



User Manual

Wireless N300 ADSL2+ Modem Router

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	April 06, 2016	• Release for revision A1

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.

Chrome™ browser, Google Play™ and Android™ are trademarks of Google Inc.

Internet Explorer®, Windows® and the Windows logo are trademarks of the Microsoft group of companies.

Copyright © 2016 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.

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: 4.165 watts

Switched Off: 0.004 watts

Table of Contents

Product Overview	1	Wireless Security	49
Package Contents	1	Time and Date	54
System Requirements	2	Support	55
Introduction	3	Logout	56
Features	4	Advanced	57
Hardware Overview	5	Advanced LAN	58
Front LED Panel	5	ADSL Settings	59
Back	6	Advanced Wireless	60
Installation	7	Wireless Advanced	61
Before you Begin	7	Wireless Access Control	63
Wireless Installation Considerations	8	Wi-Fi Protected Setup	64
Manual Setup	9	MBSSID Security Settings	65
Getting Started	12	Port Triggering	70
Web-based Configuration Utility	13	Port Forwarding	72
Wizard	14	DMZ	74
Configuration	20	Parent Control	75
Setup	21	URL Block	76
Local Network	22	Online Time Limit	77
Local Network	23	Schedules	78
IPv6 Local Network	25	Filtering Options	79
Internet Setup	28	IP/Port Filter	80
Create a New Connection	29	IPv6/Port Filter	82
Modify an Existing Connection	40	MAC Filter	84
Wireless Setup	47	Anti-Attack Settings	85
Wireless Basics	48	DNS	86
		DNS	87
		IPv6 DNS	88

Dynamic DNS	89	ADSL	120
Network Tools	90	Diag Test.....	121
Port Mapping	91	System Log.....	122
IGMP Proxy Configuration	92	Status	123
IP QoS.....	93	Device Info	124
UPnP	94	Wireless Clients.....	125
ARP Binding	95	DHCP Clients	126
Routing.....	96	ADSL Status.....	127
Static Routing.....	97	Statistics	128
IPv6 Static Route	99	Route Info	129
RIP.....	100	Help	130
ALG.....	101	Connect a Wireless Client to your Router	131
NAT ALG.....	102	WPS Button.....	131
NAT Exclude IP	103	Windows® 10	132
NAT Forwarding.....	104	Windows® 8.....	134
FTP ALG Config	105	WPA/WPA2	134
NAT IP Mapping.....	106	Windows® 7.....	136
Wireless Schedules.....	107	WPA/WPA2	136
Management.....	108	WPS.....	139
System	109	Troubleshooting	143
Firmware Update	110	Wireless Basics	147
Access Control List.....	111	What is Wireless?.....	148
Access Control List.....	112	Tips.....	150
Access Control List IPv6	113	Wireless Modes.....	151
Password.....	115	Networking Basics	152
Diagnostics	116	Check your IP address.....	152
Ping	117	Statically assign an IP address.....	153
Ping6.....	118		
Traceroute.....	119		

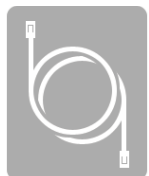
Technical Specifications154

Regulatory Statements155

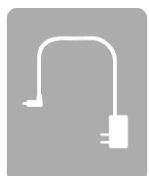
Package Contents



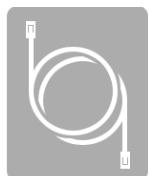
Wireless N300 ADSL2+ Modem Router



Ethernet Cable



Power Adapter



ADSL Telephone Cable



Quick Installation Guide

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">• Wired 10/100 Ethernet Devices/Computers or Wireless Ethernet 802.11 n/g/b Devices/Computers• A DSL enabled Internet Connection with a subscription to an Internet Service Provider
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:</p> <ul style="list-style-type: none">• Internet Explorer 8 or higher• Firefox 20 or higher• Safari 4 or higher• Chrome 25 or higher <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-2745 Wireless N300 ADSL2+ Modem Router is a versatile, high-performance router for homes and small offices. With integrated ADSL2/2+ supporting up to 24 Mbps download speeds, 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.

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.

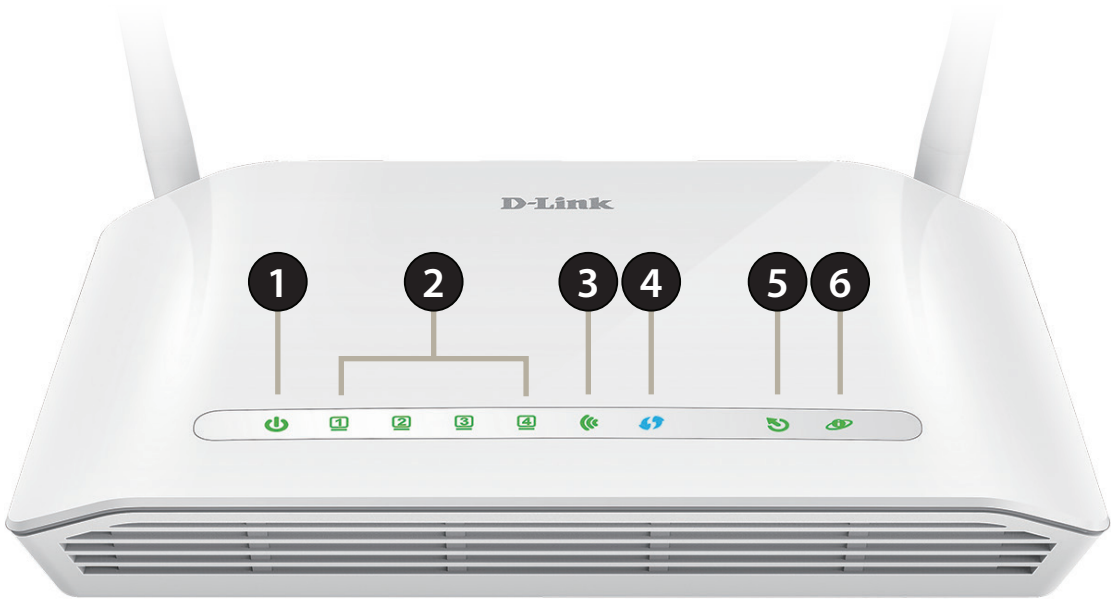
Features

- **Faster Wireless Networking** - The DSL-2745 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-2745 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-2745 incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via a Telnet connection.
- **Easy Installation** - The DSL-2745 can be configured and managed easily using a web-based UI. Any common web browser software can be used to manage the router.
- **IPv6 Connection Support** - Compatible with IPv6 networks, the DSL-2745 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

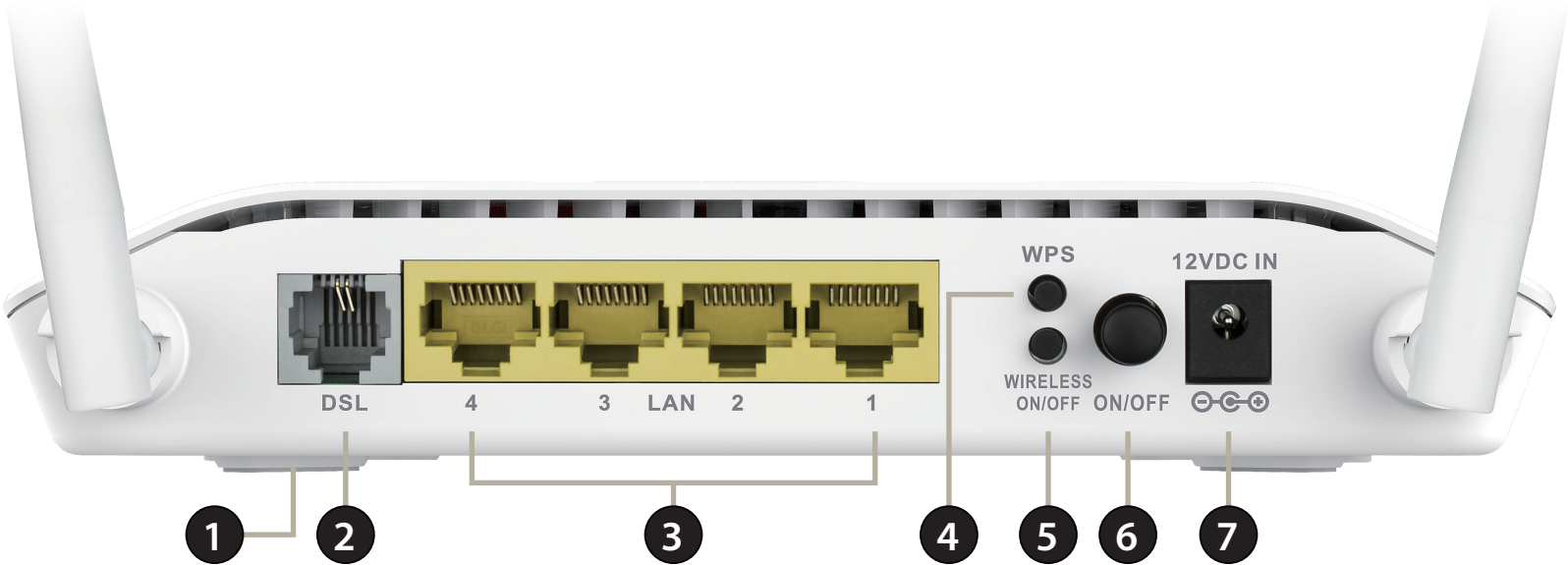
Front LED Panel



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 connection to a device. The light will blink during data transmission.
3	WLAN LED	A solid green light indicates that the Wi-Fi is ready.
4	WPS LED	The light will blink during the WPS process.
5	DSL LED	A solid green light indicates a proper connection to the ADSL enabled telephone line.
6	Internet	A solid green light indicates a proper connection to a broadband service. A red light indicates that IP assignment has failed.

Hardware Overview

Back



1	Reset Button	To reset the DSL-2745 to the default settings, insert a paperclip into the hole on the bottom of the device located near the label and wait several seconds.
2	DSL Port	Connects to an DSL-enabled telephone line.
3	LAN Ports (1-4)	Connects Ethernet devices such as computers, switches, storage (NAS) devices and game consoles.
4	WPS Button	Press to start the WPS process and automatically create a secure connection to a WPS client.
5	Wireless On/Off	Press and hold this button for about 5 seconds to enable or disable the Wi-Fi network.
6	Power Button	Press to power the DSL-2745 on or off.
7	Power Connector	Connector for the supplied power adapter.

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, attic, or garage.

Note: This installation section is written for users who are setting up their home Internet service with the DSL-2745 Wireless N300 ADSL2+ Modem Router for the first time. If you are replacing an existing DSL modem and/or router, you may need to modify these steps.

Before you Begin

- Make sure to have your DSL service information provided by your Internet Service Provider handy. This information is likely to include your DSL account's Username and Password. Your ISP may also supply you with additional WAN configuration settings which are necessary to establish a connection. This information may include the connection type (DHCP IP, Static IP, PPPoE, or PPPoA) and/or ATM PVC details.
- If you are connecting a considerable amount of networking equipment, it may be a good idea to take the time to label each cable or take a picture of your existing setup before making any changes.
- We suggest setting up your DSL-2745 from a single device and verifying that it is connected to the Internet before connecting additional devices.
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE connection software such as WinPoET, BroadJump, or EnterNet 300 from your computer as the DSL-2745 will be providing this functionality.

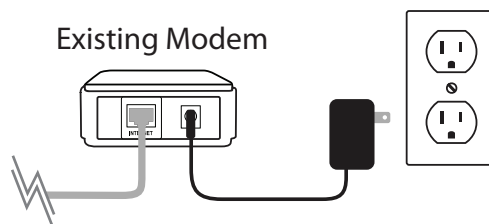
Wireless Installation Considerations

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.

Manual Setup

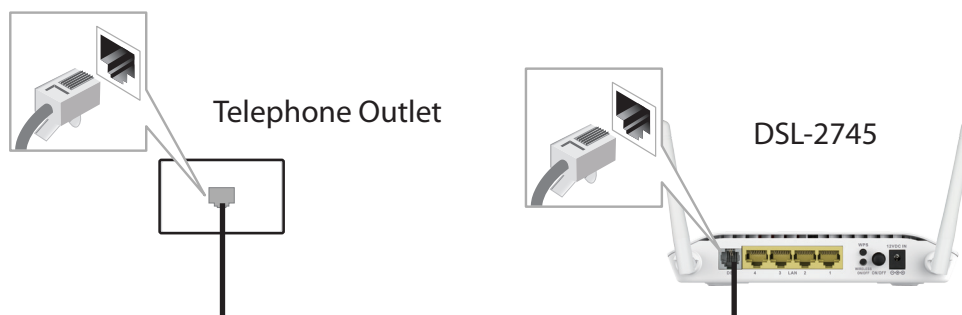
- 1 Turn off and unplug your existing DSL broadband modem. This is required.



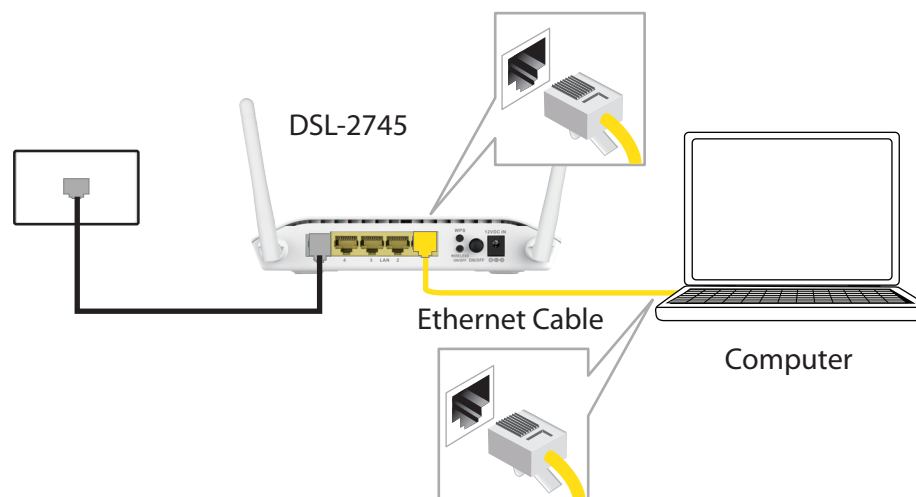
- 2 Position your DSL-2745 close to a telephone outlet which provides DSL service. Place the router in an open area of your intended work area for better wireless coverage.



- 3 Connect the included ADSL Telephone Cable from a telephone outlet to the DSL port on your DSL-2745.

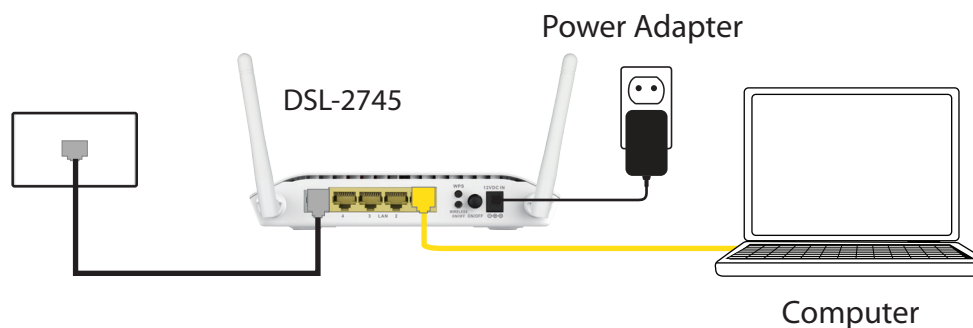


- 4** If you wish to use a wired connection, connect the Ethernet cable from a LAN port of the DSL-2745 to the Ethernet port on your computer.

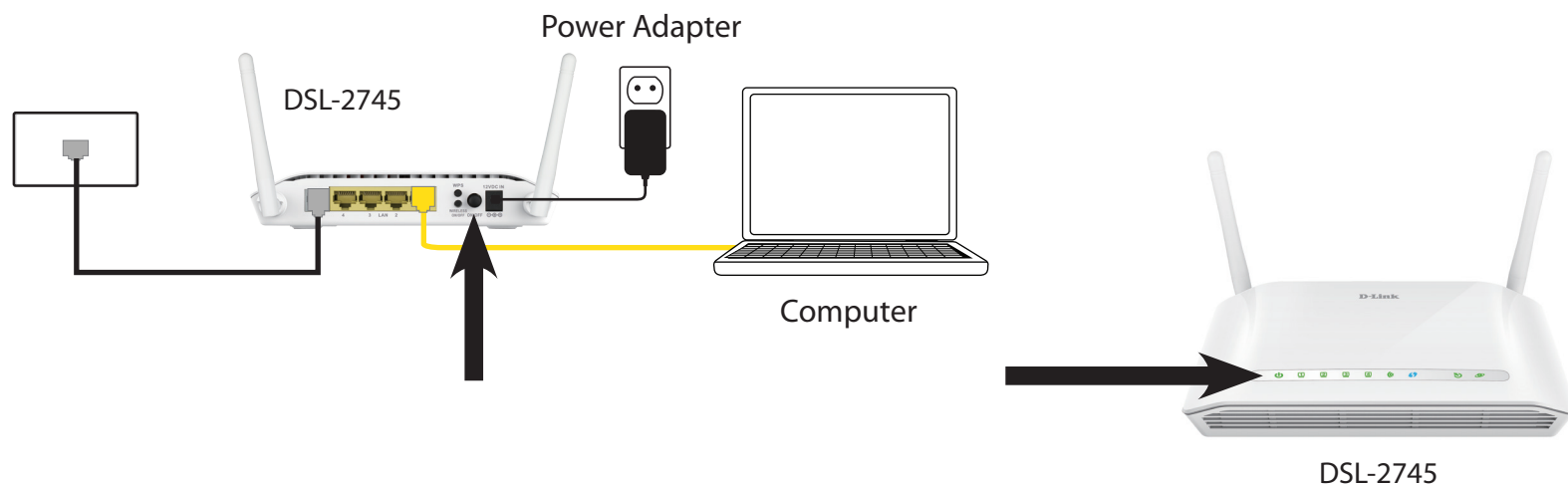


- 5** Plug the power adapter into your DSL-2745 and connect to an available power outlet or surge protector.

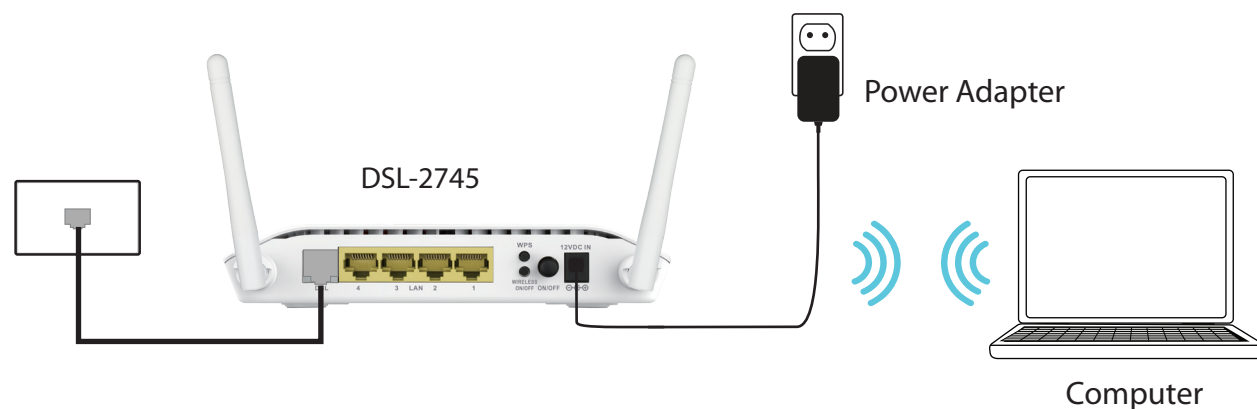
Caution: - Only use the included power adapter with this product.



- 6** Press the power button and verify that the power LED is lit. Allow 1 minute for the router to boot up.



- 7** If connecting to the DSL-2745 wirelessly, access the wireless utility on your computer or mobile device. Scan for available Wi-Fi networks (SSID). Select and join the Wi-Fi network printed on the label on the bottom of your DSL-2745.



Getting Started

There are two different ways you can configure your router to connect to the Internet and connect to your clients:

- **Web-based Setup Wizard** - This wizard will launch when you log into the DSL-2745 for the first time.
Refer to **Web-based Configuration Utility** on page 13.
- **Manual Setup** - Log into the DSL-2745 and manually configure your it, refer to **Manual Setup** on page 9.

Web-based Configuration Utility

This section will show you how to configure your D-Link DSL-2745 using the web-based configuration utility.

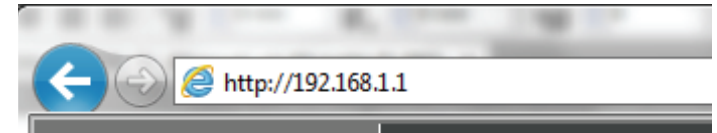
If you wish to change the default settings or adjust the configuration of the DSL-2745 you may use the web-based configuration utility.

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**.

On your first login, you will be directed to the **Setup Wizard** page.

If you want to configure the router manually without running the wizard, skip to **Configuration** on page 20.

A screenshot of the "LOGIN" page. The page has an orange header with the word "LOGIN" in white. Below the header, it says "Input username and password". There are three fields: "Language" with a dropdown menu set to "English", "Username" with a dropdown menu set to "admin", and "Password" with a text input field. A "login" button is located at the bottom right of the form.

Wizard

Use the **Setup Wizard** to quickly and easily configure the DSL-2745. 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.

If you want to configure the DSL-2745 manually without running the wizard, skip to **Configuration** on page 20.

SETUP WIZARD

The Setup Wizard will guide you through the following steps:

Step 1: Set Time and Date

Step 2: Setup Internet Connection

Step 3: Configure Wireless Network

Step 4: Change Password

Step 5: Completed and Apply

Click **Next** to begin.

SETTING UP YOUR INTERNET

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

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

INTERNET CONNECTION WIZARD

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

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 D-LINK SETUP WIZARD

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

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

Next

Cancel

Step 1: Set Time and Date

This step of the wizard allows you to configure your Time and Date settings.

SYSTEM TIME

The current system time is displayed. Select your **Time Zone** from the drop-down menu. From the **Mode** select either **Set NTP Server Manually** or **Copy Computer time**.

NTP CONFIGURATION:

If necessary, change the Network Time Protocol (NTP) servers or interval.

Click **Next** to continue.

The screenshot shows the 'STEP 1: SET TIME AND DATE' configuration page. At the top, there is a progress bar with steps 1 through 5, where step 1 is highlighted. Below the progress bar, a text box explains: '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.' The main configuration area is divided into two sections. The 'SYSTEM TIME' section shows the 'System time' as 'Sun Jan 1 3:53:25 2012', the 'Time Zone' as '(GMT+08:00) Taipei' (selected from a dropdown), and the 'Mode' as 'Set NTP Server Manually' (selected from a dropdown). The 'NTP CONFIGURATION:' section shows the 'Server' as 'ntp1.dlink.com' (selected from a dropdown), 'Server2' as 'None' (selected from a dropdown), and the 'Interval' as 'Every 1 hours' (with '1' in a text box). At the bottom right, there are three buttons: 'Back', 'Next', and 'Cancel'.

Step 2: Setup Internet Connection

This step of the wizard allows you to configure your Internet connection type. Choose your **Country** and **Internet Service Provider** (ISP) from the drop down menu. The necessary settings will automatically populate. If you cannot find your country or ISP, select **Others**. You will need to enter the connection details, provided by your ISP, manually. Select the **Protocol** used by your ISP: **Dynamic IP**, **Static IP**, **PPPoE**, **PPPoA**, or **Bridge**, along with the **Connection Type**: **VC-MUX** or **LLC** and input the **VPI**, **VCI**, and **MTU** settings.

PPPOE/ PPPOA

If you selected **PPPoE** or **PPPoA**, a box will appear to enter your PPPoE/PPPoA username and password. Once you have entered your PPPoE/PPPoA credentials, 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.

STATIC IP

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

BRIDGE/DYNAMIC

Bridge or Dynamic IP require no additional configuration. Click **Next** to continue.

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

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

Country : Others ▾

Internet Service Provider : Others ▾

Protocol : PPPoE ▾

Connection Type : VC-Mux ▾

VPI : 8 (0-255)

VCI : 35 (32-65535)

MTU : 1492 (1-1500)

PPPoE

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

Username :

Password :

Confirm Password :

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 :

STATIC IP

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

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

Click Next to continue.

IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

Step 3: Configure Wireless Network

This step of the wizard allows you to configure your Wireless network settings.

By default, wireless is enabled. If you want to disable the DSL-2745's wireless capability, uncheck **Enable Your Wireless Network**.

Under **Wireless Network Name (SSID)** you can change the SSID of your wireless network, for easier identification by wireless clients. If **Visibility Status** is set to **Visible**, this name will show up when a client in range scans for wireless networks. Otherwise, if your network is **Invisible**, clients will have to enter the SSID in order to connect.

Choose the best security level that is compatible with your wireless clients. **WPA2-PSK** is recommended. Unless you chose **None** (this is NOT recommended), you will need to enter a key below.

WPA/WPA2 Pre-Shared Key - Wireless clients requesting a connection with the network will need to enter this key in order to connect.

Click **Next** to continue.

1 2 STEP 3: CONFIGURE 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) : (1~32 characters)

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

Visibility Status : ☒ Visible ☐ Invisible

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

Security Level :

☐ None ☐ WEP ☐ WPA2(AES) ☒ WPA/WPA2 Mixed

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

Now, please enter your wireless security key.

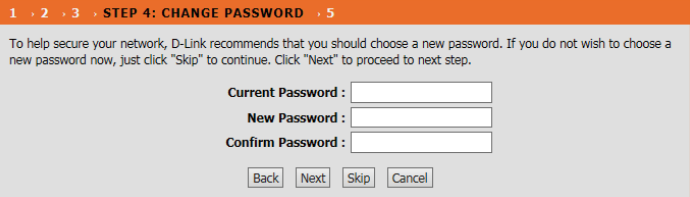
WPA/WPA2 Pre-Shared Key : (8-63 characters, such as a~z, A~Z, or 0~9)

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

Step 4: Change Device Login Password

This step of the wizard allows you to configure your password settings. Enter your **Current Password**, Enter a new **Password**, and **Confirm Password** to secure your DSL-2745.

Click **Next** to continue. Otherwise, click **Skip** to leave the password unchanged.



1 2 3 STEP 4: CHANGE PASSWORD 5

To help secure your network, D-Link recommends that you should choose a new password. If you do not wish to choose a new password now, just click "Skip" to continue. Click "Next" to proceed to next step.

Current Password :

New Password :

Confirm Password :

Step 5: Completed and Apply

Congratulations! You have completed the setup of your DSL-2745. You will see a summary of the settings you chose. It is recommended that you make a note of this information for future reference.

If you are satisfied with these settings, click **Save** to complete the setup wizard.

Otherwise, click **Back** to return to the previous step(s) or **Cancel** to exit the wizard without saving your changes.

1 **2** **3** **4** **STEP 5: COMPLETED AND APPLY**

Setup complete. Click "Back" to review or modify settings. Click "Apply" to apply current settings.
If your Internet connection does not work after apply, you can try the Setup Wizard again with alternative settings or use Manual Setup instead if you have your Internet connection details as provided by your ISP.

SETUP SUMMARY

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

Time Settings :	Copy from NTP Server
NTP State :	Enable
NTP Server 1 :	ntp1.dlink.com
NTP Server 2 :	None
Interval :	1
Time Zone :	(GMT+08:00) Taipei
VPI / VCI :	8/35
MTU :	1492
Protocol :	PPPoE
Connection Type :	VC-Mux
Username :	username
Password :	password
Wireless Network :	Enabled
Wireless Network Name (SSID) :	dlink-5c4260
Visibility Status :	Visible
Encryption :	WPA/WPA2-PSK (also known as WPA/WPA2 Personal)
Pre-Shared Key :	inlc0mdad

Back Save Cancel

Configuration

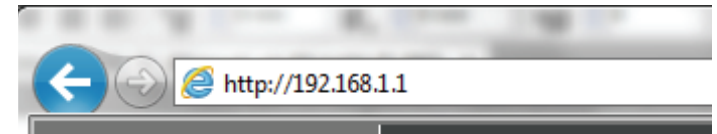
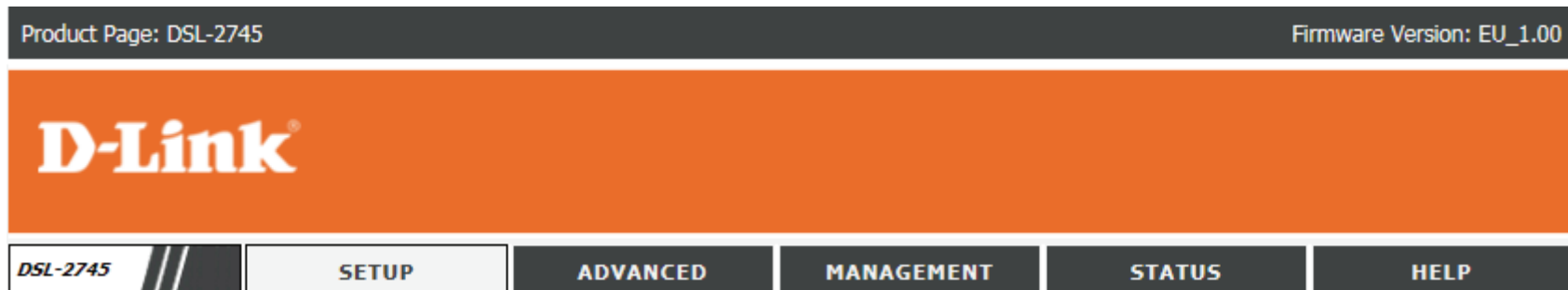
This section will show you how to configure your D-Link wireless router using the web-based configuration utility.

If you wish to change the default settings or adjust the configuration of the DSL-2745 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**.


Once logged in you will see that the user interface is divided into five horizontal tabs, each with a vertical menu bar running along the left side.

A screenshot of the D-Link login page. It has an orange header with the word "LOGIN". Below it, it says "Input username and password". There are three fields: "Language" with a dropdown menu set to "English", "Username" with a dropdown menu set to "admin", and "Password" with a text input field. A "login" button is at the bottom right.

Setup

Product Page: DSL-2745

Firmware Version: EU_1.00



DSL-2745

WIZARD

Local Network


Internet Setup

Wireless Setup

Time and Date

Support

Logout



SETUP



ADVANCED

MANAGEMENT

STATUS

HELP

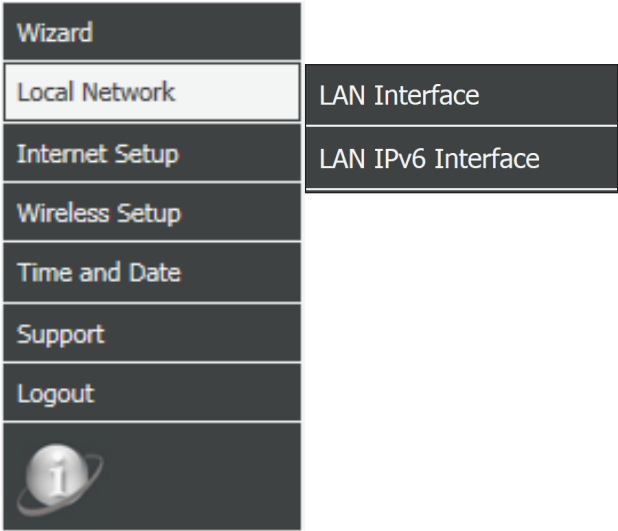
The Setup Tab provides access to configure the most commonly used settings of your DSL-2745.

-  Indicates the Internet is disconnected.
-  Indicates the DSL-2745 is successfully connected to the Internet.

Local Network

Hover your mouse over the **Local Network** option on the vertical menu bar running along the left side to access:

- LAN Interface
- LAN IPv6 Interface



Local Network

This optional section allows you to configure the local network and DHCP settings of your device. The DHCP service supplies IP settings to clients configured to automatically obtain IP settings that are connected to the device through the Ethernet port. You may also set static DHCP reservations from this screen. Click **Apply** when you are done.

LAN INTERFACE SETTINGS

Interface Name: **LAN** indicates you are configuring the LAN address settings.

IP Address: Enter the IP address of the DSL-2745. The default IP address is **192.168.1.1**. **Note:** If you change the IP address, once you click **Apply** you will need to enter the new IP address in your browser in order to access the configuration utility.

Subnet Mask: Enter the subnet mask. The default subnet mask is **255.255.255.0**.

Secondary IP: If you wish to add another IP address to use to configure the DSL-2745, check this box and enter the IP address and subnet mask.

IGMP Snooping: Check the box to enable Internet Group Management Protocol (IGMP) snooping for extra network traffic security.

DHCP SERVER SETTINGS

LAN IP: The current Router LAN IP and Subnet mask are displayed.

DHCP Server: By default, DHCP is enabled. Select **None** to disable the DHCP server.

IP Pool Range Enter the starting and ending IP addresses for the DHCP server's IP assignment.

LAN SETTING

This page is used to configure the LAN interface and DHCP Server Settings of your ADSL Router.

LAN INTERFACE SETTINGS

Interface Name: LAN

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

☐ Secondary IP

IGMP Snooping: ☐ Disable ☒ Enable

DHCP SERVER SETTINGS

LAN IP: 192.168.1.1/255.255.255.0

DHCP Mode: DHCP Server

IP Pool Range: 192.168.1.2 - 192.168.1.254

Show Client

Max Lease Time: 10080 minutes

Domain Name: domain.name

DNS Servers: 192.168.1.1

Local Network (continued)

DHCP SERVER SETTINGS (CONTINUED)

- Max Lease Time:** Note: If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may experience an IP address conflict.
- Domain Name:** Enter a domain name (optional) to provide along with DHCP assigned addresses.
- DNS Servers:** Enter a DNS server to distribute to DHCP clients.

Click **Apply Changes** when you are done.

DHCP SERVER SETTINGS

LAN IP: 192.168.1.1/255.255.255.0

DHCP Mode: DHCP Server

IP Pool Range: 192.168.1.2 - 192.168.1.254

Show Client

Max Lease Time: 10080 minutes

Domain Name: domain.name

DNS Servers: 192.168.1.1

Apply Changes

DHCP STATIC IP CONFIGURATION

DHCP Reservation allows you to reserve IP addresses for specific machines based on their unique hardware MAC addresses. During DHCP IP address assignment, these devices will receive the same IP address. This is particularly useful if you run servers on your network.

- IP Address:** Enter the IP address you want to assign to the computer or device. This IP address must be within the DHCP IP address range.
- MAC Address:** Enter the MAC address of the computer or device you wish to reserve an IP for.

After inputting an IP address and the associated MAC address, click **Add**.

DHCP STATIC IP CONFIGURATION

IP Address: 0.0.0.0

Mac Address: 00:00:00:00:00:00 (ex. 00:E0:86:71:05:02)

AddModifyDelete Selected

DHCP STATIC IP TABLE

This table lists the current reserved DHCP IP addresses by MAC address and IP address. Press **Select** radio button and the **Modify or Delete Selected** above to make adjustments.

DHCP STATIC IP TABLE

Select

IP Address

MAC Address

IPv6 Local Network

This section allows you to configure your IPv6 local network settings.

LAN GLOBAL ADDRESS SETTING

Global Address Enter your IPv6 global address.

Click **Apply Changes** when you are done.

RA SETTING

Enable: Check this box to enable Router Advertisement.

M Flag: Check this box to set the managed address configuration flag to 1.

O Flag: Check this box to set the other flag to 1.

Max Interval: Set the maximum interval between each router advertisement message.

Min Interval: Set the minimum interval between each router advertisement message.

Prefix Mode: Select **Auto** or **Manual** and enter your prefix address and length.

The following settings are available if **Prefix Mode** is set to **Manual**:

Prefix Address: Enter the prefix address.

Prefix length: Enter the prefix length.

Preferred Time: Enter the preferred amount of time the address is used for.

Valid Time: Enter the amount of time the address is valid for.

LAN IPV6 SETTING

This page is used to configurate ipv6 LAN setting. User can set LAN RA server work mode and LAN DHCPv6 server work mode.

LAN GLOBAL ADDRESS SETTING

Global Address: /

Apply Changes

RA SETTING

Enable: ☒
 M Flag: ☐
 O Flag: ☒
 Max Interval: Secs
 Min Interval: Secs
 Prefix Mode:
 Prefix Address:
 Prefix Length: [16 - 64]
 Preferred Time: [600 - 2147483647 S] or [-1 S]
 Valid Time: [600 - 2147483647 S] or [-1 S]
 ULA Enable: ☐
 RA DNS Enable: ☐

Apply Changes

IPv6 Local Network (continued)

ULA Enable: Check this box to enable ULA.

RA DNS Enable: Check this box to enable router advertisement DNS.

Click **Apply Changes** when you are done.

DHCPV6 SETTING

DHCPv6 Mode: Choose the desired DHCPV6 mode **None**, **Auto Mode**, or **Manual Mode**.

The following settings are available if **DHCPv6 Mode** is set to **Auto Mode**:

IPv6 Address Suffix Pool: Enter the IPv6 address suffix pool range.

The following settings are available if **DHCPv6 Mode** is set to **Manual Mode**:

Address Mode: Select either **Prefix Mode** or **Pool Mode**.

The following settings are available if **Address Mode** is set to **Prefix Mode**:

IPv6 Address Pool: Enter the IPv6 address prefix.

The following settings are available if **Address Mode** is set to **Pool Mode**:

IPv6 Address Pool: Enter the IPv6 address pool range.

ULA Enable: <input type="checkbox"/> RA DNS Enable: <input type="checkbox"/>
Apply Changes

DHCPV6 SETTING
DHCPv6 Mode: None ▼

DHCPV6 SETTING
DHCPv6 Mode: Auto Mode ▼
IPv6 Address Suffix Pool: ::1 - ::ffff (ex. ::1:1:1:1:1 or ::1)
IPv6 DNS Mode: Auto ▼

DHCPV6 SETTING
DHCPv6 Mode: Manual Mode ▼
Address Mode: Prefix Mode ▼
IPv6 Address Pool:
Prefix Length: 64
Preferred Time: 120 Secs
Valid Time: 120 Secs
IPv6 DNS Mode: Auto ▼

DHCPV6 SETTING
DHCPv6 Mode: Manual Mode ▼
Address Mode: Pool Mode ▼
IPv6 Address Pool: -
Prefix Length: 64
Preferred Time: 120 Secs
Valid Time: 120 Secs
IPv6 DNS Mode: Auto ▼

IPv6 Local Network (continued)

Prefix length: Enter the prefix length.

Preferred Time: Enter the preferred amount of time the address is used for.

Valid Time: Enter the amount of time the address is valid for.

IPv6 DNS Mode: Select either **Auto** or **Manual**.

The following settings are available if **IPv6 DNS Mode** is set to **Manual**:

DNS Servers: Enter up to three IPv6 DNS servers.

Click **Apply Changes** when you are done.

DHCPV6 SETTING	
DHCPv6 Mode:	Manual Mode ▾
Address Mode:	Pool Mode ▾
IPv6 Address Pool:	<input type="text"/> -
Prefix Length:	64
Preferred Time:	120 Secs
Valid Time:	120 Secs
IPv6 DNS Mode:	Auto ▾

DHCPV6 SETTING	
DHCPv6 Mode:	Manual Mode ▾
Address Mode:	Pool Mode ▾
IPv6 Address Pool:	<input type="text"/> -
Prefix Length:	64
Preferred Time:	120 Secs
Valid Time:	120 Secs
IPv6 DNS Mode:	Manual ▾
DNS Servers:	<input type="text"/> <input type="text"/> <input type="text"/>

Apply Changes

Internet Setup

Click **Internet Setup** on the left menu to configure your connection manually. This section is only recommended for advanced users. It is recommended to use the **Setup Wizard** to set up your Internet connection.

The following sections describe how to Create a New Connection, Modify an existing connection, or Delete a connection.

CURRENT WAN TABLE

This table lists the current WAN configuration. It displays the **Interface Name**, **Mode**, **Vlan Id**, **VPI/VCI** settings, the **Encapsulation** method, and **Status**.

To modify an existing entry, select the radio button of the row you wish to alter and click on the **Modify** button below the **WAN Configuration** box. If you wish to make more detailed changes, click on the pencil icon in the **Edit** column. Refer to **Modify an Existing Connection** on page 40.

To delete an existing connection, select the radio button of the row you wish to alter and click on the **Delete** button below the **WAN Configuration** box or click on the trash can icon in the **Edit** column.



To create a new connection, proceed to the next page.

INTERNET SETUP

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

ATM Setting is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for QoS etc ...

CURRENT WAN TABLE:

Select	Interface	Mode	Vlan Id	VPI/VCI	Encap	Status	Edit
<input type="radio"/>	pppoe1	PPPoE	0	8/35	VCMUX	Down	 

WAN CONFIGURATION

VPI: VCI:
 Channel Mode:
 802.1q: ☒ Disable ☐ Enable
 Encapsulation: ☒ LLC ☐ VC-Mux
 Enable NAPT: ☐ Enable IGMP: ☐
 VLAN ID(1-4095):
 PPP Settings: User Name: Password:
 Type: Idle Time (min):
 WAN IP Settings: Type: ☐ Fixed IP ☒ DHCP
 Local IP Address: Remote IP Address:
 Netmask:
 Default Route: ☐ Disable ☐ Enable ☒ Auto
 Unnumbered ☐

Add Modify Delete

ATM SETTING

Select	VPI	VCI	QoS	PCR	CDVT	SCR	MBS
<input type="radio"/>	8	35	UBR	6144	0	---	---

Create a New Connection

To set up your Internet Connection, use the **WAN Configuration** box. Begin by selecting the channel mode or network encapsulation protocol your ISP uses, then proceed to fill in the **IP**, **PPP**, and **WAN IP** parameters.

PPPoE

WAN CONFIGURATION

Channel Mode: Select **PPPoE**.

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.

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

Encapsulation: Select the type of encapsulation your ISP uses, either Logical Link Control (**LLC**) or Virtual Circuit Multiplexing (**VC-Mux**).

Enable NAPT: Check this box to enable NAT, which allows devices on your network to share one public IP address.

Enable IGMP: Check to enable IGMP Multicast.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

IP Protocol: Select the type of IP addressing: **IPv4/v6**, **IPv4**, or **IPv6**.

PPP Settings: Enter your PPP authentication information.

INTERNET SETUP

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

ATM Setting is used to configure the parameters for the ATM of your ADSL Router. Here you may change the setting for QoS etc ...

WAN CONFIGURATION

VPI: **VCI:**
Channel Mode: **Encapsulation:** ☒ LLC ☐ VC-Mux
802.1q: ☒ Disable ☐ Enable **Enable NAPT:** ☒ **Enable IGMP:** ☐
VLAN ID(1-4095):
IP Protocol:
PPP Settings: **User Name:** **Password:**
Type: **Idle Time (min):**
WAN IP Settings: **Type:** ☒ Fixed IP ☐ DHCP
Local IP Address: **Remote IP Address:**
Netmask:
Default Route: ☐ Disable ☐ Enable ☒ Auto
Unnumbered ☐
IPv6 WAN Setting:
Address Mode:
DHCPv6 Mode:
Request DHCPv6 PD: ☒

Add Modify Delete

PPPoE Mode (continued)

User Name: Enter your DSL account username provided by your ISP.

Password: Enter your DSL account password provided by your ISP.

Type: Select how your DSL-2745 connects to your ISP. Choose either **Continuous**, **Connect on Demand**, and **Manual**.

Idle Time (min): If you selected **Connect on Demand**, enter the amount time the router waits if there is no activity before disconnecting.

WAN IP Settings: If **IPv4** or **IPv4/IPv6** is selected, these settings are disabled. The router will use **DHCP** only, **Fixed** (Static IP) is unavailable.

IPv6 WAN Settings: Configure the IPv6 WAN settings. If the IP Protocol is set to **IPv4**, these settings are unavailable.

Address Mode: Select either **Slaac** or **Static**.

IPv6 Address: Enter your IPv6 Static Address. Only available in Static mode.

IPv6 Gateway: Enter your IPv6 Gateway. Only available in Static mode.

DHCPv6 Mode: Select either **Auto**, **Enable**, or **Disable**.

Request DHCPv6 Address: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Enable** or **Auto**:

Request DHCPv6 PD: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Enable**.

Click **Add** to create your connection.

WAN CONFIGURATION

VPI: VCI: Encapsulation: ☒ LLC ☐ VC-Mux

Channel Mode: PPPoE Enable NAPT: ☒ Enable IGMP: ☐

802.1q: ☒ Disable ☐ Enable VLAN ID(1-4095):

IP Protocol: IPv4/IPv6

PPP Settings: User Name: Password:

Type: Continuous Idle Time (min):

WAN IP Settings: Type: ☒ Fixed IP ☐ DHCP

Local IP Address: Remote IP Address:

Netmask:

Default Route: ☐ Disable ☐ Enable ☒ Auto

Unnumbered ☐

IPv6 WAN Setting: Address Mode: Slaac

DHCPv6 Mode: Auto

Request DHCPv6 PD: ☒

PPPoA Mode

WAN CONFIGURATION

Channel Mode: Select **PPPoA**.

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.

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

Encapsulation: Select the type of encapsulation your ISP uses, either Logical Link Control (**LLC**) or Virtual Circuit Multiplexing (**VC-Mux**).

Enable NAPT: Check this box to enable NAT, which allows devices on your network to share one public IP address.

Enable IGMP: Check to enable IGMP Multicast.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

IP Protocol: Select the type of IP addressing: **IPv4/v6**, **IPv4**, or **IPv6**. This will effect the **WAN IP Settings** and **WAN IPv6 Settings**.

PPP Settings: Enter your PPP authentication information.

User Name: Enter your DSL account username provided by your ISP.

Password: Enter your DSL account password provided by your ISP.

Type: Select how your DSL-2745 connects to your ISP. Choose either **Continuous**, **Connect on Demand**, and **Manual**.

The screenshot shows the WAN CONFIGURATION page for PPPoA mode. The interface includes the following fields and options:

- VPI:** 0
- VCI:** (empty)
- Encapsulation:** ☒ LLC ☐ VC-Mux
- Channel Mode:** PPPoA (selected in a dropdown)
- Enable NAPT:** ☐ **Enable IGMP:** ☐
- 802.1q:** ☒ Disable ☐ Enable
- VLAN ID(1-4095):** 0
- IP Protocol:** Ipv4/Ipv6 (selected in a dropdown)
- PPP Settings:**
 - User Name:** (empty)
 - Password:** (empty)
 - Type:** Continuous (selected in a dropdown)
 - Idle Time (min):** (empty)
- WAN IP Settings:**
 - Type:** ☒ Fixed IP ☐ DHCP
 - Local IP Address:** (empty)
 - Remote IP Address:** (empty)
 - Netmask:** (empty)
 - Default Route:** ☐ Disable ☐ Enable ☒ Auto
 - Unnumbered:** ☐
- IPv6 WAN Setting:**
 - Address Mode:** Slaac (selected in a dropdown)
 - DHCPv6 Mode:** Auto (selected in a dropdown)
 - Request DHCPv6 PD:** ☒

At the bottom of the form are three buttons: Add, Modify, and Delete.

PPPoA Mode (continued)

Idle Time (min): If you selected **Connect on Demand**, enter the amount the router waits if there is no activity before disconnecting from the Internet.

WAN IP Settings: If **IPv4** or **IPv4/IPv6** is selected, these settings are disabled. The router will use **DHCP** only, **Fixed** (Static IP) is unavailable.

IPv6 WAN Settings: Configure the IPv6 WAN settings. If the IP Protocol is set to **IPv4**, these settings are unavailable.

Address Mode: Select either **Slaac** or **Static**.

IPv6 Address: Enter your IPv6 Static Address. Only available in Static mode.

IPv6 Gateway: Enter your IPv6 Gateway. Only available in Static mode.

DHCPv6 Mode: Select either **Auto**, **Enable**, or **Disable**.

Request DHCPv6 Address: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Enable** or **Auto**:

Request DHCPv6 PD: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Enable**.

The screenshot shows the 'WAN CONFIGURATION' page with the following settings:

- VPI:** 0, **VCI:** (empty)
- Encapsulation:** ☒ LLC, ☐ VC-Mux
- Channel Mode:** PPPoA (selected in dropdown)
- Enable NAPT:** ☐, **Enable IGMP:** ☐
- 802.1q:** ☒ Disable, ☐ Enable
- VLAN ID(1-4095):** 0
- IP Protocol:** Ipv4/Ipv6 (selected in dropdown)
- PPP Settings:**
 - User Name:** (empty), **Password:** (empty)
 - Type:** Continuous (selected in dropdown)
 - Idle Time (min):** (empty)
- WAN IP Settings:**
 - Type:** ☒ Fixed IP, ☐ DHCP
 - Local IP Address:** (empty), **Remote IP Address:** (empty)
 - Netmask:** (empty)
 - Default Route:** ☐ Disable, ☐ Enable, ☒ Auto
 - Unnumbered:** ☐
- IPv6 WAN Setting:**
 - Address Mode:** Slaac (selected in dropdown)
- DHCPv6 Mode:** Auto (selected in dropdown)
- Request DHCPv6 PD:** ☒

At the bottom, there are three buttons: **Add**, **Modify**, and **Delete**.

Click **Add** to create your connection.

1483 Bridged Mode

WAN CONFIGURATION

Channel Mode: Select **1483 Bridged**.

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.

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

Encapsulation: Select the type of encapsulation your ISP uses, either Logical Link Control (**LLC**) or Virtual Circuit Multiplexing (**VC-Mux**).

Enable NAPT: 1483 Bridged mode does not support NAPT.

Enable IGMP: 1483 Bridged mode does not support IGMP.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

1483 Bridged does not support PPP or WAN IP settings.

Click **Add** to create your connection. Further configuration of your other network equipment may be necessary.

The screenshot shows the 'WAN CONFIGURATION' interface. It includes the following fields and options:

- VPI:** Input field with value 0.
- VCI:** Input field.
- Encapsulation:** Radio buttons for LLC (selected) and VC-Mux.
- Channel Mode:** Dropdown menu showing '1483 Bridged'.
- Enable NAPT:** Checkbox (unchecked).
- Enable IGMP:** Checkbox (unchecked).
- 802.1q:** Radio buttons for Disable (selected) and Enable.
- VLAN ID(1-4095):** Input field with value 0.
- PPP Settings:**
 - User Name:** Input field.
 - Password:** Input field.
 - Type:** Dropdown menu showing 'Continuous'.
 - Idle Time (min):** Input field.
- WAN IP Settings:**
 - Type:** Radio buttons for Fixed IP and DHCP (selected).
 - Local IP Address:** Input field.
 - Remote IP Address:** Input field.
 - Netmask:** Input field.
 - Default Route:** Radio buttons for Disable, Enable, and Auto (selected).
 - Unnumbered:** Checkbox (unchecked).

At the bottom, there are three buttons: 'Add', 'Modify', and 'Delete'.

1483 MER Mode

WAN CONFIGURATION

Channel Mode: Select **1483 MER**.

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.

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

Encapsulation: Select the type of encapsulation your ISP uses, either Logical Link Control (**LLC**) or Virtual Circuit Multiplexing (**VC-Mux**).

Enable NAPT: Check this box to enable NAT, which allows devices on your network to share one public IP address.

Enable IGMP: Check to enable IGMP Multicast.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

IP Protocol: Select the type of IP addressing: **IPv4/v6**, **IPv4**, or **IPv6**. This will effect the **WAN IP Settings** and **WAN IPv6 Settings**.

PPP Settings: 1483 MER does not support PPP authentication.

WAN IP Settings: Configure the IPv4 WAN settings. If the IP Protocol is set to **IPv6**, these settings are unavailable.

Type: Choose either **Fixed** (Static IP), or **Dynamic IP**.

WAN CONFIGURATION

VPI: VCI: Encapsulation: ☒ LLC ☐ VC-Mux

Channel Mode: Enable NAPT: ☒ Enable IGMP: ☐

802.1q: ☒ Disable ☐ Enable VLAN ID(1-4095):

IP Protocol:

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings: Type: ☒ Fixed IP ☐ DHCP

Local IP Address: Remote IP Address:

Netmask:

Default Route: ☐ Disable ☐ Enable ☒ Auto

Unnumbered ☐

IPv6 WAN Setting: Address Mode:

DHCPv6 Mode:

Request DHCPv6 PD: ☒

Add Modify Delete

1483 MER Mode (continued)

The following settings are available if **Type** is set to **Fixed**:

Local IP Address: Enter your local IP address.

Netmask: Enter your subnet mask.

Default Route: This defaults to **Auto**.

Unnumbered: This option is unavailable.

IPv6 WAN Settings: Configure the IPv6 WAN settings. If the IP Protocol is set to **IPv4**, these settings are unavailable.

Address Mode: Select either **Static** or **Dynamic**.

IPv6 Address: Enter your IPv6 Static Address. Only available in Static mode.

IPv6 Gateway: Enter your IPv6 Gateway. Only available in Static mode.

DHCPv6 Mode: Select either **Static**, **Dynamic**, or **Disable**.

Request DHCPv6 Address: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Static** or **Dynamic**:

Request DHCPv6 PD: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Static** or **Dynamic**.

Click **Add** to create your connection.

WAN CONFIGURATION

VPI: VCI: Encapsulation: ☒ LLC ☐ VC-Mux

Channel Mode: 1483 MER Enable NAPT: ☒ Enable IGMP: ☐

802.1q: ☒ Disable ☐ Enable VLAN ID(1-4095): 0

IP Protocol: Ipv4/Ipv6

PPP Settings: User Name: Password:

Type: Continuous Idle Time (min):

WAN IP Settings: Type: ☒ Fixed IP ☐ DHCP

Local IP Address: Remote IP Address:

Netmask:

Default Route: ☐ Disable ☐ Enable ☒ Auto

Unnumbered ☐

IPv6 WAN Setting: Address Mode: Static

DHCPv6 Mode: Auto

Request DHCPv6 PD: ☒

Add Modify Delete

1483 Routed Mode

WAN CONFIGURATION

Channel Mode: Select **1483 Routed**.

VPI: The 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.

VCI: The virtual channel identifier (VCI) is the virtual channel between two points in an ATM network. Its valid value is between 32 and 65535. Enter the correct VCI provided by your ISP.

Encapsulation: Select the type of encapsulation your ISP uses, either Logical Link Control (**LLC**) or Virtual Circuit Multiplexing (**VC-Mux**).

Enable NAPT: Check this box to enable NAT, which allows devices on your network to share one public IP address.

Enable IGMP: Check to enable IGMP Multicast.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

IP Protocol: Select the type of IP addressing: **IPv4/v6**, **IPv4**, or **IPv6**. This will effect the **WAN IP Settings** and **WAN IPv6 Settings**.

PPP Settings: 1483 Routed mode does not support PPP authentication.

WAN IP Settings: Configure the IPv4 WAN settings. If the IP Protocol is set to **IPv6**, these settings are unavailable.

Type: Only **Fixed** (Static IP) is available for 1483 Routed Mode.

The screenshot shows the WAN CONFIGURATION page with the following settings:

- VPI:** 0, **VCI:** (empty)
- Encapsulation:** ☒ LLC, ☐ VC-Mux
- Channel Mode:** 1483 Routed (selected in dropdown)
- Enable NAPT:** ☐, **Enable IGMP:** ☐
- 802.1q:** ☒ Disable, ☐ Enable
- VLAN ID(1-4095):** 0
- IP Protocol:** Ipv4/Ipv6 (selected in dropdown)
- PPP Settings:**
 - User Name:** (empty), **Password:** (empty)
 - Type:** Continuous (selected in dropdown), **Idle Time (min):** (empty)
- WAN IP Settings:**
 - Type:** ☒ Fixed IP, ☐ DHCP
 - Local IP Address:** (empty), **Remote IP Address:** (empty)
 - Netmask:** (empty)
 - Default Route:** ☐ Disable, ☐ Enable, ☒ Auto
 - Unnumbered:** ☐
- IPv6 WAN Setting:**
 - Address Mode:** Slaac (selected in dropdown)
 - DHCPv6 Mode:** Auto (selected in dropdown)
 - Request DHCPv6 PD:** ☒

Buttons at the bottom: Add, Modify, Delete.

1483 Routed Mode Continued

Local IP Address: Enter your local IP address.

Remote IP Address: Enter your default gateway.

Netmask: Enter your subnet mask.

Default Route: This defaults to **Auto**.

Unnumbered: This option is unavailable.

IPv6 WAN Settings: Configure the IPv6 WAN settings. If the IP Protocol is set to **IPv4**, these settings are unavailable.

Address Mode: Select either **Static** or **Dynamic**.

IPv6 Address: Enter your IPv6 Static Address. Only available in Static mode.

IPv6 Gateway: Enter your IPv6 Gateway. Only available in Static mode.

DHCPv6 Mode: Select either **Static**, **Dynamic**, or **Disable**.

Request DHCPv6 Address: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Dynamic** or **Static**.

Request DHCPv6 PD: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Dynamic**.

Click **Add** to create your connection.

WAN CONFIGURATION

VPI: VCI: Encapsulation: ☒ LLC ☐ VC-Mux

Channel Mode: **1483 Routed** Enable NAPT: ☐ Enable IGMP: ☐

802.1q: ☒ Disable ☐ Enable VLAN ID(1-4095):

IP Protocol:

PPP Settings: User Name: Password:

Type: Idle Time (min):

WAN IP Settings: Type: ☒ Fixed IP ☐ DHCP

Local IP Address: Remote IP Address:

Netmask:

Default Route: ☐ Disable ☐ Enable ☒ Auto

Unnumbered ☐

IPv6 WAN Setting: Address Mode:

DHCPv6 Mode:

Request DHCPv6 PD: ☒

IPoA Mode

WAN CONFIGURATION

Channel Mode: Select **IPoA**.

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.

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

Encapsulation: Only Logical Link Control (**LLC**) encapsulation is supported.

Enable NAPT: Check this box to enable NAT, which allows devices on your network to share one public IP address.

Enable IGMP: Check to enable IGMP Multicast.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

IP Protocol: Select the type of IP addressing: **IPv4/v6**, **IPv4**, or **IPv6**. This will effect the **WAN IP Settings** and **WAN IPv6 Settings**.

PPP Settings: IPoA mode does not support PPP authentication.

WAN IP Settings: Configure the IPv4 WAN settings. If the IP Protocol is set to **IPv6**, these settings are unavailable.

Type: Choose either **Fixed** (Static IP), or **Dynamic IP**.

The screenshot shows the WAN CONFIGURATION page for IPoA Mode. The interface includes the following fields and options:

- VPI:** 0
- VCI:** (empty)
- Encapsulation:** ☒ LLC ☐ VC-Mux
- Channel Mode:** IPoA (selected in a dropdown)
- Enable NAPT:** ☐ **Enable IGMP:** ☐
- 802.1q:** ☒ Disable ☐ Enable
- VLAN ID(1-4095):** 0
- IP Protocol:** Ipv4/Ipv6 (selected in a dropdown)
- PPP Settings:**
 - User Name:** (empty)
 - Password:** (empty)
 - Type:** Continuous (selected in a dropdown)
 - Idle Time (min):** (empty)
- WAN IP Settings:**
 - Type:** ☒ Fixed IP ☐ DHCP
 - Local IP Address:** (empty)
 - Remote IP Address:** (empty)
 - Netmask:** (empty)
 - Default Route:** ☐ Disable ☐ Enable ☒ Auto
 - Unnumbered:** ☐
- IPv6 WAN Setting:**
 - Address Mode:** Slaac (selected in a dropdown)
 - DHCPv6 Mode:** Auto (selected in a dropdown)
 - Request DHCPv6 PD:** ☒

At the bottom of the form are three buttons: **Add**, **Modify**, and **Delete**.

IPoA Mode (continued)

The following settings are available if **Type** is set to **Fixed**:

Local IP Address: Enter your local IP address.

Netmask: Enter your subnet mask.

Remote IP Address: Enter your default gateway.

Default Route: This defaults to **Auto**.

Unnumbered: This option is unavailable.

IPv6 WAN Settings: Configure the IPv6 WAN settings. If the IP Protocol is set to **IPv4**, these settings are unavailable.

Address Mode: Select either **Slaac** or **Static**.

IPv6 Address: Enter your IPv6 Static Address. Only available in Static mode.

IPv6 Gateway: Enter your IPv6 Gateway. Only available in Static mode.

DHCPv6 Mode: Select either **Auto**, **Enable**, or **Disable**.

Request DHCPv6 Address: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Enable** or **Auto**:

Request DHCPv6 PD: Check this box to enable. Only available if **DHCPv6 Mode** is set to **Enable**.

Click **Add** to create your connection.

The screenshot displays the 'WAN CONFIGURATION' interface. At the top, it shows 'VPI: 0' and 'VCI: 0'. The 'Channel Mode' is set to 'IPoA'. 'Encapsulation' is set to 'LLC'. '802.1q' is set to 'Disable'. 'Enable NAPT' and 'Enable IGMP' are both unchecked. 'VLAN ID(1-4095)' is set to '0'. The 'IP Protocol' is set to 'IPv4/IPv6'. Below this, 'PPP Settings' include 'User Name', 'Password', 'Type' (set to 'Continuous'), and 'Idle Time (min)'. The 'WAN IP Settings' section shows 'Type' set to 'Fixed IP', with fields for 'Local IP Address', 'Netmask', and 'Remote IP Address'. 'Default Route' is set to 'Auto'. 'Unnumbered' is unchecked. The 'IPv6 WAN Setting' section shows 'Address Mode' set to 'Slaac'. 'DHCPv6 Mode' is set to 'Auto', and 'Request DHCPv6 PD' is checked. At the bottom, there are 'Add', 'Modify', and 'Delete' buttons.

Modify an Existing Connection

To modify an existing entry in detail, select the radio button of the row you wish to alter and click on the pencil icon in the **Edit** column.

CURRENT WAN TABLE:							
Select	Interface	Mode	Vlan Id	VPI/VCI	Encap	Status	Edit
<input type="radio"/>	pppoe1	PPPoE	0	0/32	LLC	Down	
<input type="radio"/>	a1	br1483	0	0/33	LLC	Down	
<input type="radio"/>	a2	mer1483	0	0/34	LLC	Down	
<input type="radio"/>	pppoa2	PPPoA	0	0/35	LLC	Down	
<input type="radio"/>	a4	rt1483	0	0/36	LLC	Down	
<input type="radio"/>	a5	IPoA	0	0/37	LLC	Down	

Modify a PPPoE Connection

PPP INTERFACE

Protocol: This shows the current protocol being modified.

ATM VCC: The shows the current ATM VCC configuration.

Login Name: You can change the currently configured DSL account username here.

Password: You can change the currently configured DSL account password here.

Authentication: Select **PAP**, **CHAP**, or **Auto**. The default is **Auto**.

Connection Type: How your DSL-2745 connects to your ISP. Choose either **Continuous**, **Connect on Demand**, and **Manual**.

Idle Time(s): If you selected **Connect on Demand**, enter the amount time the router waits if there is no activity before disconnecting.

Bridge: Select **Bridged Ethernet (Transparent Bridging)**, **Bridged PPPoE(implies Bridged Ethernet)**, or **Disable Bridge**.

AC-Name: Used for PPPoE tagging, normally this should be left blank.

PPP INTERFACE - MODIFY

This page is used for advanced PPP interface configuration.

PPP INTERFACE

Protocol: PPPoE
ATM VCC: 0/32
Login Name:
Password:
Authentication Method:
Connection Type:
Idle Time (s):
Bridge: ☐ Bridged Ethernet (Transparent Bridging)
☐ Bridged PPPoE (implies Bridged Ethernet)
☒ Disable Bridge
AC-Name:
Service-Name:
802.1q: ☒ Disable ☐ Enable
VLAN ID(1-4095):
MTU (1-1500):
Static IP:
Source Mac address: (ex:00:E0:86:71:05:02)

Modify a PPPoE Connection (continued)

Service-Name: Used for PPPoE tagging, normally this should be left blank.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

MTU(1-1500): Enter the packet size. The default is **1492**.

Static IP: If you have been assigned a static IP by your ISP, enter it here.

Source Mac address: By default the DSL-2745's MAC address is listed. Press **MACCLONE** to clone your configuring device's MAC address.

Click **Apply Changes** to have your changes take effect. Click **Return** to discard your changes and return to the **Internet Setup** page. Click **Undo** to revert back to the existing settings.

PPP INTERFACE

Protocol: PPPoE

ATM VCC: 0/32

Login Name:

Password:

Authentication Method:

Connection Type:

Idle Time (s):

Bridge:

☐ Bridged Ethernet (Transparent Bridging)
 ☐ Bridged PPPoE (Implies Bridged Ethernet)
 ☒ Disable Bridge

AC-Name:

Service-Name:

802.1q:

☒ Disable
 ☐ Enable

VLAN ID(1-4095):

MTU (1-1500):

Static IP:

Source Mac address: (ex:00:E0:86:71:05:02)

MACCLONE

Apply Changes

Return

Undo

Modify a PPPoA Connection

PPP INTERFACE

Protocol: This shows the current protocol being modified.

ATM VCC: This shows the current ATM VCC configuration.

Login Name: You can change the currently configured DSL account username here.

Password: You can change the currently configured DSL account password here.

Authentication: Select **PAP**, **CHAP**, or **Auto**. The default is **Auto**.

Connection Type: How your DSL-2745 connects to your ISP. Choose either **Continuous**, **Connect on Demand**, and **Manual**.

Idle Time(s): If you selected **Connect on Demand**, enter the amount time the router waits if there is no activity before disconnecting.

Static IP: If you have been assigned a static IP by your ISP, enter it here.

Click **Apply Changes** to have your changes take effect. Click **Return** to discard your changes and return to the **Internet Setup** page. Click **Undo** to revert back to the existing settings.

PPP INTERFACE - MODIFY

This page is used for advanced PPP interface configuration.

PPP INTERFACE

Protocol:	PPPoA
ATM VCC:	0/35
Login Name:	<input type="text" value="username"/>
Password:	<input type="password" value="••••••"/>
Authentication Method:	<input type="text" value="AUTO"/>
Connection Type:	<input type="text" value="Continuous"/>
Idle Time (s):	<input type="text" value="0"/>
MTU (1-1500):	<input type="text" value="1500"/>
Static IP:	<input type="text"/>

Modify a 1483 MER Connection

IP INTERFACE

IP Interface: This shows the current interface being modified.

Protocol: This shows the current protocol being modified.

ATM VCC: This shows the current ATM VCC configuration.

Bridge: Select **Bridged Ethernet (Transparent Bridging)**, **Bridged PPPoE(implies Bridged Ethernet)**, or **Disable Bridge**.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

Click **Apply Changes** to have your changes take effect. Click **Return** to discard your changes and return to the **Internet Setup** page. Click **Undo** to revert back to the existing settings.

The screenshot shows the 'IP INTERFACE - MODIFY' configuration page. It includes a header bar with the title, a sub-header 'IP INTERFACE', and a note: 'This page is used for advanced IP interface configuration.' The configuration fields are as follows:

- IP Interface:** vc2
- Protocol:** MER
- ATM VCC:** 0/34
- Bridge:** Three radio button options:
 - Bridged Ethernet (Transparent Bridging)
 - Bridged PPPoE (implies Bridged Ethernet)
 - **Disable Bridge** (selected)
- 802.1q:** Two radio button options:
 - **Disable** (selected)
 - Enable
- VLAN ID(1-4095):** A text input field containing the value '0'.

At the bottom of the form are three buttons: 'Apply Changes', 'Return', and 'Undo'.

Modify a 1483 Bridged Connection

BRIDGED INTERFACE

IP Interface: This shows the current interface being modified.

Protocol: This shows the current protocol being modified.

ATM VCC: This shows the current ATM VCC configuration.

802.1q: Choose to either **Disable** or **Enable** the use of VLANs.

VLAN ID(1-4095): If you enabled 802.1q, enter the VLAN ID.

Click **Apply Changes** to have your changes take effect. Click **Return** to discard your changes and return to the **Internet Setup** page. Click **Undo** to revert back to the existing settings.

BRIDGED INTERFACE - MODIFY

This page is used for advanced Bridge interface configuration.

BRIDGE INTERFACE

Bridged Interface: vc1
Protocol: ENET
ATM VCC: 0/33
802.1q: ☒ Disable ☐ Enable
VLAN ID(1-4095):

Modify a 1483 Routed Connection

BRIDGED INTERFACE

- IP Interface:** This shows the current interface being modified.
- Protocol:** This shows the current protocol being modified.
- ATM VCC:** The shows the current ATM VCC configuration.

No advanced configuration settings are available.

IP INTERFACE - MODIFY

This page is used for advanced IP interface configuration.

IP INTERFACE

IP Interface:

vc4

Protocol:

1483 routed

ATM VCC:

0/36

Apply Changes

Return

Undo

Modify an IPoA Connection

IP INTERFACE

- IP Interface:** This shows the current interface being modified.
- Protocol:** This shows the current protocol being modified.
- ATM VCC:** The shows the current ATM VCC configuration.

No advanced configuration settings are available.

IP INTERFACE - MODIFY

This page is used for advanced IP interface configuration.

IP INTERFACE

IP Interface:

vc5

Protocol:

IPoA

ATM VCC:

0/37

Apply Changes

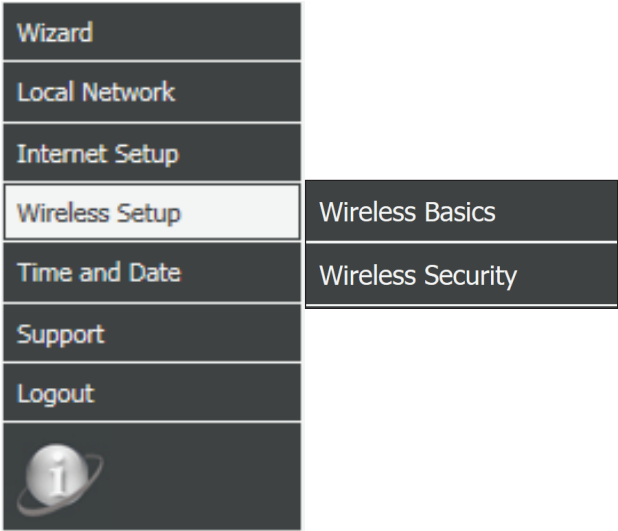
Return

Undo

Wireless Setup

Hover your mouse over the **Wireless Setup** option on the vertical menu bar running along the left side to access:

- Wireless Basics
- Wireless Security



Wireless Basics

This page allows you to manually configure the router’s wireless connectivity settings. To change your wireless network security settings refer to **Wireless Security** on page 49.

WIRELESS NETWORK SETTINGS

- Disable Wireless LAN Interface:

Check this box to disable the Wireless functionality of this device.
- Band:

Select the wireless standards to use on your wireless network. The options are **2.4 GHz (B)**, **2.4 GHz (G)**, **2.4 GHz (B+G)**, **2.4 GHz (N)**, **2.4 GHz (N+G)**, or **2.4 GHz (N+G+B)**.
- Mode:

The DSL-2745 operates in AP mode by default.
- SSID:

Enter a unique Network Name (SSID) to identify your network.
- Channel Number:

Select the channel number for your wireless network to operate on. Choose **1-13**, or **Auto**. The default is **Auto**.
- Radio Power (Percent):

Choose the wireless transmission power strength. The options are **100%**, **60%**, or **20%**. The default is **100%**.
- Associated Clients:

Click this button to see a list of the currently connected wireless clients.
- Channel Width:

Choose the transmission channel bandwidth. The options are **20 MHz** or **20/40 MHz**.

WIRELESS BASIC SETTINGS

This page is used to configure the parameters for wireless LAN clients which may connect to your Access Point. Here you may change wireless encryption settings as well as wireless network parameters.

WIRELESS NETWORK SETTINGS

☐ Disable Wireless LAN Interface

Schedule

Band:

2.4 GHz (B+G+N)

Mode:

AP

SSID:

dlink-5c4260

Channel Number:

Auto

Current Channel: 1

Radio Power (Percent):

100%

Associated Clients:

Show Active Clients

Channel Width:

20/40MHZ

Apply Changes

Click **Apply Changes** to have your changes take effect.

Wireless Security

This page allows you to manually configure the router’s wireless security settings. To change your wireless network settings refer to **Wireless Setup** on page **47**.

Remember to keep your wireless network passwords safe. Remember that if you change the wireless password of your DSL-2745, you must re-input this password on all of your wireless devices.

WIRELESS SECURITY SETTINGS

Encryption: Select the type of Encryption you wish to use. The available options are **None**, **WEP**, **WPA/WPA2 Mixed**, and **WPA2(AES)**. Using **WPA2(AES)** is recommended.

The following pages describe the wireless configuration settings. They are separated by encryption type.

WIRELESS SECURITY SETTINGS

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

WIRELESS SECURITY SETTINGS

Encryption:

None

Encryption:

WEP

Encryption:

WPA/WPA2 Mixed

Encryption:

WPA2(AES)

Encryption: WPA2(AES)

WPA2(AES) is the recommended wireless security encryption type. Using it you can be reasonably assured that your wireless connection is secure.

WIRELESS SECURITY SETTINGS

Encryption: Choose **WPA2(AES)** from the drop-down menu.

WPA Authentication Mode: Choose either **Enterprise (Radius)** or **Personal (Pre-shared Key)**. Most small home/business networks will want to use **Personal (Pre-shared Key)**. If you are running a dedicated RADIUS authentication server, choose **Enterprise (RADIUS)**

If **Personal (Pre-Shared Key)** is selected:

Pre-Shared Key Format: Select the Encryption key format. Choose either **Passphrase** or **HEX(26 Characters)**.

Pre-Shared Key: Enter a wireless key to use on your wireless network.

If **Enterprise (Radius)** is selected:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

WIRELESS SECURITY SETTINGS

Encryption: WPA2(AES)

WPA Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: inlcn0mdad

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

WIRELESS SECURITY SETTINGS

Encryption: WPA2(AES)

WPA Authentication Mode: ☒ Enterprise (RADIUS) ☐ Personal (Pre-Shared Key)

Authentication RADIUS Server: Port 1812 IP address 0.0.0.0 Password

Backup RADIUS Server: Port 1813 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Encryption: WPA/WPA2 Mixed

WPA/WPA2 Mixed(AES) is a reasonably strong wireless security encryption type. This is for wireless clients which do not support WPA2 encryption, otherwise use of WPA2(AES) is recommended.

WIRELESS SECURITY SETTINGS

Encryption: Choose **WPA/WPA2 Mixed** from the drop-down menu.

WPA Authentication Mode: Choose either **Enterprise (Radius)** or **Personal (Pre-shared Key)**. Most small home/business networks will want to use **Personal (Pre-shared Key)**. If you are running a dedicated RADIUS authentication server, choose **Enterprise (RADIUS)**.

If **Personal (Pre-Shared Key)** is selected:

Pre-Shared Key Format: Select the Encryption key format. Choose either **Passphrase** or **HEX(26 Characters)**.

Pre-Shared Key: Enter a wireless key to use on your wireless network.

If **Enterprise (Radius)** is selected:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

WIRELESS SECURITY SETTINGS

Encryption: WPA/WPA2 Mixed

WPA Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key: inlcn0mdad

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

WIRELESS SECURITY SETTINGS

Encryption: WPA/WPA2 Mixed

WPA Authentication Mode: ☒ Enterprise (RADIUS) ☐ Personal (Pre-Shared Key)

Authentication RADIUS Server: Port 1812 IP address 0.0.0.0 Password

Backup RADIUS Server: Port 1813 IP address 0.0.0.0 Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Encryption: WEP

Use of WEP encryption is not recommended, as it only offers a trivial amount of protection for your wireless data. Unless your clients do not support WPA encryption, it is recommended that you select **WPA2(AES)** or **WPA/WPA2 Mixed** instead of **WEP** as they are more secure.

WIRELESS SECURITY SETTINGS

Encryption: Choose **WEP** from the drop-down menu.

Key Length: Select the Encryption cipher key bit strength. The available options are **64-bit** and **128-bit**.

Key Format: Select the Encryption key format. If you selected a **64-bit** key length, you may choose **ASCII (5 Characters)** or **HEX(10 Characters)**. If you selected a **128-bit** key length, you may choose **ASCII (13 Characters)** or **HEX(26 Characters)**.

Default Tx Key: Select the default Tx key.

Encryption Key 1-4: Enter a wireless key to use on your wireless network.

The following settings are available if **Use 802.1x Authentication** is checked:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

The screenshot shows the 'WIRELESS SECURITY SETTINGS' section. The 'Encryption' dropdown is set to 'WEP'. 'Key Length' is set to '64-bit' and 'Key Format' is set to 'ASCII (5 characters)'. 'Default Tx Key' is set to 'Key 1'. There are four 'Encryption Key' fields, each containing five asterisks. The 'Use 802.1x Authentication' checkbox is unchecked.

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

This screenshot shows the same 'WIRELESS SECURITY SETTINGS' page, but with additional options visible. The 'Use 802.1x Authentication' checkbox is now checked. Below it, there are radio buttons for 'WEP 64bits' (unchecked) and 'WEP 128bits' (checked). The 'Authentication RADIUS Server' section is now active, showing fields for 'Port' (1812), 'IP address' (0.0.0.0), and 'Password'. The 'Backup RADIUS Server' section is also active, showing fields for 'Port' (1813), 'IP address' (0.0.0.0), and 'Password'.

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Encryption: None

Disabling encryption and leaving your wireless network open is not recommended. Any wireless client will be able to access your network, be able to use your Internet connection, and leaves you open to security threats.

WIRELESS SECURITY SETTINGS

Encryption: Choose **None** from the drop-down menu.

No configuration settings are available if **Encryption** is set to **None**.

The following settings are available if **Use 802.1x Authentication** is checked:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

The screenshot shows the 'WIRELESS SECURITY SETTINGS' section. The 'Encryption' dropdown is set to 'None'. The 'Use 802.1x Authentication' checkbox is unchecked. A red note at the bottom states: 'Note: When encryption WEP is selected, you must set WEP key value.' An 'Apply Changes' button is at the bottom right.

The screenshot shows the 'WIRELESS SECURITY SETTINGS' section. The 'Encryption' dropdown is set to 'None'. The 'Use 802.1x Authentication' checkbox is checked. Below it, the 'Authentication RADIUS Server' section has fields for 'Port' (1812), 'IP address' (0.0.0.0), and 'Password'. The 'Backup RADIUS Server' section has fields for 'Port' (1813), 'IP address' (0.0.0.0), and 'Password'. A red note at the bottom states: 'Note: When encryption WEP is selected, you must set WEP key value.' An 'Apply Changes' button is at the bottom right.

Time and Date

This section enables you to use an international time server to set the internal time and date for the DSL-2745.

SYSTEM TIME

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

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

Daylight Saving Settings: **Enable** or **disable** Daylight Savings.

Synchronize time with: Select the method of setting the time from **NTP Server automatically**, **PC's Clock**, or **Manually**.

NTP CONFIGURATION

Server: Select **ntp1.dlink.com**, **ntp.dlink.com**, or **other**. If **other** is selected, enter the NTP server address in the box provided.

Server2: Select **ntp1.dlink.com**, **ntp.dlink.com**, or **other**. If **other** is selected, enter the NTP server address in the box provided.

Interval: Enter the frequency which the time is updated.

GMT time: The current time is displayed.

Click **Apply Changes** when you are done or **Reset** to revert to the previous settings.

SYSTEM TIME CONFIGURATION

This page is used to configure the system time and Network Time Protocol(NTP) server. Here you can change the settings or view some information on the system time and NTP parameters.

SYSTEM TIME

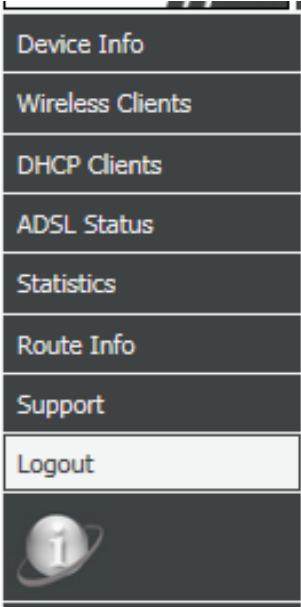
System Time: 2012 Year Jan Month 1 Day 9 Hour 32 min 9 sec
Time Zone: (GMT+08:00) Taipei
Daylight Saving Settings: ☐ Enable ☒ Disable
Synchronize time with: ☒ NTP Server automatically ☐ PC's Clock ☐ Manually

NTP CONFIGURATION:

Server: ntp1.dlink.com
Server2: None
Interval: Every 1 hours
GMT time: Sun Jan 1 1:32:9 2012

Support

Clicking **Support** will direct you to **<http://www.dlink.com/support>**.



Logout

Click **Logout** when you are done configuring your DSL-2745.

WEB LOGOUT

This page is used to logout.

LOGOUT

Logout

Advanced

Product Page: DSL-2745

Firmware Version: EU_1.00

D-Link®

DSL-2745

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

Advanced LAN

ADSL Settings

Advanced Wireless

Port Triggering

Port Forwarding

DMZ

Parent Control

Filtering Options

Anti-Attack Settings

DNS

Dynamic DNS

Network Tools

Routing

ALG

Wireless Schedules

Support

Logout

The Advanced tab provides access to features used for network management, security, and administrative tools to manage the device. You can use diagnostic tools to examine performance and troubleshoot problems your DSL-2745 may have.

Advanced LAN

The Advanced LAN settings page allows you to configure the LAN ports of your DSL-2745. This page allows you to manually configure the Speed and Duplex Mode of your Ethernet connections. You can also limit connections to your LAN and WLAN based on MAC address.

LAN LINK MODE SETTINGS

LAN Port: Select the LAN port to modify. The options are **LAN1**, **LAN2**, **LAN3**, and **LAN4**.

Link Speed/Duplex Mode: Select the link speed and duplex mode. The options are **100 Mbps/Full Duplex**, **100 Mbps/Half Duplex**, **10 Mbps/Full Duplex**, **10 Mbps/Half Duplex**, or **Auto Negotiation**.

The Ethernet Status Table displays the current Ethernet LAN configuration.

MAC ADDRESS CONTROL SETTINGS

MAC Address Control: Select the LAN interfaces to apply the MAC address control to. The options are **LAN1**, **LAN2**, **LAN3**, **LAN4**, and **WLAN**.

Add your client device MAC addresses below, then select the interfaces to apply MAC Address Control to, and click **Apply Changes**.

New MAC Address: Enter the MAC address of your client devices and click **Add**.

CURRENT ALLOWED MAC ADDRESS TABLE

This list displays the currently allowed devices, listed by their MAC address. If you wish to remove a device, click the **Delete** button. Take care when removing devices so you don't accidentally block your configuring device.

ADVANCED LAN SETTINGS

This page is used to configure the LAN link mode and LAN mac address control.

LAN LINK MODE SETTINGS

LAN Port:
Link Speed/Duplex Mode:

ETHERNET Status Table:		
Select	Port	Link Mode
<input type="radio"/>	LAN1	AUTO Negotiation
<input type="radio"/>	LAN2	AUTO Negotiation
<input type="radio"/>	LAN3	AUTO Negotiation
<input type="radio"/>	LAN4	AUTO Negotiation

MAC ADDRESS CONTROL SETTINGS

MAC Address Control: ☐ LAN1 ☐ LAN2 ☐ LAN3 ☐ LAN4 ☐ WLAN

New MAC Address:

CURRENT ALLOWED MAC ADDRESS TABLE

MAC Addr	Action
----------	--------

ADSL Settings

The ADSL Settings allows you to select the DSL standards your DSL-2745 uses to connect to your ISP.

ADSL SETTINGS

To configure the ADSL modulation, click **ADSL Settings**.

In most cases you can leave the settings at their default values.

Click **Apply Changes** when you are done.

ADSL SETTINGS

This page allows you to choose which ADSL modulation settings your modem router will support.

ADSL SETTINGS

ADSL modulation:

☒ G.Lite
☒ G.Dmt
☒ T1.413
☒ ADSL2
☒ ADSL2+

AnnexL Option:

☒ Enabled

AnnexM Option:

☒ Enabled

ADSL Capability:

☒ Bitswap Enable
☐ SRA Enable

Apply Changes

Advanced Wireless

Hover your mouse over the **Advanced Wireless** option on the vertical menu bar running along the left side to access:

- Wireless Advanced
- Access Control
- WPS
- MBSSID Security

Advanced LAN	
ADSL Settings	
Advanced Wireless	Wireless Advanced
Port Triggering	Access Control
Port Forwarding	WPS
DMZ	MBSSID Security
Parent Control	
Filtering Options	
Anti-Attack Settings	
DNS	
Dynamic DNS	
Network Tools	
Routing	
ALG	
Wireless Schedules	
Support	
Logout	

Wireless Advanced

This section allows for advanced configuration of wireless settings.

ADVANCED WIRELESS SETTINGS

Authentication Type: Select the type of authentication, either **Open System**, **Shared Key**, or **Auto**. **Open System** is not recommended.

Fragmentation Threshold: **2346** is the default and recommended setting. Packets exceeding this threshold, in bytes, are fragmented before transmission. Advanced users may wish to adjust this value to improve performance in the presence of radio frequency (RF) interference.

RTS Threshold: **2347** is the default and recommended setting. Advanced users may wish to make minor adjustments if data flow problems exist.

Beacon Interval: **100** is the default and recommended setting. Specify a value for the beacon interval. Beacons are packets sent to synchronize a wireless network.

DTIM Interval: **1** is the default and recommended setting. Delivery traffic indication messages inform wireless clients of how often to listen for buffered multicast or broadcast data.

Data Rate: Select the data rate from the drop down menu. Be careful when selecting speeds as your legacy devices may not support higher speeds or bandwidths. The default and recommended setting is **Auto**.

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.

WIRELESS ADVANCED SETTINGS

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

ADVANCED WIRELESS SETTINGS

Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto
Fragment Threshold: (256-2346)
RTS Threshold: (0-2347)
Beacon Interval: (20-1024 ms)
DTIM Interval: (1-255)
Data Rate:
Preamble Type: ☒ Long Preamble ☐ Short Preamble
Broadcast SSID: ☒ Enabled ☐ Disabled

Apply Changes

WIRELESS MULTIPLE BSSID SETTINGS- VAP0

☐ **Enable VAP0**
SSID:
Broadcast SSID: ☒ Enable ☐ Disable
Relay Blocking: ☐ Enable ☒ Disable
Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

WIRELESS MULTIPLE BSSID SETTINGS- VAP1

☐ **Enable VAP1**
SSID:
Broadcast SSID: ☒ Enable ☐ Disable
Relay Blocking: ☐ Enable ☒ Disable
Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

WIRELESS MULTIPLE BSSID SETTINGS- VAP2

☐ **Enable VAP2**
SSID:
Broadcast SSID: ☒ Enable ☐ Disable
Relay Blocking: ☐ Enable ☒ Disable
Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

Apply Changes

Wireless Advanced (continued)

Broadcast SSID: **Visible** networks conveniently advertise their existence to devices looking for Wi-Fi networks to join. **Invisible**, or hidden, networks do not. To join an invisible network users must manually input its SSID. **Note:** Making a network **Invisible** is not a form of security.

Click **Apply Changes** when you are done.

Guest Networks

The following sections allow you to create guest wireless networks. These networks are separate from your main wireless network.

WIRELESS MULTIPLE BSSID SETTINGS - VAP0 - VAP2

Enable VAP0-VAP2 Check **Enable** to create a guest wireless network.

SSID: Enter a unique Network Name (SSID) to identify your guest network.

Broadcast SSID: **Visible** networks conveniently advertise their existence to devices looking for Wi-Fi networks to join. **Invisible**, or hidden, networks do not. To join an invisible network users must manually input its SSID. **Note:** Making a network **Invisible** is not a form of security alone.

Relay Blocking: **Enable** user isolation to prevent wireless clients from communicating with each other. This may be desired if the DSL-2745 is used in a public setting.

Authentication Type: Select the type of authentication, either **Open System**, **Shared Key**, or **Auto**. **Open System** is not recommended.

Click **Apply Changes** when you are done.

WIRELESS ADVANCED SETTINGS

These settings are only for more technically advanced users who have a sufficient knowledge about wireless LAN. These settings should not be changed unless you know what effect the changes will have on your Access Point.

ADVANCED WIRELESS SETTINGS

Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto
Fragment Threshold: (256-2346)
RTS Threshold: (0-2347)
Beacon Interval: (20-1024 ms)
DTIM Interval: (1-255)
Data Rate:
Preamble Type: ☒ Long Preamble ☐ Short Preamble
Broadcast SSID: ☒ Enabled ☐ Disabled

Apply Changes

WIRELESS MULTIPLE BSSID SETTINGS- VAP0

☐ **Enable VAP0**
SSID:
Broadcast SSID: ☒ Enable ☐ Disable
Relay Blocking: ☐ Enable ☒ Disable
Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

WIRELESS MULTIPLE BSSID SETTINGS- VAP1

☐ **Enable VAP1**
SSID:
Broadcast SSID: ☒ Enable ☐ Disable
Relay Blocking: ☐ Enable ☒ Disable
Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

WIRELESS MULTIPLE BSSID SETTINGS- VAP2

☐ **Enable VAP2**
SSID:
Broadcast SSID: ☒ Enable ☐ Disable
Relay Blocking: ☐ Enable ☒ Disable
Authentication Type: ☐ Open System ☐ Shared Key ☒ Auto

Apply Changes

Wireless Access Control

The Wireless Access Control setup section enables you to configure MAC Address filters to control which wireless clients can or cannot connect to your network.

WIRELESS ACCESS CONTROL MODE

Wireless Access Control Mode: Select **Allow Listed**, **Deny Listed**, or **Disable**.

Click **Apply Changes** when you are done.

WIRELESS ACCESS CONTROL SETTINGS

MAC Address: Enter the MAC address of the device you wish to add to the current access control list.

Click **Add** to add a device to the access control list or click **Reset** to clear the MAC address.

CURRENT ACCESS CONTROL LIST

This list currently displays the MAC addresses of the devices being filtered. To remove a device from the list, select the radio button next to the MAC address and click the **Delete Selected** button. To remove all the entries from the list, click **Delete All**.

WIRELESS ACCESS CONTROL

If you choose 'Allowed Listed', only those clients whose wireless MAC addresses are in the access control list will be able to connect to your Access Point. When 'Deny Listed' is selected, these wireless clients on the list will not be able to connect the Access Point.

WIRELESS ACCESS CONTROL MODE

Wireless Access Control Mode: Disable

Apply Changes

WIRELESS ACCESS CONTROL SETTINGS

MAC Address: (ex. 00E086710502)

Add Reset

CURRENT ACCESS CONTROL LIST

MAC Address	Select

Delete Selected Delete All

Wi-Fi Protected Setup

This section allows you to configure how the DSL-2745 uses Wi-Fi Protected Setup (WPS) to create a secure wireless connection.

WIFI PROTECTED SETTINGS

Check the box to **Disable WPS**.

WPS Status: WPS is configured by default.

Self-PIN Number: Enter a 4 or 8 digit WPS pin, or click **Regenerate PIN** to create a new random WPS PIN.

PIN Configuration: Click **Start PIN** to activate the WPS-PIN (PIN) method. You will then have 120 seconds to connect and enter the PIN on your device.

Push Button Configuration: Click **Start 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.

Click **Apply Changes** when you are done or click **Reset** to undo any changes you may have made.

CURRENT KEY INFO

This box shows the type of Authentication, Encryption, and wireless key.

CLIENT PIN INFO

Some wireless configuration utilities on client devices allow you to generate a WPS PIN. This can be useful in various situations, such as to ensure that you are adding the correct wireless device to your network. To use this feature, create a PIN on your wireless client, enter it into the **Client PIN Number** box, and click **Start PIN**.

WI-FI PROTECTED SETUP

This page allows you to change the setting for WPS (Wi-Fi Protected Setup). Using this feature could let your wireless client automatically synchronize its setting and connect to the Access Point in a minute without any hassle.

WIFI PROTECTED SETTINGS

☐ Disable WPS

WPS Status: ☒ Configured ☐ UnConfigured

Self-PIN Number:

PIN Configuration:

Push Button Configuration:

CURRENT KEY INFO

Authentication	Encryption	Key
WPA2-Mixed PSK	TKIP+AES	inlc0mdad

CLIENT PIN INFO

Client PIN Number:

MBSSID Security Settings

The following sections allow you to adjust the security used on guest wireless networks.

MBSSID SECURITY SETTINGS

SSID Type: Select either **VAP0**, **VAP1**, or **VAP2**.

Encryption: Select the type of Encryption you wish to use. The available options are **None**, **WEP**, **WPA/WPA2 Mixed**, and **WPA2(AES)**. Using **WPA2(AES)** is recommended.

The following pages describe the wireless configuration settings. They are separated by encryption type.

MBSSID SECURITY SETTINGS

This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.

MBSSID SECURITY SETTINGS

SSID TYPE:

☒ VAP0 ☐ VAP1 ☐ VAP2

Encryption:

None

☐ Use 802.1x Authentication

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

MBSSID Encryption: WPA2(AES)

WPA2(AES) is the recommended wireless security encryption type. Using it you can be reasonably assured that your wireless connection is secure.

MBSSID SECURITY SETTINGS

SSID Type: Select either **VAP0**, **VAP1**, or **VAP2**.

Encryption: **WPA2(AES)**

WPA Authentication Mode: Choose either **Enterprise (Radius)** or **Personal (Pre-shared Key)**. Most small home/business networks will want to use **Personal (Pre-shared Key)**. If you are running a dedicated RADIUS authentication server, choose **Enterprise (RADIUS)**

If **Personal (Pre-Shared Key)** is selected:

Pre-Shared Key Format: Select the Encryption key format. Choose either **Passphrase** or **HEX(26 Characters)**.

Pre-Shared Key: Enter a wireless key to use on your wireless network.

If **Enterprise (Radius)** is selected:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

MBSSID SECURITY SETTINGS

SSID TYPE: ☒ VAP0 ☐ VAP1 ☐ VAP2

Encryption: WPA2(AES)

WPA Authentication Mode: ☐ Enterprise (RADIUS) ☒ Personal (Pre-Shared Key)

Pre-Shared Key Format: Passphrase

Pre-Shared Key:

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

MBSSID SECURITY SETTINGS

SSID TYPE: ☒ VAP0 ☐ VAP1 ☐ VAP2

Encryption: WPA2(AES)

WPA Authentication Mode: ☒ Enterprise (RADIUS) ☐ Personal (Pre-Shared Key)

Authentication RADIUS Server: Port IP address

Password:

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

MBSSID Encryption: WPA/WPA2 Mixed

WPA/WPA2 Mixed(AES) is a reasonably strong wireless security encryption type. This is for wireless clients which do not support WPA2 encryption, otherwise use of WPA2(AES) is recommended.

MBSSID SECURITY SETTINGS

SSID Type: Select either **VAP0**, **VAP1**, or **VAP2**.

Encryption: **WPA/WPA2 Mixed**

WPA Authentication Mode: Choose either **Enterprise (Radius)** or **Personal (Pre-shared Key)**. Most small home/business networks will want to use **Personal (Pre-shared Key)**. If you are running a dedicated RADIUS authentication server, choose **Enterprise (RADIUS)**

If **Personal (Pre-Shared Key)** is selected:

Pre-Shared Key Format: Select the Encryption key format. Choose either **Passphrase** or **HEX(26 Characters)**.

Pre-Shared Key: Enter a wireless key to use on your wireless network.

If **Enterprise (Radius)** is selected:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

The screenshot shows the 'MBSSID SECURITY SETTINGS' form. The 'SSID TYPE' is set to VAP0. The 'Encryption' dropdown is set to WPA2(AES). The 'WPA Authentication Mode' has 'Personal (Pre-Shared Key)' selected. The 'Pre-Shared Key Format' is set to 'Passphrase'. The 'Pre-Shared Key' field is empty. A red note at the bottom states: 'Note: When encryption WEP is selected, you must set WEP key value.' An 'Apply Changes' button is at the bottom right.

The screenshot shows the 'MBSSID SECURITY SETTINGS' form. The 'SSID TYPE' is set to VAP0. The 'Encryption' dropdown is set to WPA2(AES). The 'WPA Authentication Mode' has 'Enterprise (RADIUS)' selected. The 'Authentication RADIUS Server' section shows 'Port' set to 1812, 'IP address' as an empty field, and 'Password' as an empty field. A red note at the bottom states: 'Note: When encryption WEP is selected, you must set WEP key value.' An 'Apply Changes' button is at the bottom right.

MBSSID Encryption: WEP

Use of WEP encryption is not recommended, as it only offers a trivial amount of protection for your wireless data. Unless your clients do not support WPA encryption, it is recommended that you select **WPA2(AES)** or **WPA/WPA2 Mixed** instead of **WEP** as they are more secure.

WIRELESS SECURITY SETTINGS

SSID Type: Select either **VAP0**, **VAP1**, or **VAP2**.

Encryption: **WEP**

Key Length: Select the Encryption cipher key bit strength. The available options are **64-bit** and **128-bit**.

Key Format: Select the Encryption key format. If you selected a **64-bit** key length, you may choose **ASCII (5 Characters)** or **HEX(10 Characters)**. If you selected a **128-bit** key length, you may choose **ASCII (13 Characters)** or **HEX(26 Characters)**.

Default Tx Key: Select which Tx key is used as the default.

Encryption Key 1-4: Enter a wireless key to use on your wireless network.

The following settings are available if **Use 802.1x Authentication** is checked:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

The screenshot shows the 'MBSSID SECURITY SETTINGS' page. The 'SSID TYPE' is set to 'VAP0'. The 'Encryption' is set to 'WEP'. The 'Key Length' is set to '64-bit'. The 'Key Format' is set to 'ASCII (5 characters)'. The 'Default Tx Key' is set to 'Key 1'. There are four 'Encryption Key' fields, each with a masked input (*****). The 'Use 802.1x Authentication' checkbox is unchecked.

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

The screenshot shows the 'MBSSID SECURITY SETTINGS' page. The 'SSID TYPE' is set to 'VAP0'. The 'Encryption' is set to 'WEP'. The 'Key Length' is set to '64-bit'. The 'Key Format' is set to 'ASCII (5 characters)'. The 'Default Tx Key' is set to 'Key 1'. There are four 'Encryption Key' fields, each with a masked input (*****). The 'Use 802.1x Authentication' checkbox is checked. Below it, there are three radio buttons: 'WEP 64bits' (selected), 'WEP 128bits', and 'WEP 128bits'. The 'Authentication RADIUS Server' section has fields for 'Port' (set to 1812), 'IP address', and 'Password'.

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

MBSSID Encryption: None

Disabling encryption and leaving your wireless network open is not recommended. Any wireless client will be able to access your network, be able to use your Internet connection, and leaves you open to security threats.

WIRELESS SECURITY SETTINGS

Encryption: None

No configuration settings are available if **Encryption** is set to **None**.

The following settings are available if **Use 802.1x Authentication** is checked:

Authentication RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the RADIUS Server.

Backup RADIUS Server: Enter the **Port**, **IP address**, and **Password** of the backup RADIUS Server.

Click **Apply Changes** to have your changes take effect.

MBSSID SECURITY SETTINGS

SSID TYPE: ☒ VAP0 ☐ VAP1 ☐ VAP2

Encryption:

☐ Use 802.1x Authentication

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

MBSSID SECURITY SETTINGS

SSID TYPE: ☒ VAP0 ☐ VAP1 ☐ VAP2

Encryption:

☒ Use 802.1x Authentication

Authentication RADIUS Server: Port IP address

Password

Note: When encryption WEP is selected, you must set WEP key value.

Apply Changes

Port Triggering

Port triggering allows ports to be opened when traffic is detected on specified ports. This is used for facilitating communication between applications and servers behind a NAT firewall.

NAT PORT TRIGGER STATUS

Nat Port Trigger: Select **Enable** or **Disable**.

Click **Apply Changes** to have your changes take effect.

APPLICATION TYPE

Usual Application Name: These commonly used applications are provided as an example of how to input port ranges.

User-defined Application name: Name the rule you are about to define for your application. You may define up to 8 port ranges per application.

Start Match Port: Enter the starting source port range your DSL-2745 will forward traffic from.

End Match Port: Enter the ending source port range your DSL-2745 will forward traffic from.

Trigger Protocol: Select the protocol to monitor for to trigger this rule.

Start Relate Port: Enter the starting destination port range your DSL-2745 will forward traffic to.

End Relate Port: Enter the ending destination port range your DSL-2745 will forward traffic to.

Click **Apply Changes** to have your changes take effect.

NAT PORT TRIGGER

Some applications require that specific ports in the Router's firewall be opened for access by the remote parties. Port Triggering dynamically opens up the "Relate Port" in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the "Match Port". The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the "Relate Port".

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

NAT PORT TRIGGER STATUS

Nat Port Trigger: ☐ Enable ☒ Disable

Apply Changes

APPLICATION TYPE

☒ **Usual Application Name:** Select One

☐ **User-defined Application Name:**

Start Match Port	End Match Port	Trigger Protocol	Start Relate Port	End Relate Port	Open Protocol	Nat Type
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing
<input type="text"/>	<input type="text"/>	UDP	<input type="text"/>	<input type="text"/>	UDP	outgoing

Apply Changes

CURRENT PORT TRIGGER TABLE

ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action
------------	------------------	-----------	------------	---------------	-------------	--------

Port Triggering (continued)

An example Port Triggering Table is shown to the right.

CURRENT PORT TRIGGER TABLE

From the table you can see the current port triggering rules and their details. To delete a rule, select the **Delete** button in the last column of the rule.

CURRENT PORT TRIGGER TABLE						
ServerName	Trigger Protocol	Direction	Match Port	Open Protocol	Relate Port	Action
CustomApp	udp	outgoing	1-2	udp	1-2	Delete
CustomApp	udp	outgoing	3-4	udp	3-4	Delete
CustomApp	udp	outgoing	5-6	udp	5-6	Delete
CustomApp	udp	outgoing	7-8	udp	7-8	Delete
CustomApp	udp	outgoing	9-10	udp	9-10	Delete
CustomApp	udp	outgoing	11-12	udp	11-12	Delete
CustomApp	udp	outgoing	13-14	udp	13-14	Delete
CustomApp	udp	outgoing	15-16	udp	15-16	Delete
CustomAPP2	udp	outgoing	17-18	udp	17-18	Delete
CustomAPP2	udp	outgoing	19-20	udp	19-20	Delete
CustomAPP2	udp	outgoing	21-22	udp	21-22	Delete
CustomAPP2	udp	outgoing	23-24	udp	23-24	Delete
CustomAPP2	udp	outgoing	25-26	udp	25-26	Delete
CustomAPP2	udp	outgoing	27-28	udp	27-28	Delete
CustomAPP2	udp	outgoing	29-30	udp	29-30	Delete
CustomAPP2	udp	outgoing	31-32	udp	31-32	Delete

Port Forwarding

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by Protocol and WAN port) to an internal server with a private IP address on the LAN side.

PORT FORWARDING SETUP

Well known Service: Commonly used protocols are pre-defined and can be easily selected.

User-defined Service: Name the rule you are about to define for your server.

Protocol: Select the protocol type to use with this service.

WAN Port: Enter the WAN port number.

LAN Port: Enter the LAN port number.

LAN IP Address: Enter the IP address traffic is forwarded to.

Click **Add** to add the new port forwarding rule. To modify an existing rule, select it using the radio selection button. The boxes of the Port Forwarding Setup section will populate with the rules parameters. Enter your changes and click **Modify**.

PORT FORWARDING

Port Forwarding allows you to direct incoming traffic from the WAN side (identified by Protocol and WAN port) to the internal server with a private IP address on the LAN side.

PORT FORWARDING SETUP

☒ **Well known Service** AUTH ▼
☐ **User-defined Service**
Protocol TCP ▼
WAN Port 113 (ex. 5001:5010)
LAN Port 113
LAN IP Address

Add Modify

CURRENT PORT FORWARDING TABLE

Select	Server Name	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action
--------	-------------	----------	------------------	------------	----------------	----------	-------	--------

Port Forwarding (continued)

An example Port Forwarding Table is shown to the right.

CURRENT PORT FORWARDING TABLE

From the table you can see the current port forwarding rules and their details. To disable a rule select the **Disable** button in the last column of the rule. To delete a rule, select the **Delete** button in the last column of the rule.

CURRENT PORT FORWARDING TABLE								
Select	Server Name	Protocol	Local IP Address	Local Port	WAN IP Address	WAN Port	State	Action
<input type="radio"/>	WEB	tcp	192.168.1.100	80-80	any	80-80	Enable	<div>DeleteDisable</div>
<input type="radio"/>	FTP	tcp	192.168.1.100	21-21	any	21-21	Enable	<div>DeleteDisable</div>
<input type="radio"/>	WEB	tcp	192.168.1.100	80-80	any	54-54	Enable	<div>DeleteDisable</div>

DMZ

This page allows you to manually configure the router’s DMZ settings. Since some applications are not compatible with NAT, the device supports the use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and it is visible on the Internet with the correct type of software. Note that any client PC in the DMZ is exposed to various types of security risks. If you use DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through DMZ.

DMZ CONFIGURATION

Select the **WAN Interface** to associate with a **DMZ Host IP address**, LAN IP address. Click **Apply Changes** when you are done or **Reset WAN Interface** to revert to the previously saved settings.

CURRENT DMZ TABLE

The currently assigned DMZ is displayed in this list. To delete the DMZ, select it using the radio button and press **Delete Selected**.

DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

DMZ CONFIGURATION

WAN Interface:pppoe1

DMZ Host IP Address:

Apply Changes

Reset

CURRENT DMZ TABLE:

Select	WAN Interface	DMZ Ip
<div>Delete Selected</div>		

Parent Control

Hover your mouse over the **Parent Control** option on the vertical menu bar running along the left side to access:

- URL Block
- Online Time Limit
- Schedules

Advanced LAN	
ADSL Settings	
Advanced Wireless	
Port Triggering	
Port Forwarding	
DMZ	
Parent Control	URL Block
Filtering Options	Online Time Limit
Anti-Attack Settings	Schedules
DNS	
Dynamic DNS	
Network Tools	
Routing	
ALG	
Wireless Schedules	
Support	
Logout	

URL Block

This page is used to configure URLs to be blocked during specific times. In order for this function to work as expected, the system time must be set correctly.

URL BLOCKING CAPABILITY

URL Blocking Capability: Check the radio button to enable URL blocking. Click **Apply Changes** to enable the feature and start adding rules.

URL BLOCKING

Block Any URL: Check the radio button to block all URLs.

Keyword: Enter a URL to be blocked.

Schedule Mode: Select either **Existing Schedule** or **Manual Schedule**. Refer to **Schedules** on page 78 for more information on creating schedules.

Days: If **Manual Schedule** is selected, select the days to apply the rule.

All day (24Hour): If **Manual Schedule** is selected, the rule will run 24 hours a day.

Time: If **All Day** is not selected, enter start and end time to apply the rule. Use a 24 hour format.

When you are satisfied with your URL blocking rule, click **Add Filter**. To edit an existing rule, select if from the **URL Blocking Table** and click **Modify Filter**.

URL BLOCKING TABLE

This table displays the current URL Blocking rules in effect. To delete an existing rule, select it from the list and click **Delete Selected URL**.

URL BLOCK

This page is used to configure the blocked URL in specified time. Here you can add/delete filtered URL. Firstly, you should enable URL Blocking Capability.

Note: Please ensure that the time and date on the router is correct. Go to Setup then choose Time and Date.

URL BLOCKING CAPABILITY

URL Blocking Capability: ☒ Disable ☐ Enable

Apply Changes

URL BLOCKING

☐ Block Any URL

☒ Keyword:

Schedule Mode: ☐ Existing Schedule ☒ Manual Schedule

Schedule:

Days: ☐ EveryDay
☐ Sun ☐ Mon ☐ Tue ☐ Wed
☐ Thu ☐ Fri ☐ Sat

All day(24Hour): ☐

Time: From : To :
(e.g. From 09:21 To 18:30)

URL BLOCKING TABLE:

Select	Filtered URL	Days	Time	Rule Name
--------	--------------	------	------	-----------

Online Time Limit

This page allows Internet browsing time to be set for a group of devices or on a per device basis. In order for this function to work as expected, the system time must be set correctly.

ONLINE TIME LIMIT

Online Time Limit: Check the radio button to enable the online time limit feature. Click **Apply** to enable the feature and start adding rules.

Date: Select the days to apply the time limit.

Time: If **All Day** is not selected, enter start and end time to apply the rule. Use a 24 hour format.

Specific PC: Select a PC to apply an online time limit to by either IP Address or MAC Address.

IP Address: Enter a single IP address or IP address range to apply the rule to.

MAC Address: Enter a MAC Address to apply the rule to.

When you are satisfied with your time limit rules, click **Add Rules**. To clear the fields and start over, click **Reset**.

CURRENT ONLINE TIMELIMIT TABLE:

This table displays the current online time limit rules in effect. To delete all the rules, click **Delete All**.

ONLINE TIME LIMIT

This page manages the time of surfing the Internet. Enabling this feature allows only specified devices to access the Internet in the predefined allocated time segment.
Note: IP or MAC address may be used to specify these devices.
Before enabling this feature, ensure that the time of the router is correct. Click [Setup->Time and Date](#) to set the time of your router.

ONLINE TIME LIMIT

Online Time Limit: ☐ Enable ☒ Disable

Apply

Date: ☐ Everyday
☐ Mon ☐ Tues ☐ Wed ☐ Thur ☐ Fri ☐ Sat
☐ Sun

Time: ☐ All day(24Hour)
Start Time End Time (ex. 09:45)

Specific PC: ☒ IP Address ☐ MAC Address

IP Address: ~

MAC Address: (ex. 00:E0:86:71:05:02)

Add Rule Reset

CURRENT ONLINE TIMELIMIT TABLE:

Select	Date	Starting Time	Ending Time	MAC Address	IP Address	Action
Delete All						

Schedules

This page allows you to input schedule rules to be used for the URL block feature.

ADD SCHEDULE RULE

Rule Name: Enter a name for the rule.

Days: Select the days to apply the rule.

All day (24Hour): Select to have the rule run 24 hours a day.

Time: If **All Day** is not selected, enter start and end time to apply the rule. Use a 24 hour format.

When you are satisfied with your time limit rules, click **Add Rules**. To clear the fields and start over, click **Reset**.

RULES TABLE:

This table displays the current rules available for selection. To delete a rule, select it and click **Delete Selected Rule**.

SCHEDULES

Schedule allows you to create scheduling rules to be applied for URL block.

ADD SCHEDULE RULE

Rule Name:

Days:

☐ EveryDay

☐ Sun ☐ Mon ☐ Tue ☐ Wed

☐ Thu ☐ Fri ☐ Sat

All day(24Hour): ☐

Time:

From : To :

(e.g. From 09:21 To 18:30)

Add Rules

RULES TABLE:

Select	Rule Name	Days	Time
--------	-----------	------	------

Delete Selected Rule

Filtering Options

Hover your mouse over the **Filtering Options** option on the vertical menu bar running along the left side to access:

- IP/Port Filter
- IPv6/Port Filter
- MAC Filter

Advanced LAN	
ADSL Settings	
Advanced Wireless	
Port Triggering	
Port Forwarding	
DMZ	
Parent Control	
Filtering Options	IP/Port Filter
Anti-Attack Settings	IPv6/Port Filter
DNS	MAC Filter
Dynamic DNS	
Network Tools	
Routing	
ALG	
Wireless Schedules	
Support	
Logout	

IP/Port Filter

The IP/Port filter is used to restrict or allow certain types of data packets through the gateway. These filters are helpful in securing or restricting traffic on your local network.

DEFAULT ACTION STATUS

Outgoing Default Action: Select whether to **Permit** or **Deny** data packets to flow out of the WAN interface. The default setting is **Permit**.

Incoming Default Action: Select whether to **Permit** or **Deny** data packets to flow into the WAN interface. The default setting is **Deny**.

RULE CONFIGURATION

To create a rule, fill out the following parameters.

Rule Action: Select whether this rule will **Permit** or **Deny** data packets.

WAN Interface: Select the WAN interface.

Protocol: Select the protocol type: **IP**, **ICMP**, **TCP**, or **UDP**.

Source IP Address & Mask Address: Enter the source IP address and subnet mask for the rule.

Destination IP Address & Mask Address: Enter the destination IP address and subnet mask for the rule.

SPort: Enter the source port number if **TCP** or **UDP** is selected.

DPort: Enter the destination port number if **TCP** or **UDP** is selected.

IP/PORT FILTERING

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

DEFAULT ACTION STATUS

Outgoing Default Action: ☒ Permit ☐ Deny

Incoming Default Action: ☐ Permit ☒ Deny

RULE CONFIGURATION

Rule Action: ☒ Permit ☐ Deny

WAN Interface:

Protocol:

Direction:

Source IP Address:

Mask Address:

Dest IP Address:

Mask Address:

SPort:

DPort:

Enable: ☒

Apply Changes

Reset

Help

CURRENT FILTER TABLE

Rule	WanItf	Protoco l	Source IP/Mas k	SPort	Dest IP/Mas k	DPort	State	Directio n	Action
------	--------	--------------	-----------------------	-------	---------------------	-------	-------	---------------	--------

IP/Port Filter (continued)

RULE CONFIGURATION (CONTINUED)

Enable: Check to enable the rule

When you are satisfied with your IP/Port Filtering rule, click **Apply Changes** to add it to the **Current Filter Table**. To clear the fields and start over, click **Reset**. To see help on creating rules, click **Help**.

CURRENT FILTER TABLE

The current filter rules in effect are listed here. Click **Disable/Enable** to disable or enable a rule. Click **Delete** to delete a rule.

IP/PORT FILTERING

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

DEFAULT ACTION STATUS

Outgoing Default Action: ☒ Permit ☐ Deny
Incoming Default Action: ☐ Permit ☒ Deny

RULE CONFIGURATION

Rule Action: ☒ Permit ☐ Deny
WAN Interface:
Protocol:
Direction:
Source IP Address:
Dest IP Address:
SPort:
DPort:
Mask Address:
Mask Address:
Enable: ☒

CURRENT FILTER TABLE

Rule	WanItf	Protoco l	Source IP/Mas k	SPort	Dest IP/Mas k	DPort	State	Directio n	Action
------	--------	--------------	-----------------------	-------	---------------------	-------	-------	---------------	--------

IPv6/Port Filter

The IPv6/Port filter is used to restrict or allow certain types of IPv6 data packets through the gateway. These filters are helpful in securing or restricting traffic on your local network.

DEFAULT ACTION STATUS

Outgoing Default Action: Select whether to **Permit** or **Deny** data packets to flow out of the WAN interface. The default setting is **Permit**.

Incoming Default Action: Select whether to **Permit** or **Deny** data packets to flow into the WAN interface. The default setting is **Permit**.

RULE CONFIGURATION

To create a rule, fill out the following parameters.

Rule Action: Select whether this rule will **Permit** or **Deny** data packets.

Protocol: Select the protocol type: **IPv6**, **ICMP6**, **TCP**, or **UDP**.

Icmp6Type: If **ICMP6** is selected, select **Ping6**.

Direction: Select the direction, either **Upstream** or **Downstream**.

Source IP Address & Prefix Length: Enter the source IPv6 address and prefix length for the rule.

Destination IP Address & Prefix Length: Enter the destination IP address and subnet mask for the rule.

SPort: Enter the source port number if **TCP** or **UDP** is selected.

DPort: Enter the destination port number if **TCP** or **UDP** is selected.

IP/PORT FILTERING

Entries in this table are used to restrict certain types of ipv6 data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

DEFAULT ACTION STATUS

Outgoing Default Action: ☒ Permit ☐ Deny
Incoming Default Action: ☒ Permit ☐ Deny

RULE CONFIGURATION

Rule Action: ☒ Permit ☐ Deny
Protocol: IPv6 Icmp6Type: PING6
Direction: Upstream
Source IPv6 Address: Prefix Length:
Dest IPv6 Address: Prefix Length:
SPort: - DPort: -
Enable: ☒

Apply Changes Reset Help

CURRENT FILTER TABLE

Rule	Protocol	Source IPv6/Prefix	SPort	Dest IPv6/Prefix	DPort	ICMP6 Type	State	Direction	Action
------	----------	--------------------	-------	------------------	-------	------------	-------	-----------	--------

IPv6/Port Filter (continued)

RULE CONFIGURATION (CONTINUED)

Enable: Check to enable the rule

When you are satisfied with your IP/Port Filtering rule, click **Apply Changes** to add it to the **Current Filter Table**. To clear the fields and start over, click **Reset**. To see help on creating rules, click **Help**.

CURRENT FILTER TABLE

The current filter rules in effect are listed here. Click **Disable/Enable** to disable or enable a rule. Click **Delete** to delete a rule.

IP/PORT FILTERING

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

DEFAULT ACTION STATUS

Outgoing Default Action: ☒ Permit ☐ Deny
Incoming Default Action: ☐ Permit ☒ Deny

RULE CONFIGURATION

Rule Action: ☒ Permit ☐ Deny
WAN Interface:
Protocol:
Direction:
Source IP Address:
Dest IP Address:
SPort:
DPort:
Mask Address:
Mask Address:
Enable: ☒

CURRENT FILTER TABLE

Rule	WanItf	Protoco l	Source IP/Mas k	SPort	Dest IP/Mas k	DPort	State	Directio n	Action
------	--------	--------------	-----------------------	-------	---------------------	-------	-------	---------------	--------

MAC Filter

The MAC filter is used to restrict or allow certain types of Ethernet Frames through the gateway based on their source or destination MAC address. These filters are helpful in securing or restricting traffic on your local network.

DEFAULT POLICY

Outgoing Default Action: Select whether to **Deny** or **Allow** frames to flow out of the WAN interface. The default setting is **Allow**.

Incoming Default Action: Select whether to **Deny** or **Allow** frames to flow into the WAN interface. The default setting is **Allow**.

ADD FILTER

To create a rule, fill out the following parameters.

Direction: Select whether this rule will apply to **Outgoing** or **Incoming** traffic.

Action: Select whether to **Deny** or **Allow** frames.

You may create a rule to apply to either a Source MAC address, Destination MAC address, or both. Broadcast MAC addresses may not be filtered.

Source MAC: Enter the source **MAC** address to filter.

Destination Mac: Enter the destination **MAC** address.

When you are satisfied with your MAC Filtering rule, click **ADD**.

CURRENT MAC FILTER TABLE

The current list of MAC filters are displayed here. To delete a filter, select it from the list and click **Delete**. To delete all the filters, click **Delete All**.

MAC FILTERING

Entries in this table are used to restrict certain types of data packets from your local network to Internet through the Gateway. Use of such filters can be helpful in securing or restricting your local network.

DEFAULT POLICY

Outgoing Default Policy: ☐ Deny ☒ Allow
Incoming Default Policy: ☐ Deny ☒ Allow

Apply Changes

ADD FILTER

Direction:
Action: ☒ Deny ☐ Allow
Source MAC: (ex. 00E086710502)
Destination MAC: (ex. 00E086710502)

Add

CURRENT MAC FILTER TABLE

Select	Direction	Source MAC	Destination MAC
Delete	Delete All		

Anti-Attack Settings

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. Attacks can be malicious security breaches or unintentional network issues that render the router unusable. Attack checks allow you to manage WAN security threats such as continual ping requests and discovery via ARP scans. Certain Denial-of-Service (DoS) attacks can be blocked. These attacks, if uninhibited, can use up processing power and bandwidth and prevent regular network services from running normally. Thresholds can be configured to temporarily restrict traffic from the offending source.

DOS CONFIGURATION

Enable DoS Prevention:

Check this box to enable DoS prevention. Types of attacks may be individually enabled, along with their thresholds. You may enable or disable all the anti-attack types by clicking **Select ALL/Clear All**.

Enable Source IP Blocking:

You may block source IP addresses for a set period of time.

Click **Apply Changes** to have your changes take effect.

ANTI-ATTACK CONFIGURATION

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

DOS CONFIGURATION

☒ Enable DoS Prevention

☒ Whole System Flood: SYN

☒ Whole System Flood: FIN

☒ Whole System Flood: UDP

☒ Whole System Flood: ICMP

☒ Per-Source IP Flood: SYN

☒ Per-Source IP Flood: FIN

☒ Per-Source IP Flood: UDP

☒ Per-Source IP Flood: ICMP

☒ TCP/UDP PortScan

☒ ICMP Smurf

☒ IP Land

☒ IP Spoof

☒ IP TearDrop

☒ PingOfDeath

☒ TCP Scan

☒ TCP SynWithData

☒ UDP Bomb

☒ UDP EchoChargen

Select ALL

Clear ALL

☐ Enable Source IP Blocking

100

Packets/Second

100

Packets/Second

100

Packets/Second

100

Packets/Second

100

Packets/Second

100

Packets/Second

100

Packets/Second

100

Packets/Second

Low

Sensitivity

300

Block time (sec)

Apply Changes

DNS

Hover your mouse over the **DNS** option on the vertical menu bar running along the left side to access:

- DNS
- IPv6 DNS

Advanced LAN	
ADSL Settings	
Advanced Wireless	
Port Triggering	
Port Forwarding	
DMZ	
Parent Control	
Filtering Options	
Anti-Attack Settings	
DNS	DNS
Dynamic DNS	IPv6 DNS
Network Tools	
Routing	
ALG	
Wireless Schedules	
Support	
Logout	

DNS

This page allows you to manually configure the router's DNS settings.

Domain Name System (DNS) is an Internet service that translates domain names into IP addresses. Because domain names are alphanumeric, 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.

DNS CONFIGURATION

If you are using the device for DHCP service on the LAN or if you are using DNS servers on the ISP network, select **Attain DNS Automatically**.

If you have alternate DNS IP addresses, select **Set DNS Manually** and enter them into the **DNS 1**, **DNS 2**, and **DNS 3** fields.

Click **Apply Changes** when you are done or **Reset Selected** to revert to your previously saved settings.

The screenshot shows the 'DNS CONFIGURATION' page. At the top, there is an orange header with the title 'DNS CONFIGURATION'. Below the header, a grey box contains the text: 'This page is used to configure the DNS server ip addresses for DNS Relay.' Below this, the main configuration area has a dark grey header with the title 'DNS CONFIGURATION'. Inside this area, there are two radio buttons: 'Attain DNS Automatically' (which is selected) and 'Set DNS Manually'. Below the radio buttons, there are three input fields labeled 'DNS 1:', 'DNS 2:', and 'DNS 3:'. The 'DNS 1' field contains the text '0.0.0.0'. At the bottom of the configuration area, there are two buttons: 'Apply Changes' and 'Reset Selected'.

IPv6 DNS

IPV6 DNS CONFIGURATION

If you are using the device for DHCP service on the LAN or if you are using DNS servers on the ISP network, select **Attain DNS Automatically**.

If you have alternate DNS IP addresses, select **Set DNS Manually** and enter them into the **DNS 1**, **DNS 2**, and **DNS 3** fields.

Click **Apply Changes** when you are done or **Reset Selected** to revert to your previously saved settings.

IPV6 DNS CONFIGURATION

This page is used to configure the DNS server ipv6 addresses.

IPV6 DNS CONFIGURATION

☒ Attain DNS Automatically

☐ Set DNS Manually

DNS 1:

DNS 2:

DNS 3:

Interface:

Interface:

Interface:

Apply Changes

Reset Selected

Dynamic DNS

This page allows you to configure the router's Dynamic DNS settings.

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.yourdomain.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.

DDNS CONFIGURATION

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.

Enable: Check this box to enable DDNS.

DynDNS Settings

Username: Enter the username for your Dynamic DNS account.

Password: Enter the password for your Dynamic DNS account.

Click **Add** when you are done. To remove an existing DDNS entry, select it from the table below and click the **Remove** button.

DYNAMIC DDNS TABLE

This list displays the current dynamic Dynamic DNS settings.

DYNAMIC DNS CONFIGURATION

This page is used to configure the Dynamic DNS details from DynDNS.org .
Sign up for D-Link's Free DDNS service at: www.DLinkDDNS.com

DDNS CONFIGURATION

DDNS provider: dlinkddns.com(Free) ▼
Hostname:
Interface: pppoe1 ▼
Enable: ☒

DynDns Settings:

Username:
Password:

DYNAMIC DDNS TABLE

Select	State	Service	Hostname	Username	Interface
--------	-------	---------	----------	----------	-----------

Network Tools

Hover your mouse over the **Network Tools** option on the vertical menu bar running along the left side to access:

- Port Mapping
- IGMP Proxy
- IP QoS
- ARP Binding

Advanced LAN	
ADSL Settings	
Advanced Wireless	
Port Triggering	
Port Forwarding	
DMZ	
Parent Control	
Filtering Options	
Anti-Attack Settings	
DNS	
Dynamic DNS	
Network Tools	Port Mapping
Routing	IGMP Proxy
ALG	IP QoS
Wireless Schedules	UPnP
Support	ARP Binding
Logout	

Port Mapping

From the Port Mapping page you can bind the WAN interfaces and the LAN interfaces to the same group.

PORT MAPPING SETUP

Port Mapping: Enable/Disable port mapping.

The procedure for manipulating a mapping group is as follows:

- Step 1** Select a group from the table.
- Step 2** Select interfaces from the WAN and LAN interface list and add them to interface group list.
- Step 3** Click **Apply** to save the changes.

PORT MAPPING CONFIGURATION

To manipulate a mapping group:

1. Select a group from the table.
2. Select interfaces from the available/grouped interface list and add it to the grouped/available interface list using the arrow buttons to manipulate the required mapping of the ports.
3. Click "Apply Changes" button to save the changes.

Note: The selected interfaces will be removed from their existing groups and added to the new group.

PORT MAPPING CONFIGURATION

Port Mapping: ☒ Disable ☐ Enable

WAN

LAN

Interface group

Add >

< Del

Select	Interfaces
Default	LAN1,LAN2,LAN3,LAN4,wlan,wlan-vap0,wlan-vap1,wlan-vap2,pppoe1
Group1	
Group2	
Group3	
Group4	

Apply

D-Link DSL-2745 Wireless N300 ADSL2+ Modem Router User Manual

91

IGMP Proxy Configuration

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 after you enable it.

IGMP PROXY CONFIGURATION

IGMP Proxy: Select to **Enable** or **Disable** the IGMP proxy. **Enable** is the default.

Multicast Allowed: Select to **Enable** or **Disable** Multicast. **Enable** is the default.

Robust Count: Set robustness value to account for packet loss on congested networks.

Last Member Query Count: Set IGMP query count. 2 is the default.

Query Interval: Set IGMP query interval. 2 is the default.

Query Response Interval: Set the IGMP response interval time in seconds. 60 seconds is the default.

Query Response Interval: Set the IGMP query response interval in ms. 100 ms is the default.

Group Leave Delay: Set the IGMP group leave delay in ms. 2000 ms is the default.

Click **Apply Changes** when you are done or **Undo** to revert to your previous settings.

IGMP PROXY CONFIGURATION

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 doing the follows:

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

IGMP PROXY CONFIGURATION

IGMP Proxy: ☐ Disable ☒ Enable
Multicast Allowed: ☐ Disable ☒ Enable
Robust Count:
Last Member Query Count:
Query Interval: (seconds)
Query Response Interval: (*100ms)
Group Leave Delay: (ms)

Apply Changes

Undo

IP QoS

From this page you can configure the Quality of Service settings on your DSL-2745 to help improve your browsing experience. Setting up QoS requires familiarity with networking technology outside the scope of this document, as well as an understanding of the traffic on your network.

IP QoS CONFIGURATION

Click the radio button to enable or disable IP QoS. If enabled, choose whether to use **WFQ(4:3:2:1)** or **strict prior**.

Click **Apply Changes** to begin using QoS.

QoS RULE LIST & QoS RULE LIST(CONTINUE)

The table shows the current QoS rules currently in effect.

Click **Add Rule** to add a rule. To modify a rule, select it from the table. The Add or Modify QoS Rule box will appear and the fields will populate with the rule credentials. To delete a rule, select it from the list and click **Delete Rule**.

ADD OR MODIFY QoS RULE

Enter the criteria for your QoS rule.

Click **Apply Changes** to add your rule to the QoS rule list.

IP QoS

Entries in this table are used to assign the precedence for each incoming packet based on specified policy.
Config Procedure:
1: set traffic rule.
2: assign the precedence or add marker for different stream.

IP QoS CONFIGURATION

IP QoS: ☐ disable ☒ enable

Schedule Mode: WFQ(4:3:2:1)

Apply Changes

QoS RULE LIST

src MAC	dest MAC	src IP	sPort	dest IP	dPort	proto	phy port
---------	----------	--------	-------	---------	-------	-------	----------

QoS RULE LIST(CONTINUE)

IPP	TOS	DSCP	TC	802.1p	Prior	IPP Mark	TOS Mark	DSCP Mark	TC Mark	802.1p Mark	sel
-----	-----	------	----	--------	-------	----------	----------	-----------	---------	-------------	-----

Delete Add Rule

ADD OR MODIFY QoS RULE

Source MAC:

Destination MAC:

Source IP:

Source Mask:

Destination IP:

Destination Mask:

Source Port:

Destination Port:

Protocol: TCP/UDP

Phy Port: LAN1

IPP/DS Field: ☒ IPP/TOS ☐ DSCP

IP Precedence Range: ~

Type of Service:

DSCP Range: ~ (Value Range:0~63)

Traffic Class Range: ~ (Value Range:0~255)

802.1p: ~

Priority: p3(Lowest)

☐ insert or modify QoS mark

Apply Changes

UPnP

This page is used to configure UPnP. The system acts as a daemon after you enable it. UPnP helps to automatically configure software and devices on your network to access the resources they require.

UPNP SETUP

Click the radio button to enable or disable Universal Plug and Play (**UPnP**).

Check the box to **Enable UPnP**.

Click **Apply Changes** when you are done.

UPNP CONFIGURATION

This page is used to configure UPnP. The system acts as a daemon when you enable UPnP.

UPNP CONFIGURATION

UPnP: ☐ Disable ☒ Enable

WAN Interface:

UPNP PORT LIST

Protocol	External Port	Server IP	Internal Port	Description
<div>Apply Changes</div>				

ARP Binding

This page allows you to bind an IP address to a MAC address.

ARP BINDING CONFIGURATION

- IP Address:** Enter the IP address to bind the MAC address to.
- MAC Address:** Enter the MAC address to have bound with an IP address.

Once you have entered the IP address to bind to a MAC address, click **Add**.

To delete an ARP binding, select it from the ARP binding table and click **Delete Selected**.

To undo your changes, click **Undo**.

ARP BINDING TABLE

The table shows a list of currently bound ARP addresses.

ARP BINDING CONFIGURATION

This page lists the permanent arp entry table.You can bind ip with corresponding mac to avoid arp spoof.

ARP BINDING CONFIGURATION

IP Address:

0.0.0.0

Mac Address:

000000000000

(ex. 00E086710502)

Add

Delete Selected

Undo

ARP BINDING TABLE

Select	IP Address	MAC Address
--------	------------	-------------

Routing

Hover your mouse over the **Routing** option on the vertical menu bar running along the left side to access:

- Static Routing
- IPv6 Static Route
- RIP

Advanced LAN	
ADSL Settings	
Advanced Wireless	
Port Triggering	
Port Forwarding	
DMZ	
Parent Control	
Filtering Options	
Anti-Attack Settings	
DNS	
Dynamic DNS	
Network Tools	
Routing	Static Route
ALG	IPv6 Static Route
Wireless Schedules	RIP
Support	
Logout	

Static Routing

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

HOST

Enable: Check this box to enable static routing.

Destination: Enter the IP address of the destination device.

Subnet Mask: Enter the subnet mask of the destination device.

Net Hop: Enter the IP address of the next hop in the IP route to the destination device.

Metric: The metric cost for the destination.

Interface: Select the interface for the specified route.

ROUTING CONFIGURATION

This page is used to configure the routing information. Here you can add/delete IP routes.

HOST

Enable

☒

Destination

Subnet Mask

Next Hop

Metric

1

Interface

Add Route

Update

Delete Selected

Show Routes

STATIC ROUTE TABLE

Select	State	Destination	Subnet Mask	NextHop	Metric	Itf
--------	-------	-------------	-------------	---------	--------	-----

Once you have entered your Static Route Criteria, click **Add Route**.

To update an existing route, select it from the table below, make your adjustments and click **Update**.

To delete a static route, select it from the table and click **Delete Selected**.

To see the current IP routes, click **Show Routes**.

STATIC ROUTE TABLE

The table shows a list of currently defined static routes.

Static Routing (Continued)

To see the current IP routes, click **Show Routes**. A window will pop-up with the current IP route table.

CURRENT IP ROUTING TABLE

The table shows a list of all the currently defined routes.

You may either **Refresh** or **Close** this pop-up window.

IP ROUTE TABLE

This table shows a list of destination routes commonly accessed by your network.

CURRENT IP ROUTING TABLE

Destination	Subnet Mask	NextHop	Interface
192.168.1.1	255.255.255.255	*	e1
222.222.222.1	255.255.255.255	*	a4
0.0.0.0	0.0.0.0	222.222.1.1	a4

Refresh

Close

IPv6 Static Route

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

CONFIGURATION

- Destination:** Enter the IPv6 address of the destination device.
- Prefix Length:** Enter the subnet prefix.
- Next Hop:** Enter the IPv6 address of the next hop in the IP route to the destination device.
- Interface:** Select the interface for the specified route.

Once you have entered your Static Route Criteria, click **Add Route**.

To delete a static route, select it from the table and click **Delete Selected**.

IPv6 Static Route Table

The table shows a list of currently defined static routes.

IPv6 ROUTING CONFIGURATION

This page is used to configure the ipv6 routing information. Here you can add/delete IPv6 routes.

CONFIGURATION

Destination

Prefix Length

Next Hop

Interface

Add Route

Delete Selected

IPv6 STATIC ROUTE TABLE

Select	Destination	NextHop	Interface
--------	-------------	---------	-----------

RIP

From this page advanced users can configure the router to use the Routing Internet Protocol (RIP). RIP is an Internet protocol you can set up to share routing table information with other routing devices on your LAN, at your ISP’s location, or on remote networks connected to your network via the ADSL line.

RIP

To enable or disable RIP, select **Off** or **On** and click **Apply**.

- Destination:** Enter the IPv6 address of the destination device.
- Interface:** Select the interface to apply the RIP rule to.
- Recv Version:** Select the version of RIP protocol to use when receiving RIP updates. The options are **RIP1**, **RIP2**, or **Both**.
- Send Version:** Select the version of RIP protocol to use when sending RIP updates. The options are **RIP1** or **RIP2**.

Once you have entered your RIP Criteria, click **Add**.

To delete a RIP rule, select it from the table and click **Delete**.

RIP CONFIGURATION

Enable the RIP if you are using this device as a RIP-enabled router to communicate with others using the Routing Information Protocol.
attention: if you want to enable RIP, please make sure remote control is enabled.

RIP

Off

On

Apply

interface

LAN

Recv Version

RIP1

Send Version

RIP1

Add

Delete

RIP CONFIG LIST

Select	interface	Recv Version	Send Version
--------	-----------	--------------	--------------

ALG

Hover your mouse over the **ALG** option on the vertical menu bar running along the left side to access:

- NAT ALG
- NAT Exclude IP
- NAT Forwarding
- FTP ALG Config
- NAT IP Mapping

Advanced LAN	
ADSL Settings	
Advanced Wireless	
Port Triggering	
Port Forwarding	
DMZ	
Parent Control	
Filtering Options	
Anti-Attack Settings	
DNS	
Dynamic DNS	
Network Tools	
Routing	
ALG	NAT ALG
Wireless Schedules	NAT Exclude IP
Support	NAT Forwarding
Logout	FTP ALG Config
	NAT IP Mapping

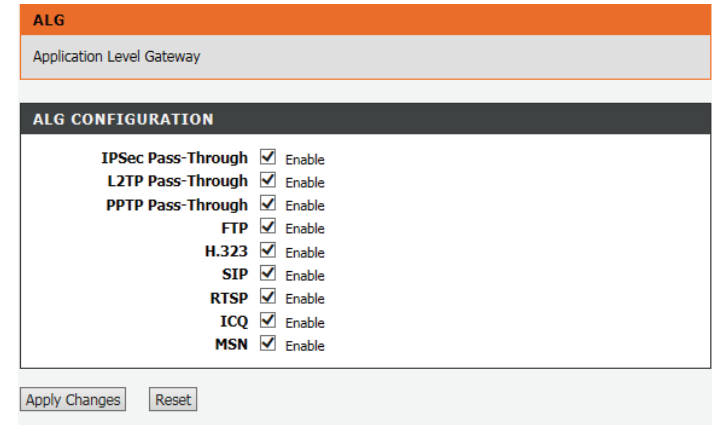
NAT ALG

Application Level Gateways (ALGs) are security components that enhance the firewall and NAT support of this router to seamlessly support application layer protocols. In some cases enabling the ALG will allow the firewall to use dynamic ephemeral TCP/UDP ports to communicate with the known ports a particular client application (such as H.323 or RTSP) requires, without which the admin would have to open large number of ports to accomplish the same support. Because the ALG understands the protocol used by the specific application that it supports, it is a very secure and efficient way of introducing support for client applications through the router's firewall.

ALG CONFIGURATION

Check or un-check the boxes next to the protocols to enable or disable them.

Click **Apply Changes** when you are done.



ALG	
Application Level Gateway	
ALG CONFIGURATION	
IPSec Pass-Through	<input checked="" type="checkbox"/> Enable
L2TP Pass-Through	<input checked="" type="checkbox"/> Enable
PPTP Pass-Through	<input checked="" type="checkbox"/> Enable
FTP	<input checked="" type="checkbox"/> Enable
H.323	<input checked="" type="checkbox"/> Enable
SIP	<input checked="" type="checkbox"/> Enable
RTSP	<input checked="" type="checkbox"/> Enable
ICQ	<input checked="" type="checkbox"/> Enable
MSN	<input checked="" type="checkbox"/> Enable

Apply Changes Reset

NAT Exclude IP

CONFIG

- Interface:** Select the interface to apply the exclusion to.
- IP Range:** Enter the IP address range to apply the exclusion to.

Click **Apply Changes** when you are done or **Reset** to undo your changes.

CURRENT NAT EXCLUDE IP TABLE

The current list of NAT ALG exceptions is listed here. To remove an exclusion, select it from the table and click **Delete**.

NAT EXCLUDE IP

In the page ,you can config some source ip address which use the purge route mode when access internet through the specified interface.

CONFIG

interface

pppoe1

IP Range

-

Apply Changes

Reset

CURRENT NAT EXCLUDE IP TABLE

WAN Interface	Low IP	High IP	Action
---------------	--------	---------	--------

NAT Forwarding

SETTINGS

- Local IP Address:** Enter the local IP address.
- Remote IP Address:** Enter the remote IP address.
- Enable:** Check the box to enable NAT Forwarding.

Click **Apply Changes** when you are done or **Reset** to undo your changes.

CURRENT NAT PORT FORWARDING TABLE

The current list of NAT Port Forwarding table is listed here. To remove an exclusion, select it from the table and click **Delete**.

NAT FORWARDING

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Gateway's NAT firewall.

SETTING

Local IP Address

Remote IP Address

Enable☒

Apply Changes

Reset

CURRENT NAT PORT FORWARDING TABLE

Local IP Address	Remote IP Address	State	Action
------------------	-------------------	-------	--------

FTP ALG Config

SETTING PORT

FTP ALG Port: Enter the FTP ALG port.

Click **Add Dest Ports** when you are done. To delete a currently assigned FTP ALG port, select it from the table and click the **Delete Selected Dest Port** button.

FTP ALG PORTS TABLE

The current list of FTP ALG ports is displayed.

FTP ALG CONFIGURATION

This page is used to configure FTP Server ALG and FTP Client ALG ports .

SETTING PORT

FTP ALG port

Add Dest Ports

Delete Selected DestPort

FTP ALG PORTS TABLE

Select	Ports
<input type="radio"/>	21

NAT IP Mapping

SETTING PORT

Type: Select the type of NAT IP mapping. The available options are **One-to-Many**, **Many-to-One**, **Many-to-many**, or **One-to-One**. The available boxes change depending upon your selection.

Local Start IP: Enter the Local Start IP.

Local End IP: Enter the Local End IP.

Global Start IP: Enter the Global Start IP.

Global End IP: Enter the Global End IP.

Click **Apply Changes** when you are done or **Reset** to undo your changes.

CURRENT NAT IP MAPPING TABLE

The current NAT IP Mapping table is displayed. To remove a mapping, select it and click the **Delete Selected** button. To remove all the entries click the **Delete All** button.

NAT IP MAPPING

Entries in this table allow you to config one IP pool for specified source ip address from LAN,so one packet which's source ip is in range of the specified address will select one IP address from pool for NAT.

SETTING

TypeOne-to-One

Local Start IP

Local End IP

Global Start IP

Global End IP

Apply Changes

Reset

CURRENT NAT IP MAPPING TABLE

Local Start IP	Local End IP	Global Start IP	Global End IP	Action
----------------	--------------	-----------------	---------------	--------

Delete Selected

Delete All

Wireless Schedules

You may disable Wireless during set periods of time from this page.

SCHEDULE CAPABILITY

WLAN Schedule Capability: Click **Enable/Disable** to enable or disable the wireless scheduling capability.

Once you have made a change to the WLAN schedule, click **Apply Changes**.

SCHEDULE RULES

This table displays the current Online Time Limit rules in effect. To delete a rule, select it from the table and click **Delete**.

To add a rule, click the **Add** button and fill out the Schedule Configuration Box and click **Apply**.

SCHEDULE CONFIGURATION

Name: Give your Wireless Schedule Rule a name.

Days: Select the days to apply the time limit.

All day(24Hour): Check this box if you would like to disable Wi-Fi for an entire day.

Time: If **All Day** is not selected, enter start and end time to apply the rule. Use a 24 hour format.

WIRELESS SCHEDULES

Schedule allows you to create scheduling rules to open wireless function within the time specified.

Maximum number of schedule rules:32

SCHEDULE CAPABILITY

WLAN Schedule Capability ☐ Disable ☒ Enable

Apply Changes

SCHEDULE RULES

Select	Rule Name	Day	Time
<input type="radio"/>	no wi-fi at the dinner table	Sun,Mon,Tue,Wed,Thu,Fri,Sat	17:00 ~ 18:00

Add Delete

SCHEDULE CONFIGURATION

Name:

Days: ☐ EveryDay ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun

All day(24Hour): ☐


Time: From : To : (e.g. From 09:21 To 18:30)

Apply Cancel

Management

Product Page: DSL-2745

Firmware Version: EU_1.00



DSL-2745

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

System

Firmware Update

Access Control List


Password

Diagnostics

System Log

Support

Logout



The Management tab provides access to the DSL-2745's administration and diagnostic tools.

System

This page allows you to reboot the device, back up your settings, or restore settings either from a file or to their default values.

SAVE/REBOOT

Reset to default: Click this button to restore all configuration settings back to the settings that were in effect at the time the device was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created.

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

Save and Reboot: Click this button to reboot the device.

BACKUP SETTINGS

Backup Settings: Click this button to save the current router configuration settings to a file on the hard disk of the computer you are using. You will see a file dialog, where you can select a location and file name for the settings.

UPDATE SETTINGS

Update Settings: To restore a saved configuration, use the **Browse...** button to find the previously saved configuration file. Then, click the **Update Settings** button to transfer those settings to the device.

SAVE/REBOOT

Click the button below to reboot the router or reset it to factory default settings.

Reset to default

Save and reboot

BACKUP SETTINGS

Backup DSL Router configurations. You can save your routers configuration to your PC.

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

Backup Settings

UPDATE SETTINGS

Update DSL Router settings. You can update your routers settings using your saved configuration file.

Config File Name :

Browse...

Update Settings

Firmware Update

This page allows you to upgrade the firmware of your router. Make sure the firmware you want to use is on the local hard drive of the computer and then click **Browse** to upload the file.

FIRMWARE UPDATE

Current Firmware Version: Displays your current firmware's version.

Current Firmware Date: Displays your current firmware's release date.

Firmware File Name: After you have downloaded a new firmware, click **Browse...** and locate the firmware on your computer. To begin the firmware update process, click **Update Firmware**. The update process takes about two minutes to complete.

Warning: You must use a computer with a wired connection to the device to upload the firmware file; do not use a wireless client. During the upgrade process, do not power off your computer or router, and do not refresh the browser window until the upgrade is complete.

UPGRADE FIRMWARE

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.

SELECT FILE

Current Firmware Version: EU_1.00

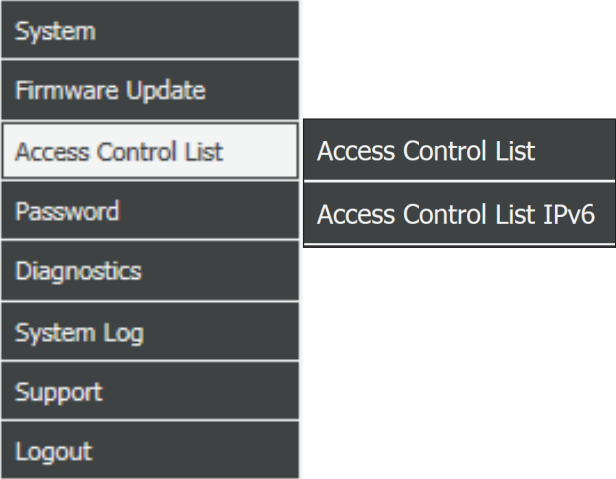
Current Firmware Date: Jan 15 2016 10:27:02

Firmware File Name:

Access Control List

Hover your mouse over the **Access Control List** option on the vertical menu bar running along the left side to access:

- Access Control List
- Access Control List IPv6



Access Control List

This page allows you to enable or disable various services from being used on the LAN or WAN side.

Click the **Apply** button once you are satisfied with your changes.

REMOTE ACCESS CONTROLS

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

ACCESS MANAGEMENT

Access Management	LAN Access	WAN Access	
	Enable	Enable	Port
HTTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	8080
Telnet	<input checked="" type="checkbox"/>	<input type="checkbox"/>	23
SSH	<input checked="" type="checkbox"/>	<input type="checkbox"/>	22
FTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	21
TFTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>	69
PING	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Apply

Access Control List IPv6

This page allows you to enable or disable various services from being used on the LAN or WAN side using IPv6 parameters.

ACLV6 CONFIGURATION -- DIRECTION

Direction Select: Choose either LAN or WAN.

The following settings are available if **Direction Select** is set to **LAN**:

LAN ACL SWITCH CONFIGURATION

LAN ACL Switch: Choose either **Enable** or **Disable**.

ACLV6 SETTINGS

IP Address: Enter the IPv6 IP address and prefix.

Services Allowed: Un-check **Any** to individually select the services which will be available on your LAN.

Click **Add** to add the ACLv6 rule.

ACL CONFIGURATION

You can specify which services are accessible from LAN or WAN side. Entries in this ACL table are used to permit certain types of data packets from your local network or Internet network to the Gateway. Using of such access control can be helpful in securing or restricting the Gateway management.

ACLV6 CONFIGURATION -- DIRECTION

Direction Select: ☒ LAN ☐ WAN

LAN ACL SWITCH CONFIGURATION

LAN ACL Switch: ☒ Enable ☐ Disable

ACLV6 SETTINGS

IP Address:

Services Allowed:

- ☐ Any
- ☐ web
 - ☐ telnet
 - ☐ ssh
 - ☐ ftp
 - ☐ tftp
 - ☐ snmp
 - ☐ ping6

Add

Access Control List IPv6 (continued)

The following settings are available if **Direction Select** is set to **WAN**:

ACLV6 SETTINGS

WAN Setting: Select either **Interface** or **Address**.

The following settings are available if **WAN Setting** is set to **Interface**:

WAN Interface: Select the WAN interface to apply the ACLv6 rule to.

Services Allowed: Select the services to allow.

The following settings are available if **WAN Setting** is set to **IP Address**:

IP Address: Enter the IPv6 IP address and prefix.

Services Allowed: Select the services to allow.

Click **Add** to add the ACLv6 rule.

CURRENT IPV6 ACL TABLE

This table displays the IPv6 ACL rules. To delete a rule, click **Delete**.

ACLV6 SETTINGS

WAN Setting:

Interface

WAN Interface:

pppoe1

Services Allowed:

☐ web

☐ telnet

☐ ssh

☐ ftp

☐ tftp

☐ snmp

☐ ping6

Add

ACLV6 SETTINGS

WAN Setting:

IP Address

IP Address:

Services Allowed:

☐ web

☐ telnet

☐ ssh

☐ ftp

☐ tftp

☐ snmp

☐ ping6

Add

CURRENT IPV6 ACL TABLE				
Direction	IPv6 Address/Interface	Service	Port	Action
WAN	any	ping6	--	<div>Delete</div>

Password

This section allows you to configure access to the router. You may configure different user names, passwords, privileges, and the idle time before automatic log out. If you forget your password, you will need to reset the device to the factory default settings and all device configuration settings will be lost.

CONFIGURATION

User Name: Enter the User Name

Privilege: Select either **Root** or **User** privilege.

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

New Password: Enter the new password.

Confirm Password: Re-enter the new password.

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

Click **Apply Changes** when you are done. Select **Add** to create a new account. Select an existing account from the user account table and click **Modify** to modify an existing account or **Delete** to delete it. Click **Reset** to undo reset modifications made to the above fields.

USERS ACCOUNT TABLE

The User Account Table displays information about the currently configured user accounts.

USER ACCOUNT CONFIGURATION

This page is used to add user account to access the web server of ADSL Router. Empty user name or password is not allowed.

CONFIGURATION

User Name:

Privilege: User ▼

Old Password:

New Password:

Confirm Password:

Idle logout time: (1-60min)

Add Modify Delete Reset

USER ACCOUNT TABLE			
Select	User Name	Privilege	Idle Time
<input checked="" type="radio"/>	admin	root	5
<input type="radio"/>	user	user	5

Diagnostics

Hover your mouse over the **Diagnostics** option on the vertical menu bar running along the left side to access:

- Ping
- Ping6
- Traceroute
- ADSL
- Diag Test

System	
Firmware Update	
Access Control List	
Password	
Diagnostics	Ping
System Log	Ping6
Support	Traceroute
Logout	ADSL
	Diag Test

Ping

The Ping section enables you to run an IPv4 connectivity test.

HOST

Enter an IPv4 address or hostname and click **Ping** and wait for the results to appear.

PING DIAGNOSTIC

This page is used to ping.

HOST

PING

Ping6

The Ping6 section enables you to run an IPv6 connectivity test.

HOST

- Target Address:** Enter an IPv6 address.
- Interface:** Select the interface to run the ping6 test on.

Click **Ping** and wait for the results.

PING6 DIAGNOSTIC

Ping6 Diagnostic

Target Address:

Interface:

PING

Traceroute

The Traceroute section enables you to run a traceroute test to see how your traffic transverses the Internet.

TRACEROUTE

Host:

Enter an IP address or hostname.

NumberOfTries:

Enter the number of attempts.

Timeout:

Enter the timeout in ms.

Datasize:

Enter the datasize in bytes.

DSCP:

Adjust the DSCP number.

MaxHopCount:

Enter the maximum number of hops.

Interface:

Select the interface to initiate the traceroute.

Click **Traceroute** to run the test and click **Show Result** to see the results.

TRACEROUTE DIAGNOSTIC

This page is used to traceroute diagnostic.

TRACEROUTE

Host

NumberOfTries

3

Timeout

5000

ms

Datasize

38

Bytes

DSCP

0

MaxHopCount

30

Interface

any

traceroute

Show Result

ADSL

This page allows you to run a diagnostic test on your ADSL connection.

ADSL TONE DIAGNOSTIC

Click **Start** to begin the test.

DIAGNOSTIC ADSL

This page is used to diagnostic ADSL.

ADSL TONE DIAGNOSTIC

Start

	Downstream	Upstream
Hlin Scale		
Loop Attenuation(dB)		
Signal Attenuation(dB)		
SNR Margin(dB)		
Attainable Rate(Kbps)		
Output Power(dBm)		

ADSL TONE LIST

Tone Number	H.Real	H.Image	SNR	QLN	Hlog
0					
1					
2					
3					
4					

Diag Test

This page is used to test the connection to your local network, the connection to your DSL service provider, and the connection to your Internet service provider. Select your **Internet Connection** and click **Run Diagnostic Test** to run the diagnostics tests.

DIAGNOSTIC TEST

The DSL Router is capable of testing your DSL connection. The individual tests are listed below. If a test d
click "Run Diagnostic Test" button again to make sure the fail status is consistent.

SELECT THE INTERNET CONNECTION

pppoe1

Run Diagnostic Test

System Log

The DSL-2745 keeps a running log of events and activities occurring on the router. You may send these logs to a SysLog server on your network.

SETTING

Error: Check this box to enable error messages.

Notice: Check this box to enable notice messages.

Click **Apply Changes** to have your changes take effect. Click **Reset** to undo your changes and revert to the previous settings.

REMOTE SETTING

Remote Setting: Check this box to enable remote logging.

Remote Log Host: Enter the IP address of your logging server.

Click **Apply Changes** to have your changes take effect.

EVENT LOG TABLE

If you have logging enabled, you will see the current log of errors. Click **Save Log to File** to save the log to your computer’s hard drive. Click **Clean Log Table** to clear the log.

LOG SETTING

This page is used to display the system event log table. By checking Error or Notice (or both)will set the log flag. By clicking the ">>|", it will display the newest log information below.

SETTING

Error: ☒

Notice: ☐

Apply Changes

Reset

REMOTE SETTING

Remote Log Enable: ☒

Remote Log Host:

Apply Changes

EVENT LOG TABLE

Save Log to File

Clean Log Table

Old New

Time

Index

Type

Log Information

Page: 1/1


D-Link DSL-2745 Wireless N300 ADSL2+ Modem Router User Manual

122

Status

Product Page: DSL-2745

Firmware Version: EU_1.00



DSL-2745

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

Device Info

Wireless Clients

DHCP Clients


ADSL Status

Statistics

Route Info

Support

Logout



The Status tab provides information about the DSL-2745's current status.

Device Info

This page displays the current information for the DSL-2745.

SYSTEM

This section displays a summary of the system settings.

DSL

This section displays of the Internet connection settings.

LAN CONFIGURATION

This section displays a summary of the local network settings.

WIRELESS INFO

This section displays a summary of the wireless network settings.

DNS STATUS

This section displays a summary of the DNS settings.

WAN CONFIGURATION

This section displays a summary of the WAN Configuration.

WAN IPV6 CONFIGURATION

This section displays a summary of the WAN IPv6 Configuration.

Click **Refresh** to refresh the list.

ADSL ROUTER STATUS

This page shows the current status and some basic settings of the device.

SYSTEM

Model Name	DSL-2745
Firmware Version	EU_1.00
Uptime	0 1:40:25
Date/Time	Sun Jan 1 9:40:25 2012
Built Date	Jan 15 2016 10:27:02

DSL

Operational Status	--
Upstream Speed	--
Downstream Speed	--

LAN CONFIGURATION

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	00:18:E7:5C:42:60

WIRELESS INFO

Status:	Disabled
MAC Address:	00:18:E7:5C:42:60
Network Name (SSID):	dlink-5c4260
Current Channel:	0
Encryption:	WPA2 Mixed

DNS STATUS

DNS Mode	Auto
DNS Servers	
IPv6 DNS Mode	Auto
IPv6 DNS Servers	

WAN CONFIGURATION

Interface	VPI /VCI	Encap	Droute	Protocol	IP Address	Gateway
pppoe1	8/35	VCMUX	Off	PPPoE	0.0.0.0	0.0.0.0

WAN IPV6 CONFIGURATION

Interface	VPI/VCI	Encap	Protocol	IPv6 Address	Prefix	Gateway	Droute
pppoe1	8/35	VCMUX	PPPoE				

Refresh

Wireless Clients

This table displays a list of wireless clients that are connected to your wireless router. It displays the MAC address, number of packets transmitted, number of packets received, the transmission speed, power saving status, and expiration time.

Click **Refresh** to refresh the list.

ACTIVE WIRELESS CLIENT TABLE

This table shows the MAC address, transmission, reception packet counters and encrypted status for each associated wireless client

ACTIVE WIRELESS CLIENT TABLE

MAC Address	Tx Packet	Rx Packet	Tx Rate (Mbps)	Power Saving	Expired Time (s)
None	---	---	---	---	---

Refresh

DHCP Clients

This table lists each DHCP client, including its hostname, MAC address, IP address, and expiration time.

Click **Refresh** to refresh the list.

ACTIVE DHCP CLIENT TABLE

This table shows the assigned IP address, MAC address and remaining time for each DHCP leased client.

ACTIVE DHCP CLIENT TABLE

Name	IP Address	MAC Address	Expiry	Type
08203PCWIN7	192.168.1.2	3c:1e:04:f3:b6:49	In 6 days 22:19:42	DHCP

Refresh

ADSL Status

This page displays the current status of your DSL-2745.

Click **Retrain** to force your DSL-2745 to disconnect and re-connect to your IP.

Click **Refresh** to refresh the page.

ADSL STATUS

This page shows the setting of the ADSL Router.

ADSL

ADSL Line Status	ACTIVATING.
ADSL Mode	--
Channel Mode	--
Up Stream	--
Down Stream	--
Attenuation Down Stream	--
Attenuation Up Stream	--
SNR Margin Down Stream	--
SNR Margin Up Stream	--
Vendor ID	RETK
Firmware Version	4926e811
CRC Errors	--
Up Stream BER	--
Down Stream BER	--
Up Output Power	--
Down Output Power	--
ES	--
SES	--
UAS	--

Retrain

Refresh

Statistics

Here you can view the packets transmitted and received passing through your router on both WAN and LAN ports, as well as the DSL information. The traffic counter will reset if the device is rebooted.

Click **Refresh** to refresh the list.

STATISTICS

This page shows the packet statistics for transmission and reception regarding to network interface.

STATISTICS

Interface	Rx pkt	Rx err	Rx drop	Tx pkt	Tx err	Tx drop
LAN	50105	0	0	40819	0	0
ADSL0	0	0	0	0	0	0
ADSL1	0	0	0	0	0	0
ADSL2	0	0	0	0	0	0
ADSL3	0	0	0	0	0	0
ADSL4	0	0	0	0	0	0
ADSL5	0	0	0	0	0	0
ADSL6	0	0	0	0	0	0
ADSL7	0	0	0	0	0	0
WLAN1	167	0	0	4	0	0
WLAN2	0	0	0	0	0	0
WLAN3	0	0	0	0	0	0
WLAN4	0	0	0	0	0	0

Refresh

Route Info

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

Click **Refresh** to refresh the list.

IP ROUTE TABLE

This table shows a list of destination routes commonly accessed by your network.

CURRENT IP ROUTING TABLE


Destination	Subnet Mask	NextHop	Interface
192.168.1.1	255.255.255.255	*	e1

Refresh

Help

Product Page: DSL-2745

Firmware Version: EU_1.00



DSL-2745

Menu

Setup


Advanced

Management

Status

Support

Logout



SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

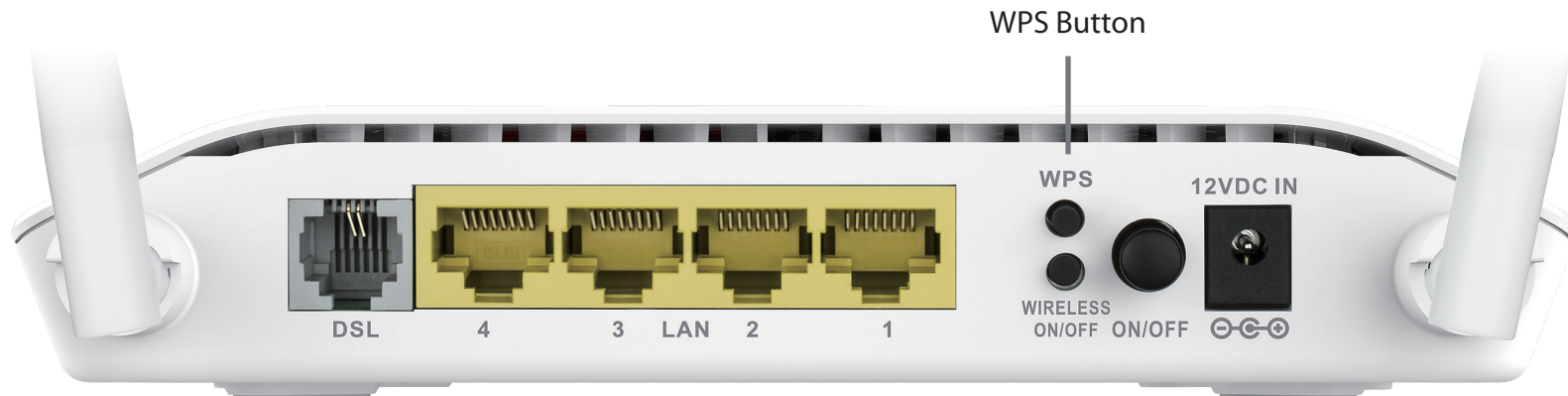
The Status tab provides online help for the DSL-2745.

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-2745 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-2745 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® 10

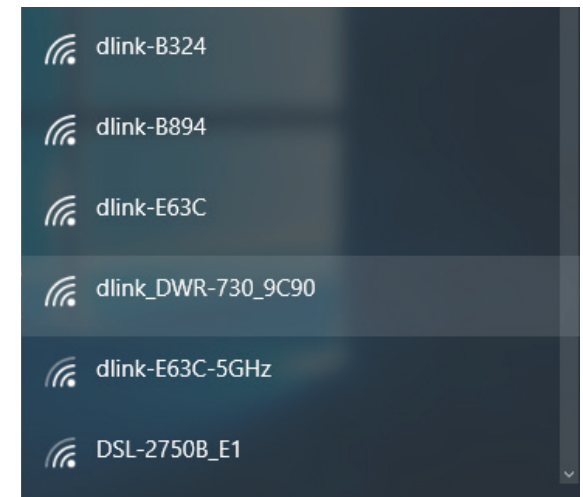
When connecting to the DSL-2745 wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key), refer to the product label for the default Wi-Fi network SSID and password or enter the Wi-Fi credentials set during the product configuration.

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



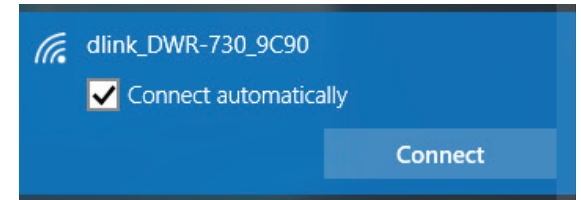
Wireless Icon

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

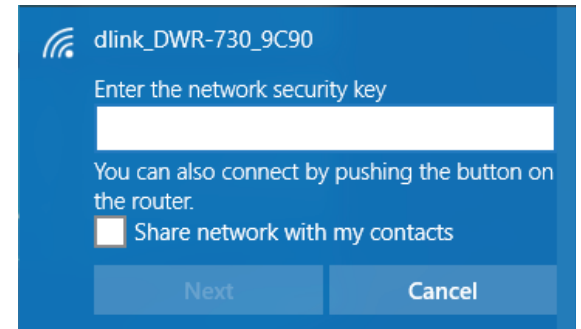


To connect to the SSID, click **Connect**.

To automatically connect with the router when your device next detects the SSID, click the **Connect Automatically** check box.



You will then be prompted to enter the Wi-Fi password (network security key) for the wireless network. Enter the password into the box and click **Next** to connect to the network. Your computer will now automatically connect to this wireless network when it is detected.



Windows® 8

WPA/WPA2

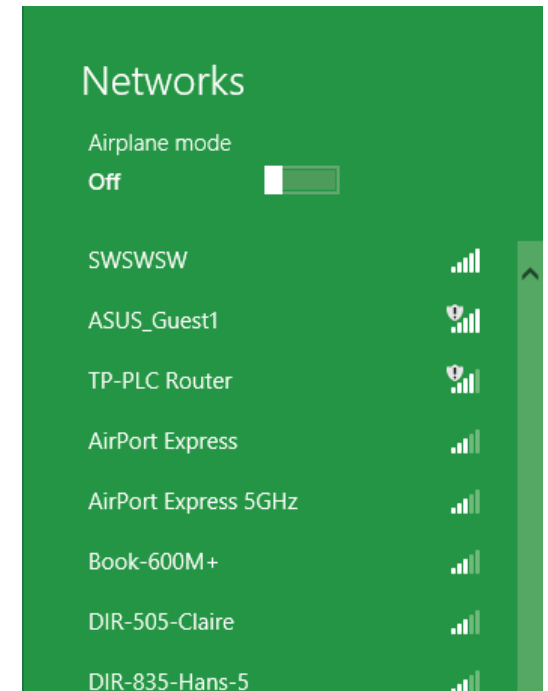
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

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



Wireless Icon

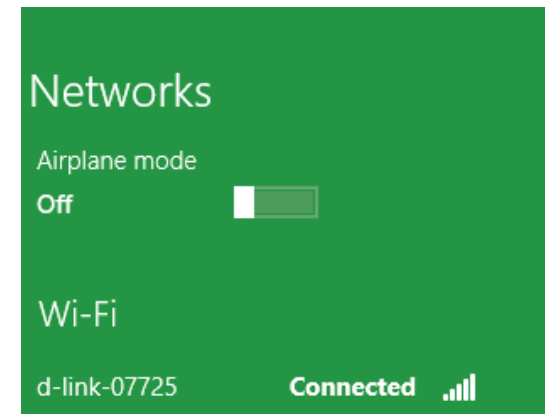
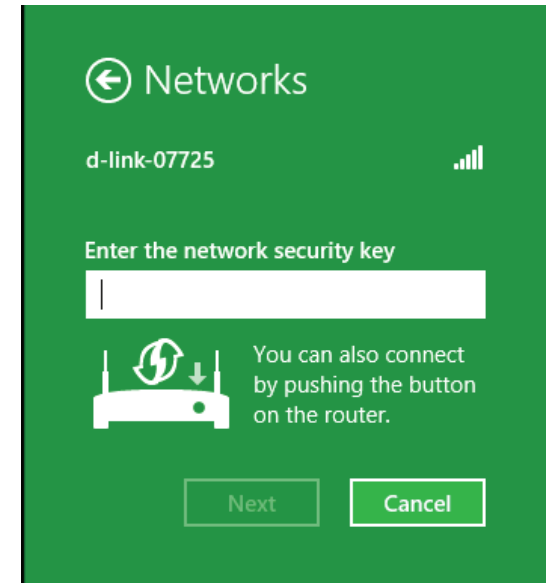
Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.



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.

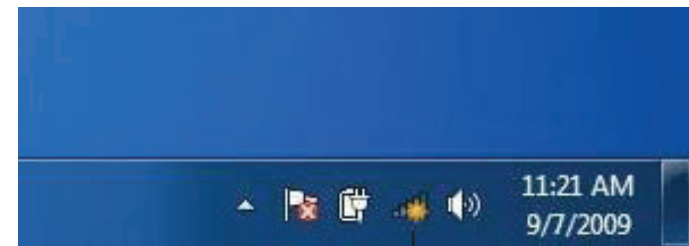


Windows® 7

WPA/WPA2

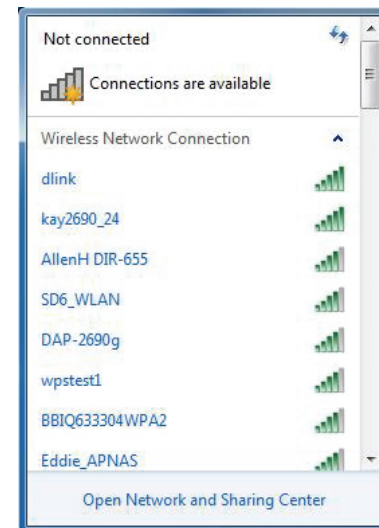
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

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.

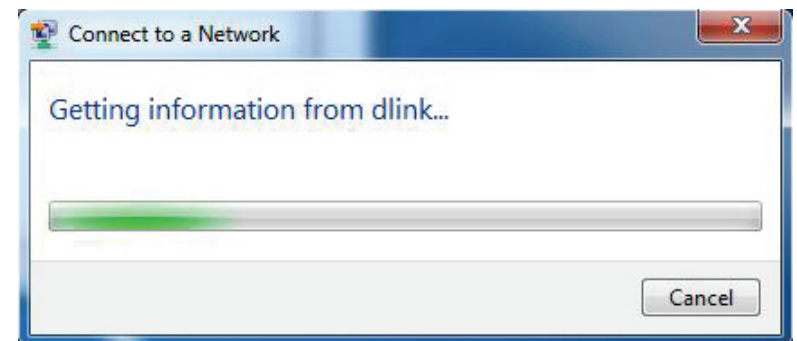


3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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.

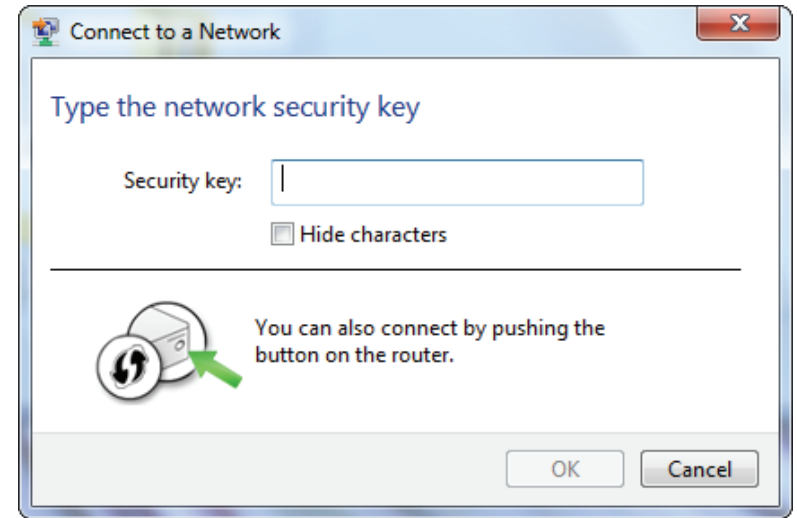


4. The following window appears while your computer tries to connect to the router.



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.

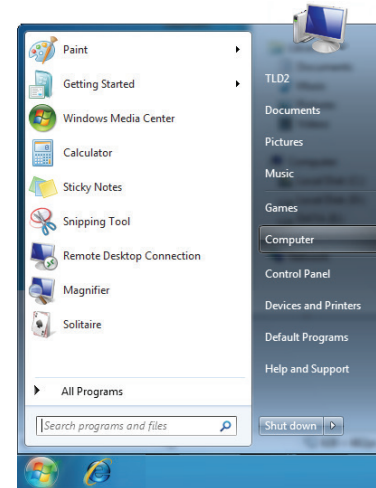
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



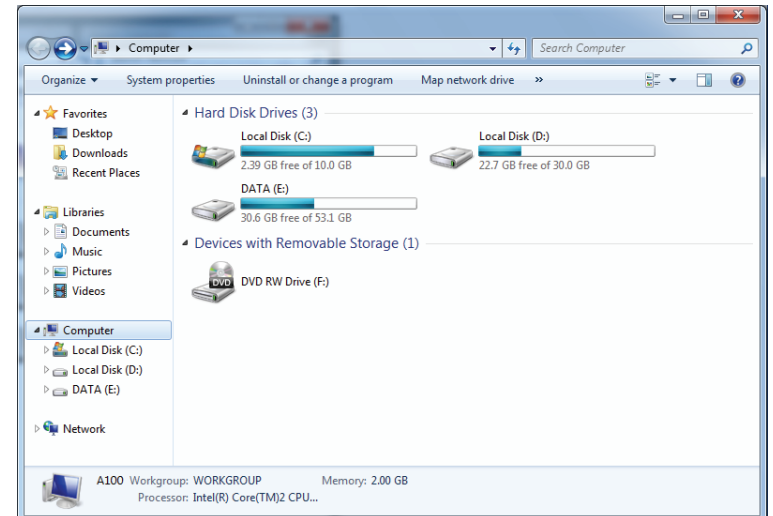
WPS

The WPS feature of the DSL-2745 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

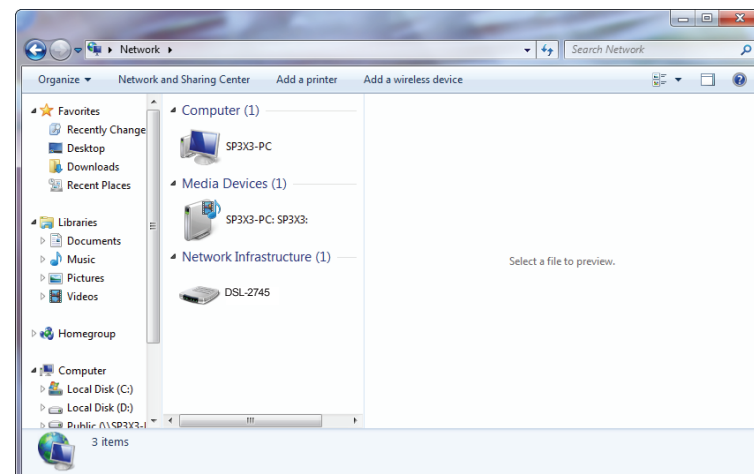
1. Click the **Start** button and select **Computer** from the Start menu.



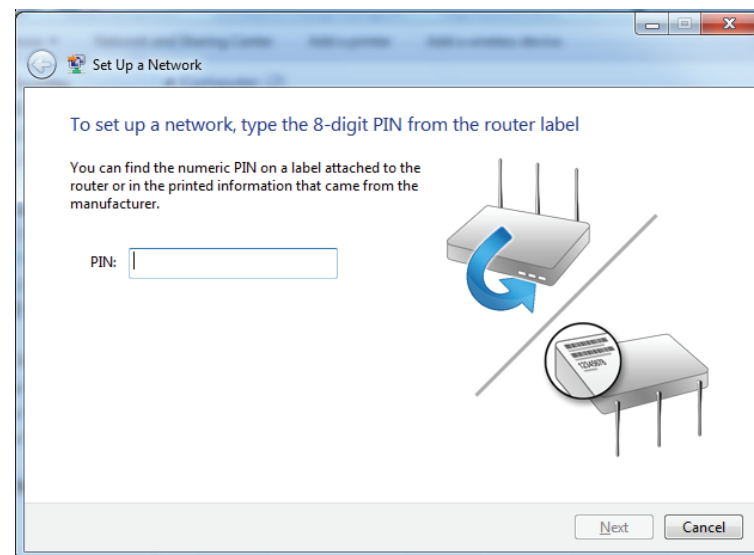
2. Click **Network** on the left side.



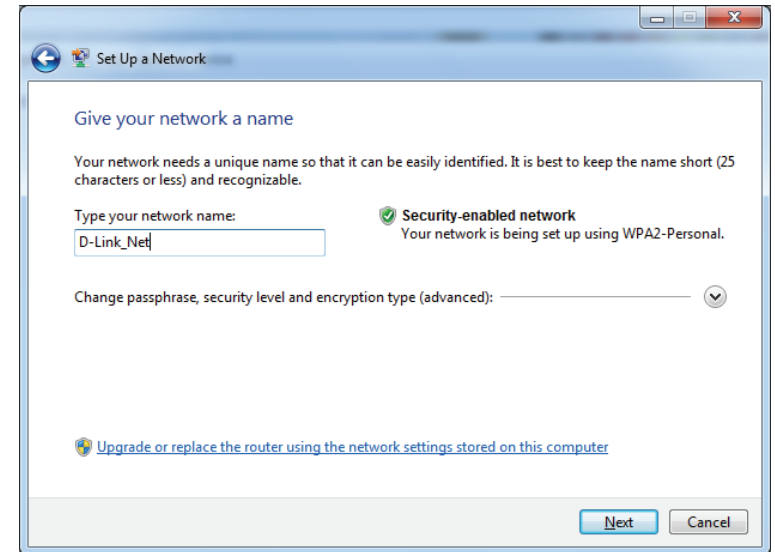
3. Double-click the DSL-2745.




4. Input the WPS PIN number (on the router label) in the **Setup > Wireless Setup** menu in the Router's Web UI) and click **Next**.

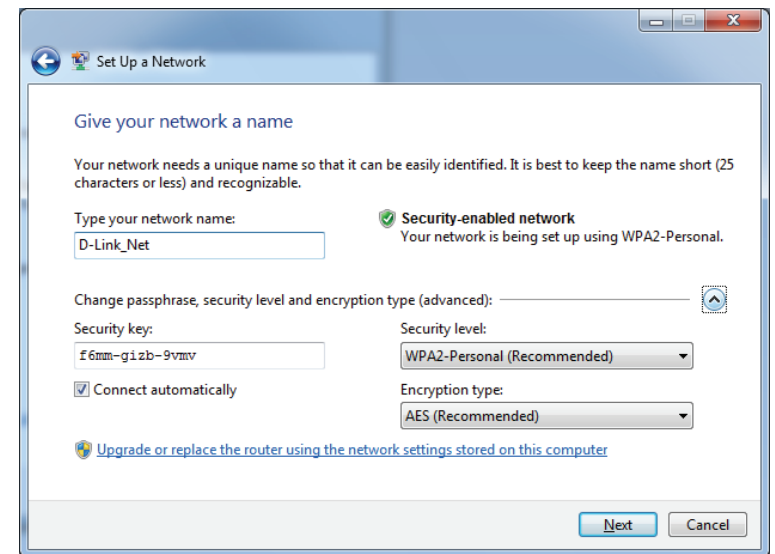


5. Type a name to identify the network.



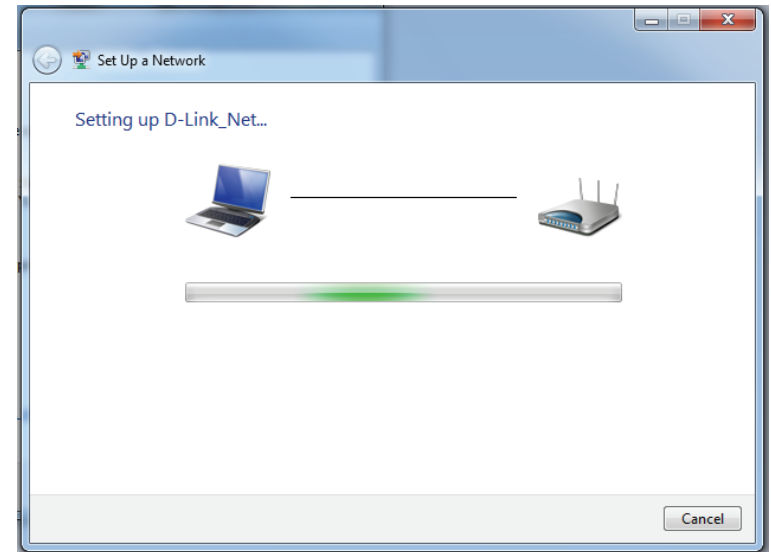
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



7. The following window appears while the Router is being configured.

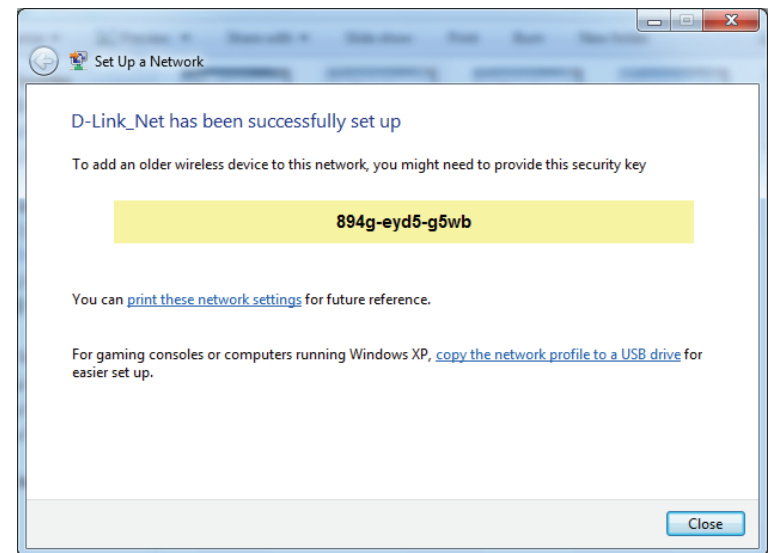
Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been set up successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click **Close** to complete WPS setup.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-2745. 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® 8 and higher
 - Mozilla Firefox 20 and higher
 - Google™ Chrome 25 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 you 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 USB 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 USB adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP address

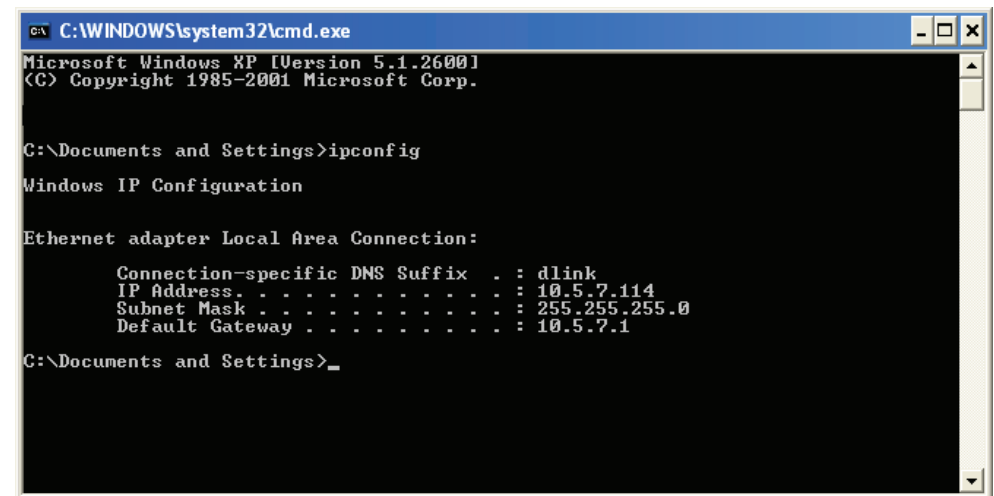
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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]
(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

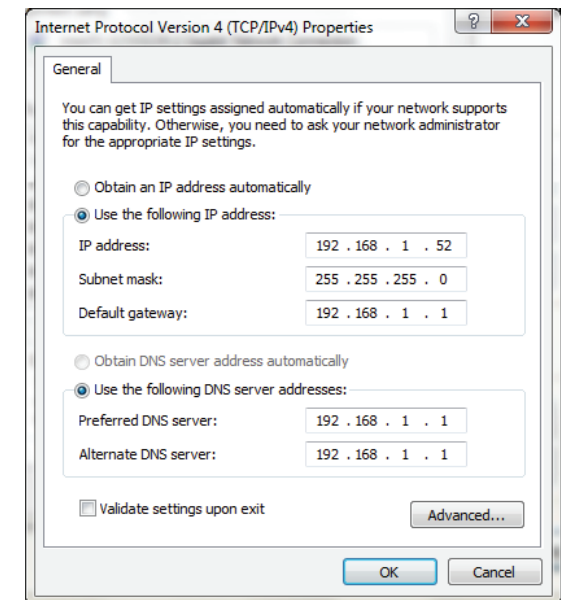
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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

- RJ-11 ADSL port
- 4 RJ-45 10/100BASE-TX Ethernet ports with auto MDI/MDIX
- Wireless Interface (2.4 GHz): IEEE 802.11n/g/b

Operating Voltage

- Input: 100~240 V AC ($\pm 20\%$), 50/60 Hz
- Output: 12 V DC, .5 A

Temperature

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

Humidity

- Operating: 0% - 90% non-condensing
- Non-Operating: 5% - 95% non-condensing

ADSL Standards

- Multi-mode
- Full-rate 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
- ITU-T G.994.1 (G.hs)

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

- Dual 2x2 built-in MIMO antennas

Wireless Security

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

Certifications

- CE
- FCC
- LVD

Dimensions & Weight

- 68 x 42 x 51 mm (2.68 x 1.65 x 2.00 inches)
- 113.4 grams (4 ounces)

Regulatory Statements

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Non-modifications Statement:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter except in accordance with FCC multi-transmitter product procedures. For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

Note

The country code selection is for non-USA models only and is not available to all USA models. Per FCC regulations, all WiFi product marketed in the USA must be fixed to USA operational channels only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

European Union:

Notice of Wireless Radio LAN Usage in The European Community (For Wireless Product Only):

- 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 is 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 EIRP 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 and Channel 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

RED 2014/53/EU			
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



5 GHz Wireless Frequency and Channel Operation in EEC Countries:

Allowable 802.11a Frequencies and Channels	Countries
5.15-5.25 GHz (Channels 36, 40, 44, 48)	Liechtenstein
5.15-5.25 GHz & 5.725-5.875 GHz (Channels 36, 40, 44, 48, 149, 153, 157, 161, 165, 169)	Austria
5.15-5.35 GHz (Channels 36, 40, 44, 48, 52, 56, 60, 64)	France
5.15-5.35 & 5.47-5.725 GHz (Channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140)	Denmark, Germany, Iceland, Finland, Netherlands, Norway, Poland, Sweden, Slovenia, Luxembourg, U.K., Ireland, Slovak, Switzerland, Hungary, Italy
5.15-5.35 GHz & 5.725-5.875 GHz (Channels 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165, 169)	Czech Republic

European Community Declaration of Conformity:

Česky [Czech]	D-Link Corporation tímto prohlašuje, že je tento produkt v souladu se směrnicí 2014/53/EU. Kompletní text prohlášení o shodě EU lze stáhnout z webové stránky produktu na adrese www.dlink.com .
Dansk [Danish]	D-Link Corporation erklærer herved, at dette produkt er i overensstemmelse med direktiv 2014/53/EU . Den fulde tekst af EU -konformitetserklæringen kan downloades fra produktsiden i www.dlink.com .
Deutsch [German]	Hiermit erklärt die D-Link Corporation, dass dieses Produkt der Richtlinie 2014/53/EU entspricht. Der vollständige Text der Konformitätserklärung der Europäischen Gemeinschaft steht Ihnen zum Herunterladen von der Produktseite unter www.dlink.com zur Verfügung.
Eesti [Estonian]	Käesolevaga kinnitab D-Link Corporation, et see toode on kooskõlas direktiiviga 2014/53/EL. Euroopa Liidu vastavusdeklaratsiooni täisteksti saab alla laadida toote lehelt www.dlink.com .
English	Hereby, D-Link Corporation, declares that this product is in compliance with Directive 2014/53/ EU. The full text of the EU declaration of conformity is available for download from the product page at www.dlink.com .
Español [Spanish]	Por la presente, D-Link Corporation declara que este producto cumple con la Directiva 2014/53/UE . El texto completo de la declaración de conformidad de la UE está disponible y se puede descargar desde la página del producto en www.dlink.com .
Ελληνική [Greek]	Με την παρούσα, η D-Link Corporation δηλώνει ότι αυτό το προϊόν συμμορφώνεται με την Οδηγία 2014/53/ΕΕ. Το πλήρες κείμενο της δήλωσης συμμόρφωσης ΕΕ είναι διαθέσιμο για λήψη από τη σελίδα του προϊόντος στην τοποθεσία www.dlink.com .
Français [French]	Par les présentes, D-Link Corporation déclare que ce produit est conforme à la directive 2014/53/ UE. Le texte complet de la déclaration de conformité de l'UE est disponible au téléchargement sur la page des produits à www.dlink.com .
Italiano [Italian]	Con la presente, D-Link Corporation dichiara che questo prodotto è conforme alla Direttiva 2014/53/UE. Il testo completo della dichiarazione di conformità UE è disponibile per il download sulla pagina del prodotto all'indirizzo www.dlink.com .
Latviski [Latvian]	Ar šo D-Link Corporation paziņo, ka šis izstrādājums atbilst Direktīvā 2014/53/ES noteiktajām prasībām. Pilnu ES atbilstības deklarācijas tekstu var lejupielādēt izstrādājuma lapā www.dlink.com .
Lietuvių [Lithuanian]	Šiuo dokumentu „D-Link Corporation“ patvirtina, kad šis gaminys atitinka Direktyvos 2014/53/ES nuostatas. Visą ES atitikties deklaracijos tekstą galima atsisiųsti įėjus į gaminio puslapį www.dlink.com .
Nederlands [Dutch]	Hierbij verklaart D-Link Corporation dat dit product voldoet aan Richtlijn 2014/53/EU. De volledige tekst van de EU conformiteitsverklaring kan gedownload worden van de productpagina op www.dlink.com .

Malti [Maltese]	B'dan, D-Link Corporation, tiddikjara li dan il-prodott huwa konformi mad-Direttiva 2014/53/UE. It-test sħiħ tad-dikjarazzjoni ta' konformità tal-UE huwa disponibbli biex jitniżżel mill-paġna talprodottfuq www.dlink.com .
Magyar [Hungarian]	A D-Link Corporation ezennel kijelenti, hogy a termék megfelel a 2014/53/EU sz. Rendeletnek. Az EU megfeleléségi nyilatkozat teljes szövege letölthető a termék weboldaláról a www.dlink.com címen.
Polski [Polish]	Spółka D-Link niniejszym oświadcza, że ten produkt spełnia wymagania określone w Dyrektywie 2014/53/UE. Pełną treść deklaracji zgodności UE można pobrać ze strony produktu pod adresem www.dlink.com .
Português [Portuguese]	Por este meio, a D-Link Corporation declara que este produto está em conformidade com a Diretiva 2014/53/UE. O texto completo da declaração de conformidade da UE está disponível para descarregar a partir da página do produto em www.dlink.com .
Slovensko[Slovenian]	Podjetje D-Link Corporation s tem izjavlja, da je ta izdelek skladen z direktivo 2014/53/EU. Celotno besedilo izjave o skladnosti EU je na voljo za prenos na strani izdelka na www.dlink.com .
Slovensky [Slovak]	Spoločnosť D-Link Corporation týmto vyhlasuje, že tento výrobok je v súlade so smernicou 2014/53/EÚ. Úplný text vyhlásenia EÚ o zhode je k dispozícii na prevzatie na stránke výrobku na adrese: www.dlink.com .
Suomi [Finnish]	Täten D-Link Corporation ilmoittaa, että tämä tuote on direktiivin 2014/53/EU vaatimusten mukainen. EU -vaatimustenmukaisuusilmoituksen koko teksti on ladattavissa tuotesivulta osoitteesta www.dlink.com .
Svenska[Swedish]	D-Link Corporation försäkrar härmed att denna produkt överensstämmer med direktiv 2014/53/EU. Hela texten i EU-försäkran om överensstämmelse kan hämtas från produktsidan på www.dlink.com .
Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara sé í samræmi við tilskipun 2014/53/ESB. Heildartexta Evróputilskipunarinnar er hægt að sækja á vörusíðunni á www.dlink.com .
Norsk [Norwegian]	D-Link Corporation erklærer herved at dette produktet er i samsvar med direktiv 2014/53/EU . Den fullstendige teksten i EU-samsvarserklæringen er tilgjengelig for nedlasting fra produktsiden på www.dlink.com .

Warning Statement:

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

Disposing of and Recycling Your Product

ENGLISH

EN



This symbol on the product or packaging means that according to local laws and regulations this product should be not be disposed of in 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

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**

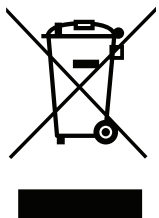
Tento symbol na výrobku nebo jeho obalu znamená, že podle místně platných předpisů se výrobek nesmí vyhazovat do komunálního odpadu, ale odeslat k recyklaci. Až výrobek doslouží, odnese jej prosím na sběrné místo určené místními úřady k tomuto účelu. Některá sběrná místa přijímají výrobky zdarma. Recyklací 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**

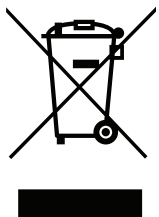
Ez a szimbólum a terméken vagy a csomagoláson azt jelenti, hogy a helyi törvényeknek és szabályoknak megfelelően ez a termék nem semmisíthető meg a háztartási hulladékkal együtt, hanem újrahasznosításra kell küldeni. Kérjük, hogy a termék élettartamának elteltét követően vigye azt a helyi hatóság által 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 elköteleztük magunkat 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**

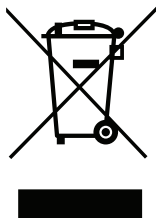
Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepterer 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**

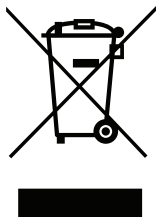
Dette symbol på produktet eller emballagen betyder, at dette produkt i henhold til lokale love og regler ikke må bortskaffes som husholdningsaffald, mens skal sendes til genbrug. Indlever produktet til et indsamlingssted som angivet af de lokale myndigheder, når det er nået til slutningen af dets levetid. 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.