



**User Manual**

# Wireless AC750 Dual-Band VDSL/ADSL 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
1.10	July 20, 2018	• Revision for Firmware 1.10

## 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 © 2018 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: 5.2 watts

Switched Off: 0.2 watts

# Table of Contents

<b>Product Overview</b> .....	<b>1</b>	Wireless Basic .....	47
Package Contents.....	1	Wireless Security .....	48
System Requirements .....	2	Local Network .....	54
Introduction .....	3	Local IPv6 Network.....	58
Features.....	4	Time and Date.....	60
Hardware Overview .....	5	Logout .....	61
LEDs .....	5	Advanced .....	62
Back Panel .....	6	2.4G Advanced Wireless .....	63
Side .....	7	Advanced Settings .....	64
<b>Installation</b> .....	<b>8</b>	MAC Filtering.....	67
Before you Begin.....	8	Security Settings .....	68
Wireless Installation Considerations.....	9	WPS Settings .....	69
Hardware Setup .....	10	5G Advanced Wireless.....	70
Device Configuration .....	13	Advanced Settings .....	71
Setup Wizard .....	14	MAC Filtering.....	74
<b>Manual Configuration</b> .....	<b>22</b>	Security Settings .....	75
Web UI Table of Contents .....	23	WPS Settings .....	76
Setup.....	24	ALG.....	77
Wizard .....	25	Port Forwarding .....	78
Internet Setup.....	26	Port Trigger .....	79
PTM/VDSL.....	27	DMZ .....	80
ATM/ADSL.....	29	SAMBA .....	81
2.4G Wireless .....	37	3G/4G Configuration .....	82
Wireless Basic .....	38	Parental Control .....	83
Wireless Security .....	39	Website Filter.....	84
5G Wireless .....	46	HTTP Content Filter.....	85
		MAC Filter .....	86

QoS.....	87	ATMF5 .....	118
Anti-Attack Settings.....	90	System Log.....	119
DNS .....	91	Logout .....	120
Dynamic DNS .....	92	Status .....	121
Network Tools .....	93	Device Info .....	122
IGMP Proxy .....	94	Wireless Clients.....	123
IGMP Snooping.....	95	DHCP Clients .....	124
UPnP .....	96	Logs .....	125
DSL.....	97	Statistics .....	126
Printer.....	98	Route Info .....	127
Routing.....	99	Logout .....	128
Static Route .....	100	Help .....	129
IPV6 Static Route .....	101	<b>Connect a USB Storage Device .....</b>	<b>130</b>
FTPD .....	102	Configure USB Storage.....	130
FTPD Setting.....	103	Connecting from a Windows Based PC .....	131
FTPD Account.....	104	Connecting from a Mac.....	136
Budget Quota.....	105	<b>Connect a Wireless Client to Your Router.....</b>	<b>140</b>
Logout .....	106	WPS Button.....	140
Management.....	107	Windows® 10.....	141
Firmware Update .....	108	Windows® 8.....	143
Access Controls.....	109	WPA/WPA2 .....	143
Account Password .....	110	Windows® 7.....	145
Local Access Control .....	111	WPA/WPA2 .....	145
Remote Access Control.....	112	Windows Vista®.....	148
IP Address .....	113	WPA/WPA2 .....	149
Diagnostics .....	114	<b>Troubleshooting .....</b>	<b>151</b>
DSL Test .....	115	<b>Wireless Basics .....</b>	<b>155</b>
Traceroute.....	116		
Ping .....	117		

What is Wireless?.....	156
Wireless Modes.....	159
<b>Networking Basics .....</b>	<b>160</b>
Check your IP address.....	160
Statically Assign an IP address .....	161
Wireless Security .....	162
What is WPA? .....	162
<b>Technical Specifications .....</b>	<b>163</b>
<b>Regulatory Information .....</b>	<b>164</b>

# Package Contents



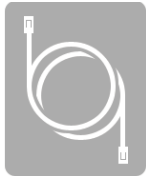
DSL-3682 Wireless AC750 Dual-Band VDSL/ADSL Modem Router



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

<b>Network Requirements</b>	<ul style="list-style-type: none"><li>• An Ethernet-based Cable or DSL modem</li><li>• IEEE 802.11ac, 802.11n, 802.11g or 802.11b wireless clients</li><li>• 10/100 Ethernet</li></ul>
<b>Web-based Configuration Utility Requirements</b>	<p><b>Computer with the following:</b></p> <ul style="list-style-type: none"><li>• Windows®, Macintosh, or Linux-based operating system</li><li>• An installed Ethernet adapter</li></ul> <p><b>Browser Requirements:</b></p> <ul style="list-style-type: none"><li>• Internet Explorer 10 or higher</li><li>• Firefox 28 or higher</li><li>• Safari 6.0 or higher</li><li>• Chrome 28 or higher</li></ul>

# Introduction

The DSL-3682 Wireless AC750 Dual-Band VDSL/ADSL Modem Router is an attractive, high-performance router that makes it easy to share your broadband Internet connection with all your devices. Equipped with a high-speed VDSL2/ADSL2+ modem, the DSL-3682 connects your home or office to the Internet at speeds of up to 100 Mbps VDSL2 or 24 Mbps ADSL2+<sup>1</sup>. To get the most out of this speed, the DSL-3682 has the latest 802.11ac wireless networking technology built-in, offering a combined data throughput rate up to 750 Mbps<sup>2</sup> (433 Mbps 5 GHz AC and 300 Mbps 2.4 GHz N) delivered through three external antennas. These external antennas increase your wireless coverage so you can avoid dead spots and get a reliable connection in more places throughout your home.

With a high-speed WAN connection, high-speed wireless LAN, and four Fast Ethernet 10/100 switch ports for your wired devices, the DSL-3682 Wireless AC750 Dual-Band VDSL/ADSL Modem Router provides all the functions that a home or small office needs to establish a secure and high-speed link to the outside world, allowing you to enjoy fast file transfers, seamless web surfing, and smooth online gaming.

<sup>1</sup> Maximum wireless signal rate derived from IEEE Standard 802.11ac, 802.11n, 802.11a, 802.11g, and 802.11b 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.

<sup>2</sup> Maximum VDSL transmission rate derived from ITU-T G.993.2, 17a profile. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, ISP service rating, and distance from telco equipment lower actual data throughput rate.



# Features

- **High Speed DSL Connection** - Very high data transfer rates of up to 100 Mbps downstream<sup>1</sup> are possible with the DSL-3682 modem router.
- **Faster Wireless Networking** - The DSL-3682 provides wireless connection of up to 750 Mbps<sup>2</sup> for other 802.11ac wireless clients. This capability allows users to participate in real-time activities online, such as video and audio streaming or online gaming.
- **Compatible with 802.11n/g/b Devices** - The DSL-3682 is fully backwards compatible with IEEE 802.11n, IEEE 802.11a, IEEE 802.11g, and IEEE 802.11b standards, so it can connect with your existing wireless equipment.
- **Advanced Firewall Features** - The web-based user interface displays a number of advanced network management features.
- **Content Filtering** - Easily applied content filtering based on URL, HTTP content, or MAC address.
- **Full Network Management** - The DSL-3682 incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via a Telnet connection.
- **User-friendly Setup Wizard** - Through its easy-to-use web-based user interface, the DSL-3682 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.
- **IPv6 Ready** - Fully compliant with IPv6. The DSL-3682 supports a variety of IPv6 connection standards preparing you for the day when your ISP implements IPv6.

<sup>1</sup> Maximum wireless signal rate derived from IEEE Standard 802.11ac, 802.11n, 802.11a, 802.11g, and 802.11b 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.

<sup>2</sup> Maximum VDSL transmission rate derived from ITU-T G.993.2, 17a profile. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, ISP service rating, and distance from telco equipment lower actual data throughput rate.

# Hardware Overview

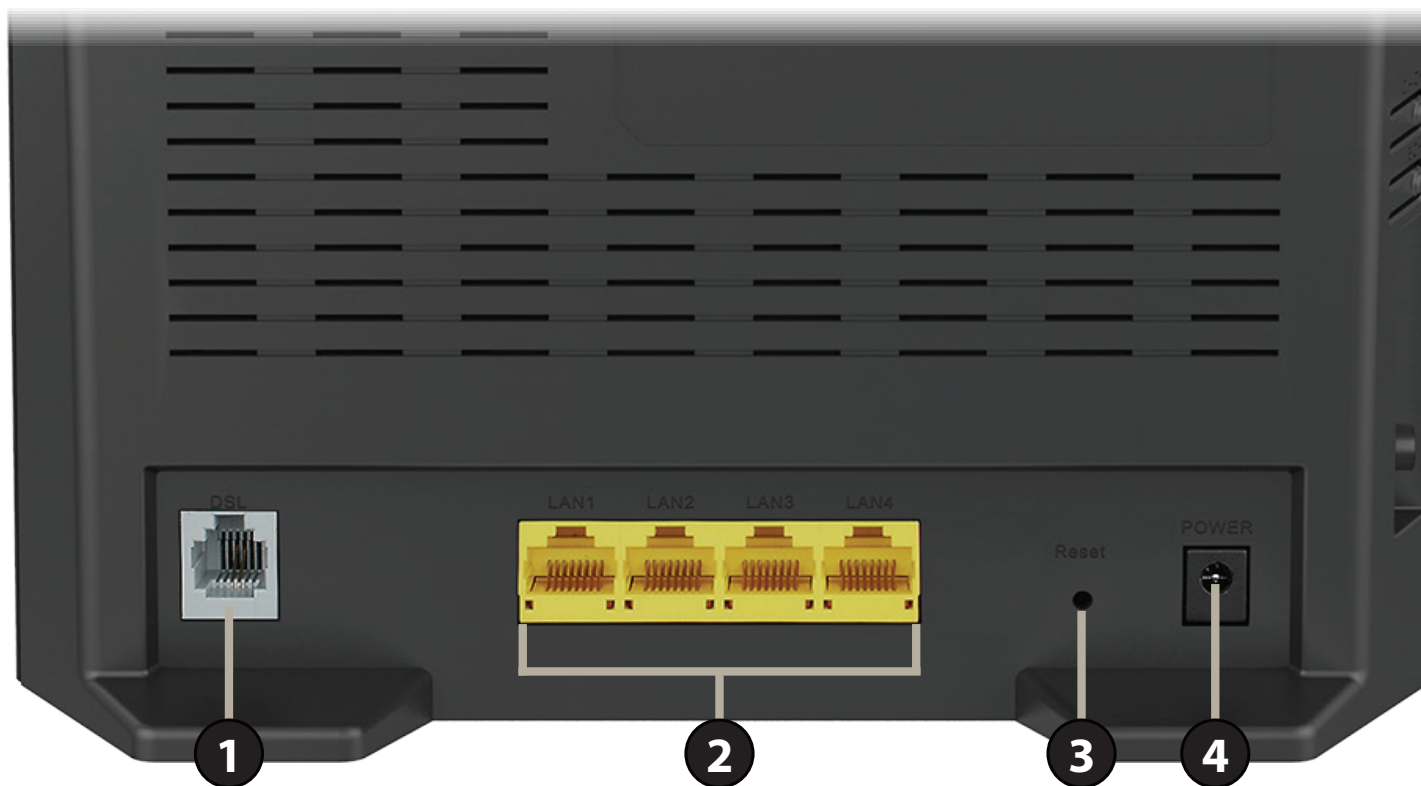
## LEDs



LED	Color	Description
<b>Power</b>	Green	The device is powered on and functioning properly.
	Red	The device is booting, encountered an error, or is in recovery mode.
	Off	The device is powered off or not receiving power.
<b>DSL</b>	Green	The device is connected to a VDSL/ADSL enabled telephone line.
	Red	The device has failed to establish a connection to the phone network.
	Off	No connection detected.
<b>Internet</b>	Green	The device is connected to a broadband service.
	Red	The device failed to connect to the Internet.
<b>LAN4-1</b>	Green	A device is connected on this port. The light blinks during data transmission.
<b>2.4GHz</b>	Green	The 2.4 GHz Wi-Fi network is ready. The light blinks during data transmission.
<b>5Ghz</b>	Green	The 5 GHz Wi-Fi network is ready. The light blinks during data transmission.
<b>WPS</b>	Blue	The light blinks during the WPS process.
<b>USB1</b>	Green	A USB device is connected.

# Hardware Overview

## Back Panel



1	<b>DSL Port</b>	Connects to a DSL-enabled telephone line.
2	<b>LAN Ports (1-4)</b>	Connects to Ethernet devices such as computers, switches, storage (NAS) devices, and game consoles.
3	<b>Reset Button</b>	To reset the device to its factory default settings, press and hold the reset button for five seconds.
4	<b>Power Connector</b>	Connector for the supplied power adapter.

# Hardware Overview

## Side



<b>1</b>	<b>2.4GHz</b>	Press for 5 seconds to start the WPS process for the 2.4 GHz network and automatically create a secure connection to a WPS client.
<b>2</b>	<b>5GHz</b>	Press for 5 seconds to start the WPS process for the 5 GHz network and automatically create a secure connection to a WPS client.
<b>3</b>	<b>USB1</b>	Connect a USB storage device to this port to share media to your network.
<b>4</b>	<b>Power Button</b>	Press to power the DSL-3682 on or off.

# Installation

This installation section is written for users who are setting up their home Internet service with the DSL-3682 Wireless AC750 Dual-Band VDSL/ADSL 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 (ISP) 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-3682 from a single device and verifying that it is connected to the Internet before connecting additional devices.
- Placement of the router is very important. Do not place the router in an enclosed area such as a closet, cabinet, attic, or garage.
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoET, BroadJump, or EnterNet 300 from your computer or you will not be able to connect to the Internet.

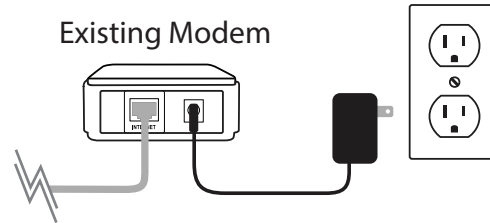
# Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 1 to 30 meters (3 to 90 feet). 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 0.5 meters (1.5 feet) thick, at a 45-degree angle appears to be almost 1 meter (3 feet) thick. At a 2-degree angle it looks over 14 meters (42 feet) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away at least 1 to 2 meters (3 to 6 feet) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4 GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone is not in use.

# Hardware Setup

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

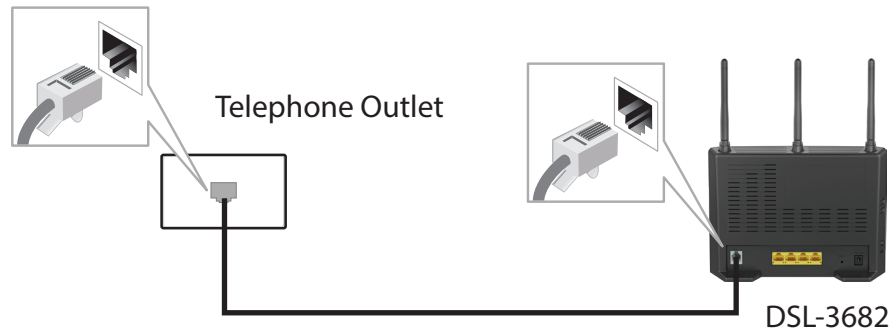


- 2 Position your DSL-3682 close to a telephone outlet which provides DSL service. Place the router in an open area of your intended work area for better wireless coverage.

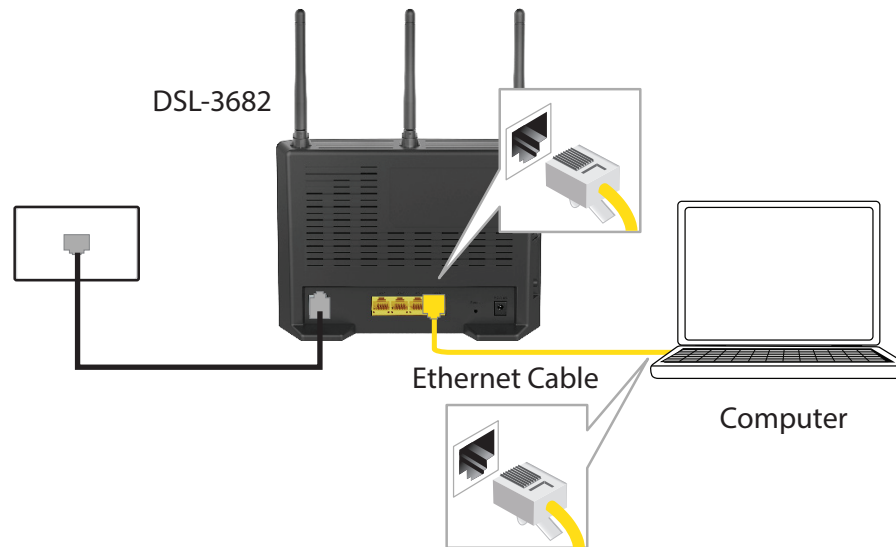


DSL-3682

- 3 Connect the included ADSL telephone cable from a telephone outlet to the DSL port on your DSL-3682.

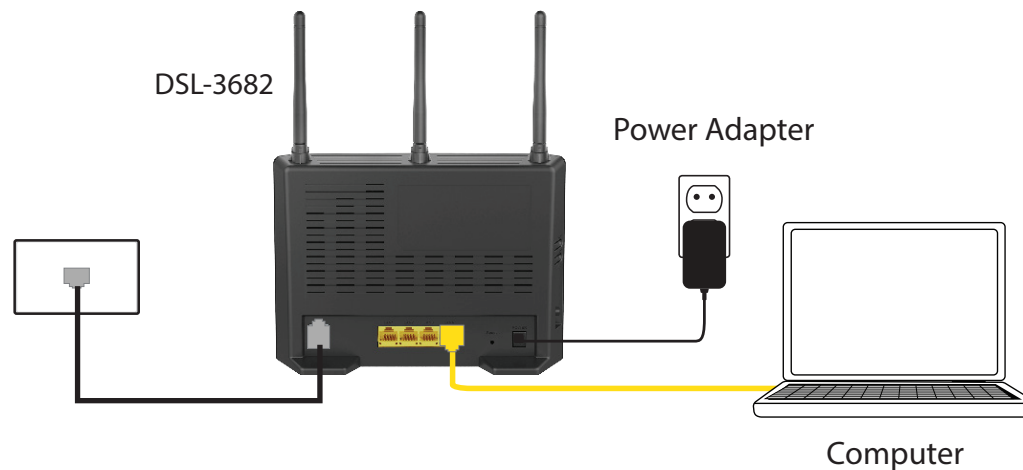


- 4 If you wish to use a wired connection, connect the Ethernet cable from a LAN port of the DSL-3682 to the Ethernet port on your computer.



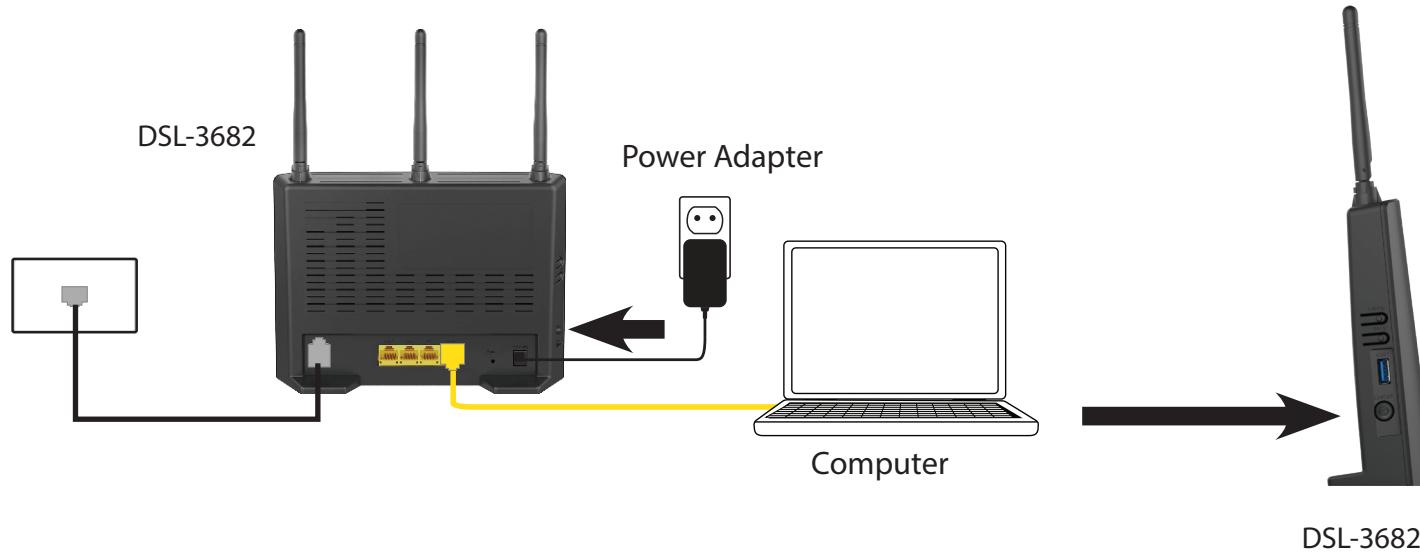
- 5 Plug the power adapter into your DSL-3682 and connect to an available power outlet or surge protector.

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

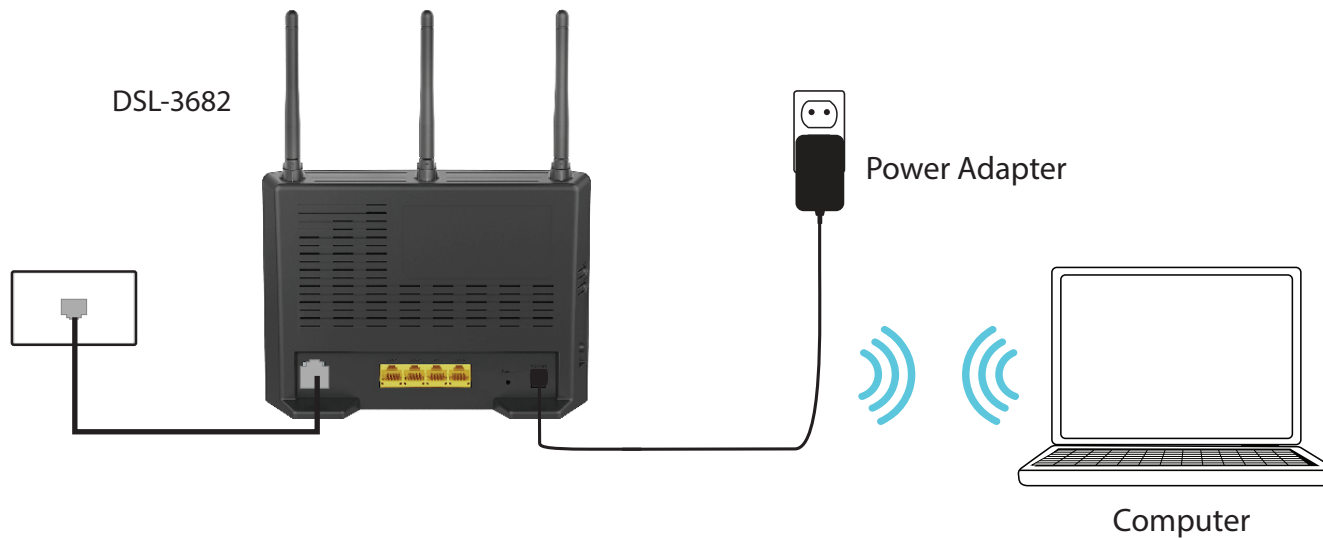




- 6** Press the power button and verify that the power LED is lit. Allow 1 minute for the router to boot up.



- 7** If connecting to the DSL-3682 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 back of your DSL-3682.



# Device Configuration

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

- **Setup Wizard** - This wizard will launch when you log into the DSL-3682 for the first time. Refer to **Setup Wizard** on page **14**.
- **Manual Setup** - To manually configure your DSL-3682, refer to **Manual Configuration** on page **22**.

# Setup Wizard

This section guides you through how to configure D-Link DSL-3682 for the first time using the web-based configuration utility's **Setup Wizard**.

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

You are greeted with the **Setup Wizard**. Click **Next** to begin.

If you want to configure the DSL-3682 manually without running the wizard, click **Cancel** and refer to **Manual Configuration** on page 22.



**Login**

Input username and password

**Language:** English ▼

**Username:** admin

**Password:**

Remember my login info. on this computer

Login

**WELCOME TO SETUP WIZARD**

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

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

Next Cancel

# Wizard - Step 1 - Time and Date

## STEP 1: SET TIME AND DATE

This step allows you to edit the system time or Network Time Protocol (NTP). You can configure, update, and maintain the correct time on the system clock, and configure Daylight Saving.

### TIME SETTING

If you choose **Automatically synchronize with Internet time servers**, please configure the following fields:

**1st NTP time server :** Enter the address of the NTP server to connect to.

**2nd NTP time server :** Enter the address of a backup NTP server to connect to.

### TIME CONFIGURATION

**Time Zone:** Select the time zone you are in from the dropdown menu.

If you choose **Enable Daylight Saving**, please configure the following fields:

**Daylight Saving Start:** Select the start date of daylight saving.

**Daylight Saving End:** Select the end date of daylight saving.

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

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

### TIME SETTING

**Automatically synchronize with Internet time servers**

**1st NTP time server :**

**2nd NTP time server :**

### Time Configuration:

**Time Zone:**  ▼

**Enable Daylight Saving**

**Daylight Saving Start:**  Year  Mon  Day

Hour  Min  Sec

**Daylight Saving End:**  Year  Mon  Day

Hour  Min  Sec

# Wizard - Step 2 - Setup Internet Connection

## STEP 2: SETUP INTERNET CONNECTION

This step of the wizard allows you to configure your Internet connection type. Choose your **Country**, **Internet Service Provider (ISP)**, and **DSL Mode**. Most of the fields will automatically populate with the correct values, simplifying configuration. If you wish to manually configure these values or cannot locate your ISP or country, select **Other**. Complete the Internet Connection Setup by selecting the protocol type and supply any additional information.

**Country:** Select your **Country** from the drop down menu.

**Internet Service Provider:** Select your **Internet Service Provider (ISP)** from the drop down menu.

**DSL Mode:** Select either **ADSL** or **VDSL**.

**Protocol:** Select the **Protocol** used by your ISP: **PPPoE**, **Dynamic IP**, **Static IP**, or **Bridge**. If you select **ADSL** as your **DSL Mode** type, **PPPoA** and **IPoA** are also available.

If you select **ADSL** the following configuration options for all **Protocol** types:

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

**VPI:** Virtual path identifier (VPI) is the virtual path between two points in an Asynchronous Transfer Network (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.

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

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

**Country :** Other ▼

**Internet Service Provider :** Other ▼

**DSL Mode :** ADSL ▼

**Protocol :** PPPoE ▼

**Encapsulation Mode :** LLC ▼

**VPI :** 8 (0 - 255)

**VCI :** 35 (32-65535)

**Search Available PVC :** Scan

# Wizard - Step 2 - Setup Internet Connection

**Search Available PVC:** Click this button to attempt to automatically discover the Permanent Virtual Circuit your provides to connect you to the Internet.

If you select **VDSL**, or select **ADSL** with **Dynamic IP**, **Bridge**, **Static IP**, or **PPPoE Protocol** types, configure your VLAN information.

**802.1Q VLAN ID:** If your ISP uses VLANs, enter the VLAN number provided. Enter 0 to leave this feature disabled.

**Priority:** If your ISP uses VLANs, enter the VLAN priority number provided.

## DYNAMIC IP OR BRIDGE

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

## 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.

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

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

**Country :**

**Internet Service Provider :**

**DSL Mode :**

**Protocol :**

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

**Priority:**  (0 - 7)




## PPPOE/PPPOA

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

**Username:**

**Password:**

**Confirm Password:**

# Wizard (Step 2 continued)

## STATIC IP/IPOA

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

**IP Address:** Enter the IP address provided by your ISP.

**Subnet Mask:** Enter the subnet mask.

**Default Gateway:** Enter the default gateway.

**Primary DNS:** Enter the primary DNS address.

## Static IP/IPOA

You have selected Static IP or IPOA 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 :**

Back

Next

Cancel

# Wizard - Step 3 - 2.4G Wireless

## STEP 3: CONFIGURE 2.4G WIRELESS NETWORK

This step of the wizard allows you to configure your 2.4 GHz wireless network settings.

**Enable Your Wireless Network:** Check this box to enable the 2.4 GHz wireless network.

**Wireless Network Name (SSID):** Create a wireless network name for your network.

**Visibility Status:** **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.

**Security Level:** Select a wireless security encryption option. The options, from least secure to most secure, are **None**, **WEP**, **WPA/WPA2-PSK**, and **WPA2-PSK**. Using **WPA2-PSK** security is recommended. Using **WEP** security is not recommended, as it only offers a trivial amount of protection for your wireless data and network. WEP is not supported by faster wireless standards. Using **None** is not recommended because any wireless client will be able to access your network, be able to use your Internet connection, and leaves you open to security threats.

**Key:** Create a Wi-Fi password (between 8-63 characters). Your wireless clients need this key to join your wireless network. The longer your password, the more secure your data. For improved security, you should change your wireless password every three to six months.

Click **Next** to continue.

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

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

Enable Your Wireless Network :

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

Wireless Network Name (SSID) :

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

Visibility Status :  Visible  Invisible

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

**None** **Security Level** **Best**

None  WEP  WPA/WPA2-PSK  WPA2-PSK

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

Now, please enter your wireless security key :

WPA/WPA2-PSK Pre-Shared Key :

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

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

Back

Next

Cancel



# Wizard - Step 3 - 5G Wireless

## STEP 3: CONFIGURE 5G WIRELESS NETWORK

This step of the wizard allows you to configure your 5 GHz wireless network settings.

**Enable Your Wireless Network:** Check this box to enable the 5 GHz wireless network.

**Wireless Network Name (SSID):** Create a wireless network name for your network.

**Visibility Status:** **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.

**Security Level:** Select a wireless security encryption option. The options, from least secure to most secure, are **None**, **WEP**, **WPA/WPA2-PSK**, and **WPA2-PSK**. Using **WPA2-PSK** security is recommended. Using **WEP** security is not recommended, as it only offers a trivial amount of protection for your wireless data and network. WEP is not supported by faster wireless standards. Using **None** is not recommended because any wireless client will be able to access your network, be able to use your Internet connection, and leaves you open to security threats.

**Key:** Create a Wi-Fi password (between 8-63 characters). Your wireless clients need this key to join your wireless network. The longer your password, the more secure your data. For improved security, you should change your wireless password every three to six months.

Click **Next** to continue.

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

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

**Enable Your Wireless Network :**

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

**Wireless Network Name (SSID) :**

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

**Visibility Status :**  Visible  Invisible

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

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

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

Now, please enter your wireless security key :

**WPA/WPA2-PSK Pre-Shared Key :**

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

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

# Wizard - Step 4 - Save and Apply Changes

## STEP 4: SAVE AND APPLY CHANGES

You will be presented with a final summary of your configuration settings. Click **Finish** to apply your settings. Click **Back** to review or modify settings.

Congratulations, setup is complete.

## STEP 4: SAVE AND APPLY CHANGES

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

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

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

Time Settings :	1
NTP Server 1 :	ntp1.dlink.com
NTP Server 2 :	N/A
Time Zone :	CET
Daylight Saving Time :	0
VPI / VCI :	8/35
Protocol :	PPPoE
Connection Type :	LLC
802.1Q VLAN ID :	0
Priority :	0
Username :	username
Password :	*****
SSID (2.4G) :	Your_2.4G Wi-Fi_Network
Visibility Status :	Visible
Encryption :	WPA2-PSK
Pre-Shared Key :	A_Str0nG_P@ssW0rd!%!
WEP Key :	N/A
SSID (5G) :	Your_5G Wi-Fi_Network
Visibility Status (5G) :	Visible
Encryption (5G) :	WPA2-PSK
Pre-Shared Key (5G) :	A_Str0nG_P@ssW0rd!%!
WEP Key (5G) :	N/A

# Manual Configuration

This section will show you how to configure or change the default settings your D-Link DSL-3682 using 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. Enter **admin** as the username and **admin** as the password. Click **Login**.

After logging in in you are taken to the Device Info page.

A screenshot of the login page for the D-Link DSL-3682 configuration utility. The page has an orange header with the word "Login" in white. Below the header, the text "Input username and password" is displayed. There are three input fields: "Language:" with a dropdown menu showing "English", "Username:" with the text "admin", and "Password:" which is empty. Below these fields is a checkbox labeled "Remember my login info. on this computer" which is checked. At the bottom of the form is a "Login" button.

# Web UI Table of Contents

The web-based interface is divided into five horizontal tabs, with a vertical menu bar running along the left side of the page. You may click on these menus to quickly navigate to a section of this document.

Product Page: DSL-3682 Firmware Version: EU\_1.00




DSL-3682	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP	
	Wizard	2.4G Advanced Wireless	QoS	System	Device Info	Menu
	Internet Setup	5G Advanced Wireless	Anti-Attack Settings	Firmware Update	Wireless Clients	Setup
	2.4G Wireless	ALG	DNS	Access Controls	DHCP Clients	Advanced
	5G Wireless	Port Forwarding	Dynamic DNS	Diagnostics	Logs	Management
	Local Network	Port Trigger	Network Tools	System Log	Statistics	Status
	Local IPv6 Network	DMZ	Routing		Route Info	
	Time and Date	SAMBA	FTPD			
		3G/4G Configuration	Budget Quota			
		Parental Control				



To return to this Web UI Table of Contents page, simply click the D-Link logo on the top right of each page.

# Setup

The **Setup** tab provides access to configure the basic configuration settings of your DSL-3682.

Product Page: DSL-3682		Firmware Version: EU_1.00	
			
<i>DSL-3682</i> //	<b>SETUP</b>	<b>ADVANCED</b>	<b>MANAGEMENT</b>
Wizard			
Internet Setup			
2.4G Wireless			
5G Wireless			
Local Network			
Local IPv6 Network			
Time and Date			
Logout			

To return to the Web UI Table of Contents page, simply click the D-Link logo on the top right of each page.

	
<i>DSL-3682</i> //	<b>SETUP</b>
Wizard	

# Wizard

Use the Setup Wizard to quickly and easily configure the DSL-3682. 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. For more information refer to **Setup Wizard** on page 14.

## INTERNET CONNECTION WIZARD

This section allows you to configure the router's Internet connection.

**Setup Wizard:** Starts the Setup Wizard.



## INTERNET CONNECTION WIZARD

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

Setup Wizard

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

## WELCOME TO SETUP WIZARD

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

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

Next

Cancel

# Internet Setup

Users may manually configure the DSL-3682 from the **Internet Setup** option. This section is recommended for advanced users.

## DSL CONFIG

The currently defined DSL interfaces are displayed here. If you wish to create a new interface, click the **Add** button. If you wish to remove a currently configured interface, select it from the table and click the **Delete** button. If you wish to edit an interface, select it from the table and click the **Edit** button.

If you selected **Add**, select the DSL Mode:

## DSL MODE CONFIGURATION

**DSL Mode:** Select Packet Transfer Mode (PTM) if you have a VDSL connection. Select Asynchronous Transfer Mode(ATM) if you have an ADSL connection.

If you selected PTM proceed to **PTM/VDSL** on page **27**.

If you selected ATM proceed to **ATM/ADSL** on page **29**.

The screenshot shows the D-Link DSL-3682 web interface. At the top, there's a navigation bar with 'DSL-3682 //', 'SETUP', and 'ADVANCED'. Below this, 'Internet Setup' is selected, and 'INTERNET SETUP' is highlighted in orange. The main content area is titled 'INTERNET SETUP' and contains the instruction: 'Choose "Add", "Edit", or "Delete" to configure WAN interfaces.'

Below this is the 'DSL CONFIG' section, which contains a table with the following data:

	VPI/VCI	VLAN ID	ENCAP	Service Name	Protocol	State	Status	3G	Action
<input type="radio"/>	8/35	0	LLC	ADSL	PPPoE	1		1	-
<input type="radio"/>	N/A	835	LLC	VDSL	PPPoE	1		1	-

Below the table are three buttons: 'Add', 'Edit', and 'Delete'.

At the bottom, the 'DSL MODE CONFIGURATION' section is visible, showing a dropdown menu for 'DSL Mode' with 'PTM' selected and 'ATM' as an option.

## PTM/VDSL

### CONNECTION TYPE

**Protocol:** Select the connection protocol your ISP uses from the drop-down menu. The options change depending upon protocol selected. You can choose between **PPP over Ethernet(PPPoE)**, **MAC Encapsulation Routing(MER)**, or **Bridging**. The most common type of connection is PPPoE. Use MER if your provider does not provide IP routing. Use Bridging if you are connecting another router to this device.

If you selected **PPP over Ethernet(PPPoE)** or **MAC Encapsulation Routing(MER)**, configure the following options.

**WAN Service Type:** Select **Internet**, **TR069**, or **Internet\_TR069**. This option effects available Network Address Translation Settings. In most cases select Internet. Select TR069 if your ISP manages your equipment remotely.

**802.1Q VLAN ID:** Enter the 802.1Q VLAN ID if your ISP offers a High Priority Committed Information Rate (CIR). This guarantees the bandwidth required for real-time voice and video applications.

**IP Protocol:** Select the Internet Protocol version your ISP uses. The options are **IPv4**, **IPv6**, or **Both**.

If you selected **PPP over Ethernet(PPPoE)**, proceed to **PPP Username and Password** on page **32**.

If you selected **MAC Encapsulation Routing(MER)**, proceed to **Network Address Translation Settings** on page **36**.

The screenshot shows two configuration panels. The top panel, titled "DSL MODE CONFIGURATION", has a "DSL Mode" dropdown menu set to "PTM". The bottom panel, titled "CONNECTION TYPE", contains several settings: a "Protocol" dropdown menu with options "PPP over Ethernet (PPPoE)", "MAC Encapsulation Routing (MER)", and "Bridging"; a "WAN Service Type" dropdown menu set to "Internet"; an "802.1Q VLAN ID" input field with the value "0" and a note "(0 = disable, 1 - 4094)"; and an "IP Protocol" dropdown menu set to "Both".



## PTM/VDSL (continued)

If you selected **Bridging**, configure the following options:

**802.1Q VLAN ID:** Enter the 802.1Q VLAN ID if your ISP offer a High Priority Committed Information Rate (CIR). This guarantees the bandwidth required for real-time voice and video applications.

**Enable Service:** Choose to enable or disable this interface upon clicking **Apply**.

**Firewall Enable:** Choose to enable or disable the firewall.

**Service Name:** Enter a name for the service.

Click **Apply** to finish, further configuration of your networking devices may be necessary.

The image shows two screenshots of a configuration interface. The top screenshot is titled "DSL MODE CONFIGURATION" and shows a dropdown menu for "DSL Mode" set to "PTM". The bottom screenshot is titled "CONNECTION TYPE" and shows a dropdown menu for "Protocol" set to "Bridging". Below this, there is a text input field for "802.1Q VLAN ID" with the value "0" and a note "(0 = disable, 1 - 4094)". There are two checkboxes: "Enable Service" (checked) and "Firewall Enable" (checked). Below these is a text input field for "Service Name" with the value "VDSL". At the bottom right of the "CONNECTION TYPE" section are two buttons: "Apply" and "Cancel".

## ATM/ADSL

### ATM PVC CONFIGURATION

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

**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.

**Service Category:** Select the Service Category your ISP uses. The options are **UBR Without PCR**, **UBR With PCR**, **CBR**, **Non Realtime VBR**, or **Realtime VBR**.

If you selected **UBR With PCR**, **CBR**, **Non Realtime VBR**, or **Realtime VBR** configure the Peak Cell Rate:

**Peak Cell Rate:** Enter the Peak Cell Rate

If you selected **Non Realtime VBR** or **Realtime VBR** configure the the following options:

**Sustainable Cell Rate:** Enter the Sustainable Cell Rate.

**Maximum Burst Size:** Enter the Maximum Burst Size.

Proceed to **Connection Type** on page **30**.

The screenshot shows two configuration panels. The top panel, titled "DSL MODE CONFIGURATION", has a "DSL Mode" dropdown menu set to "ATM". The bottom panel, titled "ATM PVC CONFIGURATION", contains the following fields:

- VPI:** Input field with value "0" and range "(0-255)".
- VCI:** Input field with value "35" and range "(32-65535)".
- Service Category:** A dropdown menu with "CBR" selected. Other options include "UBR Without PCR", "UBR With PCR", "Non Realtime VBR", and "Realtime VBR".
- Peak Cell Rate:** Input field with value "0" and unit "(cells/s)".
- Sustainable Cell Rate:** Input field with value "0" and unit "(cells/s)".
- Maximum Burst Size:** Input field with value "0" and unit "(cells)".

## Connection Type

### CONNECTION TYPE

**Protocol:** Select the connection protocol your ISP uses from the drop-down menu. The options change depending upon protocol selected. You can choose between **PPP over Ethernet(PPPoE)**, **MAC Encapsulation Routing(MER)**, **IP over ATM (IPoA)**, or **Bridging**. The most common type of connection is PPPoE. Use MER if your provider does not provide IP routing. Use Bridging if you are connecting another router to this device.

If you selected **PPP over Ethernet(PPPoE)**, **PPP over ATM(PPPoA)**, **IP over ATM (IPoA)**, or **MAC Encapsulation Routing(MER)**, configure the following options.

**WAN Service Type:** Select **Internet**, **TR069**, or **Internet\_TR069**. This option effects available Network Address Translation Settings. In most cases select Internet. Select TR069 if your ISP manages your equipment remotely.

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

**802.1Q VLAN ID:** Enter the 802.1Q VLAN ID if your ISP offer a High Priority Committed Information Rate (CIR). This guarantees the bandwidth required for real time voice and video applications. Not available for IPoA.

**IP Protocol:** Select the IP protocol your ISP uses. The options are **IPv4**, **IPv6**, or **Both**.

If you selected **PPP over Ethernet(PPPoE)** or **PPP over ATM(PPPoA)**, proceed to **PPP Username and Password** on page 32.

If you selected **MAC Encapsulation Routing(MER)** or **IP over ATM (IPoA)**, proceed to **WAN IP Settings** on page 34.

The screenshot shows the 'CONNECTION TYPE' configuration page. The 'Protocol' dropdown menu is open, displaying the following options: PPP over ATM (PPPoA), PPP over Ethernet (PPPoE), MAC Encapsulation Routing(MER), IP over ATM (IPoA), and Bridging.

The screenshot shows the 'CONNECTION TYPE' configuration page with the following settings: 'Protocol' is set to PPP over Ethernet (PPPoE), 'WAN Service Type' is set to Internet, 'Encapsulation Mode' is set to LLC, '802.1Q VLAN ID' is set to 0 (with a note '(0 = disable, 1 - 4094)'), and 'IP Protocol' is set to Both.

## ATM/ADSL (continued)

If you selected **Bridging**, configure the following options:

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

**802.1Q VLAN ID:** Enter the 802.1Q VLAN ID if your ISP offer a High Priority Committed Information Rate (CIR). This guarantees the bandwidth required for real time voice and video applications.

**Enable Service:** Choose to enable or disable this interface upon clicking **Apply**.

**Firewall Enable:** Choose to enable or disable the firewall.

**Service Name:** Enter a name for the service.

Click **Apply** to finish, further configuration of your networking devices may be necessary.

CONNECTION TYPE	
Protocol :	Bridging
Encapsulation Mode :	LLC
802.1Q VLAN ID :	0 (0 = disable, 1 - 4094)
Enable Service :	<input checked="" type="checkbox"/>
Firewall Enable :	<input checked="" type="checkbox"/>
Service Name :	ADSL

# PPP Username and Password

If you selected **PPPoE over Ethernet (PPPoE)** or **PPP over ATM (PPPoA)**, configure the **PPP Username and Password** options:

## PPP USERNAME AND PASSWORD

**PPP Username:** Enter the username provided by your ISP.

**PPP Password:** Enter the password provided by your ISP.

**Confirm PPP Password:** Enter the password provided by your ISP one more time.

**Authentication Method:** Select the authentication protocol your ISP uses. The options are **PAP**, **CHAP**, **MS-CHAP**, or **AUTO**.

**Dial-up mode:** Select how your DSL-3682 connects to your ISP. Choose either **AlwaysOn**, **OnDemand**, and **Manual**. This may be useful if you are using a metered connection.

**Inactivity Timeout:** If you selected **OnDemand**, enter the amount time the router waits if there is no activity before disconnecting.

**MRU Size:** Enter the maximum receive unit (MRU) packet size. The default is 1492.

**MTU Size:** Enter the maximum transmission unit (MTU) packet size. The default is 1400.

**Keep Alive:** Check the box in order to maintain your connection.

**Lcp Echo Interval (sec):** Enter the Lcp Echo frequency.

**Lcp Echo Failure:** Enter the Lcp Echo Failure.

**CONNECTION TYPE**

Protocol: PPP over Ethernet (PPPoE)  
PPP over ATM (PPPoA)

**PPP USERNAME AND PASSWORD**

PPP Username:

PPP Password:

Confirm PPP Password:

Authentication Method: AUTO

Dial-up mode: AlwaysOn

Inactivity Timeout:  (Minute 1~1092)

MRU Size:  (V4:576~1492 V6:1280~1492)

MTU Size:  (V4:576~1492 V6:1280~1492)

Keep Alive:

Lcp Echo Interval (sec):

Lcp Echo Failure:

Use Static IP Address:

IP Address:

IANA:

Prefix Delegation:

## PPP Username and Password (continued)

If you selected **IPv4** or **Both** as the IP Protocol, configure the following options:



A screenshot of a configuration window showing the following options:

- Use Static IP Address :
- IP Address :
- IANA :
- Prefix Delegation :

**Use Static Address:** If you want to use a static IP address or your ISP provided you with one, check this box.

**IP address:** Enter your Static IPv4 address here.

If you selected **IPv6** or **Both** as the IP Protocol, configure the following options:

**IANA:** Check this box to enable Internet Assigned Numbers Authority IPv6 compatibility.

**Prefix Delegation:** Check this box to enable Prefix Delegation.

Proceed to **Network Address Translation Settings** on page **36**.

# WAN IP Settings

If you selected **MAC Encapsulation Routing(MER)** or **IP over ATM (IPoA)**, configure the **WAN IP Settings** options:

## WAN IP SETTINGS

**Use the following address:** Check the box if you would like to enter IP address information. (**MAC Encapsulation Routing Only.**)

If you selected **Use the following address** and **IPv4** or **Both** as the **IP Protocol**, configure the following options.

**WAN IP Address:** Enter your WAN IP address.

**WAN Subnet Mask:** Enter your WAN subnet mask address.

**Default gateway:** Enter your Default Gateway.

**Preferred DNS server:** Enter your preferred DNS server.

**Alternate DNS server:** Enter your alternate DNS server.

If you selected **Use the following address** and **IPv6** or **Both** as the **IP Protocol**, configure the following options.

**WAN IPv6 Address:** Enter your WAN IPv6 address.

**Address Prefix length:** Enter your WAN IPv6 address prefix length.

**WAN IPv6 Gateway:** Enter your IPv6 Gateway.

CONNECTION TYPE	
Protocol :	MAC Encapsulation Routing(MER) IP over ATM (IPoA)
WAN IP SETTINGS	
<input type="checkbox"/> Use the following address :	
WAN IP Address :	<input type="text"/>
WAN Subnet Mask :	<input type="text"/>
Default gateway :	<input type="text"/>
Preferred DNS server :	<input type="text"/>
Alternate DNS server :	<input type="text"/>
WAN IPv6 Address :	<input type="text"/>
Address Prefix length :	<input type="text"/>
WAN IPv6 Gateway :	<input type="text"/>
WAN IPv6 Prefix :	<input type="text"/>
WAN IPv6 Prefix length :	<input type="text"/>
Preferred IPv6 DNS server :	<input type="text"/>
Alternate IPv6 DNS server :	<input type="text"/>
IANA :	<input type="checkbox"/>
IPv6 Prefix Delegation :	<input type="checkbox"/>

## WAN IP Settings (continued)

**WAN IPv6 Prefix:** Enter your IPv6 prefix.

**WAN IPv6 Prefix length:** Enter your IPv6 prefix length.

**Preferred IPv6 DNS server:** Enter your preferred DNS server.

**Alternate IPv6 DNS server:** Enter your alternate DNS server.

**IANA :** Check this box to enable Internet Assigned Numbers Authority IPv6 compatibility.

**IPv6 Prefix Delegation:** Check this box to enable Prefix Delegation.

CONNECTION TYPE	
Protocol :	MAC Encapsulation Routing(MER) IP over ATM (IPoA)

WAN IP SETTINGS	
<input type="checkbox"/> Use the following address :	
WAN IP Address :	<input type="text"/>
WAN Subnet Mask :	<input type="text"/>
Default gateway :	<input type="text"/>
Preferred DNS server :	<input type="text"/>
Alternate DNS server :	<input type="text"/>
WAN IPv6 Address :	<input type="text"/>
Address Prefix length :	<input type="text"/>
WAN IPv6 Gateway :	<input type="text"/>
WAN IPv6 Prefix :	<input type="text"/>
WAN IPv6 Prefix length :	<input type="text"/>
Preferred IPv6 DNS server :	<input type="text"/>
Alternate IPv6 DNS server :	<input type="text"/>
IANA :	<input type="checkbox"/>
IPv6 Prefix Delegation :	<input type="checkbox"/>

Proceed to **Network Address Translation Settings** on page **36**.



# Network Address Translation Settings

## NETWORK ADDRESS TRANSLATION SETTINGS

If you selected **IPv4** or **Both** as the **IP Protocol**, configure the following options.

**Enable NAT:** Check this box to Enable Network Address Translation (NAT).

**NAT Type:** Select either **Symmetric NAT** or **Full Cone NAT**.

If you selected **IPv6** or **Both** as the **IP Protocol**, configure the following options.

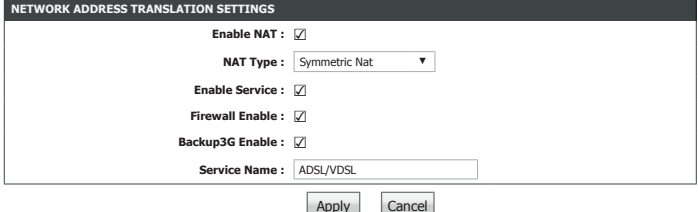
**Enable Service:** Check this box to enable the service once added.

**Firewall Enable:** Check this box to enable the firewall.

**Backup3G Enable:** As of this writing 3G/4G is not supported with current firmware.

**Service Name:** Enter a name for this service.

Click **Apply** when you are done.




The screenshot shows a configuration window titled "NETWORK ADDRESS TRANSLATION SETTINGS". It contains the following options:

- Enable NAT:**
- NAT Type:** Symmetric Nat (dropdown menu)
- Enable Service:**
- Firewall Enable:**
- Backup3G Enable:**
- Service Name:** ADSL/VDSL (text input field)

At the bottom right, there are two buttons: "Apply" and "Cancel".

## 2.4G Wireless

The **2.4G Wireless** tab provides access to configure the 2.4 GHz wireless settings of your DSL-3682.

Product Page: DSL-3682		Firmware Version: EU_1.00				
						
DSL-3682 //		SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
<ul style="list-style-type: none"> <li>Wizard</li> <li>Internet Setup</li> <li>2.4G Wireless</li> <li>5G Wireless</li> <li>Local Network</li> <li>Local IPv6 Network</li> <li>Time and Date</li> <li>Logout</li> </ul>		<p><b>WIRELESS SETTINGS -- WIRELESS BASIC</b></p> <p>Configure your wireless basic settings.</p> <p style="text-align: center;"><a href="#">Wireless Basic</a></p>				
		<p><b>WIRELESS SETTINGS -- WIRELESS SECURITY</b></p> <p>Configure your wireless security settings.</p> <p style="text-align: center;"><a href="#">Wireless Security</a></p>				

To return to the Web UI Table of Contents page, simply click the D-Link logo on the top right of each page.

		
DSL-3682 //	SETUP	ADVANCED
2.4G Wireless		

## Wireless Basic

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 39.

### WIRELESS BASIC CONFIGURATION

- Enable Wireless:** Check this box to enable the 2.4 GHz wireless network.
- AP Isolate:** Check this box to enable AP isolation. AP isolation forces wireless clients to communicate with each other through the access point.
- SSID:** The wireless network name for your network. To change your SSID, enter a new name and click **Apply**. Remember to update the settings on your devices.
- Visibility Status:** **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.
- Continent/Country:** This section shows the current regional/country wireless frequencies the device is set to use. This option may be set by the firmware/factory and unable to modify.
- 802.11 Mode:** Select the wireless standards to use on your network. The options are **802.11b only**, **802.11b/g mixed**, or **802.11b/g/n mixed**.
- Band Width:** Choose the transmission channel band width. The options are **20M** or **20/40M**.
- Wireless Channel:** Select the channel number for your wireless network to operate on. These options are region-dependent. The default is **Auto Scan**.
- The wireless channel currently in use is displayed in red text.
- Click **Apply** to have your changes take effect.

<b>D-Link</b>		
DSL-3682 //	SETUP	ADVANCED
2.4G Wireless	<b>WIRELESS BASIC CONFIGURATION</b>	

**WIRELESS BASIC CONFIGURATION**  
Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

<b>WIRELESS BASIC CONFIGURATION</b>	
<b>Enable Wireless :</b>	<input checked="" type="checkbox"/>
<b>AP Isolate :</b>	<input type="checkbox"/>
<b>SSID :</b>	Your_2.4G Wi-Fi_Network
<b>Visibility Status :</b>	<input checked="" type="radio"/> Visible <input type="radio"/> Invisible
<b>Continent/Country :</b>	Europe ▼
<b>802.11 Mode :</b>	802.11b/g/n mixed ▼
<b>Band Width:</b>	20/40M ▼
<b>Wireless Channel:</b>	Auto Scan(recommended) ▼
<b>Currently used wireless channel is 4</b>	

## Wireless Security

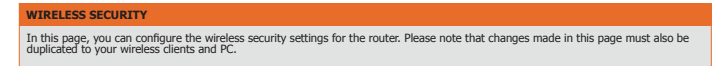
This page allows you to manually configure the router's wireless security settings. To change your wireless network settings refer to **2.4G Wireless** on page 37.

Remember to keep your wireless network passwords safe. Remember that if you change the wireless password of your DSL-3682, you must re-input this password on all of your wireless devices.

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Select the type of security you wish to use. The available options are **None**, **WEP**, **WPA/WPA2 Mixed**, and **WPA2 only**. Using **WPA2 only** is recommended.

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



## WPA2 Only

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Using **WPA2 Only** is recommended. It is the strongest wireless security option supported.

### WIRELESS SECURITY MODE :

**Wireless Security Mode :**  ▼

### WPA 2 Only

**WPA Mode:** Choose either **Personal** or **Enterprise**. Most small home and business networks use **Personal**. If you are running a dedicated RADIUS authentication server, choose **Enterprise**.

**Encryption Mode:** Select either **TKIP**, **AES**, or **TKIP + AES**. AES is recommended. Using TKIP or AES + TKIP encryption is not recommended due to its security vulnerabilities. TKIP encryption does not support WPS.

**Group Key Update Interval:** Enter the number of seconds for the group key update.

### WIRELESS BASIC CONFIGURATION

**WPA Mode :**  ▼

**Encryption Mode :**  ▼

**Group Key Update Interval :**  (60 - 65535)

If you select **Personal** as the **WPA Mode**, the following configuration options are available:

### PRE-SHARED KEY

**Pre-Shared Key:** The current password for your wireless network. To change your password, enter a new one (between 8-63 characters) and click **Apply**. Your wireless clients need this key to join your wireless network. The longer your password, the more secure your data. For improved security, you should change your wireless password every three to six months.

Remember to update the settings on your devices.

### PRE-SHARED KEY

**Pre-Shared Key:**

(ASCII < 64, HEX = 64)

## WPA2 Only (continued)

If you select **Enterprise** as the **WPA Mode**, the following configuration options are available:

### EAP (802.1X)

**RADIUS server IP Address:** Enter your RADIUS Server's IP address.

**RADIUS server Port:** Enter your RADIUS server's port number.

**RADIUS server Shared Secret:** Enter your RADIUS server's shared secret.

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

### EAP (802.1X)

**RADIUS server IP Address :**

**RADIUS server Port :**  (1 - 65535)

**RADIUS server Shared Secret:**  (8-63 characters or 64 Hex strings)

Apply

Cancel

## WPA/WPA2 Mixed

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Use **WPA/WPA2 Mixed** if you have older clients which do not support WPA2 Only. Your wireless network will be less secure.

### WIRELESS SECURITY MODE :

**Wireless Security Mode :**  ▼

### WPA/WPA2 Mixed

**WPA Mode:** Choose either **Personal** or **Enterprise**. Most small home and business networks use **Personal**. If you are running a dedicated RADIUS authentication server, choose **Enterprise**.

**Encryption Mode:** Select either **TKIP**, **AES**, or **TKIP+AES**. AES is recommended. Using TKIP or AES + TKIP encryption is not recommended due to its security vulnerabilities. TKIP encryption does not support WPS.

**Group Key Update Interval:** Enter the group key update interval.

### WPA/WPA2 MIXED

**WPA Mode :**  ▼

**Encryption Mode :**  ▼

**Group Key Update Interval :**  (60 - 65535)

If you select **Personal** as the **WPA Mode**, the following configuration options are available:

### PRE-SHARED KEY

**Pre-Shared Key:** The current password for your wireless network. To change your password, enter a new one (between 8-63 characters) and click **Apply**. Your wireless clients need this key to join your wireless network. The longer your password, the more secure your data. For improved security, you should change your wireless password every three to six months.

Remember to update the settings on your devices.

### PRE-SHARED KEY

**Pre-Shared Key:**

(ASCII < 64, HEX = 64)

## WPA/WPA2 Mixed (continued)

If you select **Enterprise** as the **WPA Mode**, the following configuration options are available:

### EAP (802.1X)

**RADIUS server IP Address:** Enter your RADIUS server's IP address.

**RADIUS server Port:** Enter your RADIUS server's port number.

**RADIUS server Shared Secret:** Enter your RADIUS server's shared secret.

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

### EAP (802.1X)

**RADIUS server IP Address :**

**RADIUS server Port :**  (1 - 65535)

**RADIUS server Shared Secret:**  (8-63 characters or 64 Hex strings)

Apply

Cancel



## WEP

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Using **WEP** security is not recommended, as it only offers a trivial amount of protection for your wireless data and network. WEP is not supported by faster wireless standards.

### WIRELESS SECURITY MODE :

**Wireless Security Mode :** WEP ▼

### WEP

**WEP Key Length:** Select the Encryption cipher key bit strength. The available options are **64 bits** or **128 bits**.

**Default TX Key:** Select WEP Key 1 - 4 to use.

**WEP Key Format:** Select the WEP key format.

**WEP Key1 - 4:** Enter a wireless key to use on your wireless network.

**Authentication:** Select either **Open** or **Share Key**.

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

### WEP

**WEP Key Length :** 128 bits ▼ ( length applies to all keys )

**Default Tx Key :** 1 ▼

**WEP Key Format :** HEX (10 characters) ▼

**WEP Key1 :** 1111111111

**WEP Key2 :**

**WEP Key3 :**

**WEP Key4 :**

**Authentication :** Open ▼

Apply

Cancel

## None

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Not using wireless security (**None**) is not recommended because any wireless client will be able to access your network and devices and use your Internet connection. Not using encryption leaves you open to security threats.

### WIRELESS SECURITY MODE :

**Wireless Security Mode :**  ▼

Apply

Cancel

# 5G Wireless

The **5G Wireless** tab provides access to configure the 5 GHz wireless settings of your DSL-3682.

Product Page: DSL-3682
Firmware Version: EU\_1.00

D-Link®

DSL-3682 //	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
-------------	-------	----------	------------	--------	------

Wizard

Internet Setup

2.4G Wireless

5G Wireless

Local Network

Local IPv6 Network

Time and Date

Logout

**WIRELESS SETTINGS -- WIRELESS BASIC**

Configure your wireless basic settings.

**WIRELESS SETTINGS -- WIRELESS SECURITY**

Configure your wireless security settings.

To return to the Web UI Table of Contents page, simply click the D-Link logo on the top right of each page.

D-Link®

DSL-3682 //	SETUP	ADVANCED
5G Wireless		

## Wireless Basic

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 48.

### WIRELESS BASIC CONFIGURATION

- Enable Wireless:** Check this box to enable the 5 GHz wireless network.
- AP Isolate:** Check this box to enable AP isolation. AP isolation forces wireless clients to communicate with each other through the access point.
- SSID:** The wireless network name for your network. To change your SSID, enter a new name and click **Apply**. Remember to update the settings on your devices.
- Visibility Status:** **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.
- Continent/Country:** This section shows the current regional/country wireless frequencies the device is set to use. This option may be set by the firmware/factory and unable to modify.
- 802.11 Mode:** Select the wireless standards to use on your network. The options are **802.11a only**, **802.11a/n mixed**, or **802.11a/n/ac mixed**.
- Band Width:** Choose the transmission channel bandwidth. The options are **20M**, **20/40M**, **40M**, or **20/40/80M**.
- Wireless Channel:** Select the channel number for your wireless network to operate on. These options are region-dependent. The default is **Auto Scan**.
- The wireless channel currently in use is displayed in red text.
- Click **Apply** to have your changes take effect.

<b>D-Link</b>		
DSL-3682 //	SETUP	ADVANCED
5G Wireless	<b>WIRELESS BASIC CONFIGURATION</b>	

**WIRELESS BASIC CONFIGURATION**  
Use this section to configure the wireless settings for your router. Please note that changes made in this section will also need to be duplicated to your wireless clients and PC.

<b>WIRELESS BASIC CONFIGURATION</b>	
<b>Enable Wireless :</b>	<input checked="" type="checkbox"/>
<b>AP Isolate :</b>	<input type="checkbox"/>
<b>SSID :</b>	Your_5G Wi-Fi_Network
<b>Visibility Status :</b>	<input checked="" type="radio"/> Visible <input type="radio"/> Invisible
<b>Continent/Country :</b>	Europe ▼
<b>802.11 Mode :</b>	802.11a/n/ac mixed ▼
<b>Band Width:</b>	20/40M/80M ▼
<b>Wireless Channel:</b>	Auto Scan(recommended) ▼
<b>Currently used wireless channel is 36</b>	

## Wireless Security

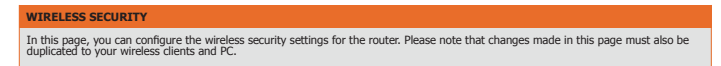
This page allows you to manually configure the router's wireless security settings. To change your wireless network settings refer to **Wireless Basic** on page **47**.

Remember to keep your wireless network passwords safe. Remember that if you change the wireless password of your DSL-3682, you must re-input this password on all of your wireless devices.

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Select the type of security you wish to use. The available options are **None**, **WPA/WPA2 Mixed**, and **WPA2 only**. Using **WPA2 only** is recommended.

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



## WPA2 Only

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Using **WPA2 Only** is recommended. It is the strongest wireless security option supported.

### WIRELESS SECURITY MODE :

**Wireless Security Mode :**  ▼

### WPA 2 Only

**WPA Mode:** Choose either **Personal** or **Enterprise**. Most small home and business networks use **Personal**. If you are running a dedicated RADIUS authentication server, choose **Enterprise**.

**Encryption Mode:** Select either **TKIP**, **AES**, or **AES + TKIP**. AES is recommended. Using TKIP or AES + TKIP encryption is not recommended due to its security vulnerabilities. TKIP encryption does not support WPS.

**Group Key Update Interval:** Enter the group key update interval.

### WIRELESS BASIC CONFIGURATION

**WPA Mode :**  ▼

**Encryption Mode :**  ▼

**Group Key Update Interval :**  (60 - 65535)

If you select **Personal** as the **WPA Mode**, the following configuration options are available:

### PRE-SHARED KEY

**Pre-Shared Key:** The current password for your wireless network. To change your password, enter a new one (between 8-63 characters) and click **Apply**. Your wireless clients need this key to join your wireless network. The longer your password, the more secure your data. For improved security, you should change your wireless password every three to six months.

Remember to update the settings on your devices.

### PRE-SHARED KEY

**Pre-Shared Key:**

(ASCII < 64, HEX = 64)

## WPA2 Only (continued)

If you select **Enterprise** as the **WPA Mode**, the following configuration options are available:

### EAP (802.1X)

**RADIUS server IP Address:** Enter your RADIUS Server's IP address.

**RADIUS server Port:** Enter your RADIUS server's port number.

**RADIUS server Shared Secret:** Enter your RADIUS server's shared secret.

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

### EAP (802.1X)

**RADIUS server IP Address :**

**RADIUS server Port :**  (1 - 65535)

**RADIUS server Shared Secret:**  (8-63 characters or 64 Hex strings)

Apply

Cancel

## WPA/WPA2 Mixed

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Use **WPA/WPA2 Mixed** if you have older clients which do not support WPA2 Only. Your wireless network will be less secure.

### WIRELESS SECURITY MODE :

**Wireless Security Mode :**  ▼

### WPA/WPA2 Mixed

**WPA Mode:** Choose either **Personal** or **Enterprise**. Most small home and business networks use **Personal**. If you are running a dedicated RADIUS authentication server, choose **Enterprise**.

**Encryption Mode:** Select either **TKIP**, **AES**, or **AES + TKIP**. AES is recommended. Using TKIP or AES + TKIP encryption is not recommended due to its security vulnerabilities. TKIP encryption does not support WPS.

**Group Key Update Interval:** Enter the group key update interval.

### WIRELESS BASIC CONFIGURATION

**WPA Mode :**  ▼

**Encryption Mode :**  ▼

**Group Key Update Interval :**  (60 - 65535)

If you select **Personal** as the **WPA Mode**, the following configuration options are available:

### PRE-SHARED KEY

**Pre-Shared Key:** The current password for your wireless network. To change your password, enter a new one (between 8-63 characters) and click **Apply**. Your wireless clients need this key to join your wireless network. The longer your password, the more secure your data. For improved security, you should change your wireless password every three to six months.

Remember to update the settings on your devices.

### PRE-SHARED KEY

**Pre-Shared Key:**

(ASCII < 64, HEX = 64)



## WPA/WPA2 Mixed (continued)

If you select **Enterprise** as the **WPA Mode**, the following configuration options are available:

### EAP (802.1X)

**RADIUS server IP Address:** Enter your RADIUS server's IP address.

**RADIUS server Port:** Enter your RADIUS server's port number.

**RADIUS server Shared Secret:** Enter your RADIUS server's shared secret.

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

### EAP (802.1X)

**RADIUS server IP Address :**

**RADIUS server Port :**  (1 - 65535)

**RADIUS server Shared Secret:**  (8-63 characters or 64 Hex strings)

Apply

Cancel

## None

### WIRELESS SECURITY MODE :

**Wireless Security Mode:** Not using wireless security (**None**) is not recommended because any wireless client will be able to access your network and devices, use your Internet connection. Not using encryption leaves you open to security threats.

### WIRELESS SECURITY MODE :

**Wireless Security Mode :**  ▼

Apply

Cancel

# Local Network

Click **Local Network** on the navigation menu to change the local network settings of the router, configure the DHCP and DNS settings, add new DHCP reservations, and view the currently assigned DHCP reservations. When you have finished configuring the **Local Network**, click the **Apply** button.

## ROUTER SETTINGS

This section allows you to configure the IP address of the router.

**Router IP Address:** Enter the IP address of the router. The default IP address is **192.168.1.1**. If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

**Configure the second IP Address and Subnet Mask for LAN:** Check this box to enable an additional IP address.

**IP Address:** Enter a secondary IP address. The address must not be on the same subnet as the primary router IP.

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



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

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

**Router IP Address :**

**Subnet Mask :**

**Domain Name :**

Configure the second IP Address and Subnet Mask for LAN

**IP Address :**

**Subnet Mask :**

**DHCP SETTINGS (OPTIONAL)**  
Use this section to configure the DHCP Relay for your network.

**Enable DHCP Relay :**

**Relay IP Address :**

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

**Enable DHCP Server :**

**DHCP IP Address Range :**  to

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

Use the following DNS server addresses:

**Enable DNS Relay :**

**Preferred DNS server :**

**Alternate DNS server :**

Apply

Cancel

## Local Network (continued)

### DHCP SETTINGS (OPTIONAL)

This section allows you to configure the router's DHCP assignment settings. You may either configure the router to act as a DHCP server, or enable DHCP Relay. You may also configure DNS Relay.

**Enable DHCP Relay:** Check the box to enable DHCP relay.

**Relay IP Address:** Enter the IP address of your relay DHCP server.

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

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

**DHCP Lease Time:** The lease time determines the period that the host retains the assigned IP addresses before a new IP address is requested. The default is 86400 seconds.

**Enable DNS Relay:** If disabled, the router will accept the first received DNS assignment from one of the PPPoA, PPPoE, or MER enabled Permanent Virtual Circuit(s) (PVC) during the initial connection setup.

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

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

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

**DHCP SETTINGS (OPTIONAL)**

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

**Enable DHCP Relay :**

Relay IP Address :

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

**Enable DHCP Server :**

**DHCP IP Address Range :**  to

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

Use the following DNS server addresses:

**Enable DNS Relay :**

Preferred DNS server :

Alternate DNS server :

## Local Network (continued)

The following options allow for finer control of DHCP addressing. Click **Add** to create a rule and fill in the fields which appear. To edit an existing rule click **Edit**. Click **Apply** when you are satisfied. To delete a rule, check the box in the left hand column and click **Delete**.

### DHCP CLIENT CLASS LIST

Client-class processing enables the DHCP server to assign the client an address from a matching scope. Addresses in this range may be assigned a unique DNS server.

**Client Class Name:** Enter a name for the DHCP class

**Min IP Address:** Enter the beginning of the IP address range to apply this rule to.

**Max IP Address:** Enter the end of the IP address range to apply this rule to.

**DNS Address:** Enter the desired DNS server address.

DHCP CLIENT CLASS LIST				
Status	Client Class	Min Address	Max Address	DNS Address

ADD DHCP CLIENT CLASS(OPTIONAL)	
Client Class Name :	<input type="text"/>
Min IP Address :	<input type="text"/>
Max IP Address :	<input type="text"/>
DNS Address :	<input type="text"/>

### DHCP CONDITIONAL OPTION(OPTIONAL)

Specify the DHCP Conditions for DHCP classes. DHCP Conditional Option rule creation is beyond the scope of this manual.

**Conditional Option Enable:** Check this box to enable the Conditional Option.

**Conditional Option Client Class:** Enter the client class to apply the Conditional Option to.

**Conditional Option Tag:** Enter the conditional tag.

**Conditional Option Value:** Enter the conditional option value.

DHCP CONDITIONAL OPTION			
Status	Client Class Name	Option Code	Option Value

ADD DHCP OPTION(OPTIONAL)	
Conditional Option Enable :	<input type="checkbox"/>
Conditional Option Client Class :	<input type="text"/>
Conditional Option Tag :	<input type="text"/>
Conditional Option Value :	<input type="text"/>

## Local Network (continued)

### DHCP RESERVATIONS LIST

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.

**Enable:** Check this box to enable the static reservation.

**Computer Name:** Enter a name for your DHCP reservation rule.

**IP Address:** Enter the IP address you wish to assign to your device.

**MAC Address:** Enter the MAC address of the device you wish to apply the DHCP reservation rule to.

DHCP RESERVATIONS LIST			
Status	Computer Name	MAC Address	IP Address

Add Edit Delete

ADD DHCP OPTION(OPTIONAL)	
Enable :	<input type="checkbox"/>
Computer Name :	<input type="text"/>
IP Address :	<input type="text"/>
MAC Address :	<input type="text"/>

Apply Cancel

### NUMBER OF DYNAMIC DHCP CLIENTS

The connected clients with IP addresses assigned by DHCP are listed here.

NUMBER OF DYNAMIC DHCP CLIENTS : 1			
Computer Name	MAC Address	IP Address	Expire Time
PCWIN7	3c:1e:04:f3:b6:49	192.168.1.2	86389

# Local IPv6 Network

Click **Local IPv6 Network** on the navigation menu if you wish use IPv6 on your local network.

## STATIC LAN IPV6 ADDRESS CONFIGURATION

**IPv6 Interface Address:** If you wish to set a static IPv6 address for your router, enter it here.

## DHCPV6 CONFIGURATION

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

**LAN Address Config Mode:** Select either **Stateless** (host requests) or **Stateful** (server provisions) LAN IPv6 addressing.

If you select **Stateful** as the **LAN Address Config Mode**, configure the following options:

**Start Interface ID:** Enter the start of the IP address range the DHCPv6 server uses.

**End Interface ID:** Enter the end of the IP address range the DHCPv6 server uses.

**DHCPv6 Lease Time:** Enter the amount of that the host retains the assigned IP addresses before requesting a new one.

Select one of the following DNS server addressing options:

**IPv6 DNS Mode:** Allow the router to accept the first received IPv6 DNS assignment from a WAN connection.

**Static DNS:** Choose this option to manually input the IPv6 DNS server information.

If you select **Static DNS Servers** configure the IPv6 DNS servers:

**Static IPv6 DNS Servers:** Manually enter the IP addresses for primary and secondary IPv6 DNS servers. Use a comma to separate the two.

The screenshot shows the D-Link router's web interface. At the top, there is a navigation bar with the D-Link logo, the model number 'DSL-3682', and tabs for 'SETUP' and 'ADVANCED'. Below this, a breadcrumb trail shows 'Local IPv6 Network' and 'IPV6 LAN SETTINGS'.

**IPV6 LAN SETTINGS**

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

**STATIC LAN IPV6 ADDRESS CONFIGURATION**

IPv6 Interface Address

**DHCPV6 CONFIGURATION**

Enable DHCPv6 Server :

LAN Address Config Mode :  Stateless  Stateful

Start Interface ID :

End Interface ID :

DHCPv6 Lease Time :

Use the following DNS server addresses.

IPv6 DNS Mode :

Static DNS Servers

Static IPv6 DNS Servers

**UNIQUE LOCAL ADDRESSES CONFIGURATION**

Enable RADVD :

RADVD DNSLL :

ULA mode  From WAN  Statically Configure  BOTH

Address  (e.g. fd80::1/64)

Site Prefix :  (e.g. fd80::/64)

Preferred Life Time

Valid Life Time

## Local IPv6 Network (continued)

### UNIQUE LOCAL ADDRESSES CONFIGURATION

**Enable RADVD:** Enable or disable the Router Advertisement Daemon.

**RADVD DNSLL:** Enter the RADVD DNSLL address.

**ULA mode:** Select either **From WAN**, **Statically Configure**, or **BOTH**

If you select **Statically Configure** or **BOTH**, as the **ULA Mode** configure these options:

**Address:** Enter your preferred ULA address.

**Site Prefix:** Enter your ULA prefix.

**Preferred Life Time:** Enter the preferred lifetime of this address.

**Valid Life Time:** Enter the valid lifetime of this address.

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

The screenshot shows the 'UNIQUE LOCAL ADDRESSES CONFIGURATION' window. It contains the following fields and options:

- Enable RADVD:** A checkbox that is currently unchecked.
- RADVD DNSLL:** An empty text input field.
- ULA mode:** Radio buttons for 'From WAN' (selected), 'Statically Configure', and 'BOTH'.
- Address:** An empty text input field with a hint '(e.g. fd80::1/64)'.
- Site Prefix:** An empty text input field with a hint '(e.g. fd80::/64)'.
- Preferred Life Time:** An empty text input field.
- Valid Life Time:** An empty text input field.
- Buttons:** 'Apply' and 'Cancel' buttons at the bottom right.



# Time and Date

This page allows you to edit the system time and Network Time Protocol (NTP). You can configure, update, and maintain the correct time on the system clock, and configure Daylight Saving.

## UNIQUE LOCAL ADDRESSES CONFIGURATION

If you enable **Automatically synchronize with Internet time servers**, enter the Network Time Protocol (NTP) server addresses:

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

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

## TIME CONFIGURATION

**Current Local Time:** Displays the current local time.

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

If you enable **Daylight Saving**, configure the daylight savings start and end times:

**Daylight Saving Start:** Specify the time and date when daylight saving should start.

**Daylight Saving End:** Specify the time and date when daylight saving should end.

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

The screenshot shows the top navigation bar with the D-Link logo and the model number DSL-3682. Below it are three tabs: 'DSL-3682 //', 'SETUP', and 'ADVANCED'. The 'SETUP' tab is active, and within it, the 'TIME AND DATE' sub-tab is selected and highlighted in orange.

The 'TIME AND DATE' section header is shown in orange. Below it is a small text box explaining the configuration options: "The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed."

The 'TIME SETTING' section contains a checkbox labeled "Automatically synchronize with Internet time servers". Below this are two input fields: "1st NTP time server:" and "2nd NTP time server:".

The 'TIME CONFIGURATION' section displays the "Current Local Time" as 2016-08-26 15:32. Below this is a dropdown menu for "Time Zone" set to "(GMT+08:00) Beijing, Hong Kong". There is a checkbox for "Enable Daylight Saving". Below the checkbox are two rows of time pickers for "Daylight Saving Start" and "Daylight Saving End", each with fields for Year, Month, Day, Hour, Min, and Sec. At the bottom are "Apply" and "Cancel" buttons.

# Logout

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



# Advanced

The Advanced tab provides access to configure the advanced features of your DSL-3682.

Product Page: DSL-3682 Firmware Version: EU\_1.00



<b>DSL-3682</b> //	<b>SETUP</b>	<b>ADVANCED</b>	<b>MANAGEMENT</b>	<b>STATUS</b>	<b>HELP</b>
2.4G Advanced Wireless	QoS				
5G Advanced Wireless	Anti-Attack Settings				
ALG	DNS				
Port Forwarding	Dynamic DNS				
Port Trigger	Network Tools				
DMZ	Routing				
SAMBA	FTPD				
3G/4G Configuration	Budget Quota				
Parental Control	Logout				

To return to the Web UI Table of Contents page, simply click the D-Link logo on the top right of each page.



## 2.4G Advanced Wireless

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
2.4G Advanced Wireless	QoS	<b>ADVANCED WIRELESS -- ADVANCED SETTINGS</b> Allows you to configure advanced features of the wireless LAN interface. <a href="#">Advanced Settings</a>			
5G Advanced Wireless	Anti-Attack Settings	<b>ADVANCED WIRELESS -- MAC FILTERING</b> Allows you to configure wireless firewall by denying or allowing designated MAC addresses. <a href="#">MAC Filtering</a>			
ALG	DNS	<b>ADVANCED WIRELESS -- SECURITY SETTINGS</b> Allows you to configure security features of the wireless LAN interface. <a href="#">Security Settings</a>			
Port Forwarding	Dynamic DNS	<b>ADVANCED WIRELESS -- WPS SETTING</b> Allows you to configure wireless WPS. <a href="#">WPS Setting</a>			
Port Trigger	Network Tools	<b>ADVANCED WIRELESS -- WDS SETTING</b> Allows you to configure wireless WDS. <a href="#">WDS Setting</a>			
DMZ	Routing				
SAMBA	FTP				
3G/4G Configuration	Budget Quota				
Parental Control	Logout				

## Advanced Settings

Click **2.4G Advanced Wireless** on the navigation menu to configure the advanced wireless settings.

### WIRELESS ENABLE

If you **Enable Wireless**, the following 2.4 GHz wireless configuration options are available:

### ADVANCED WIRELESS SETTINGS

**Transmit Power:** Set the transmit power of the antennas in percentage.

**Beacon Period:** Set the AP advertisement frame interval.

**RTS Threshold:** This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

**Fragmentation Threshold:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

**DTIM Interval:** DTIM range can be set from 1 to 255. A delivery traffic indication message (DTIM) is a kind of traffic indication message (TIM) which informs the clients of the presence of buffered multicast/broadcast data on the access point.

**Preamble Type:** Use the drop-down menu to specify whether the router should use the **Short** Preamble or **Long** preamble type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the router and roaming wireless adapters.



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

**WIRELESS ENABLE**  
Enable Wireless

**ADVANCED WIRELESS SETTINGS**

Transmit Power : 100% ▼

Beacon Period : 100 (20 ~ 1023)

RTS Threshold : 2346 (1 ~ 2347)

Fragmentation Threshold : 2346 (256 ~ 2346)

DTIM Interval : 1 (1 ~ 255)

Preamble Type : short ▼

**SSID**

SSID : Your\_2.4G Wi-Fi\_Network

Visibility Status :  Visible  Invisible

User Isolation : Off ▼

Disable WMM Advertise : On ▼

Max Clients : 16 (1 ~ 32)

**GUEST/VIRTUAL ACCESS POINT- 1 - 3**

Enable

SSID : Your\_Guest\_Wi-Fi\_Network

Visibility Status :  Visible  Invisible

User Isolation : Off ▼

Disable WMM Advertise : On ▼

Max Clients : 32 (1 ~ 32)

Apply Cancel

## Advanced Settings (continued)

### SSID

**SSID:** The wireless network name for your network. To change your SSID, enter a new name and click **Apply**. Remember to update the settings on your devices.

**Visibility Status:** **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.

**User Isolation:** Check this box to enable user isolation. User isolation forces wireless clients to communicate with each other through the access point.

**Disable WMM Advertise:** Enable or disable Wi-Fi Multimedia QoS.

**Max Clients:** Use this option to specify the maximum number of allowed clients.

### GUEST/VIRTUAL ACCESS POINT-1/2/3

**Enable:** Check to enable the guest/virtual access point.

**Guest SSID:** Specify a name for each guest network.

**Visibility Status:** **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.

**User Isolation:** Check this box to enable user isolation. User isolation forces wireless clients to communicate with each other through the access point.

The screenshot shows the top navigation bar with the D-Link logo and 'DSL-3682 //'. Below it are tabs for 'ADVANCED' and 'MANAGE'. The '2.4G Advanced Wireless' section is active, and the 'ADVANCED SETTINGS' sub-tab is selected.

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

The 'WIRELESS ENABLE' section has a single checkbox labeled 'Enable Wireless' which is checked.

The 'ADVANCED WIRELESS SETTINGS' section includes several adjustable parameters:
 

- Transmit Power: 100% (dropdown)
- Beacon Period: 100 (range 20 ~ 1023)
- RTS Threshold: 2346 (range 1 ~ 2347)
- Fragmentation Threshold: 2346 (range 256 ~ 2346)
- DTIM Interval: 1 (range 1 ~ 255)
- Preamble Type: short (dropdown)

The 'SSID' section for a guest/virtual access point shows:
 

- SSID: Your\_2.4G Wi-Fi\_Network
- Visibility Status: Visible (radio selected), Invisible (radio unselected)
- User Isolation: Off (dropdown)
- Disable WMM Advertise: On (dropdown)
- Max Clients: 16 (range 1 ~ 32)

The 'GUEST/VIRTUAL ACCESS POINT- 1 - 3' section shows:
 

- Enable: unchecked checkbox
- SSID: Your\_Guest\_Wi-Fi\_Network
- Visibility Status: Visible (radio selected), Invisible (radio unselected)
- User Isolation: Off (dropdown)
- Disable WMM Advertise: On (dropdown)
- Max Clients: 32 (range 1 ~ 32)

Apply Cancel

## Advanced Settings (continued)

**Disable WMM Advertise:** Enable or disable Wi-Fi Multimedia QoS.

**Max Clients:** Use this option to specify the maximum number of clients.

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

The screenshot shows a configuration window titled "GUEST/VIRTUAL ACCESS POINT- 1 - 3". The settings are as follows:

- Enable:**
- Guest SSID:** Your\_Guest\_Wi-Fi\_Network
- Visibility Status:**  Visible  Invisible
- User Isolation:** Off
- Disable WMM Advertise:** On
- Max Clients:** 32 (1 ~ 32)

At the bottom of the window are two buttons: **Apply** and **Cancel**.

## MAC Filtering

Click **MAC Filtering** on the **2.4G Advanced Wireless** navigation menu to configure the MAC address filtering feature. This feature allows you to configure filters to control which wireless clients can access your network, and which network resources they can access.

### ACCESS CONTROL -- MAC ADDRESSES

**Wireless SSID:** Select the Wireless SSID from the dropdown menu which you wish to apply MAC filtering to.

**Access Control Mode:** Select the access control type: **Allow** to allow only the listed clients, **Disable** to disable the MAC filter, or **Deny** to deny the listed clients.

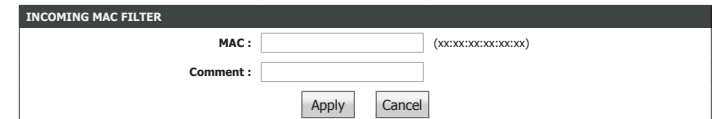
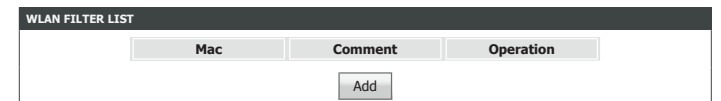
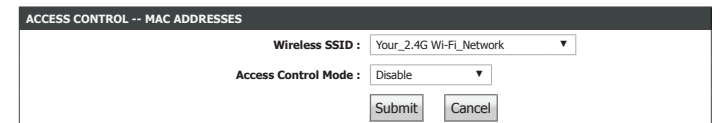
Click the **Add** button to add an item to the filter list.

### INCOMING MAC FILTER

**MAC:** Enter the MAC address of a device you wish to control access to the WLAN.

**Comment:** Enter a comment to help you to identify the device.

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





## Security Settings

Click **Security Settings** on the **2.4G Advanced Wireless** navigation menu to configure the wireless security settings. Refer to **Wireless Security** on page **39** for more information.



## WPS Settings

The WPS Settings page allows you to configure the Wi-Fi Protected Setup (WPS) feature of your DSL-3682 which allows to create a secure wireless connection.

### WPS

**Wireless SSID:** Select the Wireless SSID of the network you wish to configure.

**WPA Mode:** The currently set WPA mode is displayed.

**Pre-Shared Key:** The current pre-shared key is displayed or obscured.

### WI-FI PROTECTED SETUP CONFIG

If you **Enable WPS**, the following configuration options are available:

**Push Button:** Click PBC to activate the WPS-PBC (push-button) method.

**Select Mode:** Select either **AP PIN** or **STA PIN**. Using WPS-PIN is no longer recommended due to security vulnerabilities.

Select **AP PIN** the following options are available:

**AP PIN:** The currently configured AP PIN is displayed. Click **New PIN** to create a new PIN.

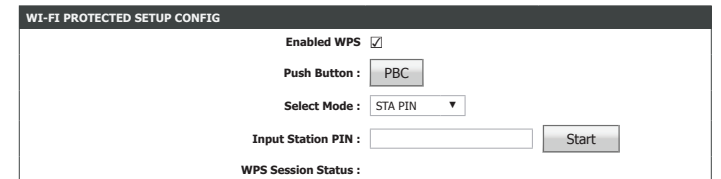
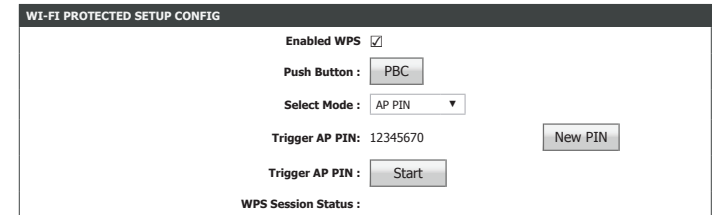
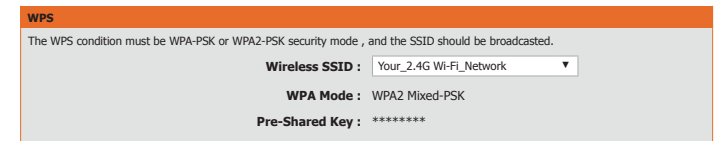
**Trigger AP PIN:** Click **Start** to connect to the device.

Select **STA PIN** the following options are available:

**Input Station PIN:** Enter a PIN. Click **Start** to begin WPS-PIN.

**WPS Session Status:** Displays the current WPS status.

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



Apply Cancel

# 5G Advanced Wireless

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682	SETUP	ADVANCED	MANAGEMENT	STATUS	HELP
2.4G Advanced Wireless	QoS	<b>ADVANCED WIRELESS -- ADVANCED SETTINGS</b> Allows you to configure advanced features of the wireless LAN interface. <input type="button" value="Advanced Settings"/>			
5G Advanced Wireless	Anti-Attack Settings	<b>ADVANCED WIRELESS -- MAC FILTERING</b> Allows you to configure wireless firewall by denying or allowing designated MAC addresses. <input type="button" value="MAC Filtering"/>			
ALG	DNS	<b>ADVANCED WIRELESS -- SECURITY SETTINGS</b> Allows you to configure security features of the wireless LAN interface. <input type="button" value="Security Settings"/>			
Port Forwarding	Dynamic DNS	<b>ADVANCED WIRELESS -- WPS SETTING</b> Allows you to configure wireless WPS. <input type="button" value="WPS Setting"/>			
Port Trigger	Network Tools	<b>ADVANCED WIRELESS -- WDS SETTING</b> Allows you to configure wireless WDS. <input type="button" value="WDS Setting"/>			
DMZ	Routing				
SAMBA	FTP				
3G/4G Configuration	Budget Quota				
Parental Control	Logout				

## Advanced Settings

Click **5G Advanced Wireless** on the navigation menu to configure the advanced wireless settings.

### WIRELESS ENABLE

If you **Enable Wireless**, the following 5 GHz wireless configuration options are available:

### ADVANCED WIRELESS SETTINGS

**Transmit Power:** Set the transmit power of the antennas in percentage.

**Beacon Period:** Beacon Interval range can be set from 20 to 1023.

**RTS Threshold:** This value should remain at its default setting of 2346. If inconsistent data flow is a problem, only a minor modification should be made.

**Fragmentation Threshold:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

**DTIM Interval:** DTIM range can be set from 1 to 255. A delivery traffic indication message (DTIM) is a kind of traffic indication message (TIM) which informs the clients of the presence of buffered multicast/broadcast data on the access point.

**Preamble Type:** Use the drop-down menu to specify whether the router should use the **Short** Preamble or **Long** preamble type. The preamble type defines the length of the CRC (Cyclic Redundancy Check) block for communication between the router and roaming wireless adapters.



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

**WIRELESS ENABLE**  
Enable Wireless

**ADVANCED WIRELESS SETTINGS**

Transmit Power : 100% ▼

Beacon Period : 100 (20 ~ 1023)

RTS Threshold : 2346 (1 ~ 2347)

Fragmentation Threshold : 2346 (256 ~ 2346)

DTIM Interval : 1 (1 ~ 255)

Preamble Type : short ▼

**SSID**

SSID : Your\_5G Wi-Fi\_Network

Visibility Status :  Visible  Invisible

User Isolation : Off ▼

Disable WMM Advertise : On ▼

Max Clients : 16 (1 ~ 32)

**GUEST/VIRTUAL ACCESS POINT- 1 - 3**

Enable

Guest SSID : Your\_Guest\_Wi-Fi\_Network

Visibility Status :  Visible  Invisible

User Isolation : Off ▼

Disable WMM Advertise : On ▼

Max Clients : 32 (1 ~ 32)

Apply Cancel

## Advanced Settings (continued)

### SSID

**SSID:** The wireless network name for your network. To change your SSID, enter a new name and click **Apply**. Remember to update the settings on your devices.

**Visibility Status:** **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.

**User Isolation:** Check this box to enable user isolation. User isolation forces wireless clients to communicate with each other through the access point.

**Disable WMM Advertise:** Enable or disable Wi-Fi Multimedia QoS.

**Max Clients:** Use this option to specify the maximum number of clients.

### GUEST/VIRTUAL ACCESS POINT-1/2/3

**Enable:** Check to enable the guest/virtual access point.

**Guest SSID:** Specify a name for each guest network.

**Visibility Status:** **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.

**User Isolation:** Check this box to enable user isolation. User isolation forces wireless clients to communicate with each other through the access point.



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

**WIRELESS ENABLE**  
Enable Wireless

**ADVANCED WIRELESS SETTINGS**

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

**SSID**

SSID : Your\_2.4G Wi-Fi\_Network

Visibility Status :  Visible  Invisible

User Isolation : Off ▼

Disable WMM Advertise : On ▼

Max Clients : 16 (1 ~ 32)

**GUEST/VIRTUAL ACCESS POINT- 1 - 3**

Enable

Guest SSID : Your\_Guest\_Wi-Fi\_Network

Visibility Status :  Visible  Invisible

User Isolation : Off ▼

Disable WMM Advertise : On ▼

Max Clients : 32 (1 ~ 32)

Apply Cancel

## Advanced Settings (continued)

**Disable WMM Advertise:** Enable or disable Wi-Fi Multimedia QoS.

**Max Clients:** Use this option to specify the maximum number of clients.

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

GUEST/VIRTUAL ACCESS POINT- 1 - 3

Enable

Guest SSID : Your\_Guest\_Wi-Fi\_Network

Visibility Status :  Visible  Invisible

User Isolation : Off ▾

Disable WMM Advertise : On ▾

Max Clients : 32 (1 ~ 32)

Apply Cancel

## MAC Filtering

Click **MAC Filtering** on the **5G Advanced Wireless** navigation menu to configure MAC address filtering feature. This feature allows you to configure filters to control which wireless clients can access your network, and which network resources they can access.

### ACCESS CONTROL -- MAC ADDRESSES

**Wireless SSID:** Select the Wireless SSID from the dropdown menu which you wish to apply MAC filtering to.

**Access Control Mode:** Select the access control type: **Allow** to allow only the listed clients, **Disable** to disable the MAC filter, or **Deny** to deny the listed clients.

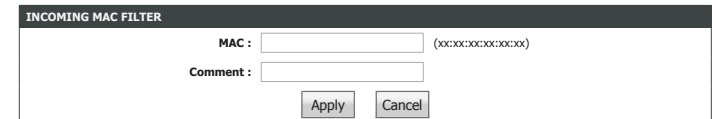
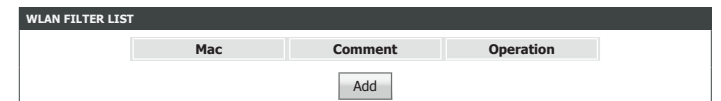
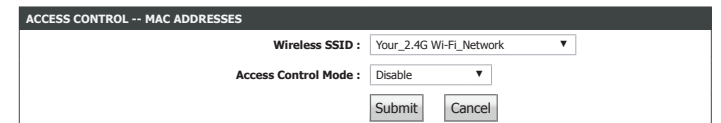
Click the **Add** button to add an item to the filter list.

### INCOMING MAC FILTER

**MAC:** Enter the MAC address of a device you wish to control access to the WLAN.

**Comment:** Enter a comment to help you to identify the device.

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



## Security Settings

Click **Security Settings** on the **5G Advanced Wireless** navigation menu to configure the wireless security settings. Refer to **Wireless Security** on page **48** for more information.





## WPS Settings

The WPS Settings page allows you to configure the Wi-Fi Protected Setup (WPS) feature of your DSL-3682 which allows to create a secure wireless connection.

### WPS

**Wireless SSID:** Select the Wireless SSID of the network you wish to configure.

**WPA Mode:** The currently set WPA mode is displayed.

**Pre-Shared Key:** The current pre-shared key is displayed or obscured.

### WI-FI PROTECTED SETUP CONFIG

If you **Enable WPS**, the following configuration options are available:

**Device PIN:** Using WPS-PIN is no longer recommended due to security vulnerabilities and is disabled by default. Click **New PIN** to generate a new PIN.

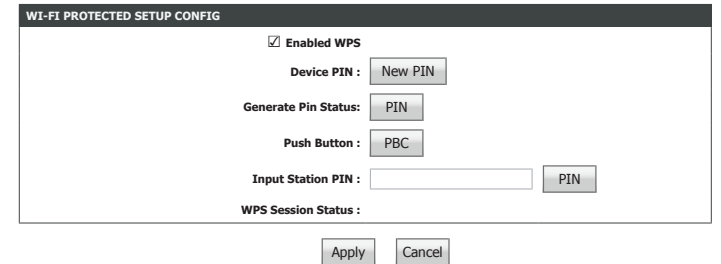
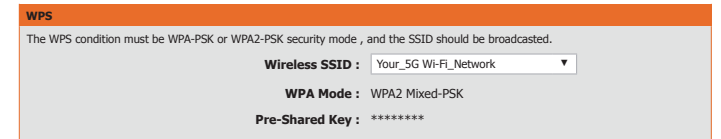
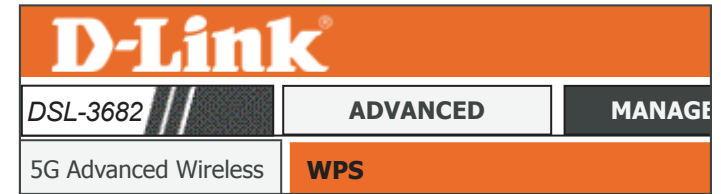
**Generate PIN Status:** Click PIN to enter a PIN for the new device that you wish to connect.

**Push Button:** Click PBC to activate the WPS-PBC (push-button) method.

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

**WPS Session Status:** Displays the current WPS status.

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



# ALG

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

## ALG CONFIGURATION

Enable or disable the desired ALG options. Click **Submit** to have your changes take effect.

The screenshot shows the D-Link DSL-3682 web interface. At the top, there is a navigation bar with the D-Link logo, the model number DSL-3682, and tabs for ADVANCED and MANAGE. Below this is a sub-menu with ALG selected. The main content area is titled ALG CONFIGURATION and contains a list of application protocols with checkboxes for enabling or disabling them. All checkboxes are currently checked. At the bottom right, there are Submit and Refresh buttons.

D-Link	
DSL-3682	ADVANCED
ALG	ALG

ALG  
Application Level Gateway.

**ALG CONFIGURATION**

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

Submit Refresh

# Port Forwarding

Port forwarding allows you to specify a port or range of ports to open for specific devices on the network. This might be necessary for certain applications to connect through the router. In some cases you may have two applications running on different devices which require the same public port. Port forwarding also allows you to remap a different external port to each device.

## PORT FORWARDING SETUP

The currently defined Port Forwarding Rules are displayed here. A total of 32 port forwarding rules may be defined. If you wish to create a new rule, click the **Add** button. If you wish to remove a rule, select it from the table and click the **Delete** button. If you wish to edit a rule, select it from the table and click the **Edit** button.

**WAN Connection:** Select the connection to apply the rule to.

**Select a Service:** A selection of legacy applications are provided for reference.

**Server Name:** Enter a name for the custom service rule.

**Server IP Address(Host Name):** Enter the internal IP address for the traffic to be forwarded to.

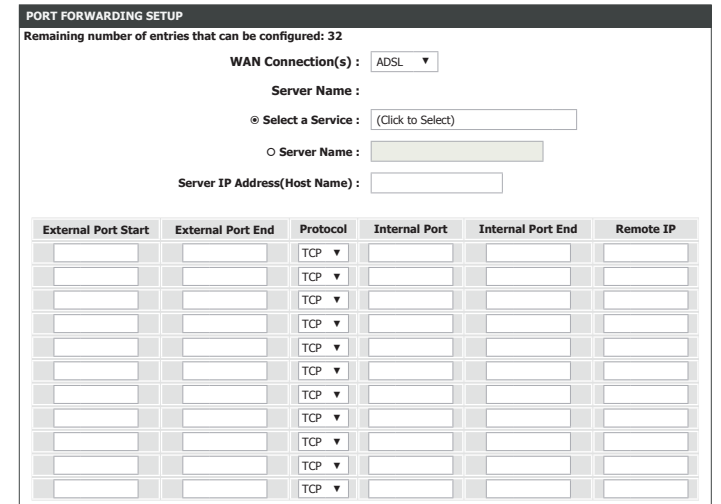
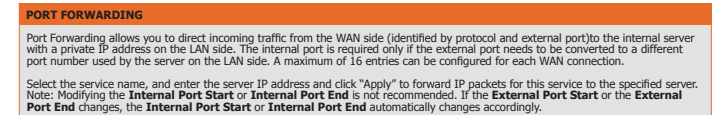
**External Port Start & End:** Enter the external ports to forward. You can enter a single port or a range of ports.

**Protocol:** Select either TCP or UDP.

**Internal Port Start & End:** Enter the internal ports to receive traffic on. Remapped port ranges are calculated in sequential blocks.

**Remote:** You may restrict IP forwarding from a single IP.

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



# Port Trigger

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

## PORT TRIGGER

The currently defined Port Trigger Rules are displayed here. A total of 32 port trigger rules may be defined. If you wish to create a new rule, click the **Add** button. If you wish to remove a rule, select it from the table and click the **Delete** button. If you wish to edit a rule, select it from the table and click the **Edit** button.

**Service Name:** Enter a name for the server or service.

**Enable Port Trigger:** Check this to enable the port trigger feature.

**Rule Status:** Select whether to **Enable** or **Disable** this rule.

**Trigger Port Start/End:** Enter the starting and ending port to monitor to trigger this rule.

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

**Open Port Start/End:** Enter the starting and ending port to open when the rule is triggered.

**Open Protocol:** Enter the protocol to allow through the opened ports.

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

**PORT TRIGGER**

Port Trigger let the device to open TCP or UDP port to access the connection from remote host when the specified port has been opened by the device. A maximum of 32 entries can be configured. Select the service name, and fill the blanks of trigger port and new opened port. Rule can be enable or disable separately.

Enable Port Trigger

**PORT TRIGGER SETUP**

Service Name	Trigger Protocol	Trigger Port Range	Open Protocol	Open Port Range	Status

Add Edit Delete

**PORT TRIGGER SETUP**

Remaining number of entries that can be configured: 32

Service Name :

Rule status :

Trigger Port Start	Trigger Port End	Trigger Protocol	Open Port Start	Open Port End	Open Protocol
<input type="text"/>	<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>	TCP

Apply Cancel

# 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.

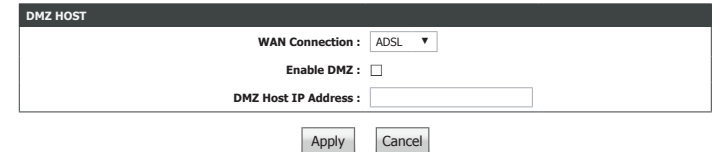
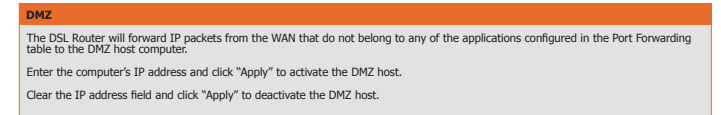
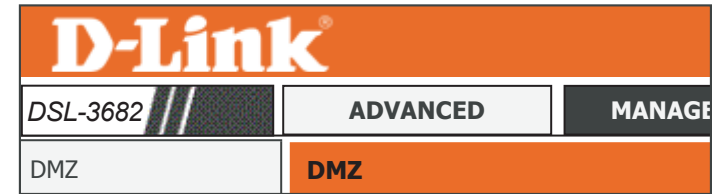
## DMZ HOST

**WAN Connection:** Specify the WAN connection to use.

**Enable DMZ:** Check to enable or disable DMZ functionality.

**DMZ Host IP Address:** Enter an IP address to be included in the DMZ.

Click **Submit** to have your changes take effect.



# SAMBA

This page will allow you to set up access to files on an external USB device plugged into the router. Samba allows file and print sharing between computers. It is an implementation of dozens of services and a dozen protocols.

## SAMBA SERVER

**Enable SAMBA:** Check to enable or disable SAMBA functionality.

**Workgroup:** Enter the name of the workgroup to be mapped.

**Netbios Name:** Enter a name for Netbios mapping.

If you wish to use or change the Samba networking password, enter it here.

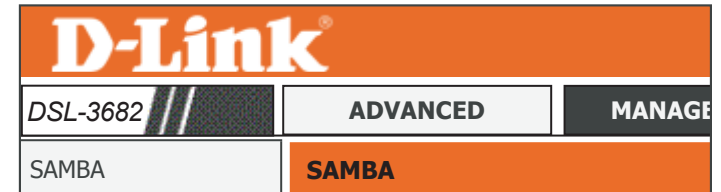
**New SMB password:** Enter a password for the root user.

**Retype new SMB password:** Re-enter the password for the root user.

**Enable USB Storage:** Check to enable or disable SAMBA functionality for USB devices.

**Enable Anonymous Access:** Check to enable or disable SAMBA functionality for USB anonymous users.

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



 A screenshot of the 'SAMBA SERVER' configuration form. The form has a dark header with the title 'SAMBA SERVER'. Below the header, there are several settings:
 

- Enable SAMBA:** A checked checkbox.
- Workgroup:** A text input field containing 'WORKGROUP'.
- Netbios Name:** A text input field containing 'dlink router'.
- modify the password for user root:** A section with two password input fields: 'New SMB password' and 'Retype new SMB password', both containing six asterisks.
- Enable USB Storage:** A checked checkbox.
- Enable Anonymous Access:** A checked checkbox.

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

# 3G/4G Configuration

As of this writing 3G/4G is not supported with current firmware.

D-Link®

DSL-3682 //
ADVANCED
MANAGE

3G/4G Configuration
3G/4G WAN CONFIGURATION

3G/4G WAN CONFIGURATION

Choose "Add", "Edit", or "Delete" to configure 3G/4G WAN interfaces.  
When you want to edit the 3G/4G configuration, please ensure the 3G/4G is in disconnection status at first.

3G/4G WAN SETUP

3G/4G Status: NoDongle  
Inform: NO USB CARD

3G/4G WAN SETUP

Service Name	Protocol	State	Status	Default Gateway	Action

3G WAN SETUP

Enable 3G Service :

Enable NDIS :

Enable DHCP :

Account :

Password :

Dial\_Number :

Net Type :  ▼

APN :

OnDemand :

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

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

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

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

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

BackupMechanism :  ▼

Checking IP address:

Timeout (in sec.):

Period time (in sec.):

Fail Tolerance:

# Parental Control

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

2.4G Advanced  
Wireless

QoS

5G Advanced Wireless

Anti-Attack Settings

ALG

DNS

Port Forwarding

Dynamic DNS

Port Trigger

Network Tools

DMZ

Routing

SAMBA

FTPD

3G/4G Configuration

Budget Quota

Parental Control

Logout

## PARENTAL CONTROL -- WEBSITE FILTER

This is a blocking function for website addresses, if this function is enabled, access to the website addresses in the list will be denied.

## PARENTAL CONTROL -- HTTP CONTENT FILTER

This is a blocking function for http content, if this function is enabled, access to the http content in the list will be denied.

## PARENTAL CONTROL -- MAC FILTER

Uses MAC address to implement filtering.



## Website Filter

The website filter settings allow you to block access to certain web sites. You can either create a list of sites to block, or create a list of sites to allow (with all other sites being blocked).

### WEBSITE FILTER

**Access Control Mode:** Select to either **Allow** or **Deny** traffic from the dropdown menu.

### WEBSITE FILTER LIST

The currently defined website filter list is displayed here.

### ADD SCHEDULE RULE

**URL:** Enter a website address.

**Day (s):** Select either **All Week** or **Select Day(s)**. If you choose Select Day(s), check the boxes next to the days of the week you wish to have the rule enabled.

**All Day - 24 hrs:** Check this box to have the rule apply all day. If you would like to only have the rule apply for a certain period of time, uncheck the box and enter the the **Start Time** and **End Time**.

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

The screenshot shows the top navigation bar with the D-Link logo and the device model DSL-3682. Below the navigation bar, there are tabs for 'ADVANCED' and 'MANAGE'. The 'WEBSITE FILTER' tab is selected and highlighted in orange.

The screenshot shows the 'WEBSITE FILTER' configuration page. It has a header bar with the title 'WEBSITE FILTER' and a sub-header with the instruction: 'Create a list of websites that you would like the devices on your network to be allowed or denied access to.'

The screenshot shows the 'WEBSITE FILTER' configuration page with the 'Access Control Mode' dropdown menu set to 'Deny'. There are 'Apply' and 'Cancel' buttons below the dropdown.

The screenshot shows the 'WEBSITE FILTER LIST' configuration page. It has a table with two columns: 'URL' and 'Schedule'. Below the table are 'Add', 'Edit', and 'Delete' buttons.

The screenshot shows the 'ADD SCHEDULE RULE' configuration page. It has a 'URL' field with 'http://' entered. Below it are radio buttons for 'All Week' (selected) and 'Select Day(s)'. Under 'Select Day(s)', there are checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat, all of which are checked. There is also an 'All Day - 24 hrs' checkbox which is checked. Below that are 'Start Time' and 'End Time' fields, both set to '00 : 00'. There are 'Apply' and 'Cancel' buttons at the bottom.

## HTTP Content Filter

The website filter settings allow you to block access to certain content based on keywords.

### HTTP CONTENT FILTER

**Access Control Mode:** Select to either **Allow** or **Deny** traffic from the dropdown menu.

### HTTP CONTENT FILTER LIST

The currently defined http content filter list is displayed here.

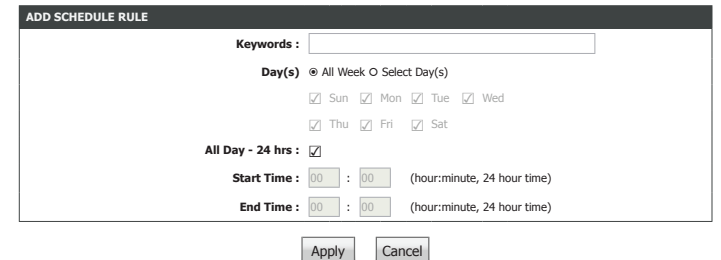
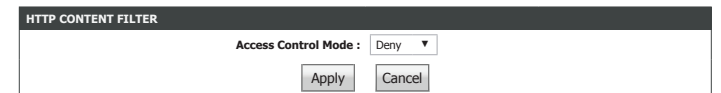
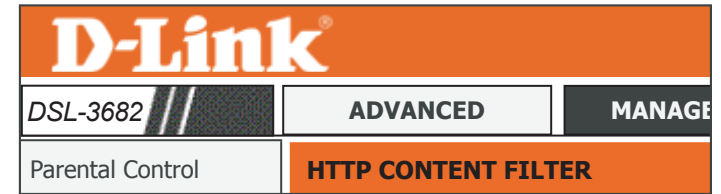
### ADD SCHEDULE RULE

**Keywords:** Enter a website address.

**Day (s):** Select either **All Week** or **Select Day(s)**. If you choose Select Day(s), check the boxes next to the days of the week you wish to have the rule enabled.

**All Day - 24 hrs:** Check this box to have the rule apply all day. If you would like to only have the rule apply for a certain period of time, uncheck the box and enter the the **Start Time** and **End Time**.

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



## MAC Filter

The website filter settings allow you to allow or block a device's access to the Internet based on its MAC address.

### MAC FILTERING GLOBAL POLICY

**Access Control Mode:** Select to either **Allow** or **Deny** traffic from the dropdown menu.

### BLOCK MAC ADDRESS--BLACKLIST

The currently defined http MAC Address Black list is displayed here.

### ADD SCHEDULE RULE

**User Name:** Enter a user name.

**Current PC's MACaddress:** The MAC address of the client you are currently using to configure the web configuration utility is listed here.

**Other MAC Address:** Enter the MAC address of a device you wish to add to the blacklist.

**Day (s):** Select either **All Week** or **Select Day(s)**. If you choose Select Day(s), check the boxes next to the days of the week you wish to have the rule enabled.

**All Day - 24 hrs:** Check this box to have the rule apply all day. If you would like to only have the rule apply for a certain period of time, uncheck the box and enter the the **Start Time** and **End Time**.

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

**BLOCK MAC ADDRESS**

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

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

Mac Filtering Global Policy:

- Black List** --Allow all packets but **DENY** those matching any of specific rules listed
- White List** --Deny all packets but **ALLOW** those matching any of specific rules listed

**BLOCK MAC ADDRESS--BLACKLIST**

Keywords	MAC	Schedule

Add Edit Delete

**ADD SCHEDULE RULE**

User Name :

**Current PC's MACAddress** :

**Other MAC Address** :

Day(s)  All Week  Select Day(s)

Sun  Mon  Tue  Wed

Thu  Fri  Sat

All Day - 24 hrs :

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

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

Apply Cancel

# QoS

QoS allows you to prioritize Internet traffic to ensure a better web browsing experience in situations where bandwidth is limited or large numbers of devices are in use. QoS can improve your online experience by ensuring that specific traffic is prioritized over other network traffic, such as VoIP, FTP, or Web.

## QUALITY OF SERVICE

**QoS** : Check to enable or disable QoS.

## QOS QUEUE

**Direction**: Select Upstream or Downstream.

**Queue Enable**: Check to enable or disable queueing.

**Bandwidth**: Enter a maximum limit for upstream traffic.

**Discipline**: Select the QoS discipline type.

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

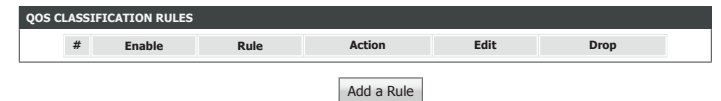
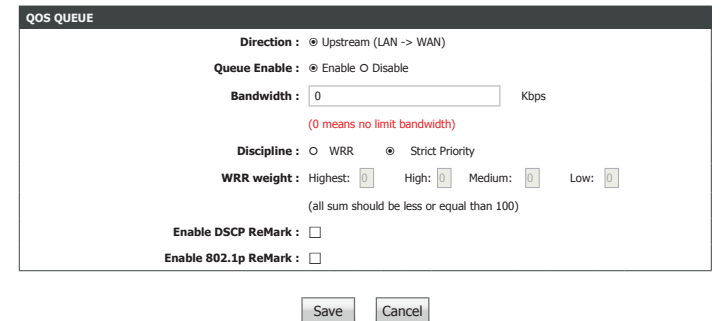
**Enable DSCP ReMark**: Check to enable or disable DSCP ReMark.

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

Click **Save** to have your changes take effect.

## QOS CLASSIFICATION RULES

The currently defined QoS rules are displayed here. Click **Add a Rule** to define QoS rules.



# QoS - Add a Rule

## RULE

**Classify Type:** Select **Upstream Flow**.

**Actions:** Choose to enable or disable this rule upon submission.

**Application:** Select the pre-defined application type or choose **Not Match**. Selecting a pre-defined application populates data to the appropriate fields.

**Physical Ports:** Choose the interface to apply the rule to.

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

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

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

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

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

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

**Source Subnet Mask:** Enter the source subnet mask.

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

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

QoS CLASSIFICATION RULES					
#	Enable	Rule	Action	Edit	Drop

Add a Rule

# D-Link®

DSL-3682
ADVANCED
MANAGE

QoS
ADD QoS CLASSIFICATION RULE

RULE	
<b>Classify Type :</b>	<input checked="" type="radio"/> Upstream Flow Classify
<b>Actions :</b>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
<b>Application :</b>	Not Match ▼
<b>Physical Ports :</b>	Local ▼
<b>Destination MAC Address :</b>	<input type="text"/>
<b>Destination IP Address :</b>	<input type="text"/>
<b>Destination Subnet Mask :</b>	<input type="text"/>
<b>Destination Port Range :</b>	<input type="text"/> ~ <input type="text"/>
<b>Source MAC Address :</b>	<input type="text"/>
<b>Source IP Address :</b>	<input type="text"/>
<b>Source Subnet Mask :</b>	<input type="text"/>
<b>Source Port Range :</b>	<input type="text"/> ~ <input type="text"/>
<b>Protocol :</b>	Not Match ▼
<b>Vlan ID :</b>	<input type="text"/>
<b>DSCP :</b>	Not Set ▼
<b>802.1p :</b>	Not Match ▼

ACTIONS	
<b>DSCP Remark :</b>	Not Set ▼
<b>802.1p Remark :</b>	Not Set ▼   Not Set ▼
<b>Queue :</b>	Unbound ▼
<input type="button" value="Save"/> <input type="button" value="Back"/>	

## QoS - Add a Rule (continued)

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

**DSCP:** Select the queue priority number.

**Queue #:** Select the queue priority number.

### ACTIONS

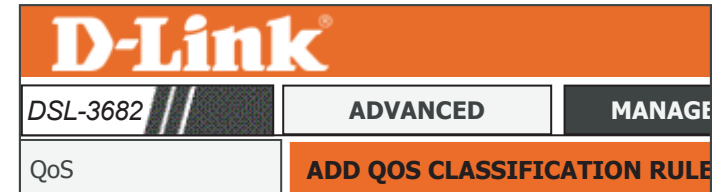
**DSCP Remark:** The DSCP range can be between 0 to 63.

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

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

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

Click **Save** to add the QoS Rule.



RULE	
Classify Type :	<input checked="" type="radio"/> Upstream Flow Classify
Actions :	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Application :	Not Match ▼
Physical Ports :	Local ▼
Destination MAC Address :	<input type="text"/>
Destination IP Address :	<input type="text"/>
Destination Subnet Mask :	<input type="text"/>
Destination Port Range :	<input type="text"/> ~ <input type="text"/>
Source MAC Address :	<input type="text"/>
Source IP Address :	<input type="text"/>
Source Subnet Mask :	<input type="text"/>
Source Port Range :	<input type="text"/> ~ <input type="text"/>
Protocol :	Not Match ▼
Vlan ID :	<input type="text"/>
DSCP :	Not Set ▼
802.1p :	Not Match ▼

ACTIONS	
DSCP Remark :	Not Set ▼
802.1p Remark :	Not Set ▼ Not Set ▼
Queue :	Unbound ▼
<input type="button" value="Save"/> <input type="button" value="Back"/>	

# Anti-Attack Settings

This section enables you to automatically configure your router to detect and protect against several known attack types. A denial-of-service (DoS) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service.

## ANTI-ATTACK CONFIGURATION

**Enable Anti-Attack:** Check this option to enable Anti-Attack settings.

**Enable Attack Log:** Check the option to enable logging.

Click **Submit** to save your changes.

The screenshot shows the D-Link DSL-3682 web interface. At the top, there is a navigation bar with the D-Link logo, the model number 'DSL-3682', and tabs for 'ADVANCED' and 'MANAGE'. Below this is a sub-menu with 'Anti-Attack Settings' and 'ANTI-ATTACK'. The main content area is titled 'ANTI-ATTACK' and contains a section for 'ANTI-ATTACK CONFIGURATION'. This section has two checked options: 'Enable Anti-Attack' and 'Enable Attack Log'. At the bottom right of the configuration area are 'Submit' and 'Refresh' buttons.

D-Link		
DSL-3682	ADVANCED	MANAGE
Anti-Attack Settings	ANTI-ATTACK	
ANTI-ATTACK		
Anti Attack		
ANTI-ATTACK CONFIGURATION		
Enable Anti-Attack <input checked="" type="checkbox"/>		
Enable Attack Log <input checked="" type="checkbox"/>		
		Submit Refresh

# DNS

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

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

## DNS SERVER CONFIGURATION

**WAN Connection:** Select WAN connection you wish to configure.

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

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

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

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

The screenshot shows the D-Link DSL-3682 web interface. At the top, there is a navigation bar with 'DSL-3682' and 'ADVANCED' tabs. Below this, a 'DNS' tab is selected. The main content area is titled 'DNS SERVER CONFIGURATION'. It contains the following configuration options:

- WAN Connection:** A dropdown menu currently set to 'ADSL'.
- IPv4 static DNS:** A checkbox labeled 'Enabled' which is currently unchecked.
- Preferred DNS server:** An empty text input field.
- Alternate DNS server:** An empty text input field.

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



# Dynamic DNS

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

Click Add or Edit to reveal Dynamic DNS configuration options.

## DYNAMIC DNS

The currently defined DDNS Rules are displayed here. If you wish to create a new DDNS mapping, click the **Add** button. If you wish to remove an existing mapping, select it from the table and click the **Delete** button. If you wish to edit a rule, select it from the table and click the **Edit** button.

## ADD DYNAMIC DNS

**DDNS provider:** Select the DDNS provider you wish to use.

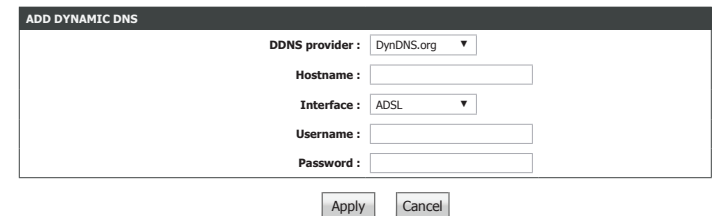
**Hostname:** Enter the hostname you registered with the Dynamic DNS provider.

**Interface:** Select the appropriate interface.

**Username:** Enter the username for your Dynamic DNS account.

**Password:** Enter the password for your Dynamic DNS account.

Click **Apply** when you are done.



# Network Tools

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

2.4G Advanced  
Wireless

QoS

5G Advanced Wireless

Anti-Attack Settings

ALG

DNS

Port Forwarding

Dynamic DNS

Port Trigger

Network Tools

DMZ

Routing

SAMBA

FTP

3G/4G Configuration

Budget Quota

Parental Control

Logout

## NETWORK TOOLS -- IGMP PROXY

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

## NETWORK TOOLS -- IGMP SNOOPING

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

## NETWORK TOOLS -- UPnP

Allows you to enable or disable UPnP.

## NETWORK TOOLS -- DSL

Allows you to configure advanced settings for DSL.

## NETWORK TOOLS -- PRINTER

Allows you to manage printer.

## IGMP Proxy

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

### IGMP PROXY CONFIGURATION

**WAN Interface:** Select the WAN interface you wish to configure.

**IGMP Version:** Select either **IGMP V1**, **IGMP V2**, or **IGMP V3** from the list.

**Enable IGMP Proxy:** Select the LAN connection to use.

**Enable PassThrough:** Select this box to enable **PassThrough**.

Click **Apply** when you are done.

### IGMP TABLE

The current IGMP Proxy Status is listed on this table.



**IGMP PROXY**

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

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

**IGMP PROXY CONFIGURATION**

WAN Connection :

IGMP Version :

Enable IGMP Proxy :

Enable PassThrough :

**IGMP TABLE**

Group Address	Interface	State

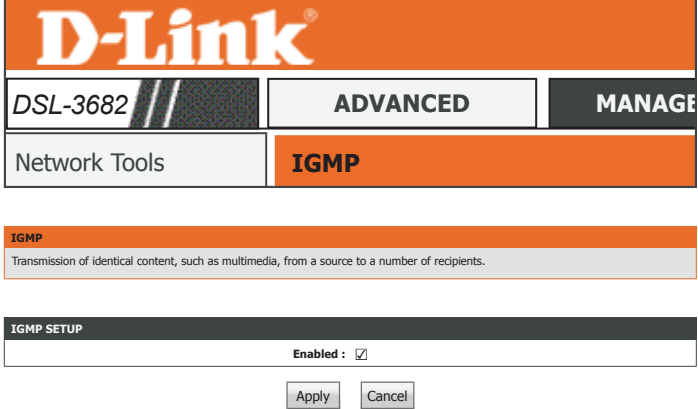
## IGMP Snooping

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

### IGMP SETUP

**Enable IGMP:** Check this box to enable IGMP.

Click **Apply** when you are done.



The screenshot shows the D-Link DSL-3682 web interface. At the top, there is a navigation bar with the D-Link logo, the model number DSL-3682, and tabs for ADVANCED and MANAGE. Below this is a sub-menu with Network Tools and IGMP. The IGMP section is highlighted. A description of IGMP is provided: "Transmission of identical content, such as multimedia, from a source to a number of recipients." The IGMP SETUP section shows the "Enabled" checkbox checked. At the bottom, there are "Apply" and "Cancel" buttons.

D-Link®	
DSL-3682	ADVANCED
MANAGE	
Network Tools	IGMP
IGMP	
Transmission of identical content, such as multimedia, from a source to a number of recipients.	
IGMP SETUP	
Enabled : <input checked="" type="checkbox"/>	
Apply	Cancel

# UPnP

This page is used to configure UPnP. UPnP helps to automatically configure software and devices on your network to access the resources they require.

## UPNP SETUP

**Enable UPnP:** Enable or disable UPnP.

Click **Apply** when you are done.

## UPNP PORT LIST

The currently configured UPnP rules are displayed here.

The screenshot shows the D-Link DSL-3682 web interface. At the top is the D-Link logo. Below it is a breadcrumb trail: DSL-3682 // ADVANCED // MANAGE. A navigation menu shows 'Network Tools' and 'UPNP'. The main content area is titled 'UPNP' and contains a sub-section 'UPNP SETUP' with a checked 'Enable UPnP' checkbox and 'Apply' and 'Cancel' buttons. Below this is a section titled 'UPNP PORT LIST' with a table header containing columns for Protocol, External Port, Server IP, Internal Port, and Description.

## DSL

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

### DISPLAY LIST

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

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

Click **Apply** when you are done.

The screenshot shows the D-Link DSL-3682 Advanced DSL Settings page. At the top, there is a navigation bar with the D-Link logo, the model number DSL-3682, and tabs for ADVANCED and MANAGE. Below the navigation bar, there is a 'Network Tools' section with a 'DSL SETTINGS' button. The DSL SETTINGS section contains a warning message: 'This page is used to configure the DSL settings of your DSL router. You need to disable DSL before you change the DSL mode.' Below the warning, there is a 'DISPLAY LIST' section with two dropdown menus: 'xDSL Mode' set to 'Auto Sync-Up' and 'xDSL Type' set to 'ANNEX A/T1/J/L/M'. An 'Apply' button is located at the bottom of the settings area.

# Printer

This page lets you set configure the print server.



**Enable:** Check this box to enable the print server.

**Printer Name:** Enter a network name for the printer.

**URL:** The url to access the printer is displayed here.

## DISPLAY LIST

The currently configured printers are displayed here.

The header of the configuration page features the D-Link logo in an orange bar. Below it, the model number 'DSL-3682' is shown next to a signal strength indicator. To the right are two tabs: 'ADVANCED' (selected) and 'MANAGE'. Below these is a 'Network Tools' section with a sub-tab for 'PRINT SERVER SETTINGS'.

**PRINT SERVER SETTINGS**  
 This page allows you to enable/disable printer support

Enable :

Printer Name :

URL : <http://192.168.1.1:631/printers/Printer>

DISPLAY LIST			
Manufacturer	Model	CMD	Firmware Version
UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN

Apply Cancel

# Routing

Product Page: DSL-3682

Firmware Version: EU\_1.00



<b>DSL-3682</b>	<b>SETUP</b>	<b>ADVANCED</b>	<b>MANAGEMENT</b>	<b>STATUS</b>	<b>HELP</b>
2.4G Advanced Wireless	QoS	<div style="border: 1px solid black; padding: 5px;"> <p><b>STATIC ROUTE</b></p> <p>Static Route.</p> <div style="text-align: center; margin-top: 20px;"> <input type="button" value="Static Route"/> </div> </div>			
5G Advanced Wireless	Anti-Attack Settings				
ALG	DNS				
Port Forwarding	Dynamic DNS				
Port Trigger	Network Tools				
DMZ	<b>Routing</b>				
SAMBA	FTP				
3G/4G Configuration	Budget Quota				
Parental Control	Logout				



## Static Route

The Static Routes section allows you to define custom routes to control how data traffic is moved around your network.

### ROUTING -- STATIC ROUTE

The currently defined Static Routes are displayed here. A total of 30 static routes may be defined. If you wish to create a new rule, click the **Add** button. If you wish to remove a rule, select it from the table and click the **Delete** button. If you wish to edit a rule, select it from the table and click the **Edit** button.

### STATIC ROUTE ADD

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

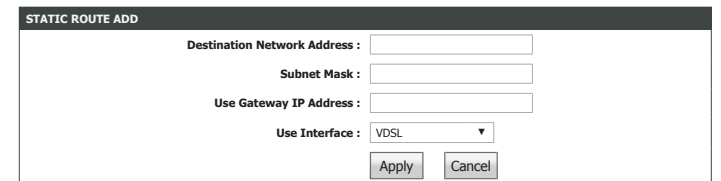
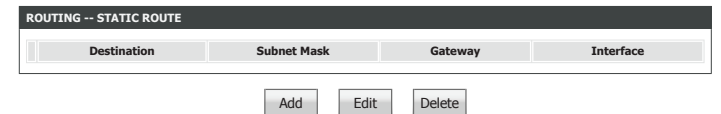
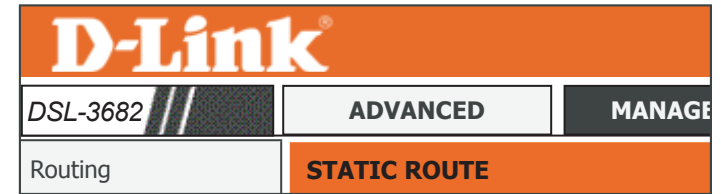
**Subnet Mask:**

**Use Gateway IP Address:** Enter the subnet mask of the destination IP address.

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

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

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



## IPV6 Static Route

The Static Routes section allows you to define custom routes to control how data traffic is moved around your network.

### ROUTING -- STATIC ROUTE

The currently defined Static Routes are displayed here. A total of 30 static routes may be defined. If you wish to create a new rule, click the **Add** button. If you wish to remove a rule, select it from the table and click the **Delete** button. If you wish to edit a rule, select it from the table and click the **Edit** button.

### IPV6 STATIC ROUTE ADD

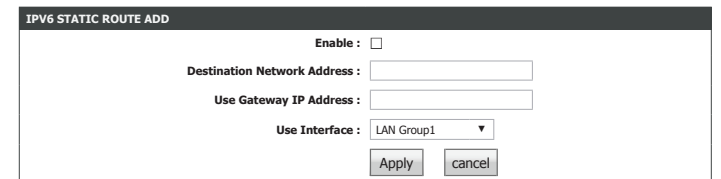
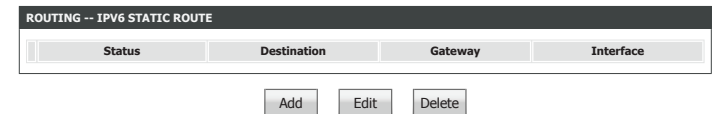
**Enable:** Check this box to enable this route.

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

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

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

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



# FTPD

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682

**SETUP****ADVANCED****MANAGEMENT****STATUS****HELP**2.4G Advanced  
Wireless

QoS

5G Advanced Wireless

Anti-Attack Settings

ALG

DNS

Port Forwarding

Dynamic DNS

Port Trigger

Network Tools

DMZ

Routing

SAMBA

FTPD

3G/4G Configuration

Budget Quota

Parental Control

Logout

## FTPD Setting

From this page you can configure the FTP server. Refer to **FTPD Account** on page **104** for more information on configuring FTP accounts.

### FTP SERVER SETTING

**FTP Server:** Displays the FTP server status.

**Enable FTP Server:** Enable or disable the FTP server.

**FTP Server Port:** Enter the port number to be used for FTP. The default is **2121**.

Click **Submit** to have your changes take effect.

The screenshot shows the top navigation bar of the D-Link DSL-3682 configuration page. The D-Link logo is on the left. Below it, there are three tabs: 'DSL-3682 //', 'ADVANCED', and 'MANAGE'. Under the 'DSL-3682 //' tab, there are two sub-tabs: 'FTPD' and 'FTP'. The 'FTP' sub-tab is currently selected and highlighted in orange.

The screenshot shows the header of the FTP configuration page. It has an orange bar with the text 'FTP' in white. Below this bar is a grey bar with the text 'You can Enable or Disable ftp server, and set ftp port here.'

The screenshot shows the 'FTP SERVER SETTING' form. It has a dark grey header with the text 'FTP SERVER SETTING' in white. Below the header, there are three fields: 'FTP Server : Off' (a dropdown menu), 'Enable FTP Server : ', and 'FTP Server Port : 2121' (a text input field). At the bottom of the form, there are two buttons: 'Submit' and 'Cancel'.

## FTPD Account

From this page you can configure the FTP server. Refer to **FTPD Setting** on page **103** for more information on configuring FTP accounts.

### FTP USER MANAGE

From this box you may add FTP user accounts.

**Username:** Enter a desired username.

**Password:** Enter a desired username.

**Rights:** Select the file access rights for the user.

Click **Append** to add this user.

### ACCOUNT TABLE

This table displays the currently configured FTP user accounts. To change a user's settings, click **Edit**. To delete a user account, click **Delete**.

The screenshot shows the top navigation bar with the D-Link logo and the model number DSL-3682. Below the logo are three tabs: 'ADVANCED' (selected), 'MANAGE', and 'MANAGE'. Underneath, there are two sub-tabs: 'FTPD' and 'FTP' (selected).

**FTP**  
You can manage ftp user information here, such as username, password, and rights.

**FTP USER MANAGE**

Username :

Password :

Rights  View  Upload  Download

**ACCOUNT TABLE**

No.	User	Password	Rights			Operation
			View	Upload	Download	

# Budget Quota

If your Internet service plan has a data cap that limits the total amount of data you can transfer, or charges you based on the amount of data you transfer, you can use the Budget Quota function to help manage your usage. Once the budget quota is exhausted, the router blocks Internet access.

## TRAFFIC QUOTA

The currently defined budget quotas are displayed here. A total of 30 static routes may be defined. If you wish to create a new rule, click the **Add** button. If you wish to remove a rule, click its corresponding trash icon. If you wish to edit a rule, click its corresponding pencil icon.

## BUDGET QUOTA SETTINGS

**Select Interface:** Select the interface to apply the budget to.

**Enable Current Rule:** Check the box to enable the budget quota.

**Limit Times(days):** Enter number of days to enforce the budget quota.

**Start Router Time:** The budget quota start time is displayed here.

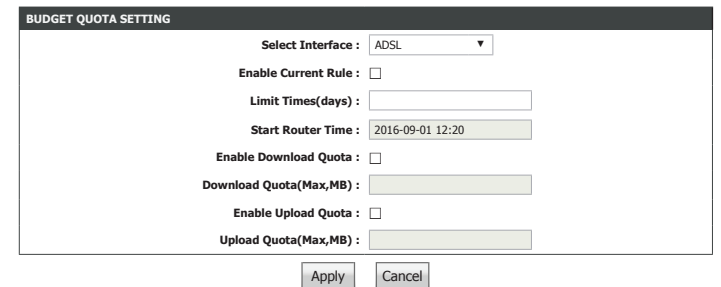
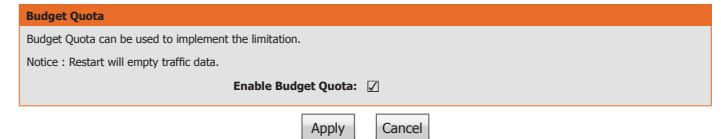
**Enable Download Quota:** Check this box to enable the download quota.

**Download Quota(Max,MB):** Enter the maximum download quota in megabytes(MB)

**Enable Upload Quota:** Check this box to enable the upload quota.

**Upload Quota(Max,MB):** Enter the maximum upload quota in megabytes(MB)

Click **Apply** to add this budget quota.



# Logout

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



# Management

The Maintenance tab provides access to administration related settings of your DSL-3682.

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

System

Firmware Update

Access Controls

Diagnostics

System Log

Logout

## SYSTEM -- REBOOT

Click the button below to reboot the router.

Reboot

## SYSTEM -- BACKUP SETTINGS IN DSL ROUTER

The last correct settings information:

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

Backup Setting

## SYSTEM -- UPDATE SETTINGS

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

**Settings File Name:** Choose File No file chosen

Update Setting

## SYSTEM -- RESTORE DEFAULT SETTINGS

Restore DSL Router settings to the factory defaults.

Restore Default Setting



# Firmware Update

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

## FIRMWARE UPDATE

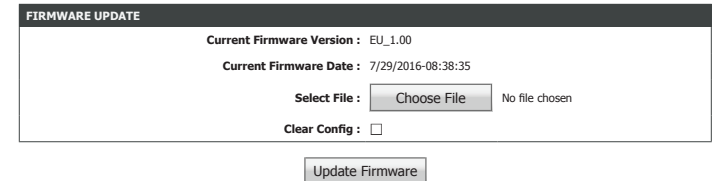
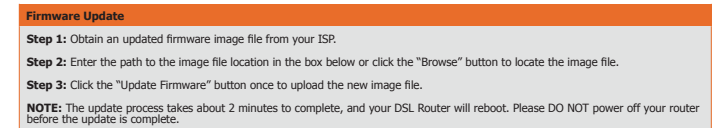
**Current Firmware Version:** This field displays information about the current firmware.

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

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

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

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



# Access Controls

The **Access Controls** option provides tools for managing access to the router.

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

System

Firmware Update

Access Controls

Diagnostics

System Log

Logout

## ACCESS CONTROLS -- ACCOUNT PASSWORD

Manage DSL Router user accounts.

[Account Password](#)

## LOCAL ACCESS CONTROLS

Manage Local Access Control List .

[LACL](#)

## REMOTE ACCESS CONTROLS

Manage Remote Access Control List.

[RACL](#)

## ACCESS CONTROLS -- IP ADDRESS

Permits access to local management services.

[IP Address](#)

## Account Password

The Account Password section enables you to manage the router password. You should change the default admin password to secure your network. Ensure that you remember the new password or write it down and keep it in a safe and separate location for future reference. If you forget the password, you will need to reset the device to the factory default settings and all configuration settings of the device will be lost.

### ACCOUNT PASSWORD

**Username:** Select the username that you want to modify.

**Current Password:** Enter the current password.

**New Password:** Enter the new password.

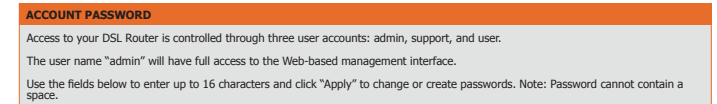
**Confirm Password:** Re-enter the new password.

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

### WEB IDLE TIME OUT SETTINGS

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

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



The screenshot shows the 'ACCOUNT PASSWORD' form. It includes a dropdown menu for 'Username' with 'admin' selected, and three text input fields for 'Current Password', 'New Password', and 'Confirm Password'. Below the form are 'Apply' and 'Cancel' buttons.

The screenshot shows the 'WEB IDLE TIME OUT SETTINGS' section. It features a text input field for 'Web Idle Time Out' with a value of '5' and a unit of '(5 ~ 30 minutes)'. Below the field are 'Apply' and 'Cancel' buttons.

## Local Access Control

The Local Access Control section enables you to specify which services can be accessed by a host on the local network. This page is used in conjunction with the IP Address ACL option. Be careful when adding or deleting ACL rules, as you may accidentally lock yourself out of the router, requiring the device to be reset.

### LOCAL ACCESS CONTROL -- SERVICE

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

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

### IPV4 ACL

Select and configure the services you wish to enable. Click **Submit** to have your changes take effect.

The screenshot shows the top navigation bar with the D-Link logo and the model number DSL-3682. Below the navigation bar, there are tabs for 'MANAGEMENT' and 'STATUS'. The 'LOCAL ACCESS CONTROL' section is highlighted in orange. Below this, there is a sub-section for 'LOCAL ACCESS CONTROL' with a note: 'You can set a service control list (SCL) to enable or disable services from being used.'

**LOCAL ACCESS CONTROL -- SERVICE**

Enable Local Access :

Choose A Connection : Lan1 ▼

**IPV4 ACL**

Service	Enable	Source IP	Source Mask	Protocol	Port
FTP	<input type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	21
HTTP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	80
ICMP	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	ICMP	-
SNMP	<input type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	161
SSH	<input type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	22
TELNET	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	23
TFTP	<input type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	69
DNS	<input checked="" type="checkbox"/>	0.0.0.0	0.0.0.0	UDP	53
TR069	<input type="checkbox"/>	0.0.0.0	0.0.0.0	TCP	7547

Submit Refresh

# Remote Access Control

The Remote Access Control section enables you to specify which services can be accessed remotely over the Internet.

## REMOTE ACCESS CONTROL -- SERVICE

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

## IPV4 ACL

Select and configure the services you wish to enable. Click **Submit** to have your changes take effect.

The image shows the top navigation bar of the D-Link DSL-3682 web interface. It includes the D-Link logo, the model number 'DSL-3682', and two main tabs: 'MANAGEMENT' and 'STATUS'. Under the 'MANAGEMENT' tab, there are two sub-tabs: 'Access Controls' and 'REMOTE ACCESS CONTROL', with the latter being highlighted in orange.

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

**REMOTE ACCESS CONTROL -- SERVICE**  
 Choose A Connection :

**IPV4 ACL**

Service	Enable	Source IP	Source Mask	Protocol	Port
ICMP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	ICMP	-
SNMP	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	<input type="text" value="161"/>
FTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="21"/>
HTTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="80"/>
SSH	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="22"/>
TELNET	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="23"/>
TFTP	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	<input type="text" value="69"/>
DNS	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	UDP	<input type="text" value="53"/>
TR069	<input checked="" type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	TCP	<input type="text" value="7547"/>

## IP Address

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

### ACCESS CONTROL -- IP ADDRESSES

**Enable Access Control Mode:** Click to enable ACL mode.

The currently defined IP Address on the ACL are displayed here. If you wish to add a new address to the table, click the **Add** button. If you wish to remove a rule, select it from the table and click the **Delete** button.

### IP ADDRESS

**IP Address:** Enter an IP Address to add to the ACL.

Click **Apply** to add the IP address to the Access Control list.

<b>D-Link</b>		
DSL-3682	<b>MANAGEMENT</b>	<b>STATUS</b>
Access Controls	<b>IP ADDRESS</b>	

#### IP ADDRESS

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

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

<b>ACCESS CONTROL -- IP ADDRESSES</b>	
<input checked="" type="checkbox"/> <b>Enable Access Control Mode</b>	
	IP

<b>IP ADDRESS</b>	
	IP Address : <input type="text"/>

# Diagnostics

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

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

System

Firmware Update

Access Controls

Diagnostics

System Log

Logout

## DIAGNOSTICS -- DSL TEST

DSL Test can diagnostics your DSL connection.

## DIAGNOSTICS -- TRACEROUTE

Traceroute diagnostics sends packets to determine the routers on the Internet.

## DIAGNOSTICS -- PING

Ping diagnostics used to test the reachability of a host on a network and to measure the round-trip time for messages sent from the originating host to a destination computer.

## DIAGNOSTICS -- ATM5

ATM5 diagnostics can diagnostics your adsl connection and list detail information.

# DSL 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.

## DIAGNOSTICS

Select your WAN Connection and click **Run Diagnostic Test** to run the diagnostics tests.

The image shows the top navigation bar of the D-Link DSL-3682 web interface. It features the D-Link logo in an orange bar. Below it, there are three tabs: 'DSL-3682' (selected), 'MANAGEMENT', and 'STATUS'. Under the 'DSL-3682' tab, there are two sub-tabs: 'Diagnostics' (selected) and 'DIAGNOSTICS'.

**DIAGNOSTICS**

The DSL router can test your DSL connection. The individual tests are listed below. If a test displays a fail status, click the "Run Diagnostic Test" button again to make sure the fail status is consistent.

WAN Connection:

**TEST THE CONNECTION TO YOUR LOCAL NETWORK**

Test your LAN 1 Connection	PASS
Test your LAN 2 Connection	PASS
Test your LAN 3 Connection	PASS
Test your LAN 4 Connection	PASS
Test your 2.4G Wireless Connection	PASS
Test your 5G Wireless Connection	PASS

**TEST THE CONNECTION TO YOUR DSL SERVICE PROVIDER**

Test DSL Synchronization	PASS
Test ATM OAM F5 Segment Loopback	PASS
Test ATM OAM F5 End-to-end Loopback	PASS
Test ATM OAM F4 Segment Loopback	PASS
Test ATM OAM F4 Segment Loopback	PASS

**TEST THE CONNECTION TO YOUR INTERNET SERVICE PROVIDER**

Ping Default Gateway	PASS
Ping Primary Domain Name Server	PASS



## Traceroute

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



Configure your settings and click **Traceroute** to run the test.

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

**WAN Connection:** Select the connection you wish to run the traceroute from.

**Host:** Enter a host to run a traceroute against.

**MaxTTL:** Enter a maximum value for TTL.

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



The results of the traceroute test are displayed here.



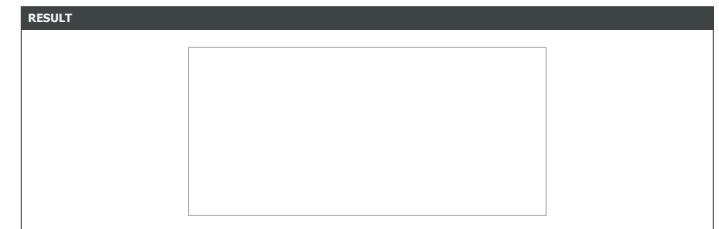
Protocol :  ▼

WAN Connection :  ▼

Host :

Max TTL :  (1-64)

Wait Times :  (>1ms)



# Ping

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



Configure your settings and click **Traceroute** to run the test.

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

**Host:** Enter a host to ping.

**Number of retries:** Enter a value for the number of times you would like to ping the host.

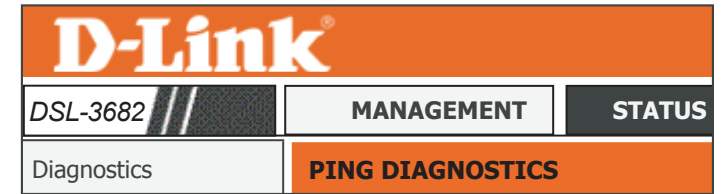
**Timeout:** Enter a timeout value before a failure is declared.

**Packet Size:** Enter a value for the ping packet size.

**WAN Connection:** Select a WAN connection from the drop-down menu to use for the ping test.

## RESULT

The results of the ping test are displayed here.



Protocol :

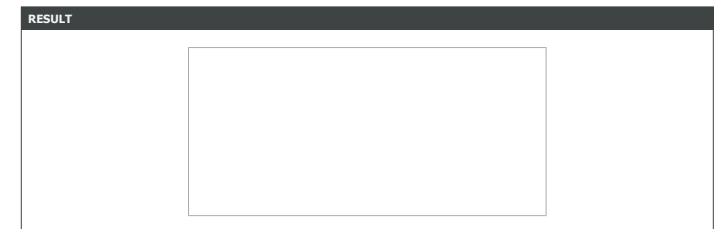
Host :

Number of retries :

Timeout :

Packet Size :

WAN Connection :



## ATMF5

The ATMF5 section enables you to run tests on your ATM WAN connection.

### ATM F5 DIAGNOSTIC

**WAN Connection:** Select the WAN connection to run the ATM test on

**Command:** Enter a command to run.

**Number Of Repetitions:** Enter a value for the number of times you would like repeat the command.

**Timeouts:** Enter a timeout value before a failure is declared.

Click **Run Diagnostic Test** to run the diagnostics tests.

### RESULT

The results of the ATMF5 test are displayed here.

The screenshot shows the D-Link DSL-3682 web interface. At the top, there is a navigation bar with 'DSL-3682' on the left, 'MANAGEMENT' in the center, and 'STATUS' on the right. Below this, there are two tabs: 'Diagnostics' and 'ATM F5 DIAGNOSTIC', with the latter being the active tab.

The screenshot shows the 'ATM F5 DIAGNOSTIC' configuration form. It includes a warning message: 'this is a atm f5 diagnostics page. the wan connection must be adsl connection'. The form has the following fields:

- WAN Connection:** A dropdown menu currently set to 'VDSL'.
- Command:** A text input field.
- NumberOfRepetitions:** A text input field.
- Timeout(s):** A text input field.

Run Diagnostic Tests

RESULT	
Success Count	
Failure Count	
Minimum Response Time	
Maximum Response Time	
Average Response Time	

# System Log

The DSL-3682 keeps a running log of events and activities occurring on the router. You may send these logs to a SysLog server on your network.

## SYSTEM LOG -- CONFIGURATION

Configure your settings and click **Traceroute** to run the test.

**Enable Log:** Check to enable or disable logging

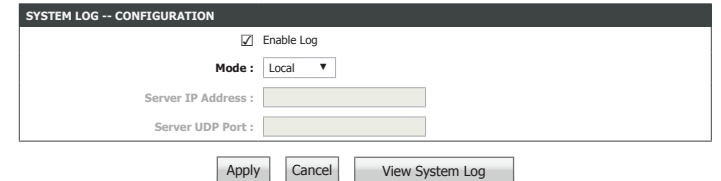
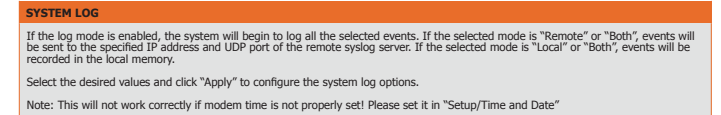
**Mode:** Select to record the log to **Local**, **Remote**, or **Both**.

**Server IP Address:** Enter an IP address for the remote logging server.

**Server UDP Port:** Enter the UDP port of the remote server.

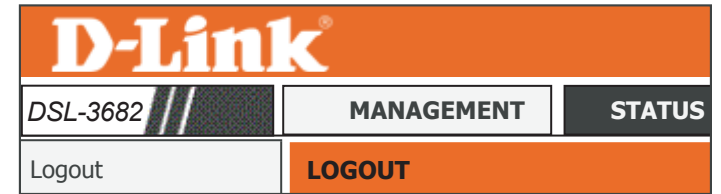
Click **Apply** to have your changes take effect.

You can view the current log by clicking the **View System Log** button.




# Logout

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



# Status

The Status tab provides information about the DSL-3682's current status.

Product Page: DSL-3682		Firmware Version: EU_1.00	
			
<i>DSL-3682</i> //	<b>SETUP</b>	<b>ADVANCED</b>	<b>MANAGEMENT</b>
	<b>STATUS</b>	<b>HELP</b>	
Device Info			
Device Info			
Wireless Clients			
DHCP Clients			
Logs			
Statistics			
Route Info			
Logout			

To return to the Web UI Table of Contents page, simply click the D-Link logo on the top right of each page.

		
<i>DSL-3682</i> //	<b>Setup</b>	<b>Advar</b>
Wizard		

# Device Info

This page displays the current information for the DSL-3682, such as LAN and wireless LAN information and statistics.

## SYSTEM INFO

This section displays a summary of the system settings

## INTERNET INFO

This section displays of the Internet connection settings.

## WIRELESS INFO

This section displays a summary of the wireless network settings.

## LOCAL NETWORK INFO

This section displays a summary of the local network settings.

## STORAGE DEVICE INFO

This section displays a summary of the storage device and its settings.

# D-Link®

DSL-3682	<b>STATUS</b>	<b>HEL</b>
Device Info	<b>DEVICE INFO</b>	

**DEVICE INFO**  
This information reflects the current status of your all connection.

**SYSTEM INFO**

Modem Name :	DSL-3682
Serial Number :	001fa4930a42
Time and Date :	2016-09-01 14:49
HardwareVersion :	A1
Firmware Version :	EU_1.00
System Up Time :	196:53:34

**INTERNET INFO**

Internet Connection Status :

IP Protocol

Internet Connection Status:	Disconnected
Wan service type:	Internet
IP Address:	N/A
Sub Mask:	N/A
Default Gateway:	N/A
DNS Server:	N/A

**Enabled WAN Connections :**

VPI/VCI	Service Name	Protocol	IGMP
N/A	VDSL	PPPoE	Disable
8/35	ADSL	PPPoE	Disable

**WIRELESS INFO**

Select Wireless :

MAC Address:	FF:FF:FF:FF:FF:FF
Status:	Enable
Network Name (SSID):	Your_2.4G Wi-Fi_Network
Visibility:	Visible
Channel :	7
Security Mode:	WPA/WPA2 Mixed

**LOCAL NETWORK INFO**

MAC Address:	FF:FF:FF:FF:FF:FF
IP Address:	192.168.1.1
Subnet Mask:	255.255.255.0
DHCP Server:	Enable

**STORAGE DEVICE INFORMATION**

Volumename	FileSystem	Total Space (MB)	Used Space (MB)

# Wireless Clients

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

## WIRELESS -- AUTHENTICATED STATIONS

This table displays detailed information of the currently connected wireless clients.

The screenshot shows the D-Link DSL-3682 web interface. At the top, there is a navigation bar with the D-Link logo, the model number 'DSL-3682', and a 'STATUS' button. Below this is a breadcrumb trail: 'Wireless Clients' > 'WIRELESS CLIENTS'. The main content area has a sub-header 'WIRELESS CLIENTS' and a message: 'This page shows authenticated wireless stations and their status.' Below this is a table with the following columns: Mac, Associated, Authorized, SSID, and Interface. A 'Refresh' button is positioned below the table.



# DHCP Clients

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

## DHCP LEASES

This table displays current DHCP clients.

**DHCP CLIENTS**  
This information reflects the current DHCP client of your modem.

DHCP LEASES			
Hostname	MAC Address	IP Address	Expires In
A PC	FF:FF:FF:FF:FF:FF	192.168.1.2	687171

Refresh

# Logs

The DSL-3682 keeps a running log of events and network activities passing through the router. If the device is rebooted, the logs are reset.

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

The screenshot displays the D-Link DSL-3682 web interface. At the top, there is a navigation bar with the D-Link logo on the left, and 'DSL-3682', 'STATUS', and 'HELP' on the right. Below this, a secondary navigation bar contains 'Logs' and 'LOGS'. The 'LOGS' option is highlighted in orange. Underneath, a section titled 'LOGS' contains the text: 'This page allows you to view system logs.' Below this is a 'System LOG' section with a white box containing the following information: Manufacturer: D-Link, ProductClass: DSL-3682, SerialNumber: 001fa4930a42, IP: 192.168.1.1, HWVer: A1, SWVer: EU\_1.00. A 'Refresh' button is located at the bottom right of the System LOG section.

# Statistics

The DSL-3682 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. The traffic counter is reset if the router point is rebooted.

## LOCAL NETWORK & WIRELESS

This section displays a statistical summary of the LAN and wireless interfaces.

## INTERNET

This section displays a statistical summary of the Internet connection.

## DSL

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

D-Link®

DSL-3682
STATUS
HEL

Statistics
DEVICE INFO

DEVICE INFO

This information reflects the current status of your all connection.

LOCAL NETWORK & WIRELESS

Interface	Received				Transmitted			
	Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
LAN1	10000	100	0	0	10000	100	0	0
Your_2.4G Wi-Fi_Network	10000	100	0	0	10000	100	0	0
Your_5G Wi-Fi_Network	10000	100	0	0	10000	100	0	0

INTERNET

Service	VPI/VCI	Protocol	Received				Transmitted			
			Bytes	Pkts	Errs	Rx drop	Bytes	Pkts	Errs	Tx drop
VDSL	N/A	PPPoE	10000	100	0	0	10000	100	0	0
ADSL	N/A	PPPoE	10000	100	0	0	10000	100	0	0

DSL

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

# Route Info

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

**D-Link®**

<i>DSL-3682</i> //	<b>STATUS</b>	<b>HELP</b>
Route Info	<b>ROUTE INFO</b>	

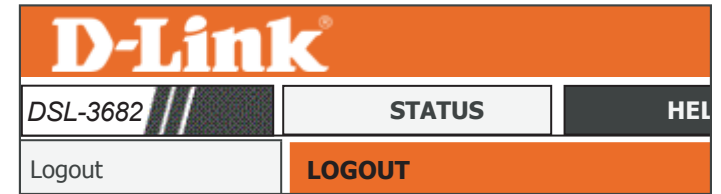
**ROUTE INFO**

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

DEVICE INFO -- ROUTE						
Destination	Gateway	Subnet Mask	Flags	Metric	Service	Service
192.168.5.0	0.0.0.0	255.255.255.0	U	0	0	br0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	br0
239.0.0.0	0.0.0.0	255.255.255.0	U	0	0	eth0

# Logout

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



# Help

The Help section provides documentation for each section of the web-based configuration utility.

Product Page: DSL-3682

Firmware Version: EU\_1.00



DSL-3682

SETUP

ADVANCED

MANAGEMENT

STATUS

HELP

Menu

Setup

Advanced

Management

Status

Logout

## HELP MENU

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

## SETUP HELP

- [Wizard](#)
- [Internet Setup](#)
- [Wireless Setup](#)
- [5G Wireless Setup](#)
- [Local Network](#)
- [Local IPv6 Network](#)
- [Time and Date](#)

## ADVANCED HELP

- [2.4G Advanced Wireless](#)
- [5G Advanced Wireless](#)
- [ALG](#)
- [Port Forwarding](#)
- [DMZ](#)
- [SAMBAs](#)
- [Parental Control](#)

# Connect a USB Storage Device

After you have successfully installed and configured your D-Link Modem Router, you are ready to enjoy the benefits of D-Link's USB sharing technology. D-Link's USB sharing technology allows you to quickly and easily share a USB printer or USB storage device with multiple computers on your network.

## Configure USB Storage

The DSL-3682 will share a FAT32 or NTFS-formatted USB storage device using the SAMBA file sharing protocol. Once connected, you can copy, move, delete, and edit files like you would with any ordinary drive attached to your computer. Refer to **SAMBA** on page **81** for information on configuring the SAMBA settings.

Connect a USB storage device to the USB port on the DSL-3682. Confirm the USB light on the display panel is lit solid green.

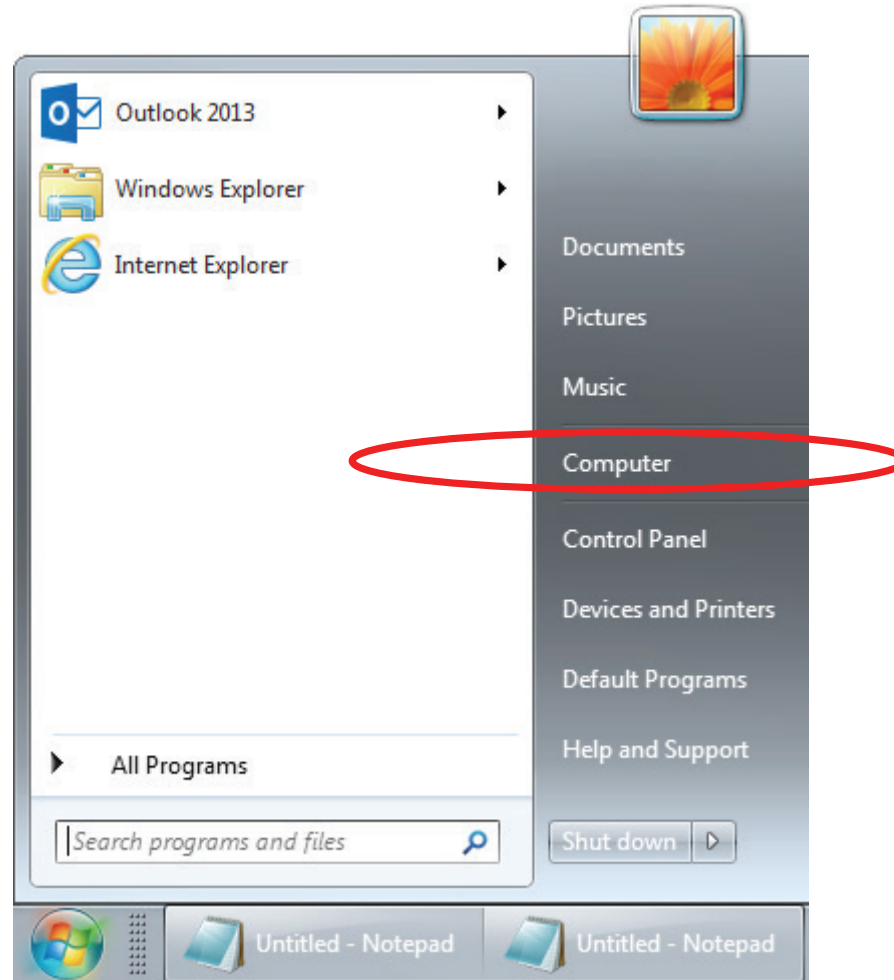


USB Storage



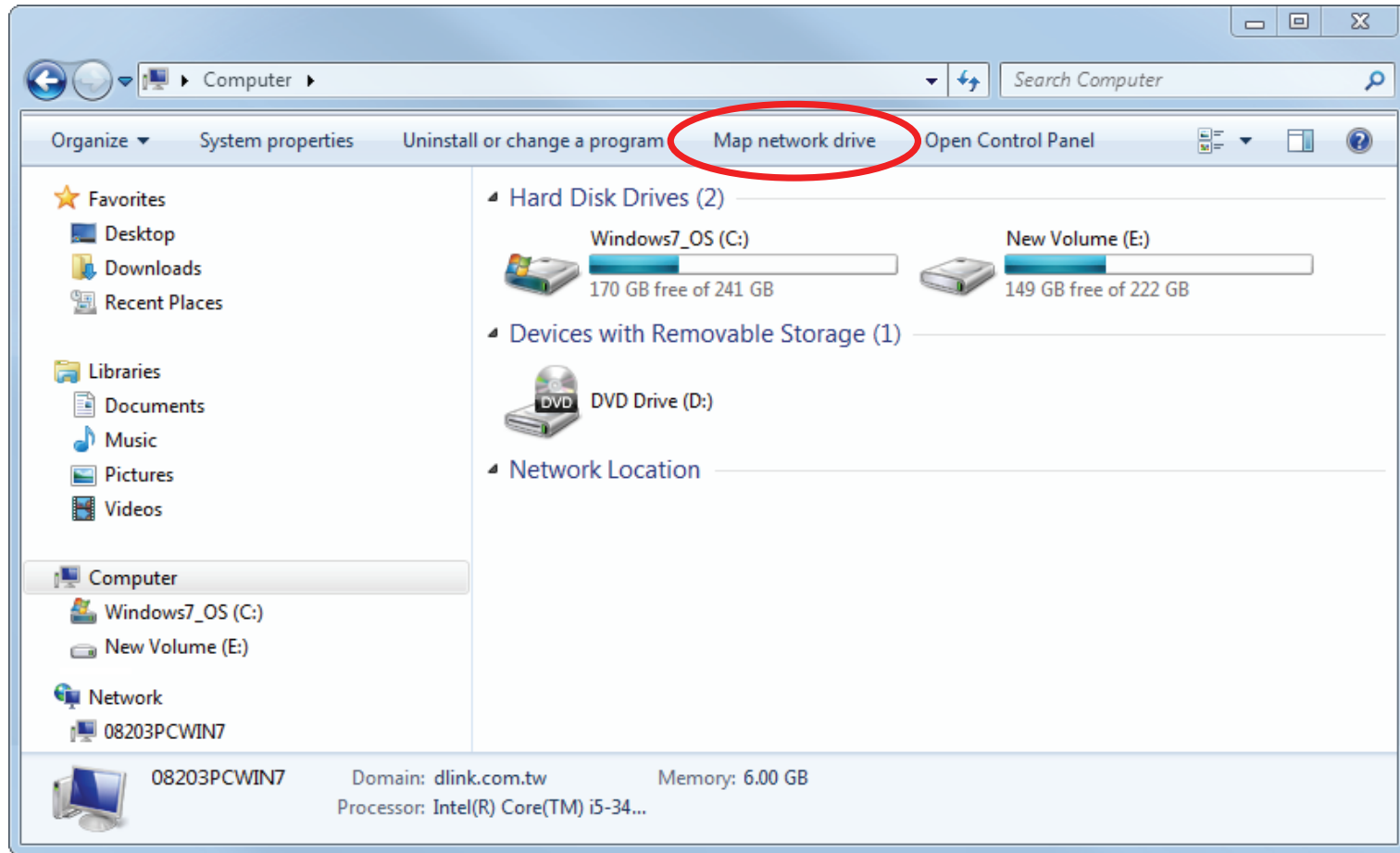
# Connecting from a Windows Based PC

**Step 1** - Click the start menu and select **Computer**.





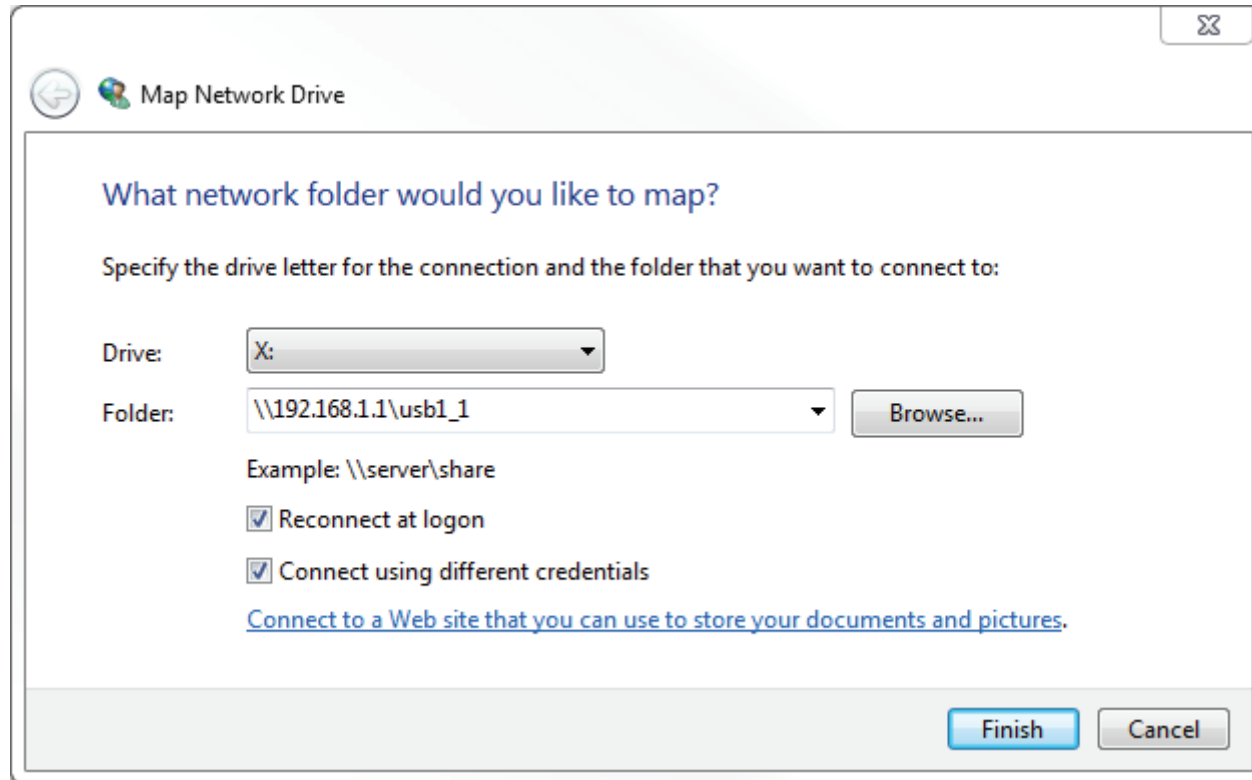
**Step 2 - Click Map network drive.**



**Step 3** - Select the drive letter you wish to map your network drive to. Enter the DSL-3682's IP address and the name of the USB volume you wish to share. For example `\\192.168.1.1\usb1_1`.

Check the boxes **Reconnect at logon** and **Connect using different credentials**.

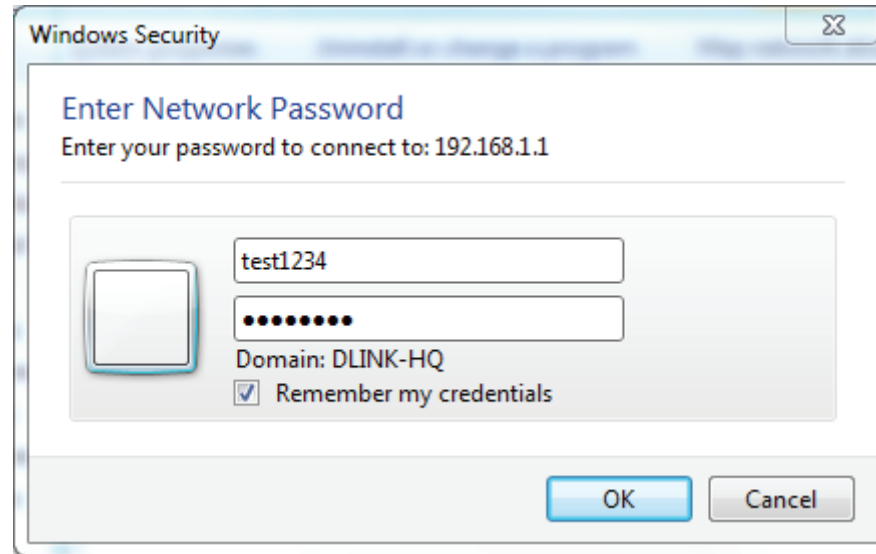
Click **Finish**.



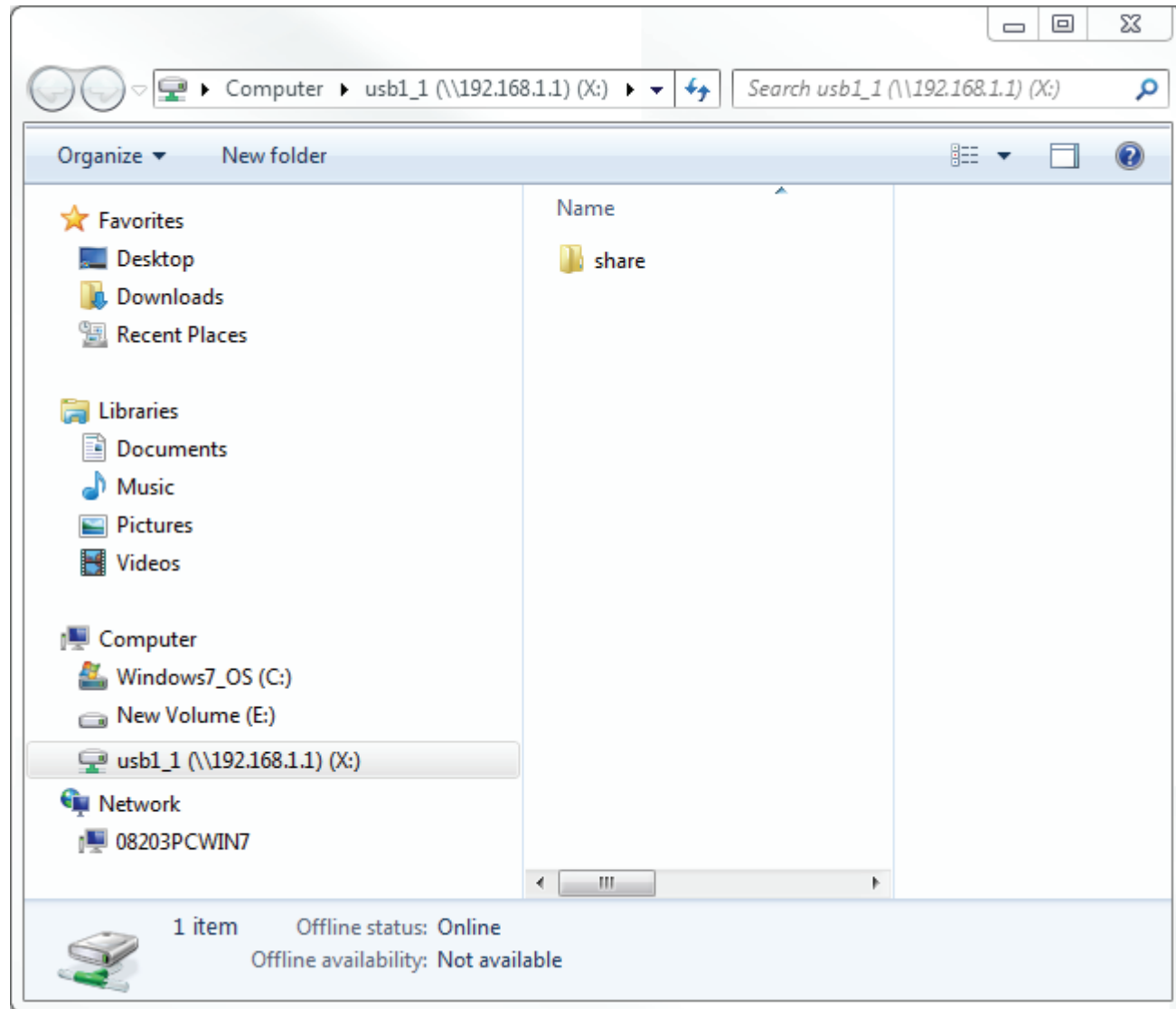
If you have multiple USB storage devices attached via a USB Hub, consult the **Status > Device Info > Storage Device Information** section of the DSL-3682's Web Configuration utility for a list of available volume names.

**Step 4** - If you unchecked **Enable Anonymous Access**, enter your account username and SAMBA password.

Click **OK**.



**Step 5** - A folder of the shared USB storage device will appear.

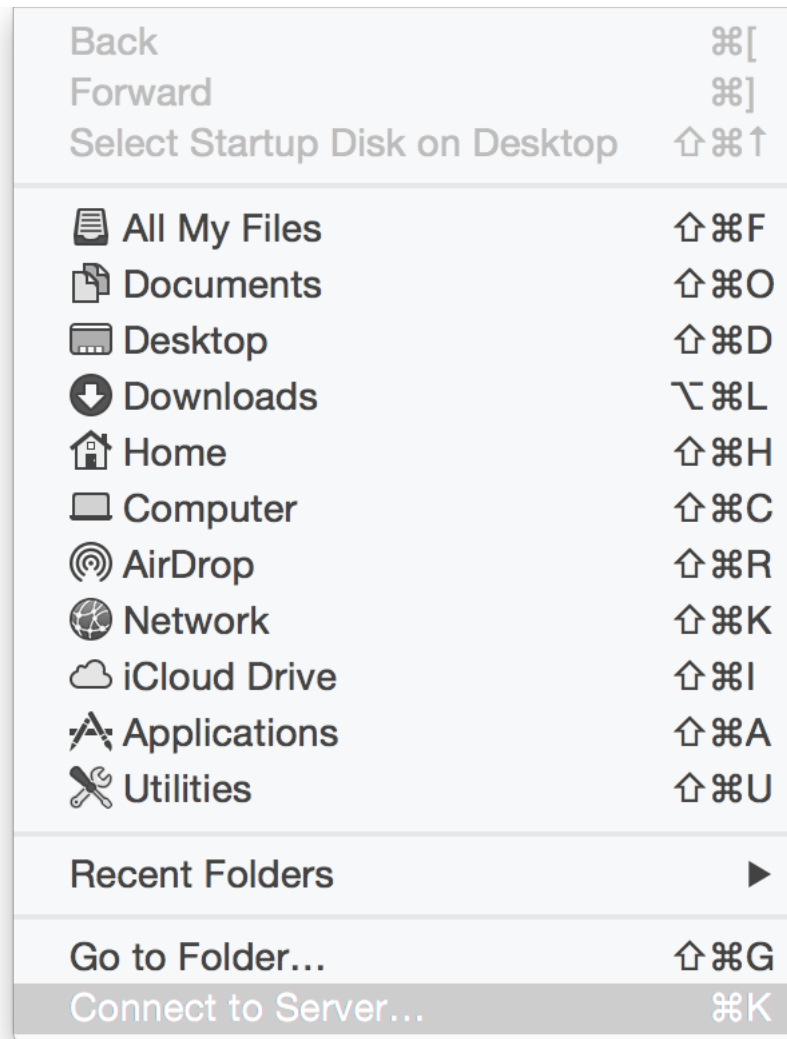


Congratulations

Your files are now shared. Repeat this process from each Windows PC you wish to share your USB drive with.

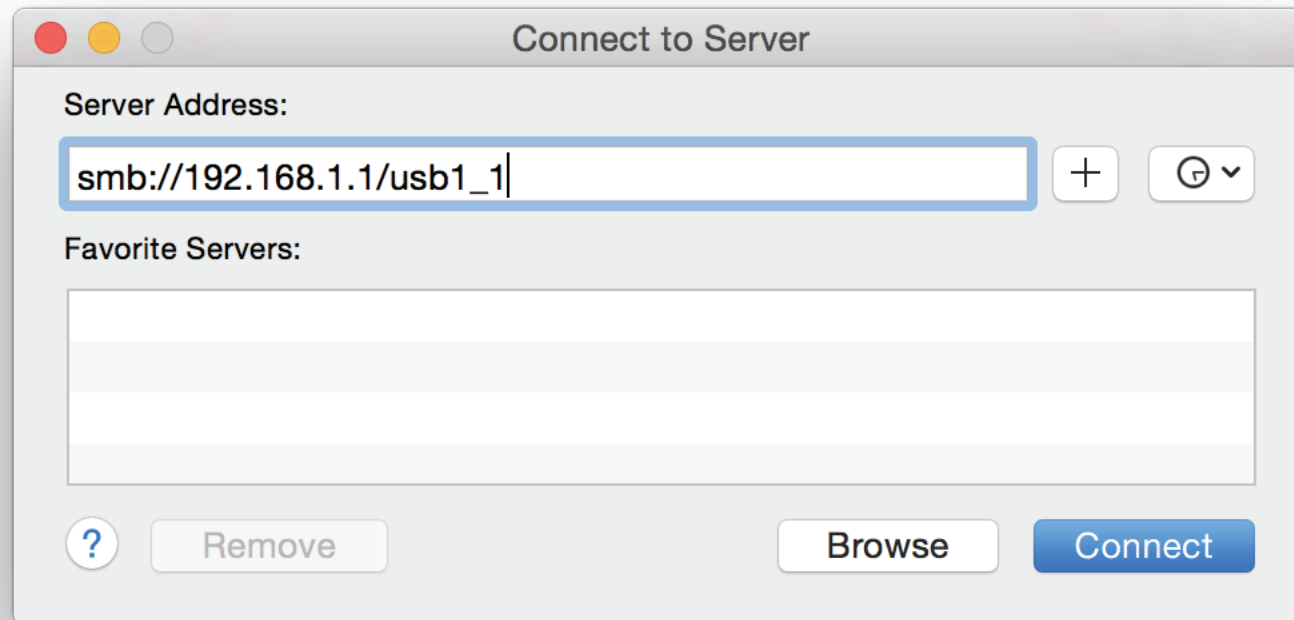
## Connecting from a Mac

**Step 1** - While in Finder, click on the **Go** menu and select **Connect to Server...**



**Step 2** -Enter the DSL-3682's IP address and the name of the USB volume you wish to share.  
For example **smb://192.168.1.1/usb1\_1**.

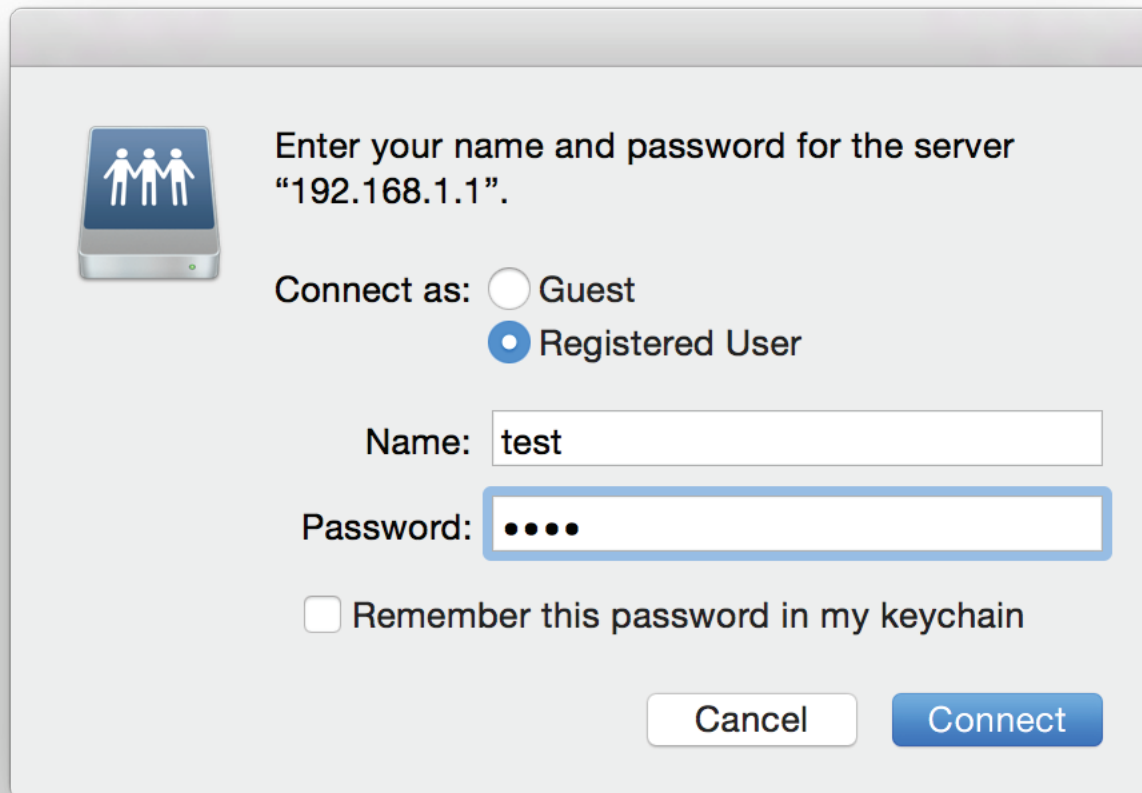
Click **Connect**.



If you have multiple USB storage devices attached via a USB Hub, consult the **Status > Device Info > Storage Device Information** section of the DSL-3682's Web Configuration utility for a list of available volume names.

**Step 4** - If you unchecked **Enable Anonymous Access**, enter your account username and SAMBA password.

Click **Connect**.



Enter your name and password for the server  
"192.168.1.1".

Connect as:  Guest  
 Registered User

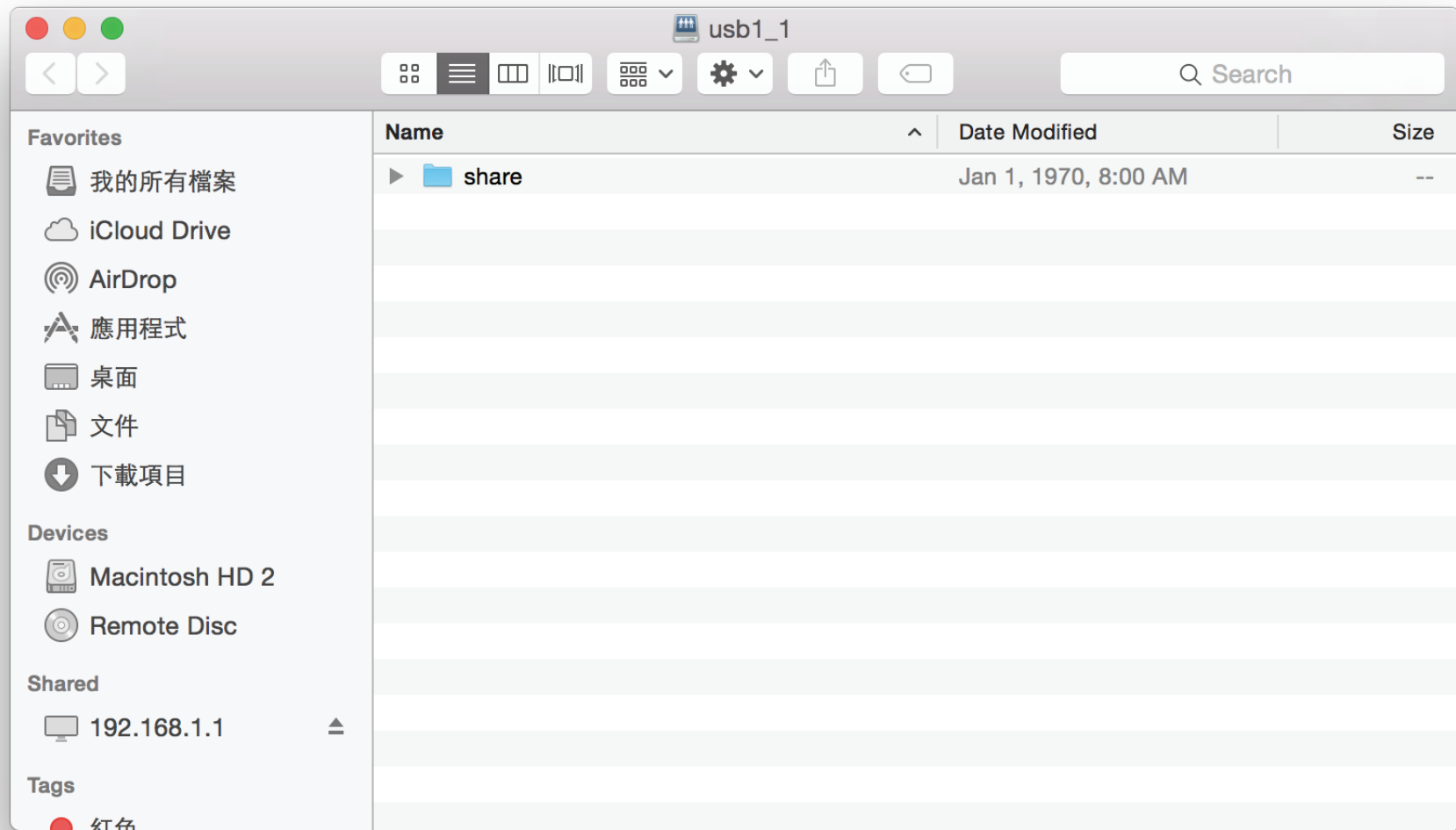
Name: test

Password: ●●●●

Remember this password in my keychain

Cancel Connect

**Step 5** - A folder of the shared USB storage device will appear.





# Connect a Wireless Client to Your Router

## WPS Button

The easiest and most secure way to connect your wireless devices to the router is with 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-3682 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 DSL-3682 which corresponds to the wireless band (2.4 GHz or 5 GHz) supported by the client you are connecting. If you have any doubt regarding WiFi band supported by your client use the 2.4GHz band that is widely supported on all the clients which you would like to connect your device to for about 5 seconds. The WPS LED on the front will start to blink.



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

**Step 3** - Allow up to 1 minute for your connection to be configured. Once the WPS LED stops blinking, you will be connected and your wireless connection will be secure with WPA2.

# Windows® 10

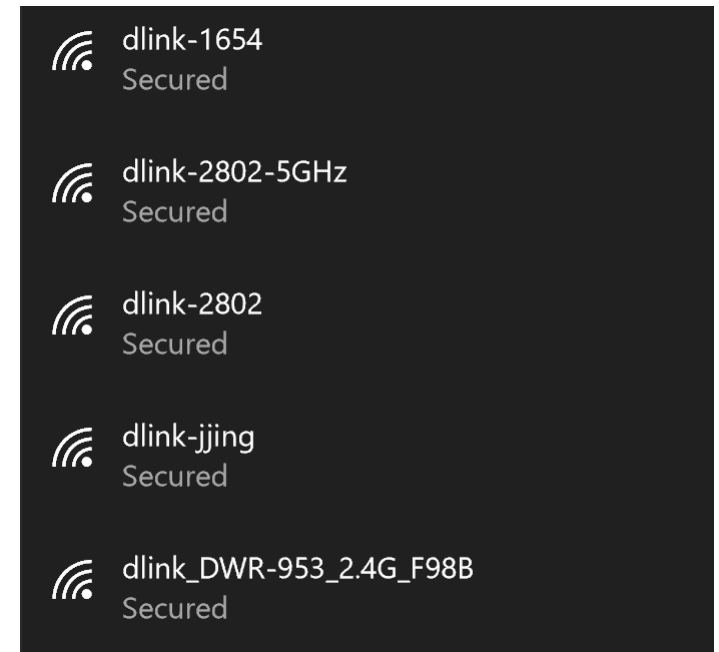
When connecting to the DSL-3682 wirelessly for the first time, you will need to input the wireless network name (SSID) and Wi-Fi password (security key) of the device you are connecting to. If your product has a Wi-Fi configuration card, you can find the default network name and Wi-Fi password here. Otherwise 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.



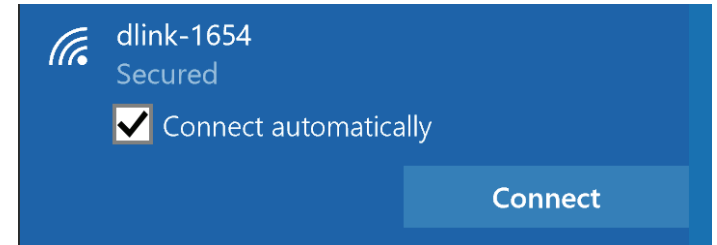
Wireless Icon

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.



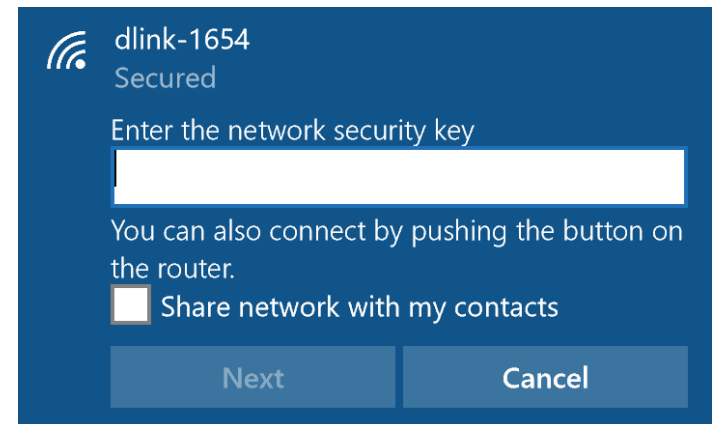
To connect to the SSID, click **Connect**.

To automatically connect to the router when your device 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.

You can also use Wi-Fi Protected Setup (WPS) to connect to the router. Press the WPS button on your D-Link device and you will be automatically connected.



# Windows® 8

## WPA/WPA2

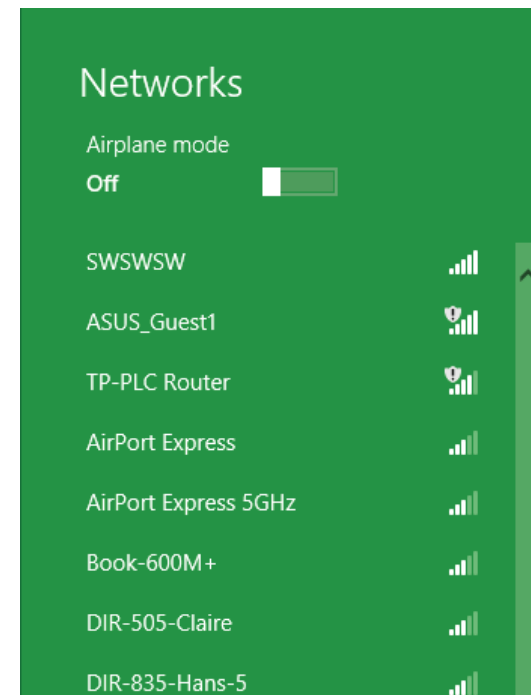
It is recommended that you enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

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



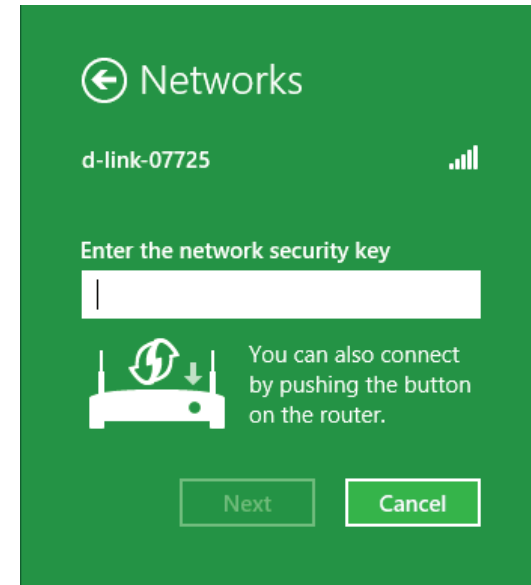
Wireless Icon

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

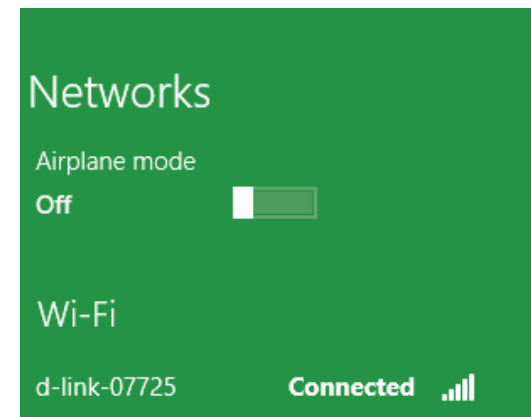


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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 during this step to enable the WPS function.



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

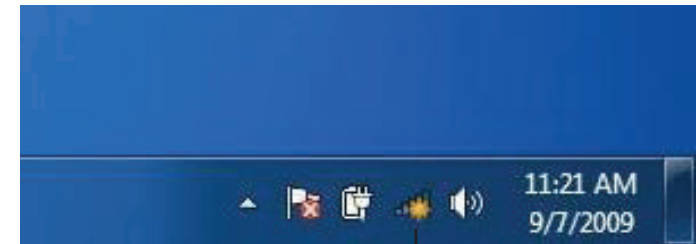


# Windows® 7

## WPA/WPA2

It is recommended that you 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.

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



Wireless Icon

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

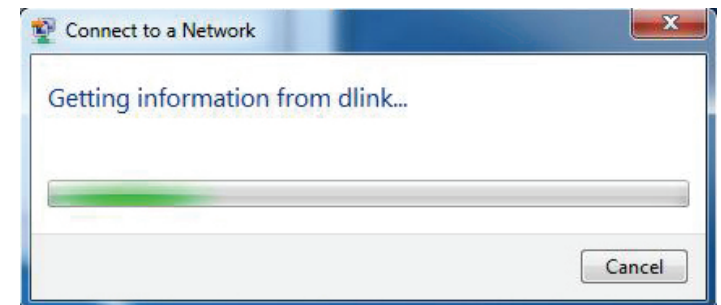


Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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.

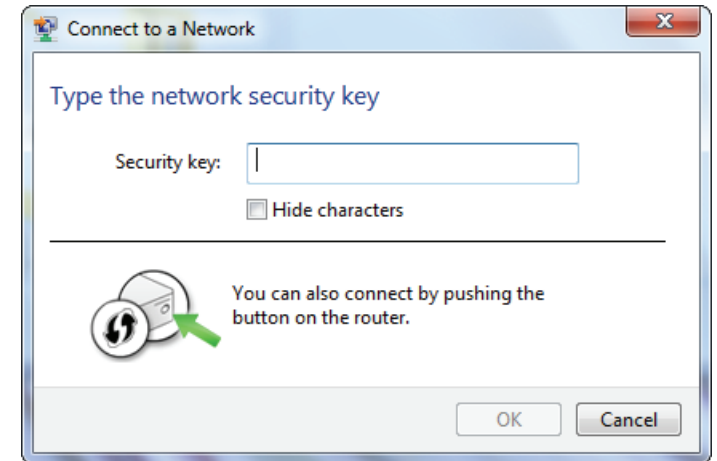


The following window appears while your computer tries to connect to the router.



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 the one on the wireless router.





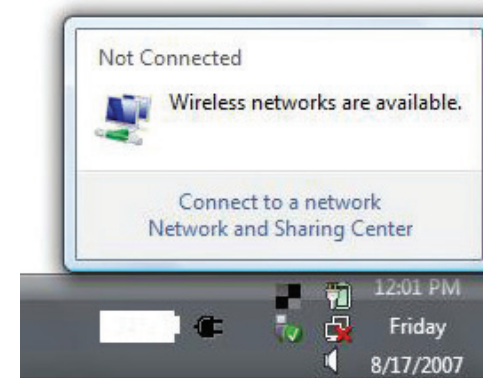
# Windows Vista®

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

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

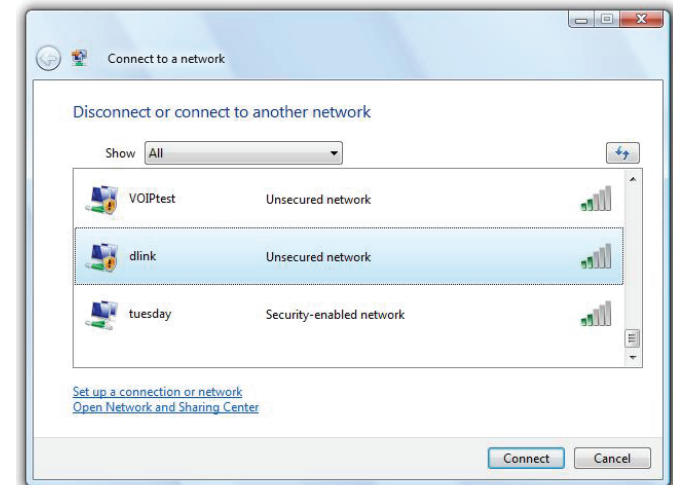
or

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



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

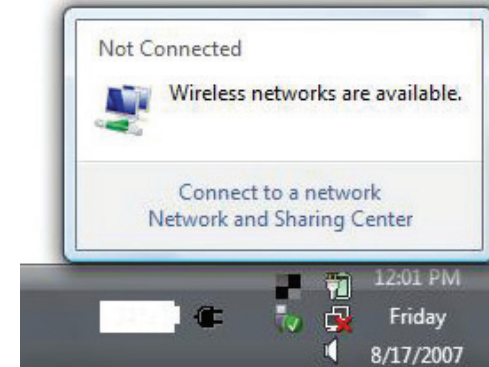
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



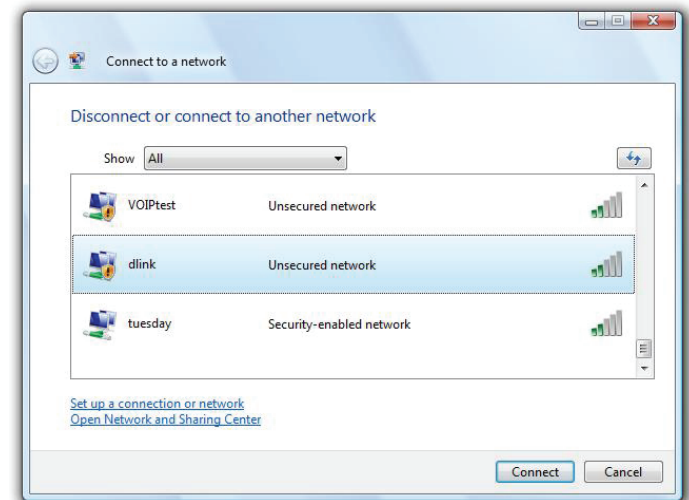
## WPA/WPA2

It is recommended that you 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.

Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.

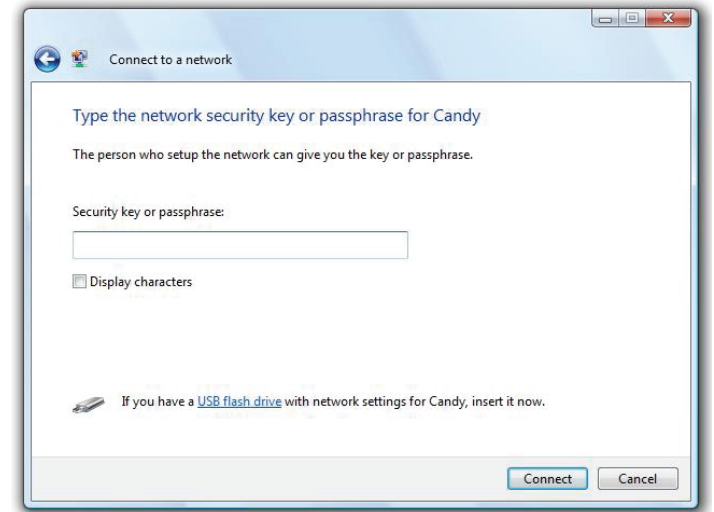


Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.



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

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



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DSL-3682. 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 these examples.

## **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® 10 or higher
  - Mozilla Firefox 28 or higher
  - Google™ Chrome 28 or higher
  - Apple Safari 6 or higher
  
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable, or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
  
- Disable any Internet security software running on the computer. Software firewalls such as 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.

### **What can I do if I forgot my password?**

If you forgot your password, you must reset your router. 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, leave the password box empty.

## 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, lets 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 (sometimes 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 on 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 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 similarly to how cordless phones work, through radio signals that 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 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, university 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. This makes

it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

## **Who uses wireless?**

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

### **Home Uses/Benefits**

- 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 Uses/Benefits**

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

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

## **Tips**

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

### **Centralize your router or access point**

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

### **Eliminate Interference**

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

### **Security**

Don't let your next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to the 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 DSL-3682 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

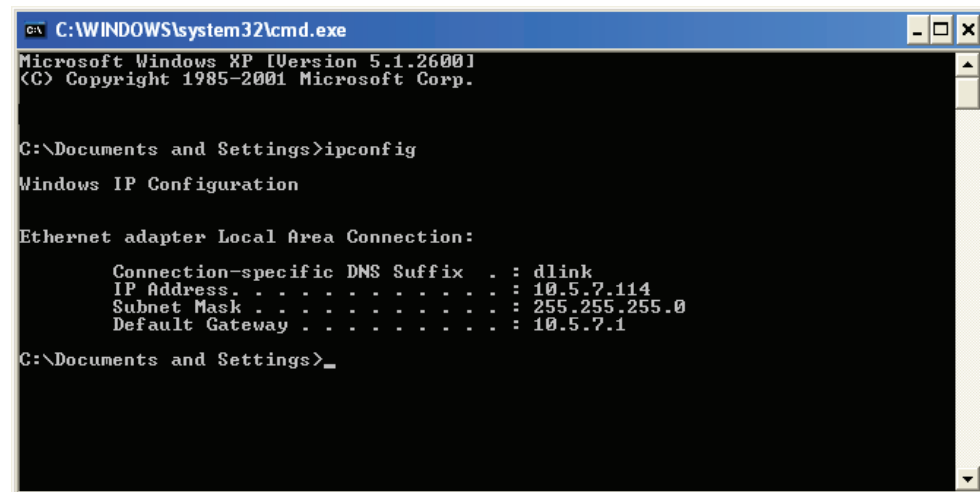
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

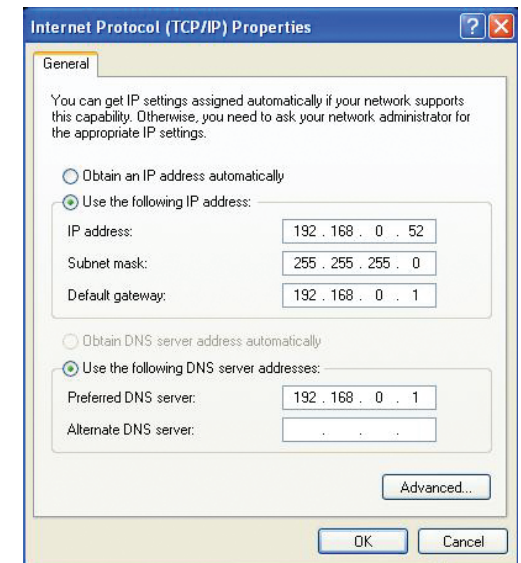
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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.



## Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DSL-3682 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

### What is WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?\*&\_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

# Technical Specifications

## Hardware Specifications

- One RJ-11 xDSL port
- 5 GHz 802.11ac/n/a Wireless LAN up to 433 Mbps<sup>1</sup>
- 2.4 GHz 802.11n/g/b Wireless LAN up to 300 Mbps<sup>1</sup>
- Four 10/100 Fast Ethernet LAN ports
- One USB 2.0 port

## Antenna Types

- Three fixed external antennas

## VDSL Compliance

- ITU-T G.993.1
- ITU-T G.993.2
- Profiles 8a, 8b, 8c, 8d, 12a, 12b, 17a

## ADSL Compliance

- 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)
- ITU-T G.992.3 (G.dmt.bis) Annex A/J/L/M (ADSL 2)
- ITU-T G.992.5 Annex A/L/M (ADSL 2+)

## Security

- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise
- Wi-Fi Protected Setup (WPS) PIN/PBC

## Power

- Input: 100 to 240 V AC, 50 to 60 Hz
- Output: 12 V DC, 1 A

## Temperature

- Operating: 0 to 40 ° C (32 to 104 ° F)
- Storage: -20 to 65 ° C (-20 to 149 ° F)

## Humidity

- 5% - 95% non-condensing

## Certifications

- CE
- Wi-Fi
- Wi-Fi Protected Setup (WPS)

## Dimensions & Weight

- 198 x 146 x 54 mm (7.79 x 5.74 x 2.12 inches)
- 302 g (9.6 oz)

<sup>1</sup> Maximum wireless signal rate derived from IEEE Standard 802.11ac, 802.11n, 802.11a, 802.11g, and 802.11b 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.



# Regulatory Information



	<b>Frequency Band(s)</b> <b>Frequenzband</b> <b>Fréquence bande(s)</b> <b>Bandas de Frecuencia</b> <b>Frequenza/e</b> <b>Frequentie(s)</b>	<b>Max. Output Power (EIRP)</b> <b>Max. Output Power</b> <b>Consommation d'énergie max.</b> <b>Potencia máxima de Salida</b> <b>Potenza max. Output</b> <b>Max. Output Power</b>
5 G	5.15 – 5.25 GHz	200 mW
	5.25 – 5.35 GHz	200 mW
	5.47 – 5.725 GHz	1 W
2.4 G	2.4 – 2.4835 GHz	100 mW

## European Community Declaration of Conformity:

Česky [Czech]	Tímto D-Link Corporation prohlašuje, že tento produkt, jeho příslušenství a software jsou v souladu se směrnicí 2014/53/EU. Celý text ES prohlášení o shodě vydaného EU a o firmwaru produktu lze stáhnout na stránkách k produktu <a href="http://www.dlink.com">www.dlink.com</a> .
Dansk [Danish]	D-Link Corporation erklærer herved, at dette produkt, tilbehør og software er i overensstemmelse med direktiv 2014/53/EU. Den fulde tekst i EU-overensstemmelseserklæringen og produktfirmware kan wnloades fra produktsiden hos <a href="http://www.dlink.com">www.dlink.com</a> .
Deutsch [German]	Hiermit erklärt die D-Link Corporation, dass dieses Produkt, das Zubehör und die Software der Richtlinie 2014/53/EU entsprechen. Der vollständige Text der Konformitätserklärung der Europäischen Gemeinschaft sowie die Firmware zum Produkt stehen Ihnen zum Herunterladen von der Produktseite im Internet auf <a href="http://www.dlink.com">www.dlink.com</a> zur Verfügung.
Eesti [Estonian]	Käesolevaga kinnitab D-Link Corporation, et see toode, tarvikud ja tarkvara on kooskõlas direktiiviga 2014/53/EL. Euroopa Liidu vastavusdeklaratsiooni täistekst ja toote püsivara on allalaadimiseks saadaval tootelehel <a href="http://www.dlink.com">www.dlink.com</a> .
English	Hereby, D-Link Corporation, declares that this product, accessories, and software are in compliance with directive 2014/53/EU. The full text of the EU Declaration of Conformity and product firmware are available for download from the product page at <a href="http://www.dlink.com">www.dlink.com</a>
Español [Spanish]	Por la presente, D-Link Corporation declara que este producto, accesorios y software cumplen con las directivas 2014/53/UE. El texto completo de la declaración de conformidad de la UE y el firmware del producto están disponibles y se pueden descargar desde la página del producto en <a href="http://www.dlink.com">www.dlink.com</a> .
Ελληνική [Greek]	Με την παρούσα, η D-Link Corporation δηλώνει ότι αυτό το προϊόν, τα αξεσουάρ και το λογισμικό συμμορφώνονται με την Οδηγία 2014/53/ΕΕ. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ και το υλικολογισμικό του προϊόντος είναι διαθέσιμα για λήψη από τη σελίδα του προϊόντος στην τοποθεσία <a href="http://www.dlink.com">www.dlink.com</a> .
Français [French]	Par les présentes, D-Link Corporation déclare que ce produit, ces accessoires et ce logiciel sont conformes aux directives 2014/53/UE. Le texte complet de la déclaration de conformité de l'UE et le icroprogramme du produit sont disponibles au téléchargement sur la page des produits à <a href="http://www.dlink.com">www.dlink.com</a> .
Italiano [Italian]	Con la presente, D-Link Corporation dichiara che questo prodotto, i relativi accessori e il software sono conformi alla direttiva 2014/53/UE. Il testo completo della dichiarazione di conformità UE e il firmware del prodotto sono disponibili per il download dalla pagina del prodotto su <a href="http://www.dlink.com">www.dlink.com</a> .

Latviski [Latvian]	Ar šo uzņēmums D-Link Corporation apliecina, ka šis produkts, piederumi un programmatūra atbilst direktīvai 2014/53/ES. ES atbilstības deklarācijas pilno tekstu un produkta aparātprogrammatūru var lejupielādēt attiecīgā produkta lapā vietnē <a href="http://www.dlink.com">www.dlink.com</a> .
Lietuvių [Lithuanian]	Šiuo dokumentu „D-Link Corporation“ pareiškia, kad šis gaminys, priedai ir programinė įranga atitinka direktyvą 2014/53/ES. Visą ES atitikties deklaracijos tekstą ir gaminio programinę aparatinę įrangą galima atsisiųsti iš gaminio puslapio adresu <a href="http://www.dlink.com">www.dlink.com</a> .
Nederlands [Dutch]	Hierbij verklaart D-Link Corporation dat dit product, accessoires en software voldoen aan de richtlijnen 2014/53/EU. De volledige tekst van de EU conformiteitsverklaring en productfirmware is beschikbaar voor download van de productpagina op <a href="http://www.dlink.com">www.dlink.com</a> .
Malti [Maltese]	Bil-preżenti, D-Link Corporation tiddikjara li dan il-prodott, l-aċċessorji, u s-software huma konformi mad-Direttiva 2014/53/UE. Tista' tniżżel it-test sħiħ tad-dikjarazzjoni ta' konformità tal-UE u l-firmware tal-prodott mill-paġna tal-prodott fuq <a href="http://www.dlink.com">www.dlink.com</a> .
Magyar [Hungarian]	Ezennel a D-Link Corporation kijelenti, hogy a jelen termék, annak tartozékai és szoftvere megfelelnek a 2014/53/EU sz. rendeletnek. Az EU Megfelelőségi nyilatkozat teljes szövege és a termék firmware a termék oldaláról tölthető le a <a href="http://www.dlink.com">www.dlink.com</a> címen.
Polski [Polish]	D-Link Corporation niniejszym oświadcza, że ten produkt, akcesoria oraz oprogramowanie są zgodne z dyrektywami 2014/53/EU. Pełen tekst deklaracji zgodności UE oraz oprogramowanie sprzętowe do produktu można pobrać na stronie produktu w witrynie <a href="http://www.dlink.com">www.dlink.com</a> .
Português [Portuguese]	Desta forma, a D-Link Corporation declara que este produto, os acessórios e o software estão em conformidade com a diretiva 2014/53/UE. O texto completo da declaração de conformidade da UE e do firmware
Slovensko[Slovenian]	Podjetje D-Link Corporation s tem izjavlja, da so ta izdelek, dodatna oprema in programnska oprema skladni z direktivami 2014/53/EU. Celotno besedilo izjave o skladnosti EU in vdelana programska oprema sta na voljo za prenos na strani izdelka na <a href="http://www.dlink.com">www.dlink.com</a> .
Slovensky [Slovak]	Spoločnosť D-Link týmto vyhlasuje, že tento produkt, príslušenstvo a softvér sú v súlade so smernicou 214/53/EÚ. Úplné znenie vyhlásenia EÚ o zhode a firmvéri produktu sú k dispozícii na prevzatie zo stránky produktu <a href="http://www.dlink.com">www.dlink.com</a> .
Suomi [Finnish]	D-Link Corporation täten vakuuttaa, että tämä tuote, lisävarusteet ja ohjelmisto ovat direktiivin 2014/53/EU vaatimusten mukaisia. Täydellinen EU-vaatimustenmukaisuusvakuutus samoin kuin tuotteen laiteohjelmisto ovat ladattavissa osoitteesta <a href="http://www.dlink.com">www.dlink.com</a> .

Svenska [Swedish]	D-Link Corporation försäkrar härmed att denna produkt, tillbehör och programvara överensstämmer med direktiv 2014/53/EU. Hela texten med EU-försäkran om överensstämmelse och produkt-firmware kan hämtas från produktsidan på <a href="http://www.dlink.com">www.dlink.com</a> .
Íslenska [Icelandic]	Hér með lýsir D-Link Corporation því yfir að þessi vara, fylgihlutir og hugbúnaður eru í samræmi við tilskipun 2014/53/EB. Sækja má ESB-samræmisýfirlýsinguna í heild sinni og fastbúnað vörunnar af vefsíðu vörunnar á <a href="http://www.dlink.com">www.dlink.com</a> .
Norsk [Norwegian]	Herved erklærer D-Link Corporation at dette produktet, tilbehøret og programvaren er i samsvar med direktivet 2014/53/EU. Den fullstendige teksten i EU-erklæring om samsvar og produktets fastvare er tilgjengelig for nedlasting fra produktsiden på <a href="http://www.dlink.com">www.dlink.com</a> .

**Warning Statement:**

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

### **NOTICE OF WIRELESS RADIO LAN USAGE IN THE EUROPEAN COMMUNITY (FOR WIRELESS PRODUCT ONLY):**

- 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. 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, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, and 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 band within the EU.
- Please refer to the product manual or datasheet to check whether your product uses 2.4 GHz and/or 5 GHz wireless.

### **HINWEIS ZUR VERWENDUNG VON DRAHTLOS-NETZWERK (WLAN) IN DER EUROPÄISCHEN GEMEINSCHAFT ( NUR FÜR EIN DRAHTLOSES PRODUKT )**

- Der Betrieb dieses Geräts in der Europäischen Gemeinschaft bei Nutzung von Kanälen im 5,15-5,35 GHz Frequenzband ist ausschließlich auf Innenräume beschränkt, um das Interferenzpotential zu reduzieren.
- Bei diesem Gerät handelt es sich um ein zum Einsatz in allen EU-Mitgliedsstaaten und in EFTA-Ländern - ausgenommen Frankreich. Der Betrieb dieses Geräts ist in den folgenden Ländern erlaubt: AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

#### **Gebrauchshinweise:**

- Um den in Europa geltenden nationalen Vorschriften zum Nutzen des Funkspektrums weiterhin zu entsprechen, werden Frequenz und Kanalbeschränkungen, dem jeweiligen Land, in dem das Gerät zum Einsatz kommt, entsprechend, auf die Produkte angewandt.
- Die Funktionalität im Ad-hoc-Modus bei Betrieb auf 5 GHz ist für dieses Gerät eingeschränkt. Bei dem Ad-hoc-Modus handelt es sich um eine Peer-to-Peer-Kommunikation zwischen zwei Client-Geräten ohne einen Access Point.
- Access Points unterstützen die Funktionen DFS (Dynamic Frequency Selection) und TPC (Transmit Power Control) wie erforderlich bei Betrieb auf 5 GHz innerhalb der EU.
- Bitte schlagen Sie im Handbuch oder Datenblatt nach, ob Ihr Gerät eine 2,4 GHz und / oder 5 GHz Verbindung nutzt.

## **AVIS CONCERNANT L'UTILISATION DE LA RADIO SANS FIL LAN DANS LA COMMUNAUTÉ EUROPÉENNE (UNIQUEMENT POUR LES PRODUITS SANS FIL)**

- Cet appareil est limité à un usage intérieur lorsqu'il est utilisé dans la Communauté européenne sur les canaux de la bande de 5,15 à 5,35 GHz afin de réduire les risques d'interférences.
- Cet appareil est un système de transmission à large bande (émetteur-récepteur) de 2,4 GHz, destiné à être utilisé dans tous les États-membres de l'UE et les pays de l'AELE. Cet équipement peut être utilisé dans les pays suivants : AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

### **Notes d'utilisation:**

- Pour rester en conformité avec la réglementation nationale européenne en matière d'utilisation du spectre, des limites de fréquence et de canal seront appliquées aux produits selon le pays où l'équipement sera déployé.
- Cet appareil ne peut pas utiliser le mode Ad-hoc lorsqu'il fonctionne dans la bande de 5 GHz. Le mode Adhoc fournit une communication directe pair à pair entre deux périphériques clients sans point d'accès.
- Les points d'accès prendront en charge les fonctionnalités DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control) au besoin lors du fonctionnement dans la bande de 5 GHz au sein de l'UE.
- Merci de vous référer au guide d'utilisation ou de la fiche technique afin de vérifier si votre produit utilise 2.4 GHz et/ou 5 GHz sans fil.

## **AVISO DE USO DE LA LAN DE RADIO INALÁMBRICA EN LA COMUNIDAD EUROPEA (SOLO PARA EL PRODUCTO INALÁMBRICO)**

- El uso de este dispositivo está restringido a interiores cuando funciona en la Comunidad Europea utilizando canales en la banda de 5,15-5,35 GHz, para reducir la posibilidad de interferencias.
- Este dispositivo es un sistema de transmisión (transceptor) de banda ancha de 2,4 GHz, pensado para su uso en todos los estados miembros de la UE y en los países de la AELC. Este equipo se puede utilizar en AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

### **Notas de uso:**

- Para seguir cumpliendo las normas europeas de uso del espectro nacional, se aplicarán limitaciones de frecuencia y canal en los productos en función del país en el que se pondrá en funcionamiento el equipo.
- Este dispositivo tiene restringido el funcionamiento en modo Ad-hoc mientras funcione a 5 Ghz. El modo Ad-hoc es la comunicación directa de igual a igual entre dos dispositivos cliente sin un punto de acceso.
- Los puntos de acceso admitirán la funcionalidad DFS (Selección de frecuencia dinámica) y TPC (Control de la potencia de transmisión) si es necesario cuando funcionan a 5 Ghz dentro de la UE.
- Por favor compruebe el manual o la ficha de producto para comprobar si el producto utiliza las bandas inalámbricas de 2.4 GHz y/o la de 5 GHz.

### **AVVISO PER L'USO DI LAN RADIO WIRELESS NELLA COMUNITÀ EUROPEA (SOLO PER PRODOTTI WIRELESS)**

- Nella Comunità europea, l'uso di questo dispositivo è limitato esclusivamente agli ambienti interni sui canali compresi nella banda da 5,15 a 5,35 GHz al fine di ridurre potenziali interferenze. Questo dispositivo è un sistema di trasmissione a banda larga a 2,4 GHz (ricetrasmittente), destinato all'uso in tutti gli stati membri dell'Unione europea e nei paesi EFTA.
- Questo dispositivo può essere utilizzato in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

#### **Note per l'uso**

- Al fine di mantenere la conformità alle normative nazionali europee per l'uso dello spettro di frequenze, saranno applicate limitazioni sulle frequenze e sui canali per il prodotto in conformità alle normative del paese in cui il dispositivo viene utilizzato.
- Questo dispositivo non può essere attivato in modalità Ad-hoc durante il funzionamento a 5 GHz. La modalità Ad-hoc è una comunicazione diretta peer-to-peer fra due dispositivi client senza un punto di accesso.
- I punti di accesso supportano le funzionalità DFS (Dynamic Frequency Selection) e TPC (Transmit Power Control) richieste per operare a 5 GHz nell'Unione europea.
- Ti invitiamo a fare riferimento al manuale del prodotto o alla scheda tecnica per verificare se il tuo prodotto utilizza le frequenze 2,4 GHz e/o 5 GHz.

### **KENNISGEVING VAN DRAADLOOS RADIO LAN-GEbruik IN DE EUROPESE GEMEENSCHAP (ALLEEN VOOR DRAADLOOS PRODUCT)**

- Dit toestel is beperkt tot gebruik binnenshuis wanneer het wordt gebruikt in de Europese Gemeenschap gebruik makend van kanalen in de 5.15-5.35 GHz band om de kans op interferentie te beperken.
- Dit toestel is een 2.4 GHz breedband transmissiesysteem (transceiver) dat bedoeld is voor gebruik in alle EU lidstaten en EFTA landen. Deze uitrusting mag gebruikt worden in AL, AD, BE, BG, DK, DE, FI, FR, GR, GW, IS, IT, HR, LI, LU, MT, MK, MD, MC, NL, NO, AT, PL, PT, RO, SM, SE, RS, SK, ES, CI, HU, CY

#### **Gebruiksaanwijzingen:**

- Om de gebruiksvoorschriften van het Europese Nationale spectrum na te leven, zullen frequentie- en kanaalbeperkingen worden toegepast op de producten volgens het land waar de uitrusting gebruikt zal worden.
- Dit toestel kan niet functioneren in Ad-hoc mode wanneer het gebruikt wordt in 5 GHz. Ad-hoc mode is directe peer-to-peer communicatie tussen twee klantenapparaten zonder een toegangspunt.
- Toegangspunten ondersteunen DFS (Dynamic Frequency Selection) en TPC (Transmit Power Control) functionaliteit zoals vereist bij gebruik in 5 GHz binnen de EU.
- Raadpleeg de handleiding of de datasheet om te controleren of uw product gebruik maakt van 2.4 GHz en/of 5 GHz.

## **SAFETY INSTRUCTIONS**

The following general safety guidelines are provided to help ensure your own personal safety and protect your product from potential damage. Remember to consult the product user instructions for more details.

- Static electricity can be harmful to electronic components. Discharge static electricity from your body (i.e. touching grounded bare metal) before touching the product.
- Do not attempt to service the product and never disassemble the product. For some products with a user replaceable battery, please read and follow the instructions in the user manual.
- Do not spill food or liquid on your product and never push any objects into the openings of your product.
- Do not use this product near water, areas with high humidity, or condensation unless the product is specifically rated for outdoor application.
- Keep the product away from radiators and other heat sources.
- Always unplug the product from mains power before cleaning and use a dry lint free cloth only.

## **SICHERHEITSVORSCHRIFTEN**

Die folgenden allgemeinen Sicherheitsvorschriften dienen als Hilfe zur Gewährleistung Ihrer eigenen Sicherheit und zum Schutz Ihres Produkts. Weitere Details finden Sie in den Benutzeranleitungen zum Produkt.

- Statische Elektrizität kann elektronischen Komponenten schaden. Um Schäden durch statische Aufladung zu vermeiden, leiten Sie elektrostatische Ladungen von Ihrem Körper ab, (z. B. durch Berühren eines geerdeten blanken Metallteils), bevor Sie das Produkt berühren.
- Unterlassen Sie jeden Versuch, das Produkt zu warten, und versuchen Sie nicht, es in seine Bestandteile zu zerlegen. Für einige Produkte mit austauschbaren Akkus lesen Sie bitte das Benutzerhandbuch und befolgen Sie die dort beschriebenen Anleitungen.
- Vermeiden Sie, dass Speisen oder Flüssigkeiten auf Ihr Produkt gelangen, und stecken Sie keine Gegenstände in die Gehäuseschlitze oder -öffnungen Ihres Produkts.
- Verwenden Sie dieses Produkt nicht in unmittelbarer Nähe von Wasser und nicht in Bereichen mit hoher Luftfeuchtigkeit oder Kondensation, es sei denn, es ist speziell zur Nutzung in Außenbereichen vorgesehen und eingestuft.
- Halten Sie das Produkt von Heizkörpern und anderen Quellen fern, die Wärme erzeugen.
- Trennen Sie das Produkt immer von der Stromzufuhr, bevor Sie es reinigen und verwenden Sie dazu ausschließlich ein trockenes fusselfreies Tuch.



## **CONSIGNES DE SÉCURITÉ**

Les consignes générales de sécurité ci-après sont fournies afin d'assurer votre sécurité personnelle et de protéger le produit d'éventuels dommages. Veuillez consulter les consignes d'utilisation du produit pour plus de détails.

- L'électricité statique peut endommager les composants électroniques. Déchargez l'électricité statique de votre corps (en touchant un objet en métal relié à la terre par exemple) avant de toucher le produit.
- N'essayez pas d'intervenir sur le produit et ne le démontez jamais. Pour certains produits contenant une batterie remplaçable par l'utilisateur, veuillez lire et suivre les consignes contenues dans le manuel d'utilisation.
- Ne renversez pas d'aliments ou de liquide sur le produit et n'insérez jamais d'objets dans les orifices.
- N'utilisez pas ce produit à proximité d'un point d'eau, de zones très humides ou de condensation sauf si le produit a été spécifiquement conçu pour une application extérieure.
- Éloignez le produit des radiateurs et autres sources de chaleur.
- Débranchez toujours le produit de l'alimentation avant de le nettoyer et utilisez uniquement un chiffon sec non pelucheux.

## **INSTRUCCIONES DE SEGURIDAD**

Las siguientes directrices de seguridad general se facilitan para ayudarle a garantizar su propia seguridad personal y para proteger el producto frente a posibles daños. No olvide consultar las instrucciones del usuario del producto para obtener más información.

- La electricidad estática puede resultar nociva para los componentes electrónicos. Descargue la electricidad estática de su cuerpo (p. ej., tocando algún metal sin revestimiento conectado a tierra) antes de tocar el producto.
- No intente realizar el mantenimiento del producto ni lo desmonte nunca. Para algunos productos con batería reemplazable por el usuario, lea y siga las instrucciones del manual de usuario.
- No derrame comida o líquidos sobre el producto y nunca deje que caigan objetos en las aberturas del mismo.
- No utilice este producto cerca del agua, en zonas con humedad o condensación elevadas a menos que el producto esté clasificado específicamente para aplicación en exteriores.
- Mantenga el producto alejado de los radiadores y de otras fuentes de calor.
- Desenchufe siempre el producto de la alimentación de red antes de limpiarlo y utilice solo un paño seco sin pelusa.

## **ISTRUZIONI PER LA SICUREZZA**

Le seguenti linee guida sulla sicurezza sono fornite per contribuire a garantire la sicurezza personale degli utenti e a proteggere il prodotto da potenziali danni. Per maggiori dettagli, consultare le istruzioni per l'utente del prodotto.

- L'elettricità statica può essere pericolosa per i componenti elettronici. Scaricare l'elettricità statica dal corpo (ad esempio toccando una parte metallica collegata a terra) prima di toccare il prodotto.
- Non cercare di riparare il prodotto e non smontarlo mai. Per alcuni prodotti dotati di batteria sostituibile dall'utente, leggere e seguire le istruzioni riportate nel manuale dell'utente.
- Non versare cibi o liquidi sul prodotto e non spingere mai alcun oggetto nelle aperture del prodotto.
- Non usare questo prodotto vicino all'acqua, in aree con elevato grado di umidità o soggette a condensa a meno che il prodotto non sia specificatamente approvato per uso in ambienti esterni.
- Tenere il prodotto lontano da caloriferi e altre fonti di calore.
- Scollegare sempre il prodotto dalla presa elettrica prima di pulirlo e usare solo un panno asciutto che non lasci filacce.

## **VEILIGHEIDSINFORMATIE**

De volgende algemene veiligheidsinformatie werd verstrekt om uw eigen persoonlijke veiligheid te waarborgen en uw product te beschermen tegen mogelijke schade. Denk eraan om de gebruikersinstructies van het product te raadplegen voor meer informatie.

- Statische elektriciteit kan schadelijk zijn voor elektronische componenten. Ontlaad de statische elektriciteit van uw lichaam (d.w.z. het aanraken van geaard bloot metaal) voordat u het product aanraakt.
- U mag nooit proberen het product te onderhouden en u mag het product nooit demonteren. Voor sommige producten met door de gebruiker te vervangen batterij, dient u de instructies in de gebruikershandleiding te lezen en te volgen.
- Mors geen voedsel of vloeistof op uw product en u mag nooit voorwerpen in de openingen van uw product duwen.
- Gebruik dit product niet in de buurt van water, gebieden met hoge vochtigheid of condensatie, tenzij het product specifiek geclassificeerd is voor gebruik buitenshuis.
- Houd het product uit de buurt van radiators en andere warmtebronnen.
- U dient het product steeds los te koppelen van de stroom voordat u het reinigt en gebruik uitsluitend een droge pluisvrije doek.

## 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 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](http://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](http://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 CO<sub>2</sub>.

Pour en savoir plus sur les produits et emballages respectueux de l'environnement, veuillez consulter le [www.dlinkgreen.com](http://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 CO<sub>2</sub>.

Para obtener más información acerca de nuestros productos y embalajes ecológicos, visite el sitio [www.dlinkgreen.com](http://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](http://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 CO<sub>2</sub>-emissies.

Breng een bezoek aan [www.dlinkgreen.com](http://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 CO<sub>2</sub>.

Aby dowiedzieć się więcej na temat produktów i opakowań mających wpływ na środowisko prosimy zapoznać się ze stroną Internetową [www.dlinkgreen.com](http://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, odnešte jej prosím na sběrné místo určené místními úřady k tomuto účelu. Někteřá 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 CO<sub>2</sub>.

Více informací o našich ekologických výrobcích a obalech najdete na adrese [www.dlinkgreen.com](http://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](http://www.dlinkgreen.com) weboldalon tudhat meg.

**NORSK****NO**

Dette symbolet på produktet eller forpakningen betyr at dette produktet ifølge lokale lover og forskrifter ikke skal kastes sammen med husholdningsavfall, men leveres inn til gjenvinning. Vennligst ta det til et innsamlingssted anvist av lokale myndigheter når det er kommet til slutten av levetiden. Noen steder aksepteres produkter uten avgift. Ved på denne måten å gjenvinne produktet og forpakningen hjelper du å verne miljøet og beskytte folks helse.

**D-Link og miljøet**

Hos D-Link forstår vi oss på og er forpliktet til å minske innvirkningen som vår drift og våre produkter kan ha på miljøet. For å minimalisere denne innvirkningen designer og lager D-Link produkter som er så miljøvennlig som mulig, ved å bruke resirkulerbare, lav-toksiske materialer både i produktene og forpakningen.

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

For mer informasjon angående våre miljøansvarlige produkter og forpakninger kan du gå til [www.dlinkgreen.com](http://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 CO<sub>2</sub>-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på [www.dlinkgreen.com](http://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](http://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 CO<sub>2</sub>-udledningerne.

Du kan finde flere oplysninger om vores miljømæssigt ansvarlige produkter og emballage på [www.dlinkgreen.com](http://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](http://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](http://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 CO<sub>2</sub>.

Para saber mais sobre os nossos produtos e embalagens responsáveis a nível ambiental visite [www.dlinkgreen.com](http://www.dlinkgreen.com).