



User Manual

Wireless N300 ADSL2+ Modem Router

DSL-2750B

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
1.00	May 15, 2015	• Release for revision E1

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Apple®, Apple logo®, Safari®, iPhone®, iPad®, iPod touch® and Macintosh® are trademarks of Apple Inc., registered in the U.S. and other countries. App StoreSM is a service mark of Apple Inc. ChromeTM browser, Google PlayTM and AndroidTM are trademarks of Google Inc. Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

Copyright © 2015 by D-Link Corporation, Inc. All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Corporation, Inc.

Power Usage

This device is an Energy Related Product (ErP) that automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed.

Network Standby: 4.58 W

Switched Off: 0.23 W

Table of Contents

Product Overview	1	2.4G Advanced Wireless	28
Package Contents.....	1	Advanced Settings	29
System Requirements	2	MAC Filtering.....	31
Introduction	3	Security Settings	32
Features.....	4	WPS Settings	33
LEDs	5	ALG.....	34
Back.....	6	FTP.....	35
Installation	7	Port Forwarding	36
Before you Begin.....	7	Port Trigger	37
Wireless Installation Considerations.....	8	DMZ	38
Hardware Installation.....	9	SAMBA	39
Getting Started	10	3G WAN Configuration.....	40
Web-based Configuration Utility.....	10	Parental Control	42
Setup Wizard	11	Website Filter.....	43
Configuration	17	HTTP Content Filter.....	44
Setup.....	17	MAC Filter	45
Internet Setup.....	18	Filtering Options	46
2.4G Wireless	20	IPv4 Filtering.....	47
2.4G Wireless Security	21	IPv6 Filtering.....	48
Local Network.....	22	QoS.....	49
Local IPv6 Network.....	24	Add QoS Classification Rules	50
USB Setup.....	25	Anti-Attack Settings.....	52
Time and Date.....	26	Share Protection.....	53
Logout	27	DNS	54
Advanced	28	Dynamic DNS	55
		Network Tools	56
		Port Mapping	57

IGMP Proxy	58	DHCP Clients	85
IGMP Snooping.....	59	Logs	86
MLD Configuration.....	60	Statistics	87
UPnP	61	Route Info	88
DSL	62	Help	89
Routing.....	63	Connect a Wireless Client to your Router	90
Static Route	64	WPS Button	90
IPv6 Static Route	65	Windows® 8.....	91
Policy Route	66	WPA/WPA2	91
RIP.....	67	Windows® 7.....	93
RIPng	68	WPA/WPA2	93
Schedules	69	Windows Vista®	96
NAT.....	70	WPA/WPA2	97
Management.....	71	Windows® XP	99
System	71	WPA/WPA2	100
Firmware Update	72	Troubleshooting	102
Access Controls.....	73	Wireless Basics	106
Account Password	74	What is Wireless?.....	107
Local Access Control	75	Tips.....	109
Remote Access Control.....	76	Wireless Modes.....	110
IP Address	77	Networking Basics	111
Diagnostics	78	Check your IP address.....	111
DSL Test	79	Statically assign an IP address.....	112
Traceroute.....	80	Technical Specifications	113
Ping	81	Regulatory Information	114
System Log.....	82		
Status	83		
Device Info	83		
Wireless Clients.....	84		

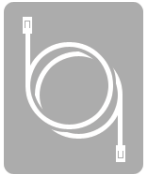
Package Contents



Wireless N300 ADSL2+ Modem Router



ADSL Telephone Cable



Ethernet Cable



Quick Installation Guide



Power Adapter



CD-ROM

If any of the above items are missing, please contact your reseller.

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

System Requirements

Network Requirements	<ul style="list-style-type: none">• An ADSL Internet service• IEEE 802.11b, 802.11g or 802.11n wireless clients• 10/100 Ethernet
Web-based Configuration Utility Requirements	<p>Computer with the following:</p> <ul style="list-style-type: none">• Windows®, Macintosh, or Linux-based operating system• An installed Ethernet adapter <p>Browser Requirements: Microsoft Internet Explorer® v7, Mozilla® Firefox® v9.0, Google® Chrome 16.0, or Safari® v4 or later</p> <p>Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.</p>

Introduction

The DSL-2750B Wireless N300 ADSL2+ Modem Router is a versatile, high-performance router for home and the small office. With integrated ADSL2/2+ supporting up to 24 Mbps 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 link to the outside world.

High-speed ADSL2/2+ Internet Connection - The latest ADSL2/2+ standards provide Internet transmission of up to 24 Mbps downstream, 1 Mbps 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 Wireless Connection with Maximum Security - This router maximizes wireless performance by connecting to computer interfaces and staying 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 prevent unauthorized access to your 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 for traffic congestion. This QoS feature allows users to enjoy high-speed ADSL transmission for applications such as VoIP and streaming multimedia over the Internet.

* Maximum wireless signal rate derived from IEEE Standard 802.11b, 802.11g, and 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 conditions will adversely affect wireless signal range.

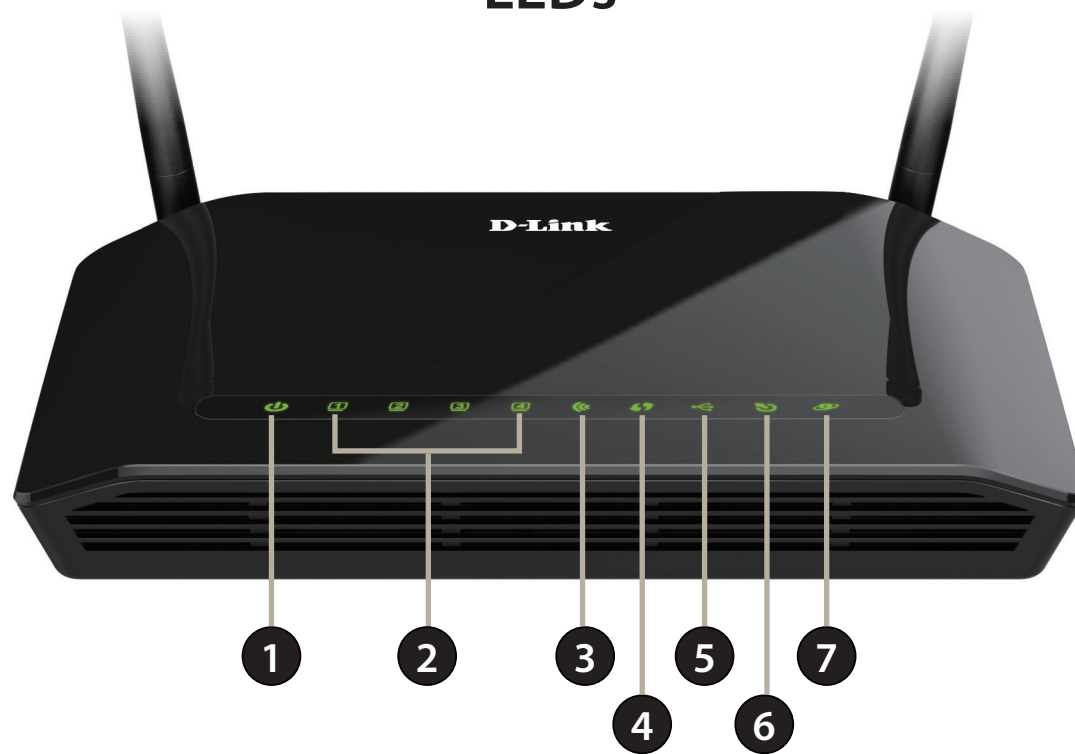
Features

- **Faster Wireless Networking** - The DSL-2750B provides up to 300 Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.
- **Compatible with 802.11b and 802.11g Devices** - The DSL-2750B is still fully compatible with the IEEE 802.11b and g standards, so you can use keep your existing 802.11b and g devices.
- **Precise ATM Traffic Shaping** - Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish Quality of Service for ATM data transfer.
- **High Performance** - Very high rates of data transfer are possible with the router-providing up to 24 Mbps downstream for ADSL2+.
- **Full Network Management** - The DSL-2750B incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via a Telnet connection.
- **Easy Installation** - The DSL-2750B uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the router.
- **USB Support** - The DSL-2750B provides a USB port for easy file sharing and printer sharing. The DSL-2750B supports USB storage devices to share files through a SAMBA file server, an FTP server, or a Web file server. It also supports sharing USB printers to network members. Besides the sharing function, the DSL-2750B also supports connection to the Internet via a USB 3G modem.
- **IPv6 Connection Support** – Compatible with IPv6 networks, the DSL-2750B provides several connection types: Link-local, Static IPv6, DHCPv6, Stateless Autoconfiguration, PPPoE, IPv6 in IPv4 Tunnel and 6to4.

* Maximum wireless signal rate derived from IEEE Standard 802.11b, 802.11g, and 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 conditions will adversely affect wireless signal range.

Hardware Overview

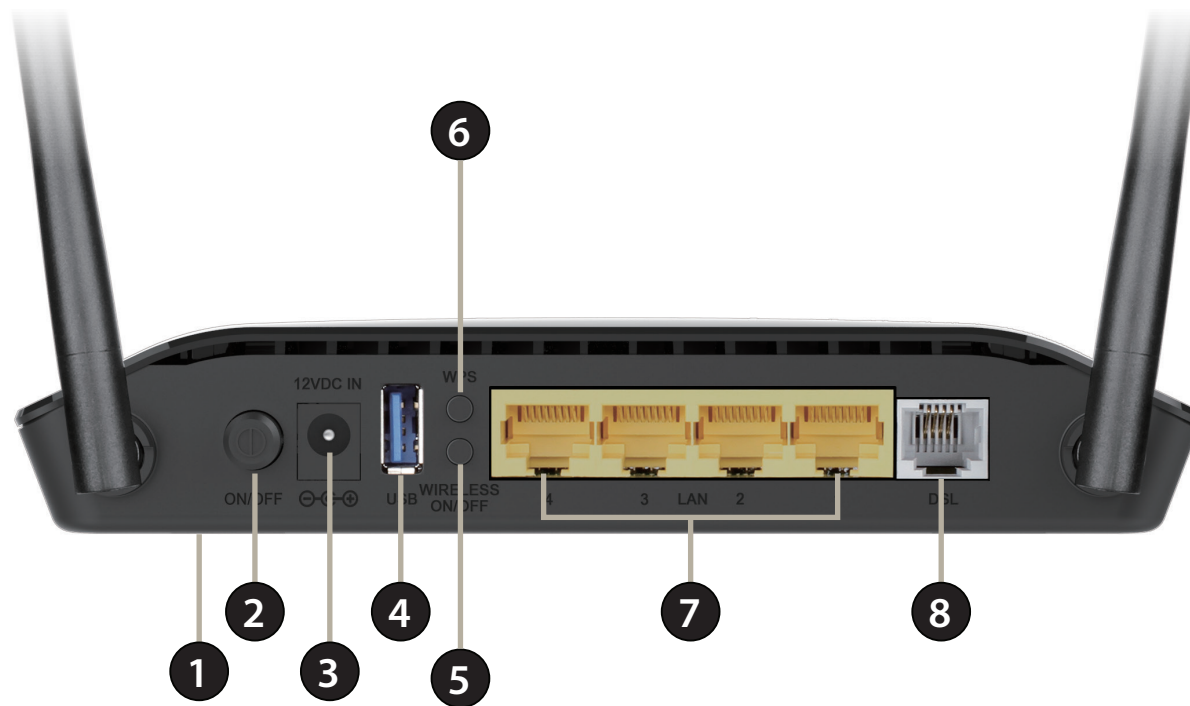
LEDs



1	Power LED	A solid green light indicates the unit is powered on. A red light indicates device malfunction.
2	LAN LEDs 1-4	A solid green light indicates a valid link on startup. These lights blink when there is activity currently passing through the Ethernet port.
3	WLAN LED	A solid green light indicates a wireless connection. A blinking green light indicates activity on the WLAN.
4	WPS LED	A solid blue light indicates a successful connection with the client. A blinking light indicates WPS is triggered and looking for a client.
5	USB LED	A solid light indicates that the wireless networks are ready.
6	ADSL LED	A solid 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.
7	Internet	A solid green light indicates a successful Internet connection. A blinking light indicates Internet is connected and data is being transmitted. A red light indicates that IP assignment has failed.

Hardware Overview

Back



1	Reset Button	Insert a paperclip in the hole and wait for several seconds to reset the router to default settings.
2	Power Button	Press to power the router on or off.
3	Power Receptor	Receptor for the supplied power adapter.
4	USB Port	Connect a USB storage device to this port to share media to your network.
5	Wireless On/Off	Press this button to enable or disable WLAN.
6	WPS Button	Press this button to start connecting a WPS-enabled client.
7	Ethernet Ports	Connect 10/100 Ethernet devices such as computers, switches, storage (NAS) devices and game consoles.
8	ADSL Port	Using the supplied telephone cable, connect your DSL modem to this port.

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 configure the router with the computer that was last connected directly to your modem.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using the router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoET, BroadJump, or EnterNet 300 from your computer or you will not be able to connect to the Internet.

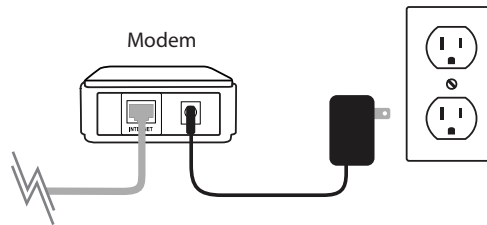
Wireless Installation Considerations

The D-Link wireless router 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:

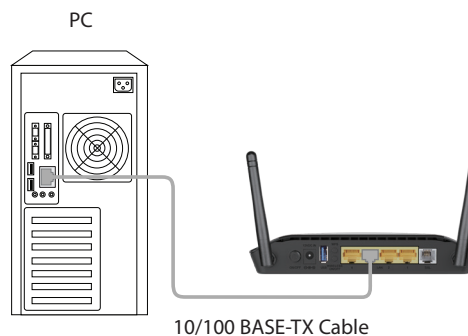
1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between 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 2.4 GHz 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 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

Hardware Installation

1. Turn off and unplug your DSL broadband modem. This is required.



2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.
3. Unplug the Ethernet cable from your modem (or existing router if upgrading) that is connected to your computer. Plug it into the LAN port labeled **1** on the back of your router. The router is now connected to your computer.



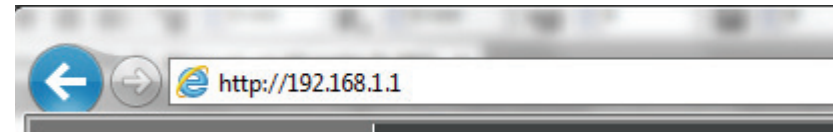
Getting Started

Web-based Configuration Utility

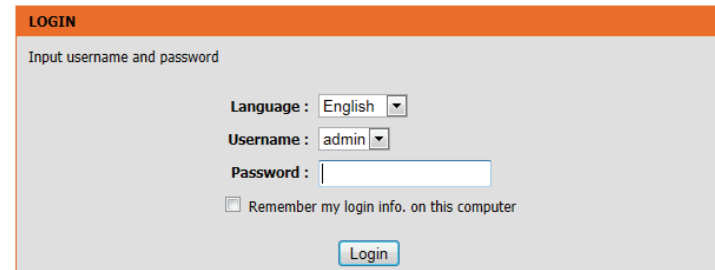
This section will show you how to configure your D-Link wireless access point using the web-based configuration utility.

If you wish to change the default settings or adjust the configuration of the DSL-2750B you may use the web-based configuration utility.

To access the configuration utility, open a web browser such as Internet Explorer and enter **http://192.168.1.1** in the address field.



Select **admin** from the drop-down menu and then enter your password. The default password is **admin**. You will be directed to the **Setup Wizard** page.

A screenshot of the "LOGIN" page in the web-based configuration utility. The page has an orange header with the word "LOGIN" in white. Below the header, the text "Input username and password" is displayed. There are three input fields: "Language" with a dropdown menu set to "English", "Username" with a dropdown menu set to "admin", and "Password" with a text input field. Below these fields is a checkbox labeled "Remember my login info. on this computer". At the bottom of the form is a blue "Login" button.

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

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

Setup Wizard

Click **Setup Wizard** to configure your router.

If you want to configure the access point manually without running the wizard, skip to **Configuration** on page 17.

Click **Next** to continue.

INTERNET CONNECTION WIZARD

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

[Setup Wizard](#)

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

WELCOME TO SETUP WIZARD

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

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

This section of the wizard enables you to use an international time server to set the internal time and date for the router.

Automatically Synchronize: Enable or disable automatic synchronisation with an Internet Time Server.

1st NTP Time Server: Specify an address for the primary Internet Time Server.

2nd NTP Time Server: Specify an address for the secondary Internet Time Server.

Time Zone: Select your time zone from the drop down menu.

Enable Daylight Saving: Enable or disable daylight saving.

Daylight Saving Start/End: Specify the time and date when daylight saving should start/end.

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

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can 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.

TIME SETTING

Automatically synchronize with Internet time servers

1st NTP time server :

2nd NTP time server :

TIME CONFIGURATION

Time Zone :

Enable Daylight Saving

Daylight Saving Start : Mon Day Hour Min Sec

Daylight Saving End : Mon Day Hour Min Sec

This section of the wizard enables you to configure your Internet connection type. Select the appropriate wan connection type which is provided by your ISP.

If the router detected or you selected **PPPoE** or **PPPoA**, enter your PPPoE/PPPoA username and password and click **Next** to continue.

Note: Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.

If the router detected or you selected **Static IP**, enter your Static IP information as supplied by your ISP. Click **Next** to continue.

If the router detected or you selected **Bridge** or **Dynamic IP**, click **Next** to continue.

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

Please select your ISP (Internet Service Provider) from the list below.

INTERNET SETUP

Country :

Internet Service Provider :

DSL Mode :

Protocol :

Encapsulation Mode :

VPI : (0-255)

VCI : (32-65535)

PPPOE/PPPOA

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

Username :

Password :

Confirm Password :

This section of the wizard enables you to configure your 2.4 GHz wireless network and security settings. If you prefer not to, untick the **Enable Your Wireless Network** box.

Choose a network name for your wireless network, and choose if you wish to make the wireless network **visible** or **invisible**.

It is highly recommended to secure your wireless network. Select from the available options, and enter the security key below.

Click **Next** to continue.

STEP 3: CONFIGURE 2.4G WIRELESS NETWORK → 4 → 5

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

Enable Your Wireless Network :

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

Wireless Network Name (SSID) :

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

Visibility Status : Visible Invisible

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

None	Security Level	Best
<input type="radio"/> None	<input type="radio"/> WEP	<input checked="" type="radio"/> WPA/WPA2-PSK
		<input type="radio"/> WPA2-PSK

Security Mode:WPA/WPA2-PSK
Select this option if your wireless adapters support WPA/WPA2-PSK.

Now, please enter your wireless security key :

WPA/WPA2-PSK Pre-Shared Key :

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

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

To change the password, enter the **Current Password**, then enter the **New Password**. Finally, re-enter the new password under **Confirm Password**.

Click **Next** to continue.

STEP 4: ACCOUNT PASSWORD → 5

Use the fields below to change or create passwords. Note: Password cannot contain a space.

ACCOUNT PASSWORD

Username :

Current Password :

New Password :

Confirm Password :

Your router is now set up.

A summary page will be displayed, showing the current settings for your WAN and 2.4 GHz wireless network. It is recommended that you make a note of this information for future reference.

Click **Finish** to save your network settings.

In order for your network settings to take effect the AP will reboot automatically.

When the device has finished rebooting the main screen will display.

STEP 5: SAVE AND APPLY CHANGES

Setup complete. Click "Back" to review or modify settings.

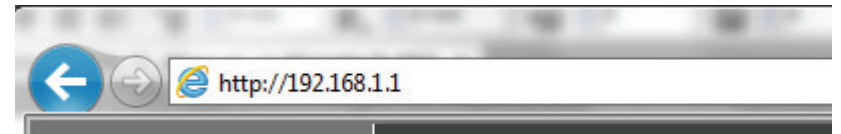
If your Internet connection does not work, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

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

Time Settings :	1
NTP Server 1 :	ntp1.dlink.com
NTP Server 2 :	ntp.dlink.com.tw
Time Zone :	CET
Daylight Saving Time :	1
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	LLC
802.1Q VLAN ID :	N/A
Priority :	N/A
Username :	123
Password :	*****
SSID (2.4G):	dlink-93ad95
Visibility Status :	Visible
Encryption :	WPA/WPA2 Mixed
Pre-Shared Key :	e12dd876gh
WEP Key :	N/A
New password :	333111

Configuration Setup

If you wish to change the default settings or adjust the configuration of the DSL-2750B you may use the web-based configuration utility. To access the configuration utility, open a web-browser such as Internet Explorer and enter the address of the router (**http://192.168.1.1**).



Select **admin** from the drop-down menu and then enter your password. The default password is **admin**. Click **login** to proceed to the web configuration home page.

A screenshot of a web page titled "LOGIN". The page has an orange header bar with the word "LOGIN" in white. Below the header, the text "Input username and password" is displayed. There are two input fields: "Username:" with a dropdown menu showing "admin" and a small downward arrow, and "Password:" with a text box containing six black dots. Below these fields is a checkbox labeled "Remember my login info. on this computer". At the bottom of the form is a blue button with the text "login".

Internet Setup

Click **Internet Setup** on the left menu to configure your connection manually.

If you want to configure your router to connect to the Internet using the wizard, click **Wizard** on the left menu and you will be directed to the Quick Setup Wizard.

Click the **Add** button to reveal the DSL configuration options, or click **Edit** to change an existing configuration.

The following parameters will be available for configuration:

VPI: Virtual path identifier (VPI) is the virtual path between two points in an ATM network. Its valid value is between 0 and 255. Enter the correct VPI provided by your ISP. By default, VPI is set to 1.

VCI: Virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is between 1 and 65535. Enter the correct VCI provided by your ISP. By default, VCI is set to 32.

Service Category: Select the Quality of Service types for this Virtual Circuit. The ATM QoS types include CBR (Constant Bit Rate), VBR (Variable Bit

Rate) and UBR (Unspecified Bit Rate). These QoS types are all controlled by the parameters specified below, including PCR, SCR and MBS.

Peak Cell Rate: Peak cell rate (PCR) is the maximum rate at which cells can be transmitted along a connection in the ATM network.

INTERNET SETUP

Choose "Add", "Edit", or "Delete" to configure WAN interfaces.

DEFAULT GATEWAY

Default GateWay Mode Auto Manual

Apply Cancel

DSL CONFIG

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	V4 Default Gateway	V6 Default Gateway	3G	Action
<input type="radio"/>	8/35	0	LLC	DSL_DHCP_0_01	DHCP	1			-	1	-

INTERNET SETUP

This screen allows you to configure an WAN connection.

ATM PVC CONFIGURATION

VPI : 0 (0-255)

VCI : 35 (32-65535)

Service Category : UBR With PCR

Peak Cell Rate : 0 (cells/s)

Sustainable Cell Rate : 0 (cells/s)

Maximum Burst Size : 0 (cells)

CONNECTION TYPE

Protocol : Bridging

Encapsulation Mode : LLC

802.1Q VLAN ID : 0 (0 = disable, 1 - 4094)

Enable Service :

Firewall Enable :

Service Name : D_Bridging_0_2

Sustainable Cell Rate: Sustainable cell rate (SCR) is the maximum rate that traffic can pass over PVC without the risk of cell loss.

Maximum Burst Size: Maximum burst size (MBS) is the maximum number of cells that can be transmitted at the PCR.

Protocol: Select the appropriate protocol from the drop-down menu. You can choose between PPPoE/PPPoA, MER, IPoA, or Bridging. The configuration options will change accordingly.

Encapsulation Mode: You can select LLC or VCMUX. In this example, the encapsulation mode is set to LLC.

802.1Q VLAN ID: Select this option to Activate/Deactivate the 4094 VID on the 4 different queues. VID (VLAN ID) is the identification of the VLAN, which is basically used by the standard 802.1Q. It has 12 bits and allows the identification of 4096 (2^{12}) VLANs. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094

Enable Service: Choose to enable or disable the service.

Firewall Enable: Choose to enable or disable the firewall.

Service Name: Enter a name for the service.

Click **Apply** to save your Internet Setup settings.

INTERNET SETUP

This screen allows you to configure an WAN connection.

ATM PVC CONFIGURATION

VPI : (0-255)

VCI : (32-65535)

Service Category :

Peak Cell Rate : (cells/s)

Sustainable Cell Rate : (cells/s)

Maximum Burst Size : (cells)

CONNECTION TYPE

Protocol :

Encapsulation Mode :

802.1Q VLAN ID : (0 = disable, 1 - 4094)

Enable Service :

Firewall Enable :

Service Name :

2.4G Wireless

On this page the user can configure the Wireless settings for this device. There are 2 options to configure 2.4G Wireless Settings. Firstly, the user can choose to make use of the **Wireless Basic** settings. Secondly, the user can choose to make use **Wireless Security** settings.

Click the **Wireless Basic** button to view the basic wireless configuration options .

WIRELESS SETTINGS -- WIRELESS BASIC

Configure your wireless basic settings.

WIRELESS SETTINGS -- WIRELESS SECURITY

Configure your wireless security settings.

WIRELESS BASIC CONFIGURATION

Enable Wireless :

AP Isolate :

SSID :

Visibility Status : Visible Invisible

Continent/Country :

802.11 Mode :

Band Width :

Wireless Channel :

Enable Wireless: Choose to enable or disable the wireless networks.

AP Isolate: Choose to enable or disable wireless isolation.

SSID: Enter an SSID for the wireless network.

Visibility Status: Choose to enable SSID broadcast so other wireless devices can find the network.

Continent/Country: Depending on what country the router is used in, regulations provide for the router to automatically set the transmit power and frequencies that may be used in that country.

802.11 Mode: Select from the drop-down menu the mode of operation you require.

Bandwidth: Use the drop-down menu to select the channel bandwidth.

Wireless Channel: Use the drop-down menu to select a wireless channel, or let the router scan automatically.

2.4G Wireless Security

Wireless security helps to prevent unauthorized users from accessing your wireless network, or seeing data being passed between the router and wireless clients. The DSL-2750B supports two popular wireless security protocols, you should select a protocol based on the wireless clients which will be accessing your network.

Wired Equivalent Privacy (WEP) - This is an older form of wireless security and should only be used if your wireless clients do not support the newer WPA or WPA2 protocols.

Wi-Fi Protected Access (WPA/WPA2) - This is a newer and more secure protocol for wireless security. It uses a cipher combined with a pre-shared key (password) to encrypt data being sent over the wireless network. It is recommended that you use this security method if it is supported by your wireless clients.

Wireless Security Mode: Select a wireless security encryption option. You can also choose to not use one by selecting **None**, but this is not recommended.

WPA Mode: Choose **Personal** or **Enterprise**.

Encryption Mode: Select TKIP + AES.

Group Key Update Interval: Enter the time in seconds that the group key will be automatically updated.

Pre-Shared Key: Enter a string of 8 characters to set a password for your wireless network.

RADIUS server IP Address: For Enterprise mode, enter the IP address of your network's RADIUS server here.

RADIUS server Port: Enter the port of your network's RADIUS server here.

RADIUS server Shared Secret: Enter the password of your network's RADIUS server here.

WIRELESS SECURITY

In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.

WIRELESS SECURITY MODE

Wireless Security Mode :

WPA/WPA2 MIXED

WPA Mode :
 Encryption Mode :
 Group Key Update Interval : (60 - 65535)

PRE-SHARED KEY

Pre-Shared Key : (ASCII < 64, HEX = 64)

Local Network

When configuring the router for the first time, we recommend that you click use the **Internet Connection Setup Wizard**, and follow the instructions on the screen. This wizard is designed to assist user with a quick and easy method to configure the Internet Connectivity of this router.

Anytime during the Internet Connection Setup Wizard, the user can click on the **Cancel** button to discard any changes made and return to the main page.

Router IP Address: Enter the IP address of LAN interface. It is recommended to use an address from a block reserved for private use. This address block is 192.168.1.2 - 192.168.1.254.

Subnet Mask: Enter the subnet mask of LAN interface. The range of subnet mask is from 255.255.255.0 to 255.255.255.254.

Domain Name: Enter a domain to be used as a static host name.

Check "**Configure the second IP Address and Subnet Mask for LAN**" to enable a local alias IP address if required.

IP Address: Enter the alias IP address.

Subnet Mask: Enter the alias subnet mask.

LOCAL NETWORK

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

ROUTER SETTINGS

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

Router IP Address :

Subnet Mask :

Domain Name :

Configure the second IP Address and Subnet Mask for LAN

IP Address :

Subnet Mask :

DHCP SETTINGS (OPTIONAL)

Use this section to configure the DHCP Relay for your network.

Enable DHCP Relay

Relay IP Address :

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 : to

DHCP Lease Time : (seconds [time not allowed less than 600s])

Use the following DNS server addresses:

Enable DNS Relay

Preferred DNS server :

Alternate DNS server :

Enable DHCP Relay: You can choose **Disabled**, **Enabled** or **Relay**. If set to DHCP server, the router can assign IP addresses, IP default gateway and DNS servers to the host.

Relay IP Address: Enter the desired DHCP relay IP address.

Enable DHCP Server: Enable or disable the DHCP server function.

DHCP IP Address Range: Enter the range of IP addresses the DHCP server can issue from.

DHCP Lease Time: The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change. The default is 259200 seconds.

Enable DNS Relay: If disabled the router will accept the first received DNS assignment from one of the PPPoA, PPPoE or MER enabled PVC(s) during the initial connection setup. If enabled you can enter the IP addresses for primary and secondary DNS servers.

Preferred DNS Server: Enter an address for a preferred DNS server.

Alternate DNS Server: Enter an address for an alternate DNS server.

DHCP Client Class List: Client-class processing enables the DHCP server to assign the client an address from a matching scope.

DHCP Conditional Option: Specify the conditions for DHCP class handling.

DHCP Reservations List: Use this option to reserve specific IP addresses.

Number of Dynamic DHCP clients: Dynamic DHCP clients will be listed here with supporting information.

DHCP SETTINGS (OPTIONAL)

Use this section to configure the DHCP Relay for your network.

Enable DHCP Relay

Relay IP Address :

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 : to

DHCP Lease Time : (seconds [time not allowed less than 600s])

Use the following DNS server addresses:

Enable DNS Relay

Preferred DNS server :

Alternate DNS server :

DHCP CLIENT CLASS LIST

Client Class	Min Address	Max Address	DNS Address

DHCP CONDITIONAL OPTION

Status	Client Class Name	Option Code	Option Value

DHCP RESERVATIONS LIST

Status	Computer Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Computer Name	MAC Address	IP Address	Expire Time
07904PCWIN7E	44:37:e6:b5:ff:3d	192.168.1.2	81718

Local IPv6 Network

This section enables you to specify various IPv6 settings.

IPv6 Address: Use this option to specify a static IPv6 Address.

Enable RADVD: Enable or disable the Router Advertisement Daemon.

Enable DHCPv6 Server: Enable or disable the DHCPv6 server function.

Lan Address Config Mode: Select either stateless (host requests) or stateful (server provisions) LAN IPv6 addressing.

Start/End Interface ID: Enter the range of IP addresses the DHCPv6 server can issue from.

DHCPv6 Lease Time: The lease time determines the period that the host retains the assigned IP addresses before the IP addresses change.

DHCPv6 Valid Time: Specify the period for which an assigned IPv6 address remains valid.

IPv6 DNS Mode: Allow the router to accept the first received IPv6 DNS assignment from a WAN connection. Alternatively, you can manually enter the IP addresses for primary and secondary IPv6 DNS servers.

WAN Interface: Specify the WAN interface to be used.

Primary DNS: Enter an address for a preferred DNS server.

Secondary DNS: Enter an address for an alternate DNS server.

Get Prefix Mode: Use this option to specify whether IPv6 prefix delegation is assigned manually or via a WAN interface.

WAN Interface: Specify the WAN interface to be used. for IPv6 prefix delegation.

Site Prefix: Manually assign an IPv6 prefix delegation.

IPv6 LAN SETTINGS

Note: Stateful DHCPv6 is supported after the IPv6 address 16-bit. For example: Interface ID range from 1 to ffff, IPv6 address range from 2111:123:123:123::1 to 2111:123:123:123::ffff.

IPv6 ADDRESS

IPv6 Address :

RADVD CONFIGURATION

Enable RADVD :

DHCPV6 CONFIGURATION

Enable DHCPv6 Server :

LAN Address Config Mode : Stateless Stateful

Start Interface ID :

End Interface ID :

DHCPv6 Lease Time :

DHCPv6 Valid Time :

IPv6 DNS Mode : From WAN Manual

WAN Interface :

Primary DNS :

Secondary DNS :

PREFIX CONFIGURATION

Get Prefix Mode : From WAN Manual

WAN Interface :

Site Prefix : /64

USB Setup

The DSL router comes with a USB 2.0 interface which you can connect a USB printer, a USB storage device (e.g. USB disk / USB external hard disk) or a USB 3G modem.

To configure the USB device on the router, click **USB Setup** in the **SETUP** tab. The router can be configured as a USB network file server when you plug-in a USB storage device. It can also be configured as a USB printer server when you plug-in a USB Printer device. Lastly, it can connect to Internet via 3G network when you plug-in a USB 3G USB Modem.

SAMBA Server: If you have connected a USB storage device to be used as a media server, clicking **Setup** here will take you to **SAMBA** on page 39.

FTP Server: If you have connected a USB storage device to be used as a file server, clicking **Setup** here will take you to **FTP** on page 35.

USB WAN Setup: If you have connected a 3G USB modem, clicking **Setup** here will take you to **3G WAN Configuration** on page 40.

The screenshot displays the 'USB SETUP' configuration page. It features an orange header with the text 'USB SETUP'. Below the header, a grey box contains the message: 'This router supports Link'n print feature, USB Storage and USB Printer. Please setup the feature below.' The page is divided into three sections, each with a dark grey header and a white body. The first section is 'USB SETUP -- SAMBA SERVER', with the text 'You can manage the storage device and configure the router as a file server.' and a 'Setup' button. The second section is 'USB SETUP -- FTP SERVER', with the text 'You can manage the storage device and configure the router as a file server.' and a 'Setup' button. The third section is 'USB SETUP -- USB WAN SETUP', with the text 'You can configure 3G USB Modem via USB port. And you device would be able to connect to Internet via 3G USB Modem.' and a 'Setup' button.

Time and Date

This section enables you to use an international time server to set the internal time and date for the router.

Automatically Synchronize: Enable or disable automatic synchronisation with an Internet Time Server.

1st NTP Time Server: Specify an address for the primary Internet time server.

2nd NTP Time Server: Specify an address for the secondary Internet Time Server.

Current Local Time: Displays the current local time.

Time Zone: Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

Enable Daylight Saving: Enable or disable daylight saving.

Daylight Saving Start/End: Specify the time and date when daylight saving should start/end.

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.

TIME SETTING

Automatically synchronize with Internet time servers

1st NTP time server : europe.pool.ntp.org

2nd NTP time server :

TIME CONFIGURATION

Current Local Time: 2013-11-11 17:23

Time Zone: (GMT+01:00) Amsterdam, Berlin, Rome, Stockholm, Vienna, Paris

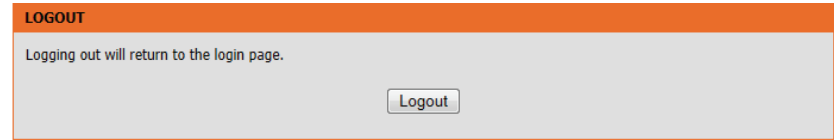
Enable Daylight Saving

Daylight Saving Start: 2012 Year 03 Mon 11 Day 02 Hour 00 Min 00 Sec

Daylight Saving End: 2012 Year 11 Mon 04 Day 02 Hour 00 Min 00 Sec

Logout

Click **Logout** when you are done configuring your router.



Advanced

2.4G Advanced Wireless

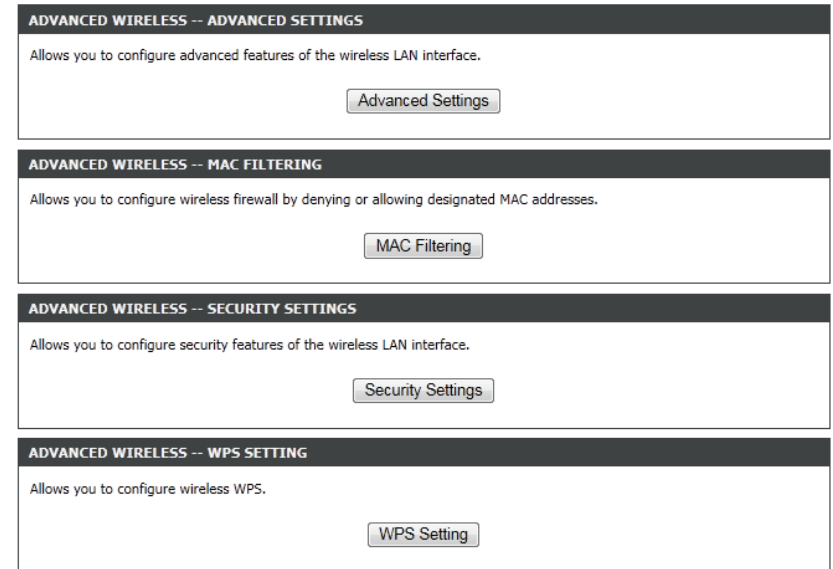
This section enables you to fine tune the wireless settings on the 2.4G wireless band.

Click **Advanced Settings** and refer to **Advanced Settings** on page 29 for more details.

Click **MAC Filtering** and refer to **MAC Filtering** on page 31 for more details.

Click **Security Settings** and refer to **Security Settings** on page 32 for more details.

Click **WPS Setting** and refer to **WPS Settings** on page 33 for more details.



Advanced Settings

- Enable Wireless:** Choose to enable or disable the wireless networks.
- Transmit Power:** Set the transmit power of the antennas in percentage.
- Beacon Period:** Beacon Interval range can be set from 20 to 1023.
- RTS Threshold:** This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.
- Fragmentation Threshold:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting..
- DTIM Interval:** DTIM range can be set from 1 to 255. A delivery traffic indication message is a kind of traffic indication message (TIM) which informs the clients of the presence of buffered multicast/broadcast data on the access point.
- Preamble Type:** Use the drop-down menu to specify whether the router should use the Short Preamble or Long Preamble type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the router and roaming wireless adapters
- SSID:** Enter an SSID for the wireless network.
- Visibility Status:** Enable the wireless network to be Visible or Invisible to wireless clients. If Invisible, the SSID of the DSL-2750B will not be seen by site survey utilities, so wireless clients will have to manually enter the SSID of your wireless network in order to connect to it.
- User Isolation:** Choose to enable or disable wireless user isolation.
- Disable WMM Advertise:** Enable or Disable WiFi MultiMedia QoS.
- Max Clients:** Use this option to specify the maximum number of clients.

ADVANCED SETTINGS

These options are for users who wish to change the behavior of their 802.11g wireless radio from the standard setting. It is not recommended to modify these settings from the factory defaults. Incorrect settings may affect your wireless performance. The default settings usually provide the best wireless performance in most environments.

WIRELESS ENABLE

Enable Wireless :

ADVANCED WIRELESS SETTINGS

Transmit Power : 100% ▼
 Beacon Period : 100 (20 ~ 1023)
 RTS Threshold : 2346 (1 ~ 2347)
 Fragmentation Threshold : 2346 (256 ~ 2346)
 DTIM Interval : 10 (1 ~ 255)
 Preamble Type : long ▼

SSID

SSID : D-Link DSL-2750B
 Visibility Status : Visible Invisible
 User Isolation : Off ▼
 Disable WMM Advertise : On ▼
 Max Clients : 32 (1 ~ 32)

Enable Guest Virtual Access Point 1/2/3: Enable or disable a guest network.

Guest SSID: Specify a name for each guest network.

Visibility Status: Enable the guest wireless network to be **Visible** or **Invisible** to wireless clients.

User Isolation: Choose to enable or disable guest wireless user isolation.

Disable WMM Advertise: Enable or Disable WiFi MultiMedia QoS on the guest network.

Max Clients: Use this option to specify the maximum number of clients on the guest network.

GUEST/VIRTUAL ACCESS POINT-1

Enable:

Guest SSID:

Visibility Status: Visible Invisible

User Isolation:

Disable WMM Advertise:

Max Clients: (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-2

Enable:

Guest SSID:

Visibility Status: Visible Invisible

User Isolation:

Disable WMM Advertise:

Max Clients: (1 ~ 32)

GUEST/VIRTUAL ACCESS POINT-3

Enable:

Guest SSID:

Visibility Status: Visible Invisible

User Isolation:

Disable WMM Advertise:

Max Clients: (1 ~ 32)

MAC Filtering

The Access Control setup tab enables you to configure filters to control which wireless clients can access your network, and which network resources they can access.

Select **Enable** to enable the Wireless Access Control Mode. In this mode, only listed wireless devices will be allowed to connect to the wireless network. Click **Submit** to save your settings.

Click the **Add** button to add an item to the filter list.

Enter the MAC address of a device you wish to allow access for to the WLAN.

Click the **Apply** button when you are done. This will add the device's MAC address to the filter list.

ACCESS CONTROL

If you enable the MAC Address Access Control mode, hosts with MAC addresses contained in the access control list are allowed to access to the router.

ACCESS CONTROL -- MAC ADDRESSES

Wireless SSID :

Access Control Mode :

WLAN FILTER LIST

Mac	Comment	Operation
<input type="button" value="Add"/>		

ACCESS CONTROL -- MAC ADDRESSES

Wireless SSID :

Access Control Mode :

WLAN FILTER LIST

Mac	Comment	Operation
<input type="button" value="Add"/>		

INCOMING MAC FILTER

MAC : (xx:xx:xx:xx:xx:xx)

Comment :

Security Settings

In this section, you can configure the wireless security settings for the router.

Wireless Security Mode: Select a wireless security encryption option. You can also choose to not use one by selecting **None**, but this is not recommended. For information on wireless security, please refer to **WPS Settings** on page 33.

WPA Mode: Select either **Personal** or **Enterprise**.

Encryption Mode: Select TKIP + AES.

Group Key Update Interval: Enter the time in seconds that the group key will be automatically updated.

Pre-Shared Key: Enter a string of 8 characters to set a password for your wireless network.

RADIUS server IP Address: For Enterprise mode, enter the IP address of your network's RADIUS server here.

RADIUS server Port: Enter the port of your network's RADIUS server here.

RADIUS server Shared Secret: Enter the password of your network's RADIUS server here.

WIRELESS SECURITY	
In this page, you can configure the wireless security settings for the router. Please note that changes made in this page must also be duplicated to your wireless clients and PC.	
WIRELESS SECURITY MODE	
Wireless Security Mode :	WPA/WPA2 Mixed
WPA/WPA2 MIXED	
WPA Mode :	Personal
Encryption Mode :	TKIP + AES
Group Key Update Interval :	100 (60 - 65535)
PRE-SHARED KEY	
Pre-Shared Key :	12345678 (ASCII < 64, HEX = 64)

WPS Settings

This section allows you to configure how the DSL-2750B uses Wi-Fi Protected Setup (WPS) to create a secure wireless connection.

Select the SSID of the virtual network you wish to configure.

Enable WPS: Check the box to enable devices to connect to the router using WPS.

Device PIN: Displays the current PIN (Personal Identification Number) for the router's WPS connection. Wireless clients connecting to the router using the PIN method should enter this PIN in order to connect. Click **New PIN** to generate a new PIN.

Generate PIN Status: Click **PIN** to enter a PIN for the new device that you wish to connect.

Push Button: Click **PBC** to activate the WPS-PBC (push-button) method. You will then have 120 seconds to press the WPS button on the new device that you wish to connect.

Input Station PIN: Enter the PIN for the station that you wish to connect to. Click **PIN** to connect to the device.

WPS Session Status: Displays the current status of WPS.

WPS

The WPS condition must be WPA-PSK or WPA2-PSK security mode, and the SSID should be broadcasted.

Wireless SSID : D-Link DSL-2750B

WPA Mode : WPA2 Mixed-PSK

Pre-Shared Key : *****

WI-FI PROTECTED SETUP CONFIG

Enabled WPS

Device PIN : New PIN

Generate Pin Status: PIN

Push Button : PBC

Input Station PIN : PIN

WPS Session Status :

ALG

An application-level gateway (ALG) is a security component that augments a firewall or NAT employed in a network. It allows customized NAT filters to support address and port translation for specified application layer protocols.

- TFTP Pass Through:** Check to enable or disable TFTP pass through functionality.
- FTP Pass Through:** Check to enable or disable FTP pass through functionality.
- PPTP Pass Through:** Check to enable or disable PPTP pass through functionality.
- RTSP Pass Through:** Check to enable or disable RTSP pass through functionality.
- L2TP Pass Through:** Check to enable or disable L2TP pass through functionality.
- H323 Pass Through:** Check to enable or disable H323 pass through functionality.
- SIP Pass Through:** Check to enable or disable SIP pass through functionality.
- IPSEC Pass Through:** Check to enable or disable IPSEC pass through functionality.

ALG
Application Level Gateway.

ALG CONFIGURATION

- TFTP Pass Through :
- FTP Pass Through :
- PPTP Pass Through :
- RTSP Pass Through :
- L2TP Pass Through :
- H323 Pass Through :
- SIP Pass Through :
- IPSEC Pass Through :

FTP

On this page you can configure the FTP server.

FTP Server:

Enable FTP Server: Check the box to enable the FTP server.

Enable FTP Server for WAN: Check the box to enable FTP connections over WAN.

Enable Anonymous Access: Check the box to allow users to connect anonymously.

FTP Server Port: Enter the port number to be used for FTP. The default is **21**.

The screenshot shows a web interface for configuring the FTP server. At the top, there is an orange header with the text "FTP". Below this is a grey box containing the instruction: "You can Enable or Disable ftp server, and set ftp port here." Underneath is a dark grey header labeled "FTP SERVER SETTING". The main content area contains the following settings: "FTP Server" is set to "Off" via a dropdown menu; "Enable FTP Server" has an unchecked checkbox; "Enable FTP Server for WAN" has an unchecked checkbox; "Enable Anonymous Access" has a checked checkbox; and "FTP Server Port" is set to "21" in a text input field.

Port Forwarding

Port forwarding is a method to direct incoming traffic to a particular server on the LAN. Up to 16 port forwarding entries are supported.

Click **Add**, **Edit**, or **Delete** to reveal the Port forward setup options.

- WAN Connection:** Specify the WAN connection to use.
- Server Name:** Enter a name for the server or service.
- Schedule:** Select whether the port will **always** or **never** be forwarded.
- Server IP Address:** Enter the internal IP address for the traffic to be forwarded to.

PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by protocol and external port) to the internal server with a private IP address on the LAN side. The internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side. A maximum of 16 entries can be configured for each WAN connection.

Select the service name, and enter the server IP address and click "Apply" to forward IP packets for this service to the specified server. Note: Modifying the **Internal Port Start** or **Internal Port End** is not recommended. If the **External Port Start** or the **External Port End** changes, the **Internal Port Start** or **Internal Port End** automatically changes accordingly.

PORT FORWARDING SETUP

Server Name	Wan Connection	External Port Start/End	Protocol	Internal Port	Server IP Address	Schedule Rule	Remote IP
-------------	----------------	-------------------------	----------	---------------	-------------------	---------------	-----------

Add Edit Delete

PORT FORWARDING SETUP

WAN Connection(s): DSL_DHCP_0_01

Server Name:

Schedule: always

Server IP Address(Host Name): 192.168.1.

External Port Start	External Port End	Protocol	Internal Port	Remote Ip
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

Apply Cancel

Port Trigger

Port triggering allows ports to be opened for remote access if triggered by activity by a local computer on specified ports.

Click **Add**, **Edit**, or **Delete** to reveal the Port Trigger setup options.

- Enable Port Trigger:** Check this to enable the port trigger feature.
- Service Name:** Enter a name for the server or service.
- Rule Status:** Select whether to **Enable** or **Disable** this rule.
- Trigger Port Start/End:** Enter the starting and ending port to monitor to trigger this rule.
- Trigger Protocol:** Select the protocol to monitor for to trigger this rule.
- Open Port Start/End:** Enter the starting and ending port to open when the rule is triggered.
- Open Protocol:** Enter the protocol to allow through the opened ports.

PORT TRIGGER

Port Trigger let the device to open TCP or UDP port to access the connection from remote host when the specified port has been opened by lanside connection according to the rule. Usually the port which has been opened is different from the port which will be opened by the device. A maximum of 32 entries can be configured.

Select the service name, and fill the blanks of trigger port and new opened port. Rule can be enable or disable separately.

Enable Port Trigger

Apply Cancel

PORT TRIGGER SETUP

Service Name	Trigger Protocol	Trigger Port Range	Open Protocol	Open Port Range	status
Add Edit Delete					

PORT TRIGGER SETUP

Remaining number of entries that can be configured: 32

Service Name :

Rule status : Enable ▼

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input style="width: 80%;" type="text"/>	<input style="width: 80%;" type="text"/>	TCP ▼	<input style="width: 80%;" type="text"/>	<input style="width: 80%;" type="text"/>	TCP ▼

DMZ

A DMZ or Demilitarized Zone is as a physical or logical subnetwork that contains and exposes external-facing services to a larger and untrusted network, usually the Internet.

- WAN Connection:** Specify the WAN connection to use.
- Enable DMZ:** Check to enable or disable DMZ functionality.
- DMZ Host IP Address:** Enter an IP address to be included in the DMZ.

DMZ

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

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

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

DMZ HOST

WAN Connection :

Enable DMZ :

DMZ Host IP Address :

Apply Cancel

SAMBA

Samba allows file and print sharing between computers. It is an implementation of dozens of services and a dozen protocols.

- Enable SAMBA:** Check to enable or disable SAMBA functionality.
- Workgroup:** Enter the name of the workgroup to be mapped.
- Netbios Name:** Enter a name for Netbios mapping.
- New SMB password:** Enter a password for the root user.
- Retype new SMB password:** Re-enter the password for the root user.
- Enable USB Storage:** Check to enable or disable SAMBA functionality for USB devices.
- Enable Anonymous Access:** Check to enable or disable SAMBA functionality for USB anonymous users.

SAMBA
configure for Samba.

SAMBA SERVER

Enable SAMBA :

Workgroup : Workgroup

Netbios Name : dsl_route

modify the password for user root

New SMB password : ●●●●●●

Retype new SMB password : ●●●●●●

Enable USB Storage :

Enable Anonymous Access :

Apply Cancel

3G WAN Configuration

This section enables you to configure a 3G Internet connection. Click the **Add** button to reveal the setup options.

- Enable 3G Service:** Check to enable or disable 3G functionality.
- Enable NDIS:** Check to enable Network Driver Interface Specification (NDIS).
- Enable DHCP:** Check to let the router act as the DHCP server for the 3G WAN connection.
- Account/Password:** Enter your account and password for your 3G WAN connection.
- Dial Number:** Enter the number to be dialed.
- Net Type:** Select your 3G network access type.
- APN:** Enter the Access Point Network (APN) if there is one.
- On Demand:** Check to connect to 3G network automatically or manually.
- Inactivity Timeout:** Enter a period to disconnect an inactive connection. Only available if **On Demand** has been checked.
- Backup delay time:** The response time allowed for 3G connection before a dial-up is initiated.
- Recovery delay time:** Specify a period to re-dial.
- Initialization Delay time:** Specify a period for the 3G connection to initialize.
- Mode Switch Delay time:** Specify a period to allow for a mode switch.
- Backup Mechanism:** Select a WAN connection to use if 3G fails.
- Checking IP address:** Specify an IP Address to test the 3G connection.

3G MOBILE SETUP

Choose "Add", "Edit", or "Delete" to configure 3G WAN interfaces.

When you want to edit the 3G configuration, please ensure the 3G is in disconnection status at first.

3G WAN CONFIGURATION

3G Status: NoDongle
Inform: NO USB CARD

Service Name	Protocol	State	Status	Default Gateway	Action
Add Edit Delete Pin Manage DongleInfo					

3G WAN CONFIGURATION

This screen allows you to configure a 3G Internet connection.

3G WAN SETUP

Enable 3G Service :

Enable NDIS :

Enable DHCP :

Account : any

Password : ●●●

Dial_Number : *99#

Net Type : EVDO

APN :

OnDemand :

Inactivity Timeout : 1 (Minuter [1~1092]. But if 0, we will set default value)

Backup delay time : 60 (Seconds [0-600])

Recovery delay time : 60 (Seconds [0-600])

Initialization Delay time : 20 (If too small, some 3g dongle will be unsupported)

Mode Switch Delay time : 20 (If too small, some 3g dongle will be unsupported)

BackupMechanism : DSL

Checking IP address: 8.8.8.8

Timeout (in sec.): 1

Period time (in sec.): 1

Fail Tolerance: 1

Timeout: Specify a period of inactivity after which an established 3G session will be ended. Set to zero or choose Auto in Reconnect Mode to disable this feature.

Period time: Specify a period for DSL or Ethernet uplink to be disconnected.

Fail Tolerance: Specify the number of failures before using the backup connection.

3G WAN SETUP

Enable 3G Service :

Enable NDIS :

Enable DHCP :

Account : any

Password : ●●●

Dial_Number : *99#

Net Type : EVDO

APN :

OnDemand :

Inactivity Timeout : 1 (Minuter [1~1092]. But if 0, we will set default value)

Backup delay time : 60 (Seconds [0-600])

Recovery delay time : 60 (Seconds [0-600])

Initialization Delay time : 20 (If too small, some 3g dongle will be unsupported)

Mode Switch Delay time : 20 (If too small, some 3g dongle will be unsupported)

BackupMechanism : DSL

Checking IP address: 8.8.8.8

Timeout (in sec.): 1

Period time (in sec.): 1

Fail Tolerance: 1

Parental Control

This section enables you to restrict access to the internet.

The **Website Filter** enables you to quickly create a list of websites to limit access to, or to block access to.

The **HTTP Content Filter** enables you to control access to HTTP content on the Internet.

The **MAC Filter** enables you to filter access by device MAC addresses.

The image displays three sequential screenshots of a web-based configuration interface for Parental Control. Each screenshot has a dark header bar with white text. The first screenshot is titled 'PARENTAL CONTROL -- WEBSITE FILTER' and contains the text: 'This is a blocking function for website addresses, if this function is enabled, access to the website addresses in the list will be denied.' Below the text is a button labeled 'Website Filter'. The second screenshot is titled 'PARENTAL CONTROL -- HTTP CONTENT FILTER' and contains the text: 'This is a blocking function for http content, if this function is enabled, access to the http content in the list will be denied.' Below the text is a button labeled 'Http Content Filter'. The third screenshot is titled 'PARENTAL CONTROL -- MAC FILTER' and contains the text: 'Uses MAC address to implement filtering.' Below the text is a button labeled 'MAC Filter'.

Website Filter

Access Control Mode: Select to **Deny** access to all listed websites, or to **Allow** access to only the listed websites.

Website Filter List: Click **Add/Edit/Delete** to manage your website list.

URL: Enter a website address.

Days/All Day/Start - End Time: Use these options to schedule when you want the website filter to be active for the specified URL.

WEBSITE FILTER

Create a list of websites that you would like the devices on your network to be allowed or denied access to.

WEBSITE FILTER

Access Control Mode : Deny

WEBSITE FILTER LIST

URL	Schedule

Add
Edit
Delete

ADD SCHEDULE RULE

URL :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed
 Thu Fri Sat

All Day - 24 hrs :

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

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

HTTP Content Filter

Access Control Mode: Select to **Deny** access to all listed websites, or to **Allow** access to only the listed websites.

HTTP Content Filter List: Click **Add/Edit/Delete** to manage your website list.

Keywords: Enter keywords you want to filter via rules.

Days/All Day/Start - End Time: Use these options to schedule when you want the HTTP filter to be active for the specified keyword.

HTTP CONTENT FILTER

Create a list of http content that you would like the devices on your network to be allowed or denied access to.

HTTP CONTENT FILTER

Access Control Mode :

HTTP CONTENT FILTER LIST

Keywords	Schedule
<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

ADD SCHEDULE RULE

Keywords :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed
 Thu Fri Sat

All Day - 24 hrs :

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

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

MAC Filter

MAC Filtering Global Policy: Choose **BLACK_LIST** or **WHITE_LIST** then click **Add/Edit/Delete** to reveal scheduling options.

User Name: Enter a user name.

Current PC's MAC Address: Select to use the MAC address of your current client.

Other MAC Address: Enter the user's alternate MAC address.

Days/All Day/Start - End Time: Enter or Check the options to create the required access control schedule.

BLOCK MAC ADDRESS

Time of Day Restrictions -- A maximum of 16 entries can be configured

This page adds a time of day restriction to a special LAN device connected to the router. The "Current PC'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".

Mac Filtering Global Policy:

BLACK_LIST --Allow all packets but **DENY** those matching any of specific rules listed
 WHITE_LIST --Deny all packets but **ALLOW** those matching any of specific rules listed

BLOCK MAC ADDRESS--BLACKLIST

Username	MAC	Schedule

ADD SCHEDULE RULE

User Name :

Current PC's MACAddress :

Other MAC Address :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed
 Thu Fri Sat

All Day - 24 hrs :

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

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

Filtering Options

This section enables you to apply advanced IPv4 or IPv6 filtering options .

Click **IPv4 Filtering** to reveal IPv4 configuration options.
Click **IPv6 Filtering** to reveal IPv6 configuration options.

FILTERING OPTIONS -- IP V4 FILTERING

Uses IPv4 address to implement filtering.

IP v4 Filtering

FILTERING OPTIONS -- IP V6 FILTERING

Uses IPv6 address to implement filtering.

IP v6 Filtering

IPv4 Filtering

Enable IP Filter: Check to enable or disable the IPv4 Filter.

Security Level: Select the security level.

Low will set the filter to **Black** in both directions.

Middle will set the filter to **White** in the WAN -> LAN direction and White in the LAN -> WAN direction.

High will set the filter to **White** in both directions.

Filter Model: Select the filter model to adjust and click **Add a Rule** to reveal further options.

Connection: Select the connection to be filtered.

Enable: Check to enable or disable the IPv4 model.

Protocol: Select the appropriate protocol for the connection.

Source IP: Enter the sending IP address to be filtered.

Source Mask: Enter the sending mask to be filtered.

Source Port: Enter the sending port to be filtered.

Destination IP: Enter the destination IP address to be filtered.

Destination Mask: Enter the destination mask to be filtered.

Destination Port: Enter the destination port to be filtered.

Description: Enter a name for the filter rule.

IP FILTER CONFIGURATION

Enable IP Filter

Security Level Low

FILTER MODEL

WAN → LAN White Black

LAN → WAN White Black

Submit Refresh

ADD IP FILTER RULES

Choose WAN → LAN Add a rule

NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name

Edit Delete

IP FILTER CONFIGURATION

Connection

Enable

Protocol TCP

Source IP

Source Mask

Source Port -

Destination IP

Destination Mask

Destination Port -

Description

Submit Refresh

IPv6 Filtering

Enable IP Filter: Check to enable or disable the IPv6 Filter.

Security Level: Select the security level.

Low will set the filter to **Black** in both directions.

Middle will set the filter to **White** in the WAN -> LAN direction and White in the LAN -> WAN direction.

High will set the filter to **White** in both directions.

Filter Model: Select the filter model to adjust and click **Add a Rule** to reveal further options.

Enable: Check to enable or disable the IPv4 model.

Connection: Select the connection to be filtered.

Protocol: Select the appropriate protocol for the connection.

Source IP: Enter the sending IP address to be filtered.

Source Mask: Enter the sending mask to be filtered.

Source Port: Enter the sending port to be filtered.

Destination IP: Enter the destination IP address to be filtered.

Destination Mask: Enter the destination mask to be filtered.

Destination Port: Enter the destination port to be filtered.

Description: Enter a name for the filter rule.

IPv6 FILTER CONFIGURATION

Enable IP Filter

Security Level

FILTER MODEL

WAN → LAN White Black

LAN → WAN White Black

ADD IP FILTER RULES

Choose

NO.	Enable	IP/Port(source)	IP/Port(destination)	Protocol	Description	Device Name

IPv6 FILTER CONFIGURATION

Connection

Enable

Protocol

Source IP

Source Prefix Length

Source Port -

Destination IP

Destination Prefix Length

Destination Port -

Description

QoS

Quality of Service (QoS) is a feature that lets you ensure throughput for specific services or devices. QoS can improve your online experience by ensuring that specific traffic is prioritized over other network traffic, such as VoIP, FTP, or Web.

QoS: Check to enable or disable QoS.

Direction: Select Upstream or Downstream.

Queue Enable: Check to enable or disable queueing.

Bandwidth: Enter a maximum limit for upstream traffic.

Discipline: Select the QoS discipline type.

WRR Weight: If WRR discipline is selected, define it here.

Enable DSCP ReMark: Check to enable or disable DSCP ReMark.

Enable 802.1p ReMark: Check to enable or disable 802.1p ReMark.

QUALITY OF SERVICE

Configuration of classification table for IP QoS.

QoS : Enable Disable

QOS QUEUE

Direction : Upstream (LAN -> WAN) Downstream (WAN -> LAN)

Queue Enable : Enable Disable

Bandwidth : Kbps (0 means no limit bandwidth)

Discipline : WRR Strict Priority

WRR weight : Highest: High: Medium: Low:
(all sum should be less or equal than 100)

Enable DSCP ReMark :

Enable 802.1p ReMark :

QOS CLASSIFICATION RULES

#	Enable	Rule	Action	Edit	Drop
<input type="button" value="Add a Rule"/>					

Click **Add a Rule** to reveal further QoS configuration options.

Add QoS Classification Rules

Classify Type: Select Upstream Flow or Downstream Flow classification.

Actions: Select to enable or disable this rule.

Application: Select the pre-defined application type or choose **Not Match**.

Physical Ports: Choose the WAN Interface.

Destination IP address: Enter the destination IP address for the rule. If data packets include the IP address, the data packets are placed into the group.

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

Destination Port Range: Enter the destination port range. (eg. UDP/TCP port range)

Source MAC address: Enter the source MAC address. If data packets include the MAC address, the data packets are placed into the group.

Source IP address: Enter the source IP address. If data packets include the IP address, the data packets are placed into the group.

Source Subnet Mask: Enter the source subnet mask.

Source Port Range: Enter the source port range. (eg. UDP/TCP port range)

Protocol: Select the pre-defined protocol type or choose **Not Match**.

Vlan ID: Enter the VID (VLAN ID) is the identification of the VLAN, which is used by the standard 802.1Q. It has 12 bits and allows the identification of 4096 (2^{12}) VLANs. The maximum possible VLAN configurations are 4,094.

DSCP: Select a matching DSCP type.

Queue #: Select the queue priority number.

DSCP Remark: The DSCP range can be between 0 to 63.

ADD QOS CLASSIFICATION RULES

RULE

Classify Type : Upstream Flow Classify Downstream Flow Classify

Actions : Enable Disable

Application :

Physical Ports :

Destination IP Address :

Destination Subnet Mask :

Destination Port Range : ~

Source MAC Address :

Source IP Address :

Source Subnet Mask :

Source Port Range : ~

Protocol :

Vlan ID :

DSCP :

Queue # :

ACTIONS

DSCP Remark :

802.1p Remark :

Queue # :

802.1p Remark: Select this option to Activate/Deactivated the 802.1p. IEEE 802.1p establishes eight levels of priority (0 ~ 7). Although network managers must determine actual mappings, IEEE has made broad recommendations.

Seven is the highest priority which is usually assigned to network-critical traffic such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) table updates. Five and six are often for delay-sensitive applications such as interactive video and voice. Data classes four through one range from controlled-load applications such as streaming multimedia and business-critical traffic - carrying SAP data, for instance - down to "loss eligible" traffic. Zero is used as a best-effort default priority, invoked automatically when no other value has been set.

Queue #: Select **Low**, **Medium**, **High** or **Highest**.

ADD QOS CLASSIFICATION RULES	
RULE	
Classify Type :	<input type="radio"/> Upstream Flow Classify <input checked="" type="radio"/> Downstream Flow Classify
Actions :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application :	Not Match
Physical Ports :	WAN
Destination IP Address :	<input type="text"/>
Destination Subnet Mask :	<input type="text"/>
Destination Port Range :	<input type="text"/> ~ <input type="text"/>
Source MAC Address :	<input type="text"/>
Source IP Address :	<input type="text"/>
Source Subnet Mask :	<input type="text"/>
Source Port Range :	<input type="text"/> ~ <input type="text"/>
Protocol :	Not Match
Vlan ID :	<input type="text"/>
DSCP :	Not Set
Queue # :	Not Match
ACTIONS	
DSCP Remark :	Not Set
802.1p Remark :	Not Set Not Set
Queue # :	Unbound
<input type="button" value="Save"/> <input type="button" value="Back"/>	

Anti-Attack Settings

This section enables you to automatically configure your router to detect and protect against several known attack types.

A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

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

Check **Enable Attack Prevent** to enable the firewall configuration options checked below it and click **Apply**.

', 'Enable Anti-attack : ', and 'Enable Anti-attack Log : '. At the bottom right of the form are two buttons: 'Submit' and 'Refresh'."/>

ANTI-ATTACK COFIGURATION

This page is used to configure SPI/DoS Protection.

SPI/DOS PROTECTION CONFIGURATION

Enable SPI Firewall :

Enable Anti-attack :

Enable Anti-attack Log :

Submit Refresh

Share Protection

The identification field is used to distinguish the fragments of one datagram from those of another. The originating protocol module of an internet datagram sets the identification field to a value that must be unique for that source-destination pair and protocol for the time the datagram will be active in the internet system.

IPID: Check to enable IPID configuration.

TTL: Check to enable TTL for IPID settings.

TTL Value: Enter a TTL value.

Connlimit: Check to enable concurrent connections limit.

**TCP
Connlimit
Value:** Enter a value for the TCP concurrent connections limit.

**UDP
Connlimit
Value:** Enter a value for the UDP concurrent connections limit.

SHARE PROTECTION SETTINGS

Shared Protection feature will allow more than one PC through the Router to share Internet access.
Please enable the relevant options and enter the appropriate values and click "Apply" to activate this function.

SHARE PROTECTION CONFIGURATION

IPID :
TTL :
TTL Value:
Connlimit :
TCP Connlimit Value:
UDP Connlimit Value:

DNS

Domain name system (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they are easier to remember. The Internet, however, is actually based on IP addresses. Each time you use a domain name, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might be translated to `198.105.232.4`.

The DNS system is, in fact, its own network. If one DNS server does not know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

WAN Connection: Select WAN connection you wish to configure.

IPv4 Static DNS: Check to enable static DNS for this DNS server.

Preferred DNS Server: Enter the provided DNS server IP address.

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

DNS

Click "Apply" button to save the new configuration.

DNS SERVER CONFIGURATION

Wan Connection : DSL_DHCP_0_01

IPv4 static DNS: Enabled

Preferred DNS server :

Alternate DNS server :

Apply Cancel

Dynamic DNS

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

Click **Add** or **Edit** to reveal Dynamic DNS configuration options.

DDNS provider: Select one of the Dynamic DNS organizations from the menu.

Hostname: Enter the hostname you registered with the Dynamic DNS provider.

Interface: Select the appropriate interface.

Username: Enter the username for your Dynamic DNS account.

Password: Enter the password for your Dynamic DNS account.

DYNAMIC DNS

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

DYNAMIC DNS

Hostname	Username	Service	Interface

Add Edit Delete

DYNAMIC DNS

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

DYNAMIC DNS

Hostname	Username	Service	Interface

Add Edit Delete

ADD DYNAMIC DNS

DDNS provider : dlinkddns.com ▼

Hostname :

Interface : DSL_DHCP_0_01 ▼

Username :

Password :

Apply Cancel

Network Tools

The Network Tools section provides several features which enable a fine degree of network management control.

Click the **Port Mapping**, **IGMP Proxy**, **IGMP Snooping**, **MLD Configuration**, **UPnP**, or **DSL** button to reveal the associated configuration options.

NETWORK TOOLS -- PORT MAPPING Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. Port Mapping
NETWORK TOOLS -- IGMP PROXY Transmission of identical content, such as multimedia, from a source to a number of recipients. IGMP Proxy
NETWORK TOOLS -- IGMP SNOOPING Transmission of identical content, such as multimedia, from a source to a number of recipients. IGMP Snooping
NETWORK TOOLS -- MLD CONFIGURATION Transmission of identical content, such as multimedia, from a source to a number of recipients. MLD Configuration
NETWORK TOOLS -- UPNP Allows you to enable or disable UPnP. Upnp
NETWORK TOOLS -- DSL Allows you to configure advanced settings for DSL. DSL

Port Mapping

This section enables you to bind the WAN interface and the LAN interface to the same group. This allows remote computers to connect to a specific computer or service within a private local-area network (LAN).

Click **Add** to reveal the Port Mapping configuration options.

Group Name: Enter a group name.

Grouped Interfaces: Select from the listed interfaces from the Available Interface then click the <- arrow button to add them to the Grouped Interface list. This creates the required mapping of the ports. The group name must be unique.

PORT MAPPING

Port Mapping -- A maximum 5 entries can be configured

Port Mapping supports multiple port to PVC and bridging groups. Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the "Add" button. The "Delete" button will remove the grouping and add the ungrouped interfaces to the Default group.

PORT MAPPING SETUP	
Group Name	Interfaces
<input type="checkbox"/> Lan1	ethernet1,ethernet2,ethernet3,ethernet4,ra0,ra1,ra2,ra3,rai0,rai1,ra...

Add Edit Delete

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

PORT MAPPING CONFIGURATION

Group Name:

Grouped Interfaces	Available Interfaces
	ethernet1 ethernet2 ethernet3 ethernet4 ra0 ra1 ra2 ra3 rai0 rai1 rai2

Apply Cancel

IGMP Proxy

Creating an IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system has discovered through standard IGMP interfaces. This allows the system to act as a proxy for its hosts after being enabled.

- WAN Interface:** Select the WAN interface you wish to configure.
- IGMP Version:** Select either IGMP V1, IGMP V2, or IGMP V3 from the list.
- Enable IGMP Proxy:** Check this box to enable IGMP proxy.
- LAN Connection:** Select the LAN connection to use.
- Enable FastLeaving:** Check this box to enable FastLeaving.
- General Query/Response Interval:** Enter the query interval and query response interval in box.
- Group Query/Response Interval:** Enter the group query interval and the group query response interval in the box.
- Group Query Count:** Enter the group query count in the box.
- Last Member Query Interval:** Enter the last member query interval in the box.
- Last Member Query Count:** Enter the last member query count in the box.

IGMP PROXY

IGMP proxy enables the system to issue IGMP host messages on behalf of hosts that the system discovered through standard IGMP interfaces. The system acts as a proxy for its hosts when you enable it by:

1. Enabling IGMP proxy on a WAN interface (upstream), which connects to a router running IGMP.
2. Enabling IGMP on a LAN interface (downstream), which connects to its hosts.

IGMP PROXY CONFIGURATION

WAN Interface :

IGMP Version : IGMP V3

Enable IGMP Proxy :

LAN Connection : Lan1

Enable FastLeaving :

General Query Interval : 150 (seconds)

General Query Response Interval : 20 (1~255)(*100 milliseconds)

Group Query Interval : 325 (seconds)

Group Query Response Interval : 20 (1~255)(*100 milliseconds)

Group Query Count : 3

Last Member Query Interval : 1 (seconds)

Last Member Query Count : 1

Apply Cancel

IGMP TABLE

Group Address	Interface	State

Refresh

IGMP Snooping

Enabling this option allows the router to listen for Internet Group Management Protocol (IGMP) traffic, which can help to detect clients which require multicast streams.

Enable IGMP: Check this box to enable IGMP.

Last Member Query Interval: Enter the last member query interval here.

Host Timeout: Enter the host timeout here.

Mrouter Timeout: Enter the Mrouter timeout here.

Leave Timeout: Enter the leave timeout here.

Max Groups: Enter the max number of groups here.

The screenshot shows the 'IGMP' configuration page. At the top, there is a header 'IGMP' and a sub-header 'Transmission of identical content, such as multimedia, from a source to a number of recipients.' Below this is the 'IGMP SETUP' section. It contains the following fields:

- Enabled:** A checkbox that is currently unchecked.
- Last Member Query Interval:** A text input field containing the value '200000'.
- Host Timeout:** A text input field containing the value '3000000'.
- Mrouter Timeout:** A text input field containing the value '1'.
- Leave Timeout:** A text input field containing the value '0'.
- Max Groups:** A text input field containing the value '100'.

At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

MLD Configuration

This section allows you to configure MLD settings for your router. Multicast Listener Discovery(MLD) snooping allows the switch to examine MLD packets and make forwarding decisions based on their content.

Enable Mld Proxy: Check this box to enable MLD proxy.

WAN Connection: Select a WAN connection from the drop-down list to allow MLD proxy on.

Enable FastLeaving: Check this box to enable Fastleaving.

Query Interval: Enter a time in seconds for the query interval.

Query Response Interval: Enter a time in 1/10s for the query response interval.

Last Member Query Interval: Enter a time in 1/10s for the last member query interval.

Enable Mld Snooping: Check this box to enable the MLD Snooping function.

MLD SETTINGS

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

MLD PROXY

Enable Mld Proxy
WAN Connection :
 Enable FastLeaving :
Query Interval : (s)
Query Response Interval: (1/10s)
Last Member Query Interval : (1/10s)

MLD SNOOPING

Enable Mld Snooping

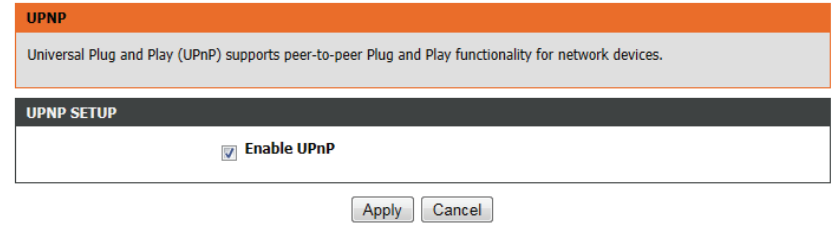
UPnP

This page enables you to enable the UPnP feature.

UPnP (Universal Plug and Play) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use. UPnP broadcasts are only allowed on the LAN.

UPnP is used for popular audio visual software. It allows automatic discovery of your device in the network. If you are concerned about UPnP security, you can disable it. Block ICMP ping should be enabled so that the device does not respond to malicious Internet requests.

Enable UPnP: Check to enable or disable UPnP.



The screenshot shows a configuration window for UPnP. At the top, there is an orange header with the text "UPNP". Below this is a grey box containing the text: "Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices." Underneath is a dark grey header with the text "UPNP SETUP". In the main white area, there is a checkbox labeled "Enable UPnP" which is checked. At the bottom right of the window, there are two buttons: "Apply" and "Cancel".

DSL

This page lets you set the xDSL mode and type. It is recommended that you use the default settings.

xDSL Mode: Select between **Auto Sync-Up, ADSL2+, ADSL2, G.DMT, T1.413, G.lite** modes.

xDSL Type: Select the correct Annex type for your DSL connection.

DSL SETTINGS

This page is used to configure the DSL settings of your DSL router. You need to disable DSL before you change the DSL mode.

DSL SETTINGS

xDSL Mode: Auto Sync-Up ▾

xDSL Type: ANNEX A/I/J/L/M ▾

Apply

Routing

The Routing sections provides an advanced method of customizing specific routes of data through your network.

Click the **Static Route**, **IPv6 Static Route**, **Policy Route**, **RIP Settings**, or **RIPng Settings** button, to reveal the associated configuration options.

STATIC ROUTE
Static Route.
Static Route

IPV6 STATIC ROUTE
IPv6 Static Route.
IPv6 Static Route

POLICY ROUTE
Policy Route.
Policy Route

RIP SETTINGS
RIP Settings.
RIP Settings

RIPNG SETTINGS
RIPng Settings.
RIPng Settings

Static Route

This section allows you to set up static routes for your network.

Click the **Add** button to reveal the associated configuration options.

Destination Network Address: Enter the IP address of the destination router.

Subnet Mask: Enter the subnet mask of the destination IP address.

Use Gateway IP Address: Enter the IP address of the gateway router to be used.

Use Interface: Select the interface to be used from the drop-down menu.

STATIC ROUTE

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 30 entries can be configured.

ROUTING -- STATIC ROUTE

Destination	Subnet Mask	Gateway	Interface

STATIC ROUTE ADD

Destination Network Address :

Subnet Mask :

Use Gateway IP Address :

Use Interface : LAN Group1 ▼

IPv6 Static Route

This section allows you to set up IPv6 static routes for your network.

Click the **Add** button to reveal the associated configuration options.

Enable: Check this box to enable the route.

Destination Network Address: Enter the IPv6 address of the destination router.

Use Gateway IP Address: Enter the IPv6 address of the gateway router to be used.

Use Interface: Select the interface to be used from the drop-down menu.

IPv6 STATIC ROUTE

Enter the destination network address, subnet mask, gateway AND/OR available WAN interface then click "Apply" to add the entry to the routing table, the Gateway IP Address should be the Default Gateway of connected V6 connection so as to take effect.

A maximum 30 entries can be configured.

ROUTING -- IPV6 STATIC ROUTE

Status	Destination	Gateway	Interface
--------	-------------	---------	-----------

Add Edit Delete

IPV6 STATIC ROUTE ADD

Enable :

Destination Network Address :

Use Gateway IP Address :

Use Interface : LAN Group1 ▾

Apply cancel

Policy Route

The Policy Route section provides a method to bind a WAN and at least one LAN connection together.

Click the **Add** button to reveal the associated configuration options.

WAN Connection: Select the WAN connection to be used for binding.

LAN Connection: Select at least one LAN connection to be bound.

The screenshot displays the 'POLICY ROUTE' configuration window. At the top, an orange header reads 'POLICY ROUTE'. Below it, a grey box contains the text: 'Policy Route : chose one Wanconnection and one Lanconnection then bind them.' The main area is titled 'POLICY ROUTE SETUP' and features two input fields labeled 'WAN' and 'LAN'. Below these fields are 'Add' and 'Delete' buttons. The bottom section, 'WAN INSTANCE AND LAN INSTANCE', contains a 'WAN Connection' dropdown menu set to 'DSL_DHCP_0_01'. Underneath, a 'LAN Connection' section lists several options with checkboxes: ethernet1, ethernet2, ethernet3, ethernet4, ra0, ra1, ra2, and ra3. 'Apply' and 'Cancel' buttons are located at the bottom right of this section.

RIP

Use this page to select the interfaces on your device that you want to use RIP for, and the version of the protocol to be used.

Dynamic Route: Select from **OFF**, **RIPv1**, **RIPv2**.

Direction: Select either **Active** or **Passive**.

RIP CONFIGURATION

To activate RIP for the device, select the "Enabled" checkbox for Global RIP Mode. 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 "Apply" button to save the configuration, and to start or stop RIP based on the Global RIP Mode selected.

RIP

Interface	Dynamic Route	Direction
DSL_DHCP_0_01	OFF ▾	Active ▾
Lan1	OFF ▾	Active ▾

Apply Cancel

RIPng

Use this page to enable or disable RIPng for the available interfaces.

RIPNG CONFIGURATION

To activate RIPng for the interface, place a check in the "Enabled" checkbox for the interface. Click the "Apply" button to save the configuration, and to start or stop RIPng based on the configuration.

RIPNG		
Interface	VPI/VCI	Enabled

Apply Cancel

Schedules

The router allows the user the ability to manage schedule rules for various firewall features on this page. Once you have finished configuring the new schedule rule, click the **Apply** button.

Name: Enter a name for the new schedule rule.

Day(s): Choose the desired day(s), either All Week or Select Day(s). If the latter is selected, please use the checkboxes directly below to specify the individual days.

All Day - 24 hrs: Tick this check box if the new schedule rule applies to the full 24-hour period.

Start Time: If the new schedule rule does not apply to the full 24-hour period, untick the previous checkbox, then enter a specific beginning time.

End Time: Enter an ending time.

SCHEDULES

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

Maximum number of schedule rules: 20

SCHEDULE RULES

Rule Name	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Start Time	Stop time
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>									

ADD SCHEDULE RULE

Name :

Day(s) : All Week Select Day(s)

Sun Mon Tue Wed
 Thu Fri Sat

All Day - 24 hrs :

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

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

NAT

This screen lets you set up NAT for your router to link external IP address with internal IP addresses.

Entry Name: Enter a name for the address to be mapped.

Internal IP Type: Select either **Single IP** or **IP Range**.

Internal IP Address: Enter the IP or the IP Range.

External IP Type: Select either **Single IP** or **IP Range**.

External IP Address: Enter the IP or the IP Range.

NAT

Traditional NAT would allow hosts within a private network to transparently access hosts in the external network, in most cases. In a traditional NAT, sessions are uni-directional, outbound from the private network. Sessions in the opposite direction may be allowed on an exceptional basis using static address maps for pre-selected hosts.

NAT TABLES

Name	Internal IP Address	External IP Address
------	---------------------	---------------------

NAT SETTINGS

Entry Name :

Internal IP Type :

Internal IP Address :

External IP Type :

External IP Address :

Management System

The System Management sections provides a number of options to manage the DSL-2750B. This section allows you to manage the router's configuration settings, reboot the router, 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.

Reboot: Click **Reboot** to immediately restart the router.

Backup Setting: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, Click **Backup Setting**. A file dialog will appear, allowing you to select a location and file name for the settings.

Update Setting: Use this option to load previously saved router configuration settings. First, use the **Browse** option to find a previously saved file of configuration settings. Then, click the **Update** button to transfer those settings to the router.

Restore Default Setting: Click **Restore Default Setting** to restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created.

The screenshot displays the Management System interface with four distinct sections, each with a dark header bar and a light content area. The sections are: 1. 'SYSTEM -- REBOOT' with a 'Reboot' button. 2. 'SYSTEM -- BACKUP SETTINGS' with a 'Backup Setting' button and a red note. 3. 'SYSTEM -- UPDATE SETTINGS' with a 'Settings File Name' input field, a 'Browse...' button, and an 'Update Setting' button. 4. 'SYSTEM -- RESTORE DEFAULT SETTINGS' with a 'Restore Default Setting' button.

SYSTEM -- REBOOT
Click the button below to reboot the router.

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

SYSTEM -- UPDATE SETTINGS
Update DSL Router settings. You may update your router settings using your saved files.
Settings File Name:

SYSTEM -- RESTORE DEFAULT SETTINGS
Restore DSL Router settings to the factory defaults.

Firmware Update

You can upgrade the firmware of the access point here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support website for firmware updates at <http://support.dlink.com>. You can download firmware upgrades to your hard drive from this site.

Current Firmware Version: This field displays information about the current firmware.

Current Firmware Date: This field displays the date of the current firmware.

Select File: Click **Browse** to locate the firmware file required.

Clear Config: Check **Clear Config** to reset all current configurations before the firmware is installed.

Update Firmware: Click **Update Firmware** to upload and install the selected firmware.

FIRMWARE UPDATE

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

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

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

NOTE: The update process takes about 2 minutes to complete, and your DSL Router will reboot. Please DO NOT power off your router before the update is complete.

FIRMWARE UPDATE

Current Firmware Version: V1.0.0.0

Current Firmware Date: 12/14/2013-12:44:47

Select File:

Clear Config:

Access Controls

Here, you can manage access to your router.

Click the **Account Password**, **LACL**, **RACL**, or **IP Address** buttons to reveal the associated configuration options.

The screenshot displays a web interface for configuring access controls on a DSL router. It consists of four vertically stacked panels, each with a dark header bar and a white content area. The first panel is titled 'ACCESS CONTROLS -- ACCOUNT PASSWORD' and contains the text 'Manage DSL Router user accounts.' with a button labeled 'Account Password'. The second panel is titled 'LOCAL ACCESS CONTROLS' and contains 'Manage Local Access Control List .' with a button labeled 'LACL'. The third panel is titled 'REMOTE ACCESS CONTROLS' and contains 'Manage Remote Access Control List.' with a button labeled 'RACL'. The fourth panel is titled 'ACCESS CONTROLS -- IP ADDRESS' and contains 'Permits access to local management services.' with a button labeled 'IP Address'.

Account Password

The Account Password section enables you to manage users' passwords.

You should change the default admin password to secure your network.

Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you will need to reset the device to the factory default settings and all configuration settings of the device will be lost.

Username: Select the username that you want to modify.

New Username: If you are adding a new user account, enter the username in this field.

Current Password: Enter the current password (existing users only).

New Password: Enter the new password.

Confirm Password: Re-enter the new password.

Web Idle Time Out: Set a period of time to automatically log the user out if the session is inactive for the specified amount of time.

ACCOUNT PASSWORD

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

The user name "support" is used to allow an ISP technician to access your DSL Router for maintenance and to run diagnostics. This user name can not be used in local.

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

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

ACCOUNT PASSWORD

Username:

New Username:

Current Password:

New Password:

Confirm Password:

WEB IDLE TIME OUT SETTINGS

Web Idle Time Out: (5 ~ 30 minutes)

Local Access Control

The Local Access Control section enables you to specify which services can be accessed by a remote host.

Enable Local Access: Check to enable or disable remote access to the following services.

Choose a Connection: Select a connection interface from the available options in the drop-down menu.

LOCAL ACCESS CONTROL

Enable Local Access

Choose A Connection

IPV4 ACL

Service	Enable	Source IP	Source Mask	Protocol	Port
FTP	<input type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	21
HTTP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	80
ICMP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	ICMP	-
SNMP	<input type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	161
SSH	<input type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	22
TELNET	<input type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	23
TFTP	<input type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	69
DNS	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	53

Remote Access Control

The Remote Access connection section enables you to allow or disallow WAN management access.

Enable Local Access: Check to enable local access control of services.

Choose a Connection: Select a connection from the drop-down menu on which to enable remote access.

REMOTE ACCESS CONTROLS

You can set a service control list (SCL) to enable or disable services from being used.

REMOTE ACCESS CONTROLS -- SERVICE

Choose A Connection : D_PPPE_0_1 ▼

IPV4 ACL

Service	Enable	Source IP	Source Mask	Protocol	Destination Port
FTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="2121"/>
HTTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="8080"/>
ICMP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	ICMP	-
SSH	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="22"/>
TELNET	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="23"/>
TFTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	<input type="text" value="69"/>
DNS	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	<input type="text" value="53"/>

IP Address

On this page, you can configure the IP address for the access control list (ACL). If ACL is enabled, only devices with the specified IP addresses can access the device.

Check **Enable Access Control Mode** to enable the ACL, then click **Add**, to reveal further options for adding an IP address to the ACL.

IP Address: Enter an IP Address to be added to the ACL.

IP ADDRESS

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

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

ACCESS CONTROL -- IP ADDRESSES

Enable Access Control Mode

IP

Add

Delete

IP ADDRESS

IP Address :

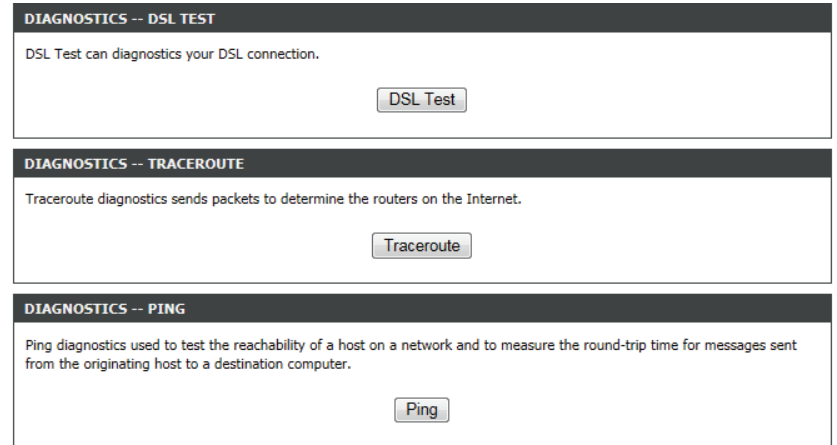
Apply

Cancel

Diagnostics

The Diagnostics section provides various method of testing your router and network.

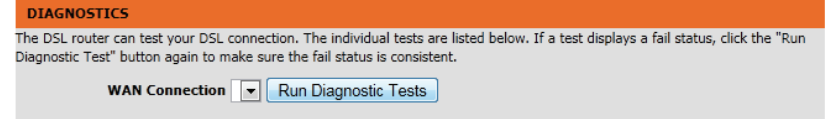
Click the **DSL Test**, **Traceroute**, or **Ping** buttons, to reveal the associated configuration options.



DSL Test

The DSL section provides a way for you to test your DSL connection.

WAN Connection: Select the connection from the drop-down menu that you would like to test. Then Click **Run Diagnostic Tests** to run the test.



Traceroute

The Traceroute section enables you to run a traceroute test. Configure your settings and click **Traceroute** to run the test.

Protocol: Select IPv4 or IPv6 to run the test on.

Host: Enter a host to run a traceroute against.

Max TTL: Enter a maximum value for TTL.

Wait times: Enter a maximum value for wait times between hops.

Result: The results of the traceroute test will be displayed here.

The screenshot shows a web interface for running a traceroute test. At the top, there is an orange header labeled "TRACEROUTE DIAGNOSIS" with a sub-header "Traceroute diagnostics sends packets to determine the routers on the Internet." Below this is a configuration section with the following fields: "Protocol" (a dropdown menu set to "IPv4"), "Host" (a text input field containing "192.168.1.1"), "Max TTL" (a text input field containing "30" with a range "(1-64)" to its right), and "Wait times" (a text input field containing "5000" with a range "(>1ms)" to its right). Below the configuration fields are two buttons: "Traceroute" and "Stop". At the bottom, there is a section labeled "RESULT" which contains a large, empty rectangular area with a vertical scrollbar on the right side, intended for displaying the test results.

Ping

The Ping section enables you to run a ping test.

- Protocol:** Select IPv4 or IPv6 to use for the ping test.
- Host:** Enter a host to ping.
- Number of retries:** Enter a value for the number of times you would like to ping the host.
- Timeout:** Enter a timeout value before a failure is declared.
- Packet Size:** Enter a value for the ping packet size.
- WAN Connection:** Select a WAN connection from the drop-down menu to use for the ping test.
- Result:** The results of the ping test will be displayed here.

The screenshot shows the 'PING DIAGNOSIS' section of a web interface. It includes a descriptive paragraph: 'Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer.' Below this is a configuration form with the following fields: 'Protocol' (a dropdown menu set to 'IPv4'), 'Host' (a text input field containing '8.8.8.8'), 'Number of retries' (a text input field containing '5'), 'Timeout' (a text input field containing '1'), 'Packet Size' (a text input field containing '56'), and 'WAN Connection' (a dropdown menu). A 'Ping...' button is located below the form. Below the form is a 'RESULT' section, which is currently empty and contains a large rectangular area with a vertical scrollbar on the right side.

System Log

The DSL-2750B keeps a running log of events and activities occurring on the router. You may send these logs to a SysLog server on your network. You can view the current log by clicking the **View System Log** button.

- Enable Log:** Check to enable or disable logging
- Mode:** Select to record the log to **Local**, **Remote**, or **Both**.
- Server IP Address:** Enter an IP address for the remote logging server.
- Server UDP Port:** Enter the UDP port of the remote server.

SYSTEM LOG

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

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

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

SYSTEM LOG -- CONFIGURATION

Enable Log

Mode : Local ▾

Server IP Address :

Server UDP Port :

Apply Cancel View System Log

Status

Device Info

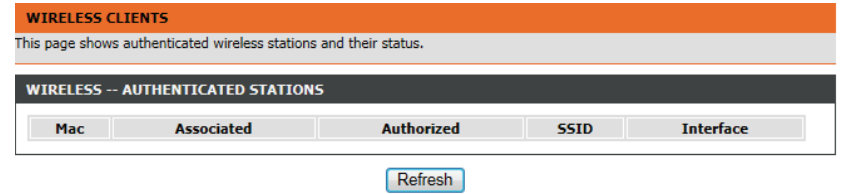
This page displays the current information for the DSL-2750B, such as LAN and wireless LAN information and statistics.

- System Info:** This section displays a summary of the system settings
- Internet Info:** This section displays of the internet connection settings.
- Wireless Info:** This section displays a summary of the wireless network settings.
- Storage Device Info:** This section displays a summary of the storage device and its settings.

DEVICE INFO			
This information reflects the current status of your all connection.			
SYSTEM INFO			
Modem Name :	DSL-2750B		
Serial Number :	001ee3470dd4		
Time and Date :	1970-01-07 13:43		
HardwareVersion :	E1		
Firmware Version :	EU_1.00		
System Up Time :	149:43:53		
INTERNET INFO			
Internet Connection Status :	DSL_DHCP_0_01 ▾		
IP Protocol :	IPv4 ▾		
Internet Connection Status:	Disconnected		
Wan service type:	Internet		
IP Address:	N/A		
Sub Mask:	N/A		
Default Gateway:	N/A		
DNS Server:	N/A		
Enabled WAN Connections :			
VPI/VCI	Service Name	Protocol	IGMP
8/35	DSL_DHCP_0_01	DHCP	Disable
WIRELESS INFO			
Select Wireless :	D-Link DSL-2750B ▾		
MAC Address:	00:1E:E3:47:0D:DD		
Status:	Enable		
Network Name (SSID):	D-Link DSL-2750B		
Visibility:	Visible		
Security Mode:	WPA/WPA2 Mixed		
STORAGE DEVICE INFORMATION			
MAC Address:	00:1E:E3:47:0D:D4		
IP Address:	192.168.0.1		
Subnet Mask:	255.255.255.0		
DHCP Server:	Enable		
STORAGE DEVICE INFORMATION			
Volumename	FileSystem	Total Space (MB)	Used Space (MB)

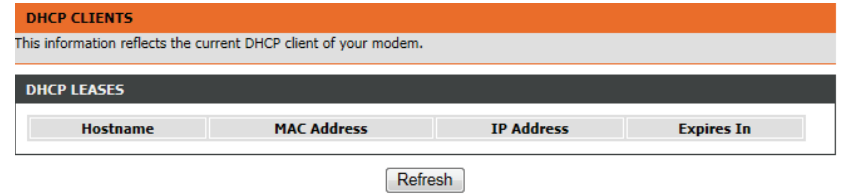
Wireless Clients

The wireless section allows you to view the wireless clients that are connected to your wireless networks.



DHCP Clients

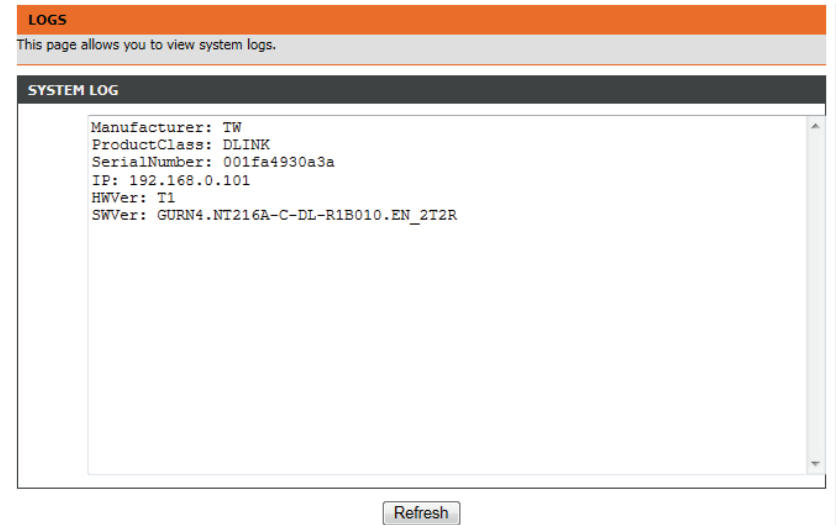
The DHCP Clients section allows you to view the clients that are connected to your router using DHCP.



Logs

The DSL-2750B keeps a running log of events and network activities passing through the router. If the device is rebooted, the logs will be cleared automatically.

The router automatically logs (records) events in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted while later events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view.



Statistics

The DSL-2750B keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the router point is rebooted.

Local Network & Wireless Info: This section displays a statistical summary of the LAN and wireless interfaces.

Internet: This section displays a statistical summary of the internet connection.

ADSL: This section displays a statistical summary of the ADSL interface. Click **Clear** to refresh the Data Counter statistics.

DEVICE INFO

This information reflects the current status of your all connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN1	1798695	17634	0	0	894625	2369	0	0
D-Link GO-DSL-AC750	0	0	0	0	0	0	0	0
D-Link GO-DSL-AC750_5G	0	0	0	0	0	0	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted				
			Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops	

ADSL

Status:	Disabled		
Mode:	N/A		
Traffic Type:	N/A		
Line Coding:	N/A		
Up Time:	N/A		
	Downstream		Upstream
SNR Margin (0.1dB):	N/A	N/A	
Attenuation (0.1dB):	N/A	N/A	
Output Power (dBm):	N/A	N/A	
Attainable Rate (Kbps):	N/A	N/A	
Rate (Kbps):	N/A	N/A	
D (interleave depth):	N/A	N/A	
Delay (msec):	N/A	N/A	
Data Counter:		N/A <input type="button" value="Clear"/>	N/A <input type="button" value="Clear"/>
HEC Errors:	N/A	N/A	
OCD Errors:	N/A	N/A	
LCD Errors:	N/A	N/A	
CRC Errors:	N/A	N/A	
FEC Errors:	N/A	N/A	
Total ES	N/A	N/A	
Total Frames	N/A	N/A	

Route Info

The Route Info page displays a summary of the current route configuration between the router and the WAN.

ROUTE INFO						
Flags: U - up, I - reject, G - gateway, H - host, R - reinstate D - dynamic (redirect), M - modified (redirect).						
DEVICE INFO -- ROUTE						
Destination	Gateway	Subnet Mask	Flags	Metric	Service	Interface
192.168.249.0	0.0.0.0	255.255.255.252	U	0	0	br0
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	br0

Help

This page provides help and explanations for different sections of the firmware.

HELP MENU

- [Setup](#)
- [Advanced](#)
- [Management](#)
- [Status](#)

SETUP HELP

- [Wizard](#)
- [Internet Setup](#)
- [Wireless Setup](#)
- [Local Network](#)
- [Local IPv6 Network](#)
- [Time and Date](#)

ADVANCED HELP

- [2.4G Advanced Wireless](#)
- [5G Advanced Wireless](#)
- [ALG](#)
- [Port Forwarding](#)
- [Port Trigger](#)
- [DMZ](#)
- [SMB](#)
- [3G](#)
- [Parental Control](#)
- [Filtering Options](#)
- [QoS](#)
- [DNS](#)
- [Anti-Attack](#)
- [DDNS](#)
- [Network Tools](#)
- [Routing](#)
- [NAT](#)
- [FTPD Setting](#)
- [FTPD Account](#)

MANAGEMENT HELP

- [System](#)
- [Firmware Update](#)
- [Access Controls](#)
- [Diagnostics](#)
- [System Log](#)

STATUS HELP

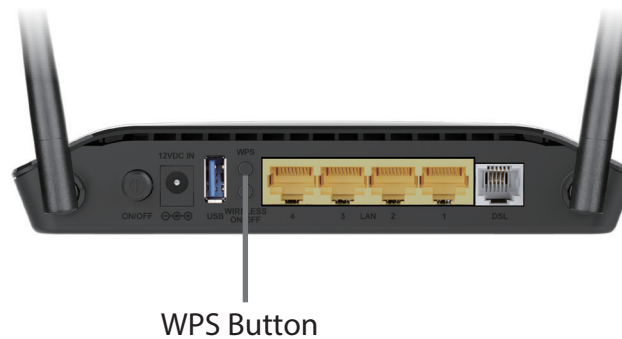
- [Device Info](#)
- [Wireless Clients](#)
- [DHCP Clients](#)
- [IPv6 Status](#)
- [Logs](#)
- [Statistics](#)
- [Route Info](#)

Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DSL-2750B router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the back of DSL-2750B for about 1 second. The Internet LED on the front will start to blink.



Step 2 - Within 2 minutes, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

Step 3 - Allow up to 1 minute to configure. Once the Internet light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

Windows® 8

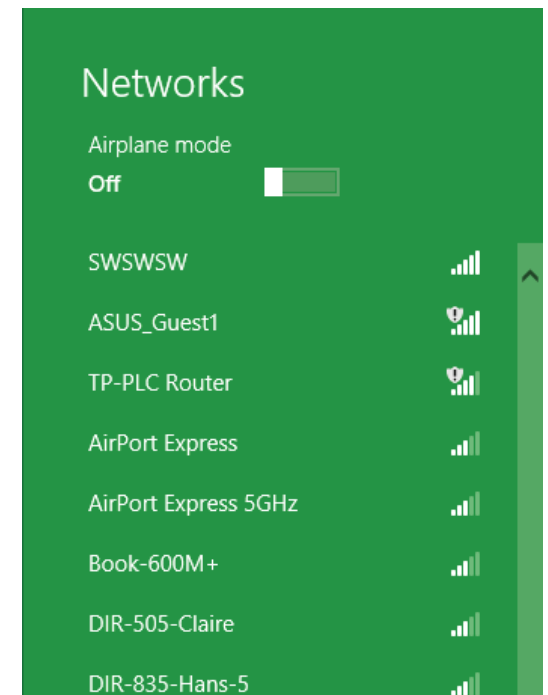
WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

To join an existing network, locate the wireless network icon in the taskbar, next to the time display.



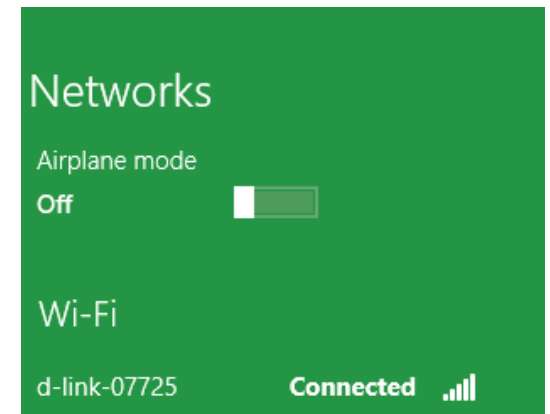
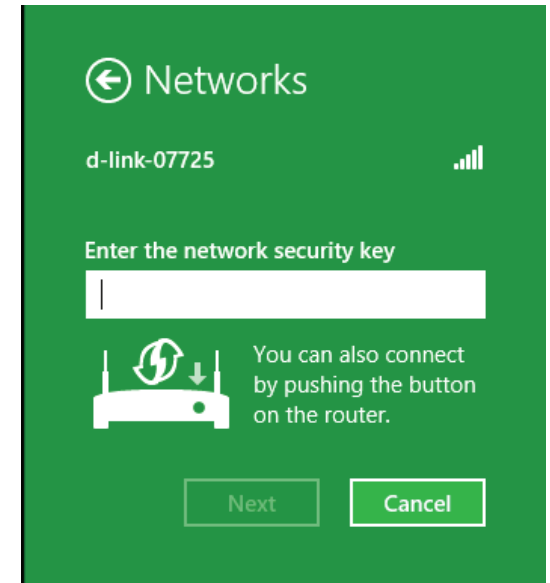
Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.



You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router at the point to enable the WPS function.

When you have established a successful connection a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.

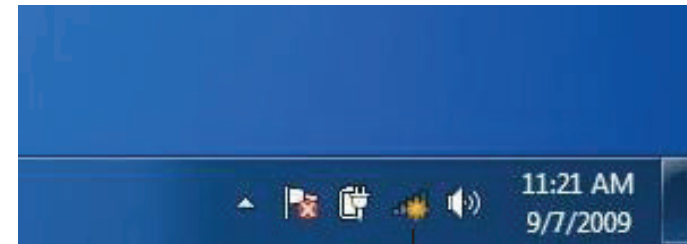


Windows® 7

WPA/WPA2

It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in your system tray (lower-right corner).



Wireless Icon

2. The utility will display any available wireless networks in your area.

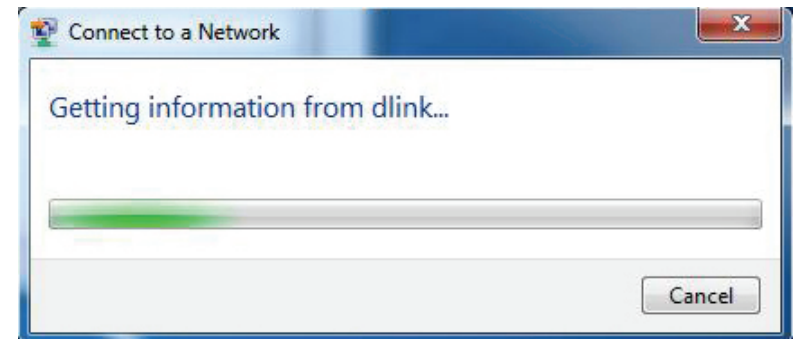


3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

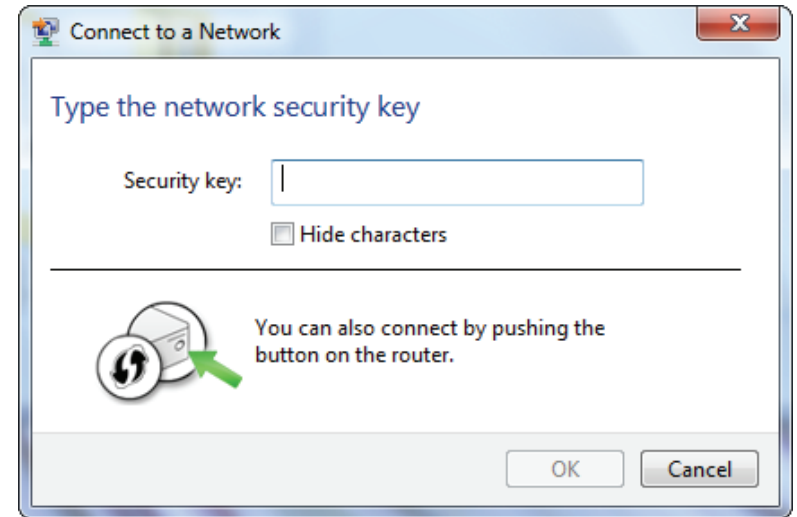


4. The following window appears while your computer tries to connect to the router.



5. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



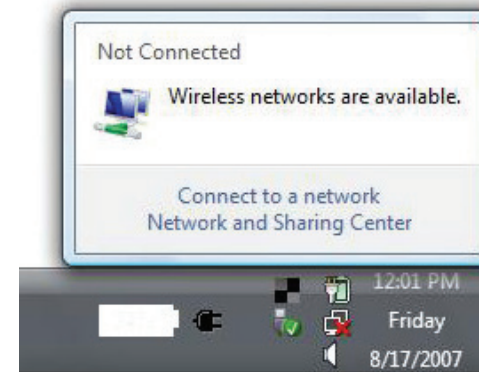
Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

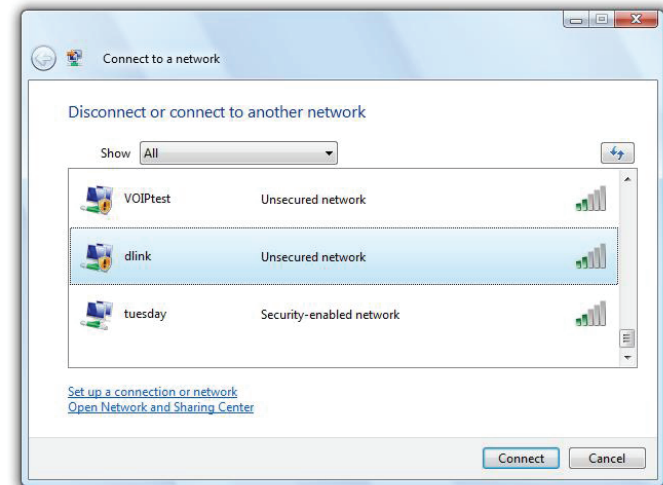
or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **Connect to a network**.



The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

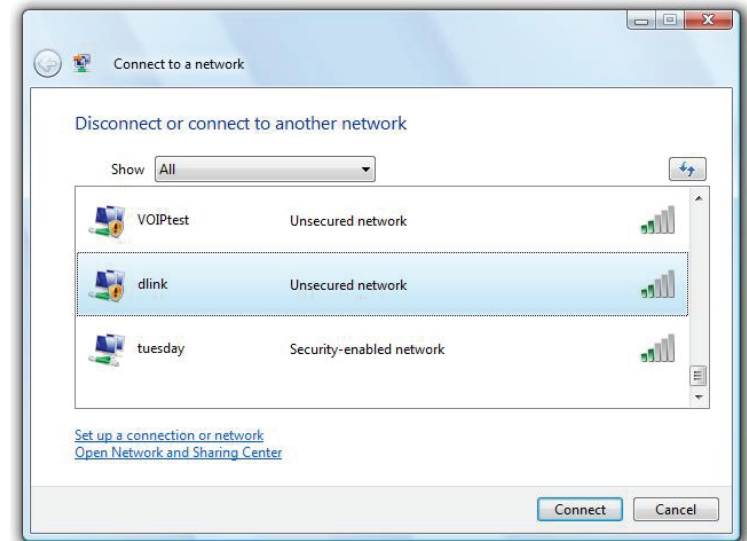
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

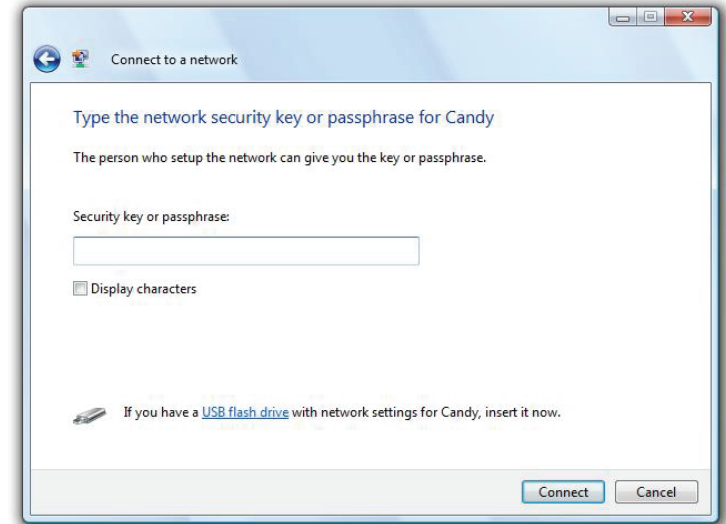
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.
2. Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



Windows® XP

Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

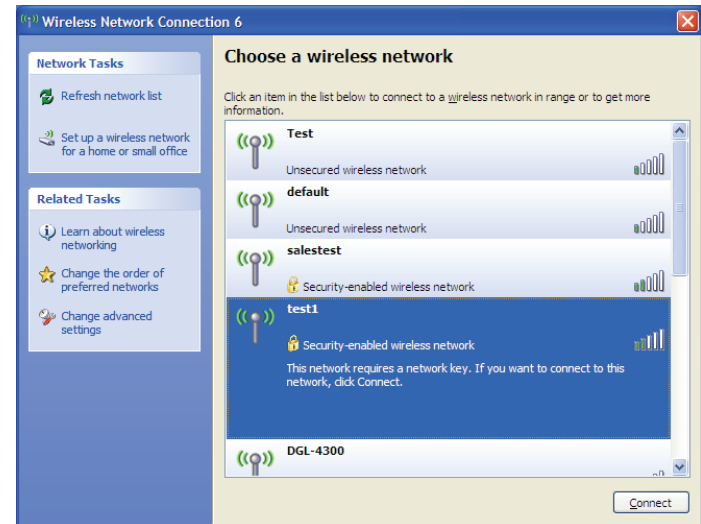
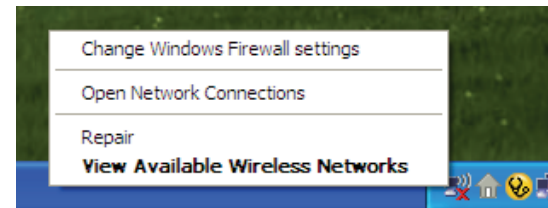
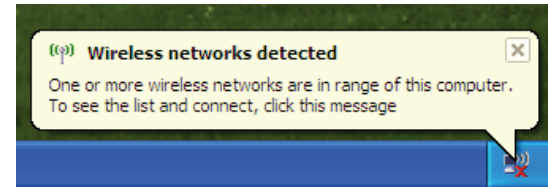
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in your system tray (lower-right corner next to the time). Select **View Available Wireless Networks**.

The utility will display any available wireless networks in your area. Click on a Wi-Fi network (displayed using the SSID) and click the **Connect** button.

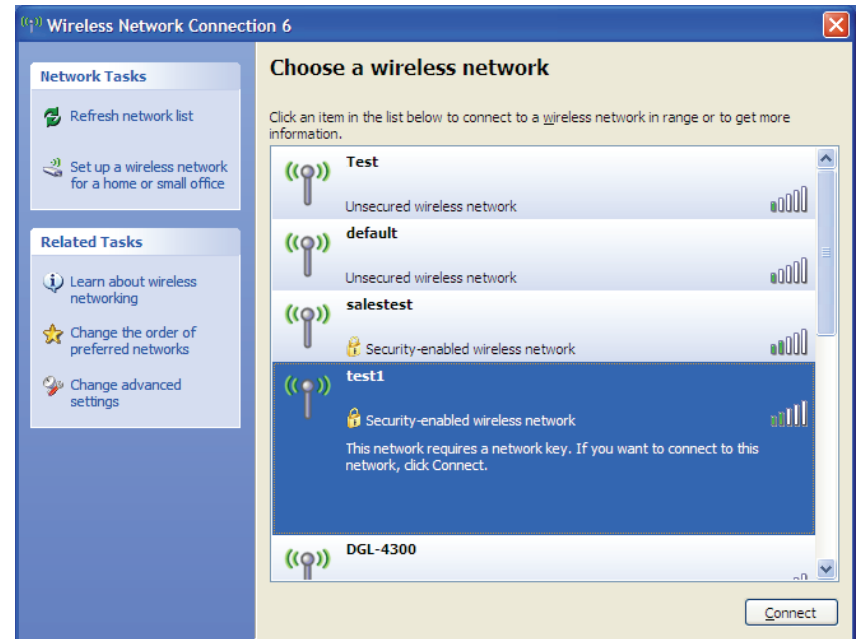
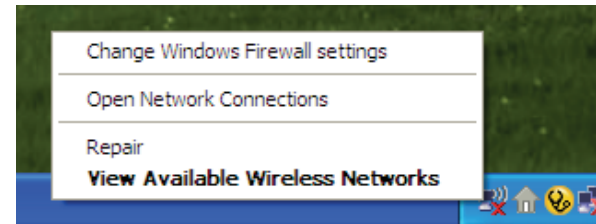
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

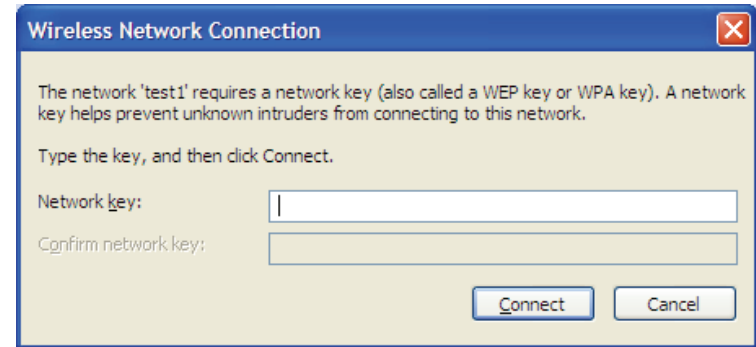
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.
2. Highlight the Wi-Fi network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK Wi-Fi password and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WPA-PSK settings are correct. The Wi-Fi password must be exactly the same as on the wireless router.



Troubleshooting

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

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

When entering the IP address of the D-Link router (**192.168.1.1** for example), you are not connecting to a website nor do you 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:
 - Microsoft Internet Explorer® 7 and higher
 - Mozilla Firefox 3.5 and higher
 - Google™ Chrome 8 and higher
 - Apple Safari 4 and 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 ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.1.1. When logging in, the username is **admin** and leave the password box empty.

3. Why can't I connect to certain sites or send and receive emails when connecting through my router?

If you are having a problem sending or receiving email, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

To find the proper MTU Size, you'll have to do a special ping of the destination you're trying to go to. A destination could be another computer, or a URL.

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

ping [url] [-f] [-l] [MTU value]

Example: **ping yahoo.com -f -l 1472**

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, let's say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with ($1452+28=1480$).

Once you find your MTU, you can now configure your router with the proper MTU size.

To change the MTU rate on your router follow the steps below:

- Open your browser, enter the IP address of your router (192.168.1.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

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 has 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, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

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

Where is wireless used?

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

Using a D-Link CardBus adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: airports, hotels, coffee shops, libraries, restaurants, and convention centers.

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

Tips

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

Centralize Your Router or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

Infrastructure – All wireless clients will connect to an access point or wireless router.

Ad-Hoc – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-850L wireless network CardBus adapters.

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

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

Networking Basics

Check your IP address

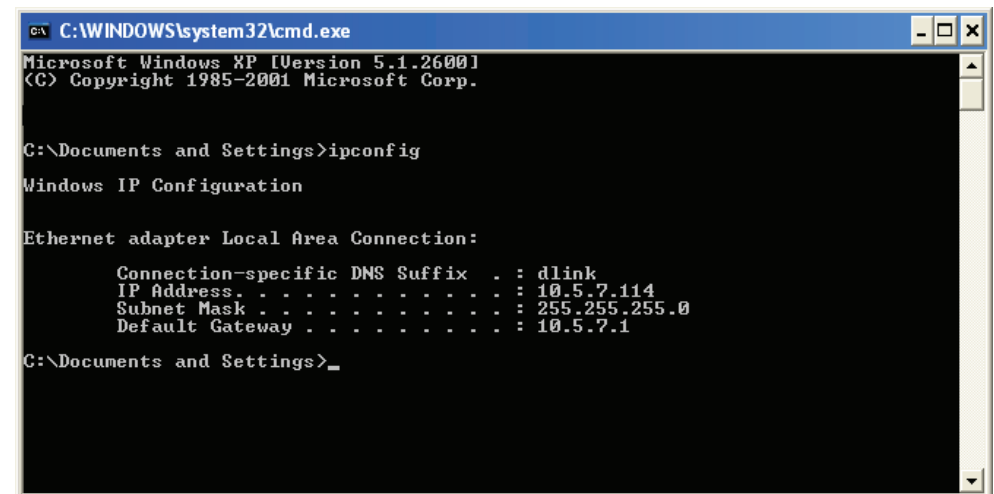
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows® 7/Vista® users type **cmd** in the **Start Search** box.)

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.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600.1
(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® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.
- Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections**.
- Windows® XP - Click on **Start > Control Panel > Network Connections**.
- Windows® 2000 - From the desktop, right-click **My Network Places > Properties**.

Step 2

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

Step 3

Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

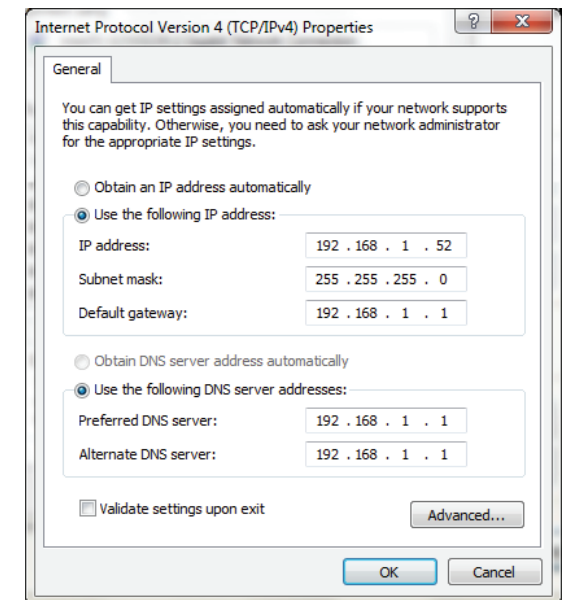
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.1.1, make your IP address 192.168.1.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.1.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.1.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5

Click **OK** twice to save your settings.



Technical Specifications

Hardware Specifications

- LAN Interface: Four 10/100 Mbps LAN ports
- Wireless Interface (2.4 GHz): IEEE 802.11b/g/n
- USB Interface: Compliant USB 2.0

Operating Voltage

- Input: 100~240 V ($\pm 20\%$), 50~60 Hz
- Output: DC 12 V, 1 A

Temperature

- Operating: 32 ~ 104 °F (0 ~ 40 °C)
- Non-Operating: -4 ~ 149 °F (-20 ~ 65 °C)

Humidity

- Operating: 10% - 90% non-condensing
- Non-Operating: 5% - 95% non-condensing

Wireless Frequency Range

- IEEE 802.11 b/g/n: 2412-2472 MHz

ADSL Standards

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

ADSL2 Standards

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

ADSL2+ Standards

- ITU-T G.992.5 Annex A/L/M

Wireless Bandwidth Rate

- IEEE 802.11b: 11, 5.5, 2, and 1 Mbps
- IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11n: 6.5 to 150 Mbps
20 MHz: 150, 130, 117, 104, 78, 52, 39, 26, 13 Mbps
40 MHz: 300, 270, 243, 216, 162, 108, 81, 54, 27 Mbps

Antenna Type

- Two non-detachable MIMO antennas

Wireless Security

- 64/128-bit WEP, WPA/WPA2-Personal
- WPA/WPA2-Enterprise
- WPS (PIN & PBC)

Certifications

- CE

Dimensions & Weight

- 173.8 x 115.1 x 32.5 mm (6.8 x 4.5 x 1.28 inches)
- 207.5 grams (7.32 ounces)

Regulatory Information

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. For more information, please refer to the Declaration of Conformity.

Notice of Wireless Radio LAN Usage in The European Community

- At the time of writing this addendum, some countries such as Italy, Greece, Portugal and Spain have not allowed operation of radio devices in the 5 GHz bands, although operation of 2.4 GHz radio devices are allowed. Please check with your local authority to confirm.
- This device is restricted to indoor use when operated in the European Community using channels in the 5.15-5.35 GHz band to reduce the potential for interference.
- This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France where restrictive use applies. This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIR P in the frequency range of 2454 –2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France. This equipment may be operated in AL, AD , BE , BG, DK, DE , FI, FR, GR, GW, IS, IT , HR , LI, LU, MT , MK, MD , MC , NL, NO, AT , OL, PT, RO, SM, SE, RS, SK, ES, CI , HU , CY.

Usage Notes:

- To remain in conformance with European National spectrum usage regulations, frequency and channel limitations will be applied on the products according to the country where the equipment will be deployed.
- This device is restricted from functioning in Ad-hoc mode while operating in 5 GHz. Ad-hoc mode is direct peer-to-peer communication between two client devices without an Access Point.
- Access points will support DFS (Dynamic Frequency Selection) and TPC (Transmit Power Control) functionality as required when operating in 5 GHz within the EU.



2.4 GHz wireless frequency operation in EEC countries

Region	Frequency Band	Max output power (EIRP)
Metropolitan	2400 - 2454 MHz	100 mW
Guadeloupe, Martinique, St Pierre et Miquelon, Mayotte	2454 - 2483.5 MHz	100 mW indoor, 10 mW outdoor
Reunion et Guyane	2400 - 2483.5 MHz	100 mW
Rest of EU community	2420 - 2483.5 MHz	100 mW

R&TTE 1999/5/EC			
WLAN 2.4 - 2.4835 GHz			
IEEE 802.11b/g/n			
Spectrum Regulation	MHz, Europa (ETSI)	max. EIRP Innenbereich	max. EIRP Außenbereich
Europa	2400 - 2483.5 MHz	100 mW	100 mW
Frankreich	2400 - 2454 MHz	100 mW	100 mW
	2454 - 2483.5 MHz	100 mW	10 mW

European Community Declaration of Conformity:

Česky [Czech]	D-Link tímto prohlašuje, že tento DSL-2750B je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede D-Link erklærer herved, at følgende udstyr DSL-2750B overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt D-Link, dass sich das Gerät DSL-2750B in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab D-Link seadme DSL-2750B vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, D-Link, declares that this DSL-2750B is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente D-Link declara que el DSL-2750B cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ D-Link ΔΗΛΩΝΕΙ ΟΤΙ DSL-2750B ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/EK.
Français [French]	Par la présente D-Link déclare que l'appareil DSL-2750B est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente D-Link dichiara che questo DSL-2750B è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo D-Link deklarē, ka DSL-2750B atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo D-Link deklaruoja, kad šis DSL-2750B atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart D-Link dat het toestel DSL-2750B in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.

Malti [Maltese]	Hawnhekk, D-Link, jiddikjara li dan DSL-2750B jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, D-Link nyilatkozom, hogy a DSL-2750B megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym D-Link oświadcza, że DSL-2750B jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	D-Link declara que este DSL-2750B está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	D-Link izjavlja, da je ta DSL-2750B v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	D-Link týmto vyhlasuje, že DSL-2750B spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	D-Link vakuuttaa täten että DSL-2750B tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.

Warning Statement

The power outlet should be nearby the device and easily accessible.

Safety Instructions

Please adhere to the following safety guidelines to help ensure your own personal safety and protect your system from potential damage. Any acts taken that are inconsistent with ordinary use of the product, including improper testing, etc., and those not expressly approved by D-Link may result in the loss of product warranty.

Unless expressly approved by an authorized representative of D-Link in writing, you may not and may not permit others to:

- Disassemble or reverse engineer the device or attempt to derive source code (underlying ideas, algorithms, or structure) from the device or from any other information provided by D-Link, except to the extent that this restriction is expressly prohibited by local law.
- Modify or alter the device.
- Remove from the device any product identification or other notices, including copyright notices and patent markings, if any.

To reduce the risk of bodily injury, electrical shock, fire, and damage to the device and other equipment, observe the following precautions:

Power Sources

- Observe and follow service markings.
- Do not push any objects into the openings of your device unless consistent with the authorized operation of the device. Doing so can cause a fire or an electrical shock by shorting out interior components.
- The powering of this device must adhere to the power specifications indicated for this product.
- Do not overload wall outlets and/or extension cords as this will increase the risk of fire or electrical shock.
- Do not rest anything on the power cord or on the device (unless the device is made and expressly approved as suitable for stacking).
- Position system cables and power cables carefully; route cables so that they cannot be stepped on or tripped over. Be sure that nothing rests on any cables.
- Operate the device only from the type of external power source indicated on the electrical ratings label.
- To help avoid damaging your device, be sure the voltage selection switch (if provided) on the power supply is set to match the power available at your location.
- Also be sure that attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided a power cable for your device or for any AC -powered option intended for your device, purchase a power cable that is approved for use in your country and is suitable for use with your device. The power cable must be rated for the device and for the voltage and current marked on the device's electrical ratings label. The voltage and current rating of the cable should be greater than the ratings marked on the device.
- To help prevent an electrical shock, plug the device and peripheral power cables into properly grounded electrical outlets. These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Ensure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80 percent of the ampere ratings limit for the extension cable or power strip.
- To help protect your device from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications. Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your device, observe the following

guidelines.

- Install the power supply before connecting the power cable to the power supply.
- Unplug the power cable before removing the power supply.
- If the system has multiple sources of power, disconnect power from the device by unplugging all power cables from the power supplies.

Servicing/Disassembling

- Do not service any product except as expressly set forth in your system documentation.
- Opening or removing covers that are marked with the triangular symbol with a lightning bolt may expose you to an electrical shock. Only a trained service technician should service components inside these compartments.
- To reduce the risk of electrical shock, never disassemble this device. None of its internal parts are user-replaceable; therefore, there is no reason to access the interior.
- Do not spill food or liquids on your system components, and never operate the device in a wet environment. If the device gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Use the device only with approved equipment.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

Environment

- Do not use this device near water (e.g. near a bathtub, sink, laundry tub, fish tank, in a wet basement or near a swimming pool).
- Do not use this device in areas with high humidity.
- This device must not be subjected to water or condensation.
- Keep your device away from radiators and heat sources. Also, do not block cooling vents.

Cleaning

- Always unplug the power before cleaning this device.
- Do not use liquid or aerosol cleaners of any kind. Use only compressed air that is recommended for electronic devices.
- Use a dry cloth for cleaning.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from

your body before you touch any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to help prevent damage from electrostatic discharge (ESD):

1. When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
2. When transporting a sensitive component, first place it in an antistatic container or packaging.
3. Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads, and an antistatic grounding strap.

ErP Power Usage

This device is an Energy Related Product (ErP) that automatically switches to a power-saving Network Standby mode within 1 minute of no packets being transmitted. It can also be turned off through a power switch to save energy when it is not needed.

Network Standby: 4.58 watts

Switched Off: 0.23 watts

Disposing of and Recycling Your Product



ENGLISH

This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in the household waste but sent for recycling. Please take it to a collection point designated by your local authorities once it has reached the end of its life, some will accept products for free.

By recycling the product and its packaging in this manner you help to conserve the environment and protect human health.

D-Link and the Environment

At D-Link, we understand and are committed to reducing any impact our operations and products may have on the environment. To minimise this impact D-Link designs and builds its products to be as environmentally friendly as possible, by using recyclable, low toxic materials in both products and packaging.

D-Link recommends that you always switch off or unplug your D-Link products when they are not in use. By doing so you will help to save energy and reduce CO2 emissions.

To learn more about our environmentally responsible products and packaging please visit www.dlinkgreen.com



DEUTSCH DE

Dieses Symbol auf dem Produkt oder der Verpackung weist darauf hin, dass dieses Produkt gemäß bestehender örtlicher Gesetze und Vorschriften nicht über den normalen Hausmüll entsorgt werden sollte, sondern einer Wiederverwertung zuzuführen ist. Bringen Sie es bitte zu einer von Ihrer Kommunalbehörde entsprechend amtlich ausgewiesenen Sammelstelle, sobald das Produkt das Ende seiner Nutzungsdauer erreicht hat. Für die Annahme solcher Produkte erheben einige dieser Stellen keine Gebühren. Durch ein auf diese Weise durchgeführtes Recycling des Produkts und seiner Verpackung helfen Sie, die Umwelt zu schonen und die menschliche Gesundheit zu schützen.

D-Link und die Umwelt

D-Link ist sich den möglichen Auswirkungen seiner Geschäftstätigkeiten und seiner Produkte auf die Umwelt bewusst und fühlt sich verpflichtet, diese entsprechend zu mindern. Zu diesem Zweck entwickelt und stellt D-Link seine Produkte mit dem Ziel größtmöglicher Umweltfreundlichkeit her und verwendet wiederverwertbare, schadstoffarme Materialien bei Produktherstellung und Verpackung.

D-Link empfiehlt, Ihre Produkte von D-Link, wenn nicht in Gebrauch, immer auszuschalten oder vom Netz zu nehmen. Auf diese Weise helfen Sie, Energie zu sparen und CO₂-Emissionen zu reduzieren.

Wenn Sie mehr über unsere umweltgerechten Produkte und Verpackungen wissen möchten, finden Sie entsprechende Informationen im Internet unter www.dlinkgreen.com.



FRANÇAIS FR

Ce symbole apposé sur le produit ou son emballage signifie que, conformément aux lois et réglementations locales, ce produit ne doit pas être éliminé avec les déchets domestiques mais recyclé. Veuillez le rapporter à un point de collecte prévu à cet effet par les autorités locales; certains accepteront vos produits gratuitement. En recyclant le produit et son emballage de cette manière, vous aidez à préserver l'environnement et à protéger la santé de l'homme.

D-Link et l'environnement

Chez D-Link, nous sommes conscients de l'impact de nos opérations et produits sur l'environnement et nous engageons à le réduire. Pour limiter cet impact, D-Link conçoit et fabrique ses produits de manière aussi écologique que possible, en utilisant des matériaux recyclables et faiblement toxiques, tant dans ses produits que ses emballages.

D-Link recommande de toujours éteindre ou débrancher vos produits D-Link lorsque vous ne les utilisez pas. Vous réaliserez ainsi des économies d'énergie et réduirez vos émissions de CO₂.

Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le www.dlinkgreen.com



ESPAÑOL ES

Este símbolo en el producto o el embalaje significa que, de acuerdo con la legislación y la normativa local, este producto no se debe desechar en la basura doméstica sino que se debe reciclar. Llévelo a un punto de recogida designado por las autoridades locales una vez que ha llegado al fin de su vida útil; algunos de ellos aceptan recogerlos de forma gratuita. Al reciclar el producto y su embalaje de esta forma, contribuye a preservar el medio ambiente y a proteger la salud de los seres humanos.

D-Link y el medio ambiente

En D-Link, comprendemos y estamos comprometidos con la reducción del impacto que puedan tener nuestras actividades y nuestros productos en el medio ambiente. Para reducir este impacto, D-Link diseña y fabrica sus productos para que sean

lo más ecológicos posible, utilizando materiales reciclables y de baja toxicidad tanto en los productos como en el embalaje.

D-Link recomienda apagar o desenchufar los productos D-Link cuando no se estén utilizando. Al hacerlo, contribuirá a ahorrar energía y a reducir las emisiones de CO2.

Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio www.dlinkgreen.com



ITALIANO IT

La presenza di questo simbolo sul prodotto o sulla confezione del prodotto indica che, in conformità alle leggi e alle normative locali, questo prodotto non deve essere smaltito nei rifiuti domestici, ma avviato al riciclo. Una volta terminato il ciclo di vita utile, portare il prodotto presso un punto di raccolta indicato dalle autorità locali. Alcuni questi punti di raccolta accettano gratuitamente i prodotti da riciclare. Scegliendo di riciclare il prodotto e il relativo imballaggio, si contribuirà a preservare l'ambiente e a salvaguardare la salute umana.

D-Link e l'ambiente

D-Link cerca da sempre di ridurre l'impatto ambientale dei propri stabilimenti e dei propri prodotti. Allo scopo di ridurre al minimo tale impatto, D-Link progetta e realizza i propri prodotti in modo che rispettino il più possibile l'ambiente, utilizzando materiali riciclabili a basso tasso di tossicità sia per i prodotti che per gli imballaggi.

D-Link raccomanda di spegnere sempre i prodotti D-Link o di scollegarne la spina quando non vengono utilizzati. In questo modo si contribuirà a risparmiare energia e a ridurre le emissioni di anidride carbonica.

Per ulteriori informazioni sui prodotti e sugli imballaggi D-Link a ridotto impatto ambientale, visitate il sito all'indirizzo www.dlinkgreen.com



NEDERLANDS NL

Dit symbool op het product of de verpakking betekent dat dit product volgens de plaatselijke wetgeving niet mag worden weggegooid met het huishoudelijk afval, maar voor recyclage moeten worden ingeleverd. Zodra het product het einde van de levensduur heeft bereikt, dient u het naar een inzamelpunt te brengen dat hiertoe werd aangeduid door uw plaatselijke autoriteiten, sommige autoriteiten accepteren producten zonder dat u hiervoor dient te betalen.

Door het product en de verpakking op deze manier te recyclen helpt u het milieu en de gezondheid van de mens te beschermen.

D-Link en het milieu

Bij D-Link spannen we ons in om de impact van onze handelingen en producten op het milieu te beperken. Om deze impact te beperken, ontwerpt en bouwt D-Link zijn producten zo milieuvriendelijk mogelijk, door het gebruik van recycleerbare producten met lage toxiciteit in product en verpakking.

D-Link raadt aan om steeds uw D-Link producten uit te schakelen of uit de stekker te halen wanneer u ze niet gebruikt. Door dit te doen bespaart u energie en beperkt u de CO₂-emissies.

Breng een bezoek aan www.dlinkgreen.com voor meer informatie over onze milieuverantwoorde producten en verpakkingen



POLSKI PL

Ten symbol umieszczony na produkcie lub opakowaniu oznacza, że zgodnie z miejscowym prawem i lokalnymi przepisami niniejszego produktu nie wolno wyrzucać jak odpady czy śmieci z gospodarstwa domowego, lecz należy go poddać procesowi recyklingu. Po zakończeniu użytkowania produktu, niektóre odpowiednie do tego celu podmioty przyjmą takie produkty nieodpłatnie, dlatego prosimy dostarczyć go do punktu zbiórki wskazanego przez lokalne władze.

Poprzez proces recyklingu i dzięki takiemu postępowaniu z produktem oraz jego opakowaniem, pomogą Państwo chronić środowisko naturalne i dbać o ludzkie zdrowie.

D-Link i środowisko

W D-Link podchodzimy w sposób świadomy do ochrony otoczenia oraz jesteśmy zaangażowani w zmniejszanie wpływu naszych działań i produktów na środowisko naturalne. W celu zminimalizowania takiego wpływu firma D-Link konstruuje i wytwarza swoje produkty w taki sposób, aby były one jak najbardziej przyjazne środowisku, stosując do tych celów materiały nadające się do powtórnego wykorzystania, charakteryzujące się małą toksycznością zarówno w przypadku samych produktów jak i opakowań.

Firma D-Link zaleca, aby Państwo zawsze prawidłowo wyłączali z użytku swoje produkty D-Link, gdy nie są one wykorzystywane. Postępując w ten sposób pozwalają Państwo oszczędzać energię i zmniejszać emisje CO₂.

"Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną internetową www.dlinkgreen.com."



ČESKY CZ

Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odneste jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklační výrobku i obalu pomáháte chránit životní prostředí i lidské zdraví.

D-Link a životní prostředí

"Ve společnosti D-Link jsme si vědomi vlivu našich provozů a výrobků na životní prostředí a snažíme se o minimalizaci těchto vlivů. Proto své výrobky navrhujeme a vyrábíme tak, aby byly co nejekologičtější, a ve výrobcích i obalech používáme recyklovatelné a nízkotoxické materiály."

"Společnost D-Link doporučuje, abyste své výrobky značky D-Link vypnuli nebo vytáhli ze zásuvky vždy, když je nepoužíváte. Pomůžete tak šetřit energii a snížit emise CO₂."

Více informací o našich ekologických výrobcích a obalech najdete na adrese www.dlinkgreen.com.



MAGYAR HU

Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által kijelölt gyűjtőhelyre. A termékek egyes helyeken ingyen elhelyezhetők. A termék és a csomagolás újrahasznosításával segíti védeni a környezetet és az emberek egészségét.

A D-Link és a környezet

A D-Linknél megértjük és elkötelezettek vagyunk a műveleteink és termékeink környezetre gyakorolt hatásainak csökkentésére. Az ezen hatás csökkentése érdekében a D-Link a lehető leginkább környezetbarát termékeket tervez és gyárt azáltal, hogy újrahasznosítható, alacsony károsanyag-tartalmú termékeket gyárt és csomagolásokat alkalmaz.

A D-Link azt javasolja, hogy mindig kapcsolja ki vagy húzza ki a D-Link termékeket a tápforrásból, ha nem használja azokat. Ezzel segít az energia megtakarításában és a széndioxid kibocsátásának csökkentésében.

Környezetbarát termékeinkről és csomagolásainkról további információkat a www.dlinkgreen.com weboldalon tudhat meg.

NORSK NO



Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning.

Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden.

Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

D-Link og miljøet

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet.

For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

D-Link anbefaler at du alltid slår av eller frakobler D-Link-produkter når de ikke er i bruk. Ved å gjøre dette hjelper du å spare energi og å redusere CO₂-utslipp.

"For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til www.dlinkgreen.com"

DANSK DK



Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever

produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. I nogle tilfælde vil produktet blive modtaget gratis. Ved at indlevere produktet og dets emballage til genbrug på denne måde bidrager du til at beskytte miljøet og den menneskelige sundhed.

D-Link og miljøet

Hos D-Link forstår vi og bestræber os på at reducere enhver indvirkning, som vores aktiviteter og produkter kan have på miljøet. For at minimere denne indvirkning designer og producerer D-Link sine produkter, så de er så miljøvenlige som muligt, ved at bruge genanvendelige materialer med lavt giftighedsniveau i både produkter og emballage.

D-Link anbefaler, at du altid slukker eller frakobler dine D-Link-produkter, når de ikke er i brug. Ved at gøre det bidrager du til at spare energi og reducere CO₂-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på www.dlinkgreen.com



SUOMI FI

Tämä symboli tuotteen pakkauksessa tarkoittaa, että paikallisten lakien ja säännösten mukaisesti tätä tuotetta ei pidä hävittää yleisen kotitalousjätteen seassa vaan se tulee toimittaa kierrätettäväksi. Kun tuote on elinkaarensa päässä, toimita se lähimpään viranomaisten hyväksymään kierrätyspisteeseen. Kierrättämällä käytetyn tuotteen ja sen pakkauksen autat tukemaan sekä ympäristön että ihmisten terveyttä ja hyvinvointia.

D-Link ja ympäristö

D-Link ymmärtää ympäristönsuojelun tärkeyden ja on sitoutunut vähentämään tuotteistaan ja niiden valmistuksesta ympäristölle mahdollisesti aiheutuvia haittavaikutuksia. Nämä negatiiviset vaikutukset minimoidakseen D-Link suunnittelee ja valmistaa tuotteensa mahdollisimman ympäristöystävällisiksi käyttämällä kierrätettäviä, alhaisia pitoisuuksia haitallisia aineita sisältäviä materiaaleja sekä tuotteissaan että niiden pakkauksissa.

Suosittellemme, että irrotat D-Link-tuotteesi virtalähteestä tai sammutat ne aina, kun ne eivät ole käytössä. Toimimalla näin autat säästämään energiaa ja vähentämään hiilidioksiidipäästöjä.

"Lue lisää ympäristöystävällisistä D-Link-tuotteista ja pakkauksistamme osoitteesta www.dlinkgreen.com"



SVENSKA SE

Den här symbolen på produkten eller förpackningen betyder att produkten enligt lokala lagar och föreskrifter inte skall kastas i hushållssoporna utan i stället återvinnas. Ta den vid slutet av dess livslängd till en av din lokala myndighet utsedd uppsamlingsplats, vissa accepterar produkter utan kostnad. Genom att på detta sätt återvinna produkten och förpackningen hjälper du till att bevara miljön och skydda människors hälsa.

D-Link och miljön

På D-Link förstår vi och är fast beslutna att minska den påverkan våra verksamheter och produkter kan ha på miljön. För att minska denna påverkan utformar och bygger D-Link sina produkter för att de ska vara så miljövänliga som möjligt, genom att använda återvinningsbara material med låg gifthalt i både produkter och förpackningar.

D-Link rekommenderar att du alltid stänger av eller kopplar ur dina D-Link produkter när du inte använder dem. Genom att göra detta hjälper du till att spara energi och minska utsläpp av koldioxid.

För mer information om våra miljöansvariga produkter och förpackningar www.dlinkgreen.com



PORTUGUÊS PT

Este símbolo no produto ou embalagem significa que, de acordo com as leis e regulamentações locais, este produto não deverá ser eliminado juntamente com o lixo doméstico mas enviado para a reciclagem. Transporte-o para um ponto de recolha designado pelas suas autoridades locais quando este tiver atingido o fim da sua vida útil, alguns destes pontos aceitam produtos gratuitamente. Ao reciclar o produto e respectiva embalagem desta forma, ajuda a preservar o ambiente e protege a saúde humana.

A D-Link e o ambiente

Na D-Link compreendemos e comprometemo-nos com a redução do impacto que as nossas operações e produtos possam ter no ambiente. Para minimizar este impacto a D-Link concebe e constrói os seus produtos para que estes sejam o mais inofensivos para o ambiente possível, utilizando materiais recicláveis e não tóxicos tanto nos produtos como nas embalagens.

A D-Link recomenda que desligue os seus produtos D-Link quando estes não se encontrarem em utilização. Com esta acção ajudará a poupar energia e reduzir as emissões de CO2.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite www.dlinkgreen.com