **ALLOW** all packets but **DENY** those matching any of specific rules listed.

BLOCKED:**DENY** all packets but **ALLOW** those matching any of specific rules listed

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

Also known as MAC address filter. You can forward or deny incoming traffic based on the source MAC address or the destination MAC address.

[Add] [Edit] [Delete]

ADD BRIDGE FILTER

Note that bridge filter will work with interfaces which are configured as bridge.

Filter Name : [   ]
Protocol Type : (Click to select) ▾
Destination MAC Address : [   ]
Source MAC Address : [   ]
Frame Direction : LAN<=>WAN ▾
Schedule: Always ▾ View Schedule Details

WAN Interfaces (Configured in Bridge mode only)

☑ Select All

Press the **Apply** button to add and apply settings.

[Apply] [Cancel]

FIREWALL SETTINGS

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

To access the **FIREWALL** setting window, click on the **Firewall Settings** button under the **ADVANCED** tab.

FIREWALL SETTING

Please enable the Enable Attack Prevention if you want to block Hacker's DoS attack.

DoS and Port Scan Protection:A DoS (denial-of-service) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person.Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

Rate & Burst The Rate is the trigger threshold. When the specified packets number has reached this rate, it triggers once.The Burst is the consecutive trigger number allowed. The router will stop all related application when the Burst is matched and resume working after the Rate is reduced below the configured number.

FIREWALL SETTINGS

Click "Apply" button to make the changes effective immediately.

FIREWALL CONFIGURATION

☐ **Enable Attack Prevention**

Type   Rate(pkt/sec)   Burst

TCP DoS :

Ping DoS :

Port Scan :

Prevent IP Spoofing : ☐

[Apply] [Cancel]

DNS SETUP

Domain Name Server(DNS) is a server that translates URL/Domain Names to the corresponding IP address. Since URL/Domain Names are alphabetical, they are easier to remember. But the internet is based on IP address. For example, the URL/Domain Name www.dlink.com is actually 207.232.83.10
To access the **DNS** setting window, click on the **DNS** button under the **ADVANCED** tab.

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 server address automatically** 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**.

DDNS

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

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

DDNS CONFIGURATION

Click the **Add** button to set DDNS setting.
Select DDNS Service provider from the **D-DNS provider** drop-down menu and enter your account data.
After configure the DDNS settings as desired, click on the **Apply Settings** button to apply settings.

D-DNS provider:
Select one of the DDNS registration organizations form those listed in the pull-down menu. Available servers include DynDns.org and dlinkddns.

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

Username: Enter the Username for your DDNS account.

Password: Enter the Password for your DDNS account

NETWORK TOOL

The **NETWORK TOOL** feature allows you to configure **PORT MAPPING, QOS, ADSL Settings** and **UPNP**

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

PORT MAPPING

Port Mapping supports multiple ports to PVC and bridging groups.

Each group will perform as an independent network.

QOS

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

ADSL Settings

Allows you to configure Default Gateway used by WAN Interface.

UPNP

Allows you to configure UPnP.
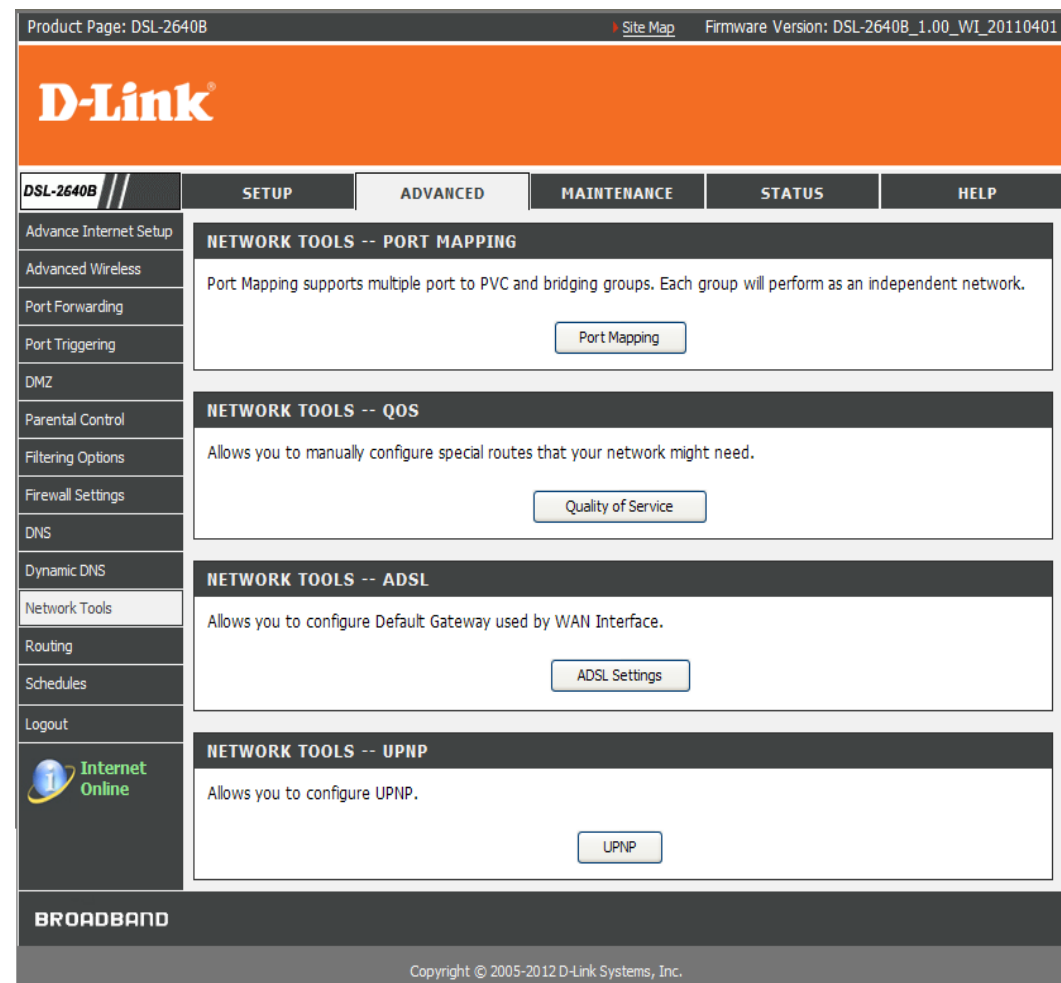
Port Mapping

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. Removing the group will add the ungrouped interfaces to the Default group. Only the default group has IP interface.

PORT MAPPING SETTINGS

This section is used to configure the port mapping to support VLAN.

Port Mapping supports multiple ports to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the Add button. The Remove button will remove the grouping and add the ungrouped interfaces to the Default group if Remove is checked. Only the default group has IP interface.

PORT MAPPING

Group Name	Interfaces	Remove	Edit
Default	ath0, atm1, eth0, eth1, eth2, eth3, ppp0_2		

[Add]   [Remove]

Please type the group name on the **Group Name**

Please select which **WAN interface** you want to combine to.

PORT MAPPING

To create a new mapping group:
1. Enter the Group name and select interfaces from the available interface list and add it to the grouped interface list using the arrow buttons to create the required mapping of the ports. The group name must be unique.

2. If you like to automatically add LAN clients to a PVC in the new group add the DHCP vendor ID string. By configuring a DHCP vendor ID string any DHCP client request with the specified vendor ID (DHCP option 60) will be denied an IP address from the local DHCP server.
Note that these clients may obtain public IP addresses.

3. Click "Apply" button to make the changes effective immediately.

PORT MAPPING CONFIGURATION

Group Name: [   ]

WAN Interface used in the grouping: [ipoe_atm1/atm1 ▼]

Grouped LAN Interfaces

Available LAN Interfaces
ath0
eth0
eth1
eth2
eth3

[->]
[<-]

Automatically Add Clients With the following DHCP Vendor IDs
[   ]
[   ]
[   ]
[   ]
[   ]

[Apply]   [Cancel]

Please take notice that you should reboot your device after you apply the port mapping

Please choose which **LAN interface** or **wireless** you want to combine to the WAN interface.

You also can type the **DHCP Vendor ID** to combine to a group.

Press the **Apply** button to save the configurations.

QoS

Quality of Service is a feature that allows you to allocate or

guarantee the throughput or speed of Internet for certain computer.

You can press the "**Add**" button to define a new policy.

Please type the Traffic Class Name.

Specify Classification Criteria

Select the physical LAN port and Ether Type.

Type the Source IP/MAC and Destination IP/MAC.

Specify Classification Results

Assign Classification Queue: priority 1~8 (ath0&key&Pre)

Mark Differentiated Service Code Point (DSCP):

Assured Forwarding (AF) Behavior Group

	Class 1	Class 2	Class 3	Class 4
Low Drop	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Med Drop	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
High Drop	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

You can double click on the QoS Queues to check the QoS Queue Setup.

Note: Lower integer values for precedence imply higher priority for this queue relative to others

Click '**Apply**' to save and activate the queue.

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

Product Page: DSL-2640B   ▸ Site Map   Firmware Version: DSL-2640B_1.00_WI_20110401

D-Link

DSL-2640B

| SETUP | ADVANCED | MAINTENANCE | STATUS | HELP |

Advance Internet Setup
Advanced Wireless
Port Forwarding
Port Triggering
DMZ
Parental Control
Filtering Options
Firewall Settings
DNS
Dynamic DNS
Network Tools
Routing
Schedules
Logout

Internet Online

QOS

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

Apply/Save

QOS -- QUEUE MANAGEMENT CONFIGURATION

If Enable QoS checkbox is selected, choose a default DSCP mark to automatically mark incoming traffic without reference to a particular classifier. Click 'Apply/Save' button to save it.

Note: If Enable Qos checkbox is not selected, all QoS will be disabled for all interfaces.

Note: The default DSCP mark is used to mark all egress packets that do not match any classification rules.

☐ Enable QoS

QOS QUEUE SETUP -- A MAXIMUM 16 ENTRIES CAN BE CONFIGURED.

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

Name	Key	Interface	Scheduler Alg	Precedence	Weight	DSL Latency	PTM Priority	Enable	Remove
WMM Voice Priority	1	ath0	SP	1				Enabled	
WMM Voice Priority	2	ath0	SP	2				Enabled	
WMM Video Priority	3	ath0	SP	3				Enabled	
WMM Video Priority	4	ath0	SP	4				Enabled	
WMM Best Effort	5	ath0	SP	5				Enabled	
WMM Background	6	ath0	SP	6				Enabled	
WMM Background	7	ath0	SP	7				Enabled	
WMM Best Effort	8	ath0	SP	8				Enabled	
Default Queue	33	atm0	SP	1		Path0		☐	
Default Queue	34	atm1	SP	1		Path0		☐	

Add   Remove   Cancel

BROADBAND

Copyright © 2005-2012 D-Link Systems, Inc.

ADSL Settings

The ADSL 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 Save/Apply button if you are finished or click on Advanced Settings if you want to configure more.

ADSL (G.DMT)	12.0 Mbit/s	1.3 Mbit/s
ADSL Lite (G.Lite)	1.5 Mbit/s	0.5 Mbit/s
ANSI T1.413	8.0 Mbit/s	1.0 Mbit/s
ADSL2	12.0 Mbit/s	1.3 Mbit/s
ADSL2(Annex L)	5.0 Mbit/s	0.8 Mbit/s
ADSL2+	24.0 Mbit/s	1.3 Mbit/s
ADSL2+(Annex M)	24.0 Mbit/s	3.3 Mbit/s

Bitswap: adapts to errors on the line:

As line conditions change, bit swapping allows the modem to swap bits around different channels, without retraining, as each channel becomes more or less capable.

SRA: SRA software allows modems to make seamless data transfer

DSL

This page allows you to configure the modems DSL modulation.

Select the modulation below.

DSL SETTINGS

Select the modulation below.
- ☑ G.Dmt Enabled
- ☑ G.lite Enabled
- ☑ T1.413 Enabled
- ☑ ADSL2 Enabled
- ☑ ADSL2+ Enabled

Select the Annex L or M mode.
- ☑ AnnexL Enabled
- ☐ AnnexM Enabled

Select the phone line pair below.
- ◉ Inner pair
- ○ Outer pair

Capability
- ☑ Bitswap Enable
- ☐ SRA Enable

[Advanced Settings] [Save/Apply] [Cancel]

rate changes to avoid dropping a connection.

You also can press the **Advanced Settings** button to enter the tes

mode.

Normal

Starts ADSL connection in normal mode

Reverb

Puts ADSL PHY in test mode in which it only sends REVERB signal

Medley
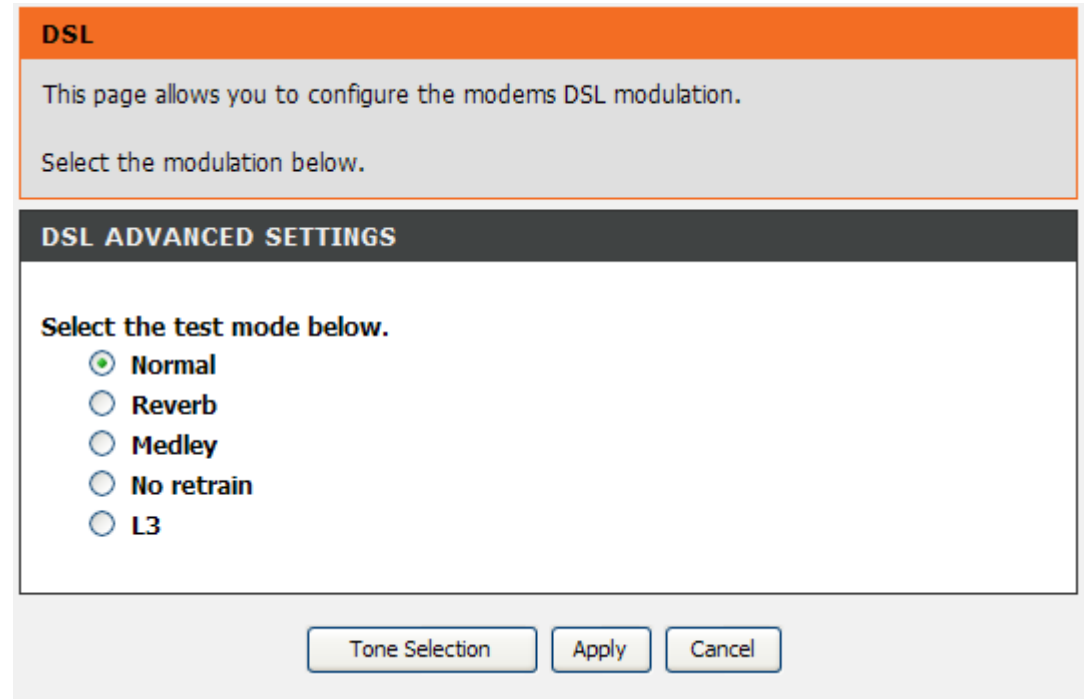
Puts ADSL PHY in test mode in which it only sends MEDLEY signal

No retrain

In this mode ADSL PHY will be trying to establish connection as in

normal mode, but once the connection is up it will not retrain even if

the signal is lost.

L3

L3 low consumption mode

UPNP CONFIGURATION

User can enable/disable UPnP functionality on this page. Click Apply button to save your setting.

You can enable the **Enable UPNP support** to have Upnp function.

ROUTING

Static route, default gateway, and RIP type routing configurations can be performed here.
To access the **Routing** setting window, click on the **Routing** button under the **ADVANCED** tab.
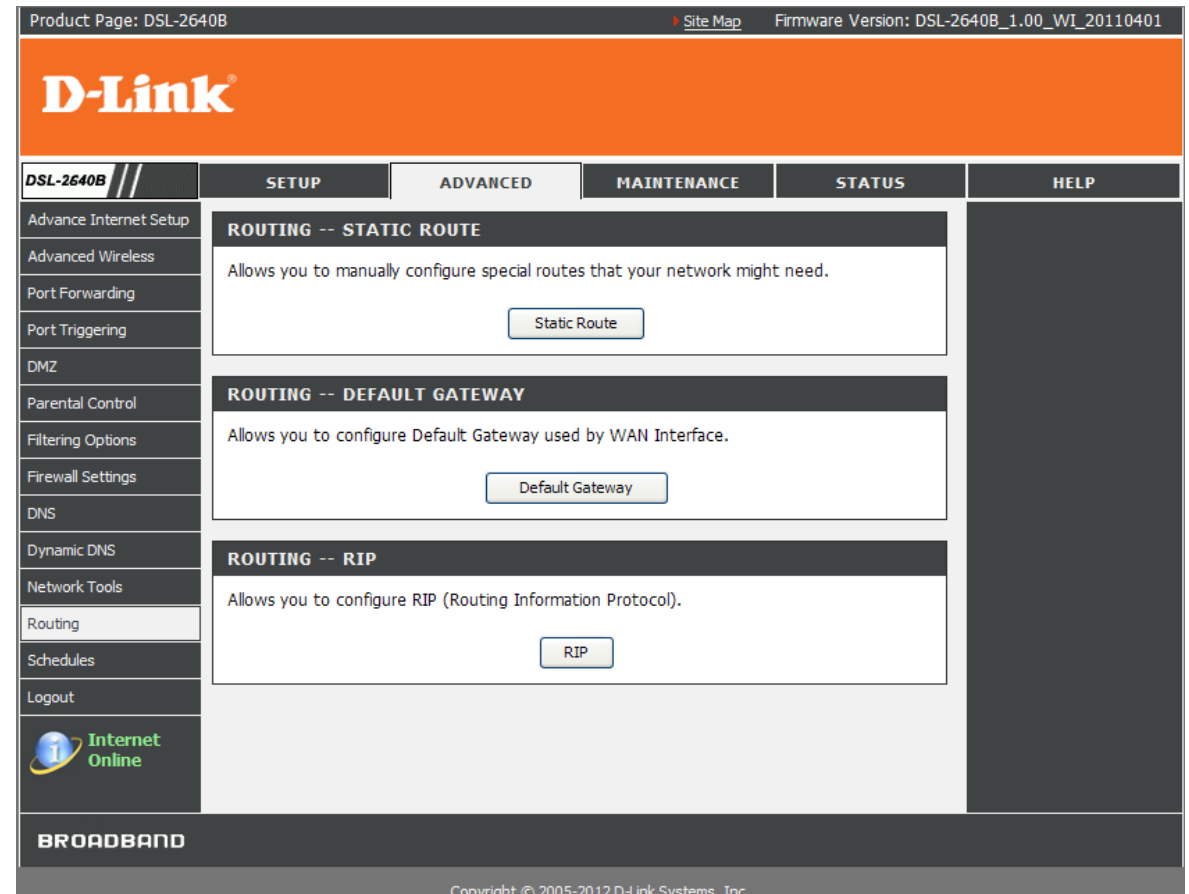
STATIC ROUTE
Allows you to manually configure special routes that your
network might need.

DEFAULT GATEWAY
Allows you to configure Default Gateway used by WAN
Interface.

RIP

Allows you to configure RIP (Routing Information Protocol).

STATIC ROUTE

Press the **Add** button to configure a route.

Enter the destination network address, subnet mask, gateway IP address or an available WAN interface and then press the **Apply** button to add the entry to the routing table.

ROUTING

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

A maximum 32 entries can be configured

STATIC ROUTE

	Destination	Subnet Mask	Gateway	Interface
☐	10.10.10.0	255.255.255.0		atm1
☐	193.76.32.0	255.255.240.0		atm1
☐	10.57.0.0	255.255.0.0		atm1
☐	10.28.0.0	255.255.0.0		atm1

[Add] [Edit] [Remove]

STATIC ROUTE ADD/EDIT

Destination Network Address : [   ]

Subnet Mask : [   ]

⦿ Use Gateway IP Address : [   ]

◯ Use Interface: [pppoe_atm0_1/ppp0_2 ▾]

[Back] [Apply] [Cancel]

DEFAULT GATEWAY

Select the proper wan interface as the system default gateway from the drop-down menu. Click "Apply" button to save it.

ROUTING -- DEFAULT GATEWAY

Select a preferred wan interface as the system default gateway. Click "Apply" button to save it.

DEFAULT GATEWAY

Use Interface: pppoe_atm0_1/ppp0_2

Apply   Cancel

RIP CONFIGURATION

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

NOTE: RIP cannot be configured on the WAN interface which has NAT enabled (such as PPPoE).

ROUTING -- RIP

NOTE: **RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled and un-pppoe .**

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

ROUTING -- RIP CONFIGURATION

Interface	Version	Operation	Enabled
br0	2	Passive	☐

SCHEDULE

To access the **SCHEDULES** setting window, click on the **SCHEDULES** button in the **ADVANCED** directory.

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

Press the **Add** button to create your own schedule.

Type the schedule policy name.

Day(s)
Select All Week or Select Day(s) to have which day(s) to be available.

Hour(s)
Set the Start time and the End time to define the working time range.

MAINTENANCE

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

SYSTEM

This section allows you to manage the router's configuration settings, reboot, back up, load previous saved settings and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.
To access the **SYSTEM** setting window, click on the **SYSTEM** button under the **MAINTENANCE** tab.

REBOOT
Click the button below to reboot the router

BACKUP SETTINGS
Backup DSL Router configurations. You may save your router configurations to a file on your PC.

Note: Please always save configuration file first before viewing it.

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

RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults

DSL ROUTER REBOOT
Please ensure you do not turn the Router off while it is rebooting.
After the Router has successfully rebooted, you can again configure the Router as desired. You can also test the WAN connection by accessing the Internet with your browser.

Close the DSL Router Configuration window and wait for 1 minute before reopening your web browser. If necessary, please reconfigure your computer's IP address to match your new configuration.

DSL ROUTER REBOOT

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

|||||||||||||| 15%

SYSTEM -- BACKUP SETTINGS

Backup DSL Router configurations. You may save your router configurations to a file on your PC.

Backup Settings

SAVE/RESTORE CONFIGURATION
Click on the **Backup Settings** button to Save Settings to Local Hard Drive. You will be prompted to select a location on your computer to locate the file. You may name the configuration file anything you like.

SYSTEM -- UPDATE SETTINGS

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

Settings File Name: [瀏覽...]

Update Settings

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

SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

Restore Default Settings

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

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 UPGRADE

To upgrade firmware, click on the **Browse…** button to search for the file and then click on the **Update Firmware** button to begin copying the file.

The Router will load the file and restart automatically.

ACCESS CONTROL

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

ADMIN

Manage DSL Router user accounts

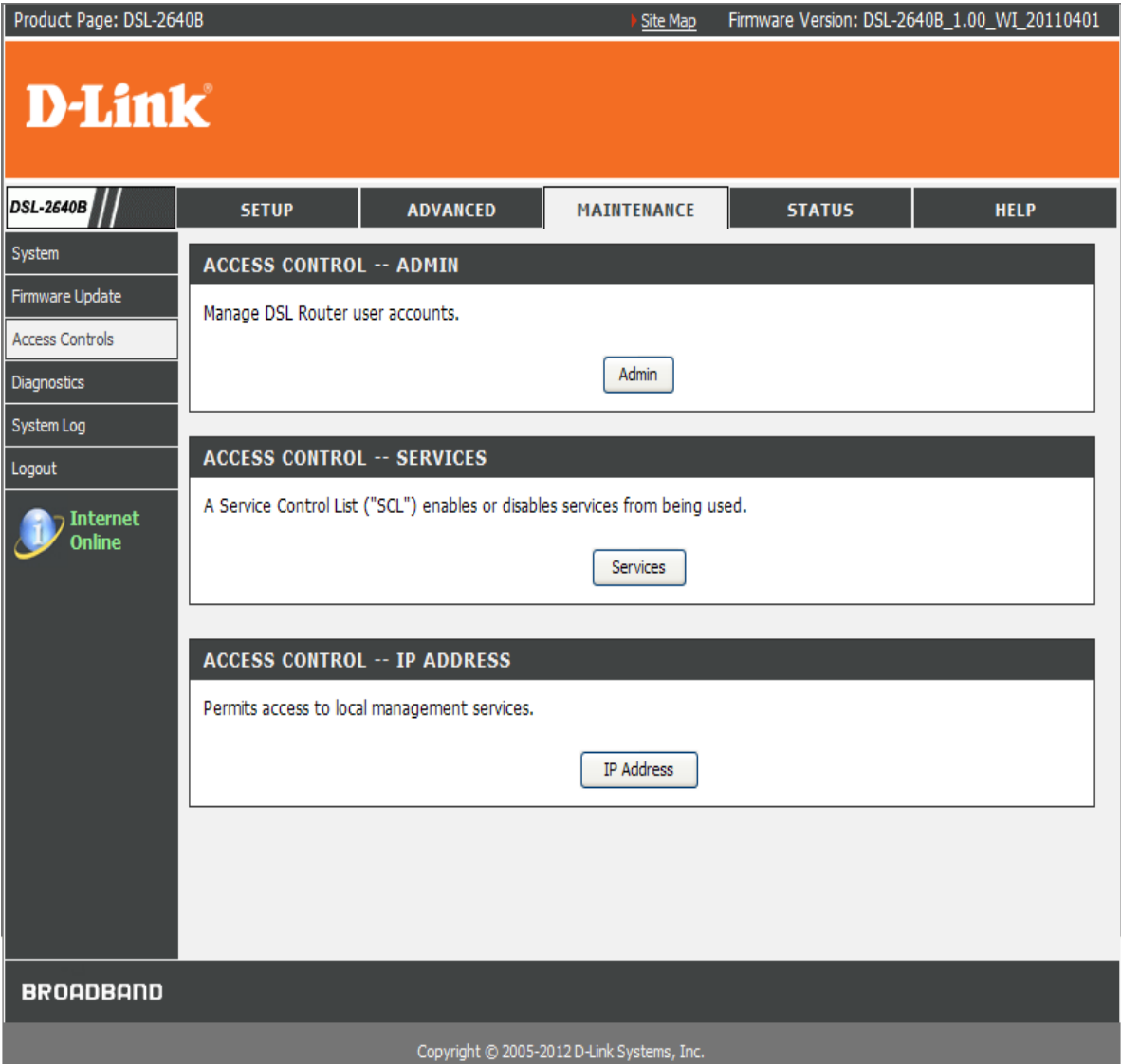## SERVICES

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

IP ADDRESS

Permits access to local management services.

Admin

The Admin option is used to set a password for access to the

Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new router secure.

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

ADMINISTRATOR SETTINGS

Username:	(Click to Select) ▾
Old Password:	
New Password:	
Confirm Password:	

[Apply] [Cancel]

Admin Password

Enter a password for the user "admin", who will have full access to the Web-based management interface.
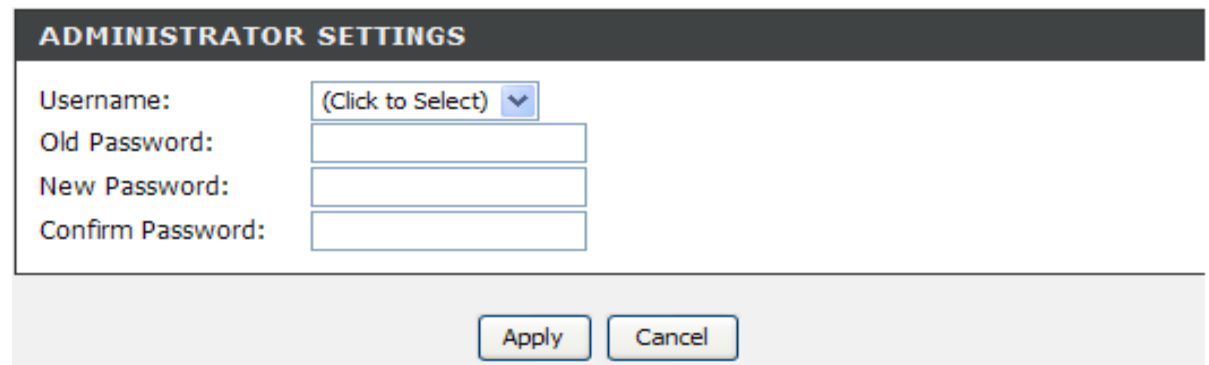
Support Password

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

User Password

Allows end user to view configuration settings and statistics, as well as update the router's firmware.

Services
Allows access to the router via FTP, HTTP, ICMP, SSH,

TELNET, and TFTP.

FTP: File Transfer Protocol

HTTP: Hypertext Transfer Protocol

ICMP: Internet Control Message Protocol

SSH: is a network protocol that allows data to be exchanged using a secure channel between two networked devices.

TELNET: is a network protocol used on the Internet or local area networks to provide a bidirectional interactive text-oriented communications facility using a virtual terminal connection.

TFTP: Trivial File Transfer Protocol is a file transfer protocol known for its simplicity.

ACCESS CONTROL -- SERVICES

Service	LAN	WAN	Remote WAN Port
FTP	☐ Enabled	☐ Enabled	2121
HTTP	☑ Enabled	☐ Enabled	80
ICMP	☑ Enabled	☐ Enabled	
SSH	☐ Enabled	☐ Enabled	22
TELNET	☐ Enabled	☐ Enabled	23
TFTP	☐ Enabled	☐ Enabled	69

Apply   Cancel

LAN
Accesses the DSL router from the local network (LAN) side.

WAN
Accesses the DSL router from the WAN side.

Press the **Apply** button to take it effect.

IP Address

When enabled allows the filtering of IP address that can

access the router. This works in conjunction with **Access Control - Services**

Type the **IP Address** which you want to control the device.

Press the **Apply** button to take it effect.

DIAGNOSTICS

This page shows the result of your router's self diagnostic and connection test results. The Internet connectivity status will only show **PASS** if you have correctly configured your Internet connection and your router is currently online.

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

INTERNET CONNECTIVITY CHECK

Choose the **Virtual Circuit** interface and then click on the **Rerun Diagnostic Tests** button to run the diagnostics again.

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

SYSTEM LOG

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

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

The System Log dialog allows you to view the System Log and configure the System Log options.
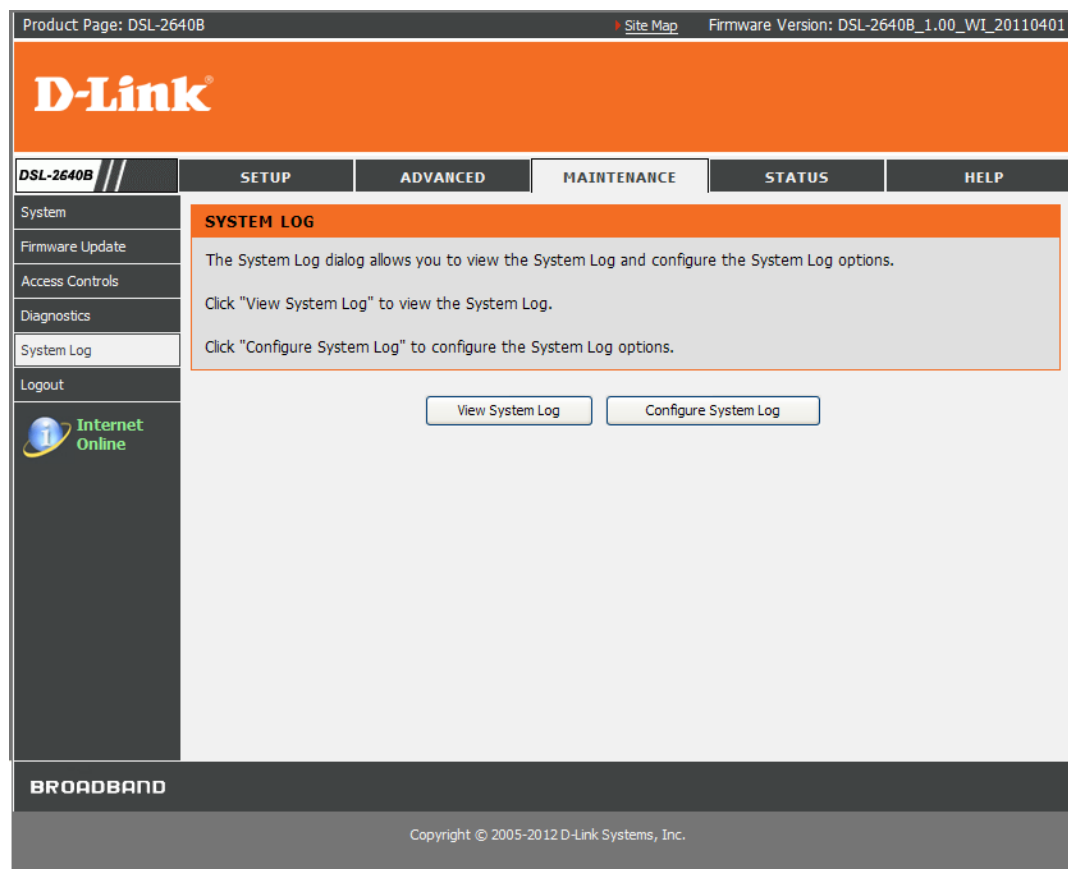
Click "**View System Log**" to view the System Log.

Click "**Configure System Log**" to configure the System Log options.

VIEW SYSTEM LOG

It links to the STATUS/Logs and the table lists the system log.

CONFIGURE SYSTEM LOG

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

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

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

Server IP Address:
IP address of the remote system log server

Server UDP Port:
UDP port number of the remote system log server

Press the **Apply** button to tale it effect.

SYSTEM LOG -- CONFIGURATION

Log: ⦿ Disable ◯ Enable

Log Level: Debugging
Display Level: Error
Mode: Local

Apply   Cancel

Troubleshooting

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

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:
    - Internet Explorer 6.0 or higher
    - Firefox 3.5 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.

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.
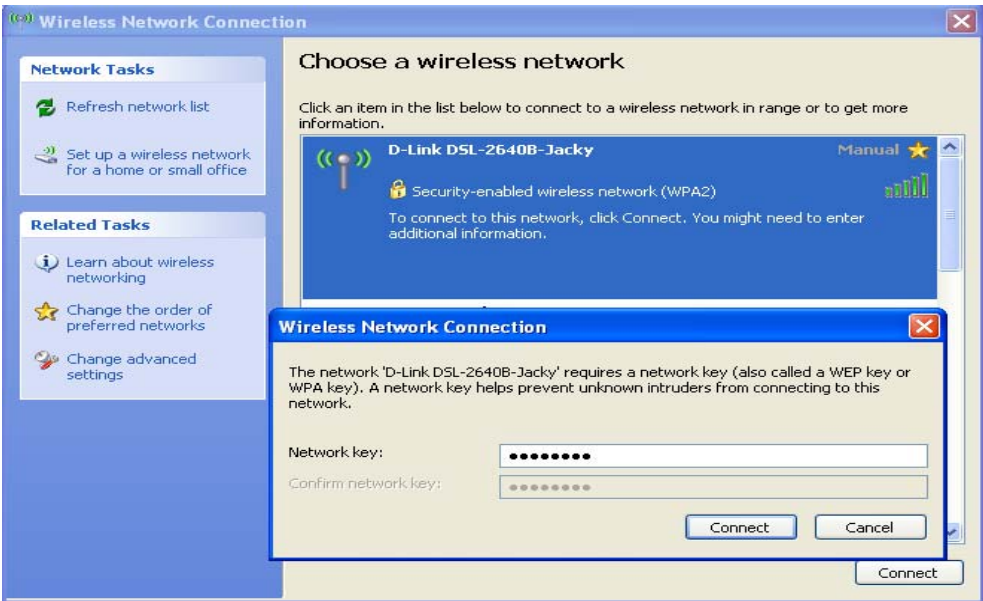
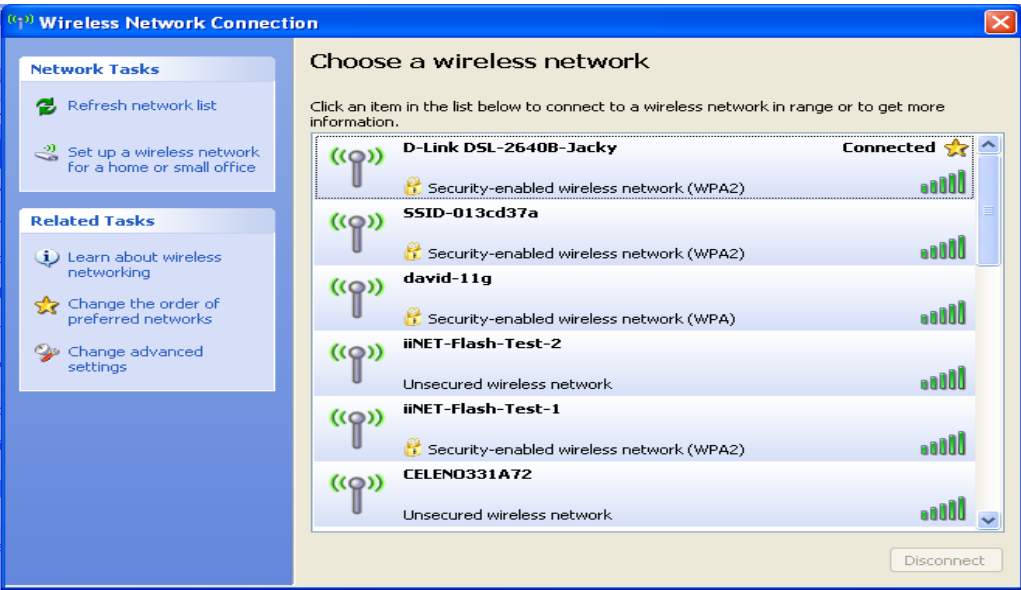# How to connect to the router via a Wireless device in XP/ Vista/ Win 7 and MAC OS X

1. **XP**

Step 1 Remember to enable the "use Windows to configure my wireless network setting" and push the "View Wireless Network" button
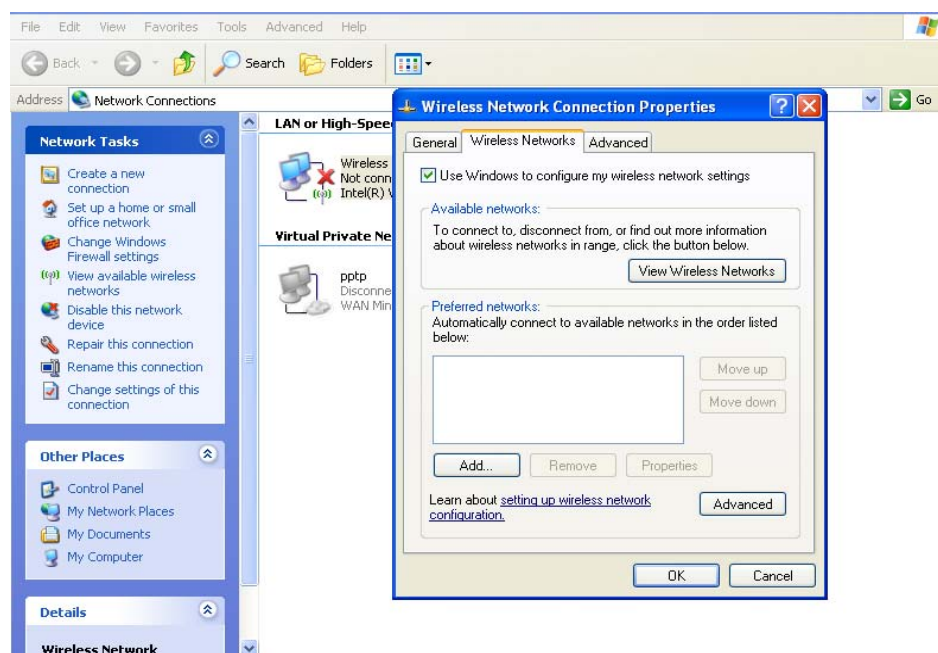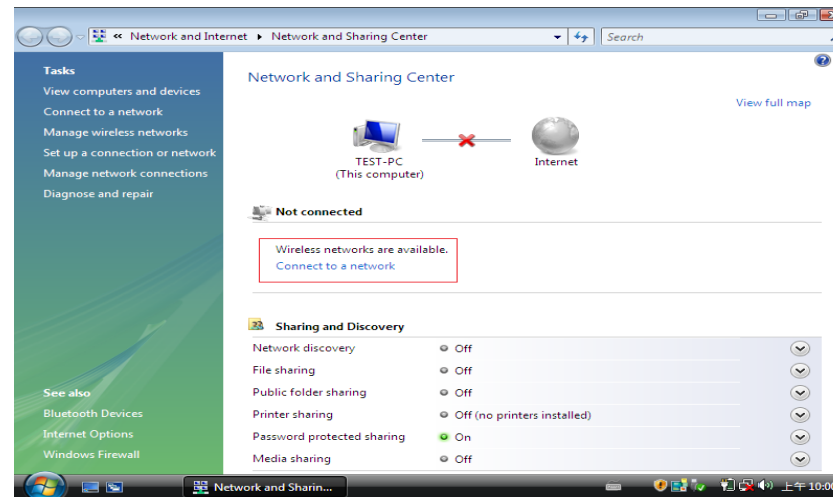
Step 2 Choose the SSID and type the Network key

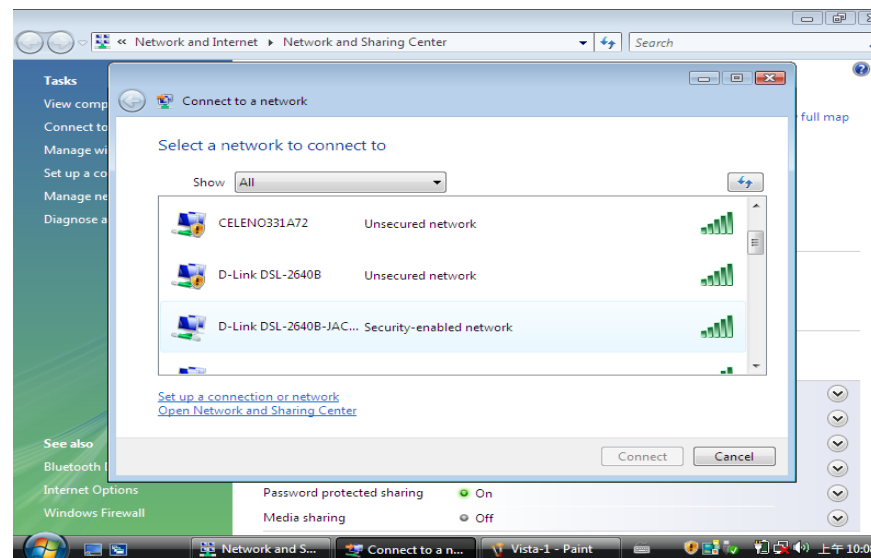**Step 3** You will see the SSID is connected.

2. Vista

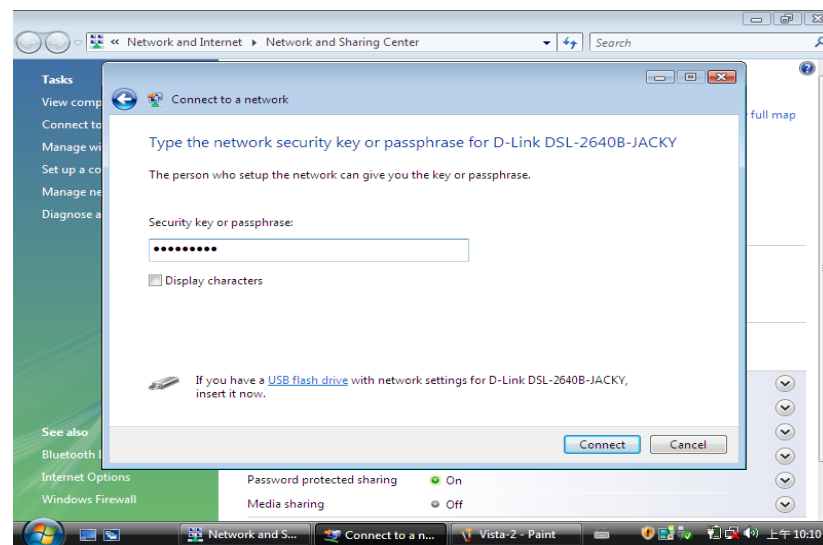**Step 1** Launch the Network and Sharing Center and click the Connect to a network.
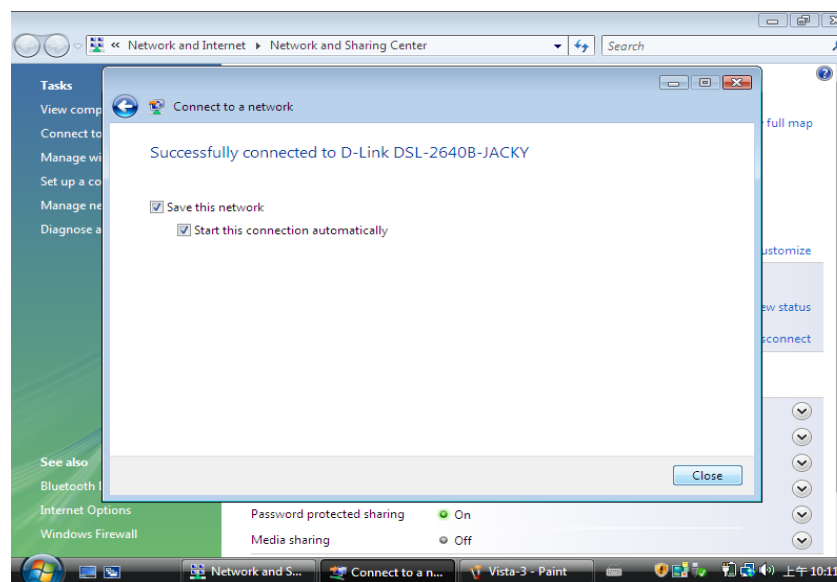

Step2 Choose the SSID which you want to link

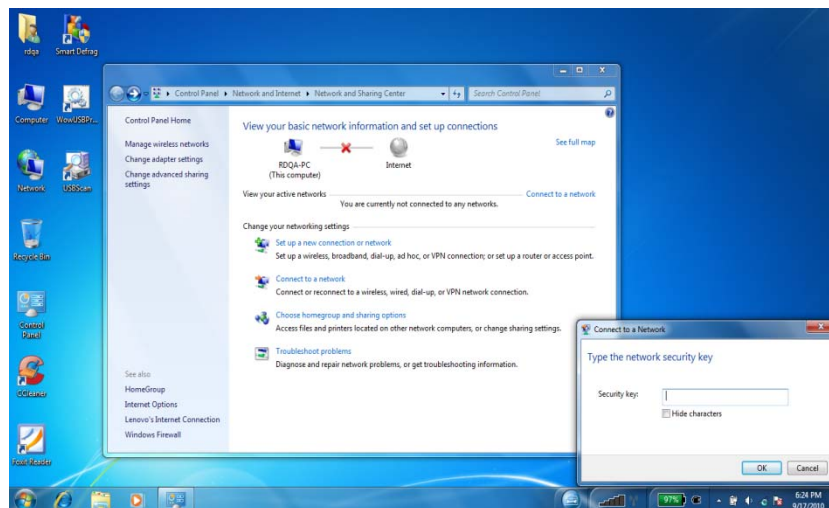**Step 3** Type the security key and click the Connect button

Step 4 You can see the successfully information.
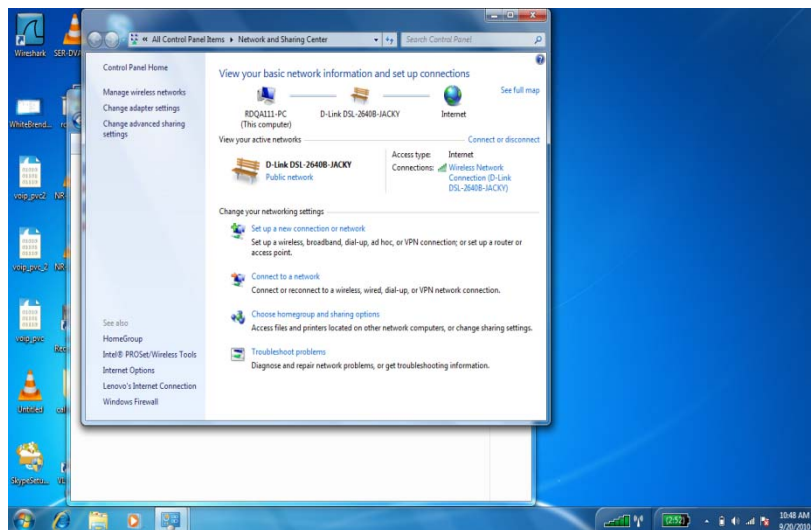
3. Windows 7

Step 1 Choose the "Connect to a Network" and choose the SSID which you want to link, and then type the Security key.

Step 2 You can see the successfully information.
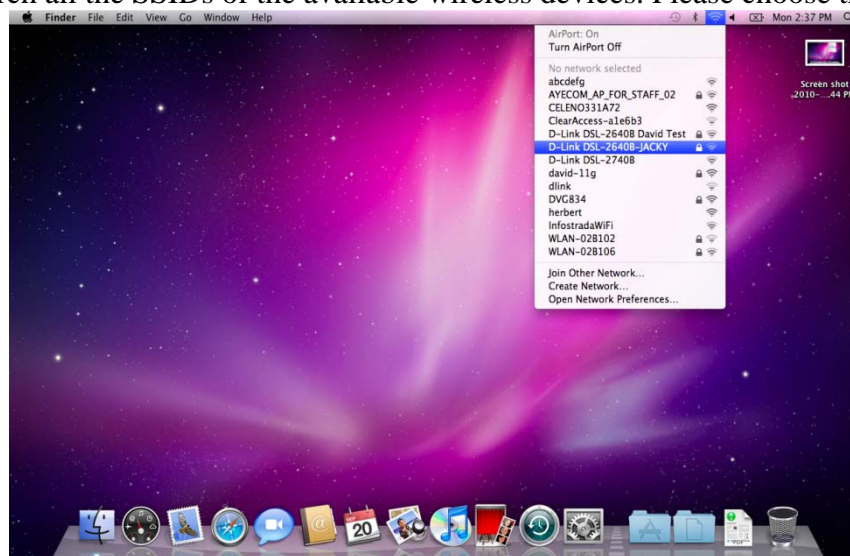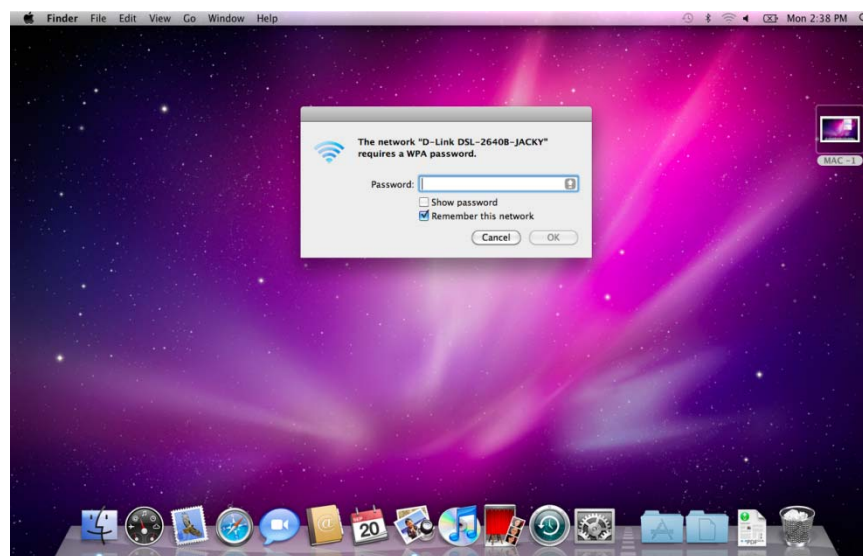
4. MAC OS

Step 1. Double click the wireless icon and it will search all the SSIDs of the available wireless devices. Please choose the SSID which you want to connect to.

Step 2 Please type the security key

Step 3 You can see it appears a ∨ symbol on the wireless device which you want to connect to. It means the wireless is successful to connect to it now.

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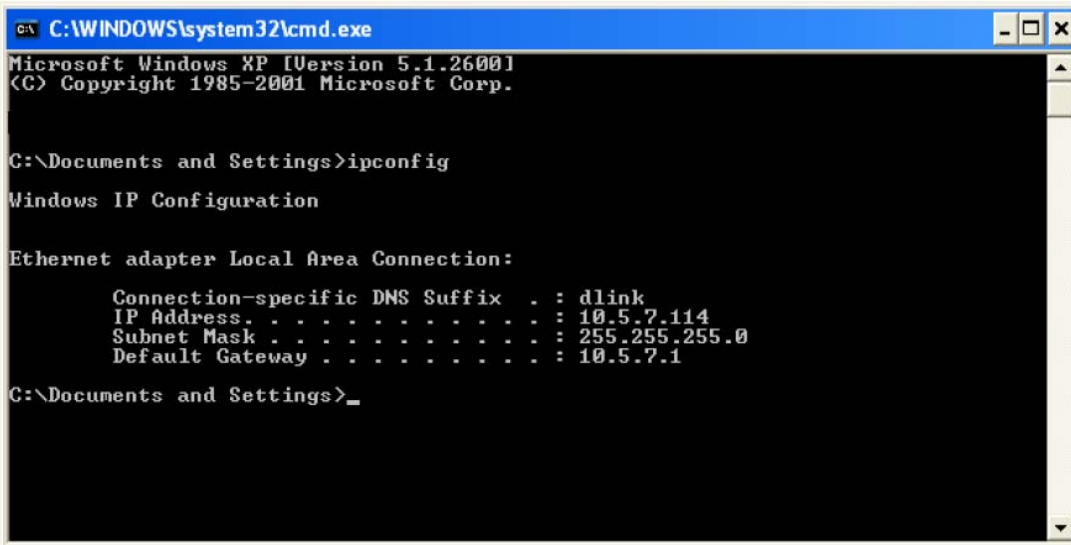
Click on **Start** > **Run**. In the run box type **cmd** and click on the **OK**.

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.

```
C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [Version 5.1.2600]
<C> Copyright 1985-2001 Microsoft Corp.


C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

Statically Assign an IP address

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

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

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

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

Step 4
Click on the **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.
Example: If the router's LAN IP address is 192.168.0.1, 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.
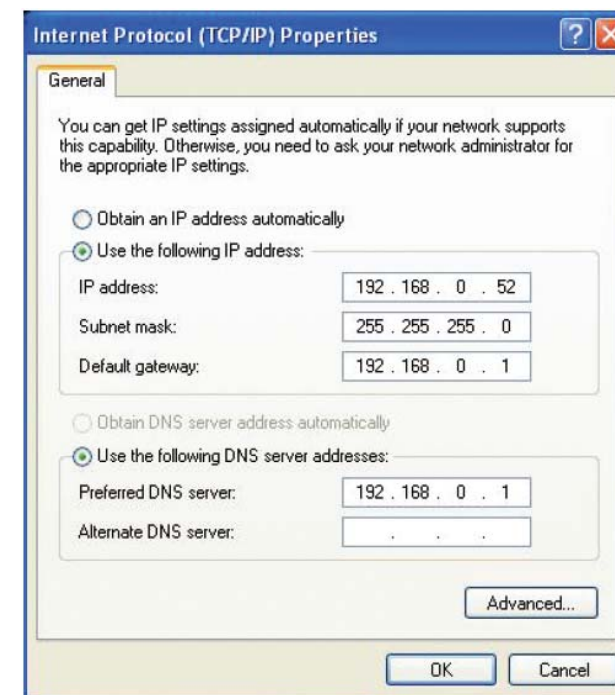
Technical Specifications

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

ADSL2 Standards
- ITU G.992.3 (G.dmt.bis) Annex A
- ITU G.992.4 (G.lite.bis) Annex A

ADSL2+ Standard
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
- G.dmt full rate downstream: up to 8 Mbps / upstream: up to 1 Mbps
- G.lite: ADSL downstream up to 1.5 Mbps / upstream up to 512 Kbps
- G.dmt.bis full rate downstream: up to 12 Mbps / upstream: up to 12 Mbps
- ADSL2+ full rate downstream: up to 24 Mbps / upstream: up to 1 Mbps

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

WIRELESS LAN
- 802.11b/g standards
- Wireless speed: up to 150Mbps (802.11n)
- Frequency range: 2.4 GHz to 2.484G Hz
- Antennas: 1 non-detachable dipole antenna.
- WEP data encryption
- WPA/WPA2 (Wi-Fi Protected Access) security
- Multiple SSID
- 802.11e Wireless QoS (WMM/WME)
- MAC address-based access control

* Maximum wireless signal rate derived from IEEE Standard 802.11n 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.