



# User Manual

## AC1200 Wi-Fi 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       |
|----------|---------------|-------------------|
| 1.0      | June 02, 2015 | • Initial release |

## 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. iPhone, iPad, and iPod touch are registered trademarks of Apple Inc. Android is a trademark of Google, Inc. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2015 by D-Link Corporation.

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

# Table of Contents

|  |           |   |    |
|--|-----------|---|----|
| <b>Preface .....</b>                       | <b>i</b>  | DS-Lite .....                               | 37 |
| Manual Revisions .....                     | i         | Wireless Connection Setup Wizard .....      | 38 |
| Trademarks .....                           | i         | Wi-Fi Protected Setup Wizard .....          | 41 |
| Package Contents .....                     | 1         | Wireless Security .....                     | 43 |
| System Requirements .....                  | 2         | What is WPA? .....                          | 43 |
| Introduction .....                         | 3         | Manual Wireless Network Setup .....         | 44 |
| Features .....                             | 4         | Network Settings .....                      | 53 |
| Hardware Overview .....                    | 5         | Router Settings .....                       | 53 |
| Connections .....                          | 5         | DHCP Server Settings .....                  | 54 |
| LEDs .....                                 | 6         | DHCP Reservation .....                      | 56 |
| <b>Installation .....</b>                  | <b>7</b>  | IPv6 .....                                  | 57 |
| Before you Begin .....                     | 7         | IPv6 Internet Connection Setup Wizard ..... | 58 |
| Wireless Installation Considerations ..... | 8         | IPv6 Manual Setup .....                     | 63 |
| Manual Setup .....                         | 9         | Advanced .....                              | 72 |
| <b>Configuration .....</b>                 | <b>10</b> | Virtual Server .....                        | 72 |
| Quick Setup Wizard .....                   | 11        | Port Forwarding .....                       | 73 |
| QRS Mobile App .....                       | 16        | Application Rules .....                     | 74 |
| Web-based Configuration Utility .....      | 20        | QoS Engine .....                            | 75 |
| Internet Connection Setup .....            | 21        | Network Filters .....                       | 77 |
| Internet Connection Setup Wizard .....     | 22        | Access Control .....                        | 78 |
| Internet (Manual) .....                    | 28        | Website Filters .....                       | 81 |
| Static (assigned by ISP) .....             | 30        | Inbound Filters .....                       | 82 |
| PPPoE (DSL) .....                          | 31        | Firewall Settings .....                     | 83 |
| PPTP .....                                 | 33        | Routing .....                               | 84 |
| L2TP .....                                 | 35        | Advanced Wireless .....                     | 85 |
|  |           | Wi-Fi Protected Setup (WPS) .....           | 86 |

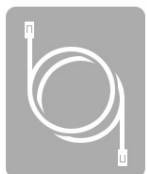
|                                 |     |   |            |
|---------------------------------|-----|---|------------|
| Advanced Network Settings ..... | 88  | <b>Connect a Wireless Client to your Router .....</b> | <b>111</b> |
| Guest Zone .....                | 89  | WPS Button .....                                      | 111        |
| IPv6 Firewall .....             | 90  | Windows® 8.....                                       | 112        |
| IPv6 Routing .....              | 91  | WPA/WPA2 .....  | 112        |
| Tools .....                     | 92  | Windows® 7.....                                       | 114        |
| Admin.....                      | 92  | WPA/WPA2 .....  | 114        |
| Time .....                      | 94  | WPS.....  | 117        |
| SysLog .....                    | 95  | Windows Vista® .....                                  | 121        |
| Email Settings.....             | 96  | WPA/WPA2 .....  | 122        |
| System .....                    | 97  | WPS/WCN 2.0 .....                                     | 124        |
| Firmware .....                  | 98  | Windows® XP .....                                     | 125        |
| Language Pack.....              | 98  | WPA/WPA2 .....  | 126        |
| Dynamic DNS .....               | 99  | <b>Troubleshooting .....</b>                          | <b>128</b> |
| Dynamic DNS for IPv6 Hosts..... | 99  | <b>Wireless Basics .....</b>                          | <b>132</b> |
| Ping Test .....                 | 100 | What is Wireless?.....                                | 133        |
| Schedules .....                 | 101 | Tips.....   | 135        |
| Status .....                    | 102 | Wireless Modes.....                                   | 136        |
| Device Info .....               | 102 | <b>Networking Basics .....</b>                        | <b>137</b> |
| Logs.....                       | 103 | Check your IP address.....                            | 137        |
| Statistics .....                | 104 | Statically Assign an IP address .....                 | 138        |
| Internet Sessions.....          | 105 | <b>Technical Specifications .....</b>                 | <b>139</b> |
| Wireless.....                   | 106 | <b>Regulatory Information .....</b>                   | <b>140</b> |
| Routing .....                   | 107 |   |            |
| IPv6 .....                      | 108 |   |            |
| IPv6 Routing .....              | 109 |   |            |
| Support .....                   | 110 |   |            |



# Package Contents



DIR-822 AC1200 Wi-Fi Router



Ethernet Cable



Power Adapter



Wi-Fi Configuration Note

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 DIR-822 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/n/g/b/a 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 9 or higher</li><li>• Firefox 20 or higher</li><li>• Safari 5.1 or higher</li><li>• Chrome 25 or higher</li></ul> <p><b>Windows® Users:</b> Make sure you have the latest version of Java installed. Visit <a href="http://www.java.com">www.java.com</a> to download the latest version.</p> |
| <b>QRS Mobile Requirements</b>                      | <ul style="list-style-type: none"><li>• iPhone®/iPad®/iPod Touch® (iOS 6.0 or higher)</li><li>• Android™ device (2.33 or higher)</li></ul>  |

# Introduction

The D-Link DIR-822 is a IEEE 802.11ac compliant device that delivers up to 3x faster speeds than 802.11n while staying backward compatible with 802.11n/g/b/a devices. Connect the DIR-822 to a cable or DSL modem and provide high-speed Internet access to multiple computers, game consoles, and media players. Create a secure wireless network to share photos, files, music, videos, printers, and network storage. Powered by the 802.11ac technology and equipped with four external antennas, this router provides superior wireless coverage for larger homes and offices, or for users running bandwidth-intensive applications. The DIR-822 also includes a 4-port 10/100 Fast Ethernet switch that connects to wired devices for uninterrupted video calling and faster file transfers.

D-Link Intelligent QoS Technology helps to increase network efficiency by analyzing wired and wireless network traffic and prioritizing it in order of importance. This way, important network traffic such as VoIP and video streaming, take priority over background network traffic such as a file downloads and print tasks, ensuring you have optimal network performance.

The DIR-822 supports the latest wireless security features to help prevent unauthorized access, be it from over a wireless network or the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption regardless of your client devices. In addition, this router is equipped with a dual-active firewall (SPI and NAT) to prevent potential attacks over the Internet.

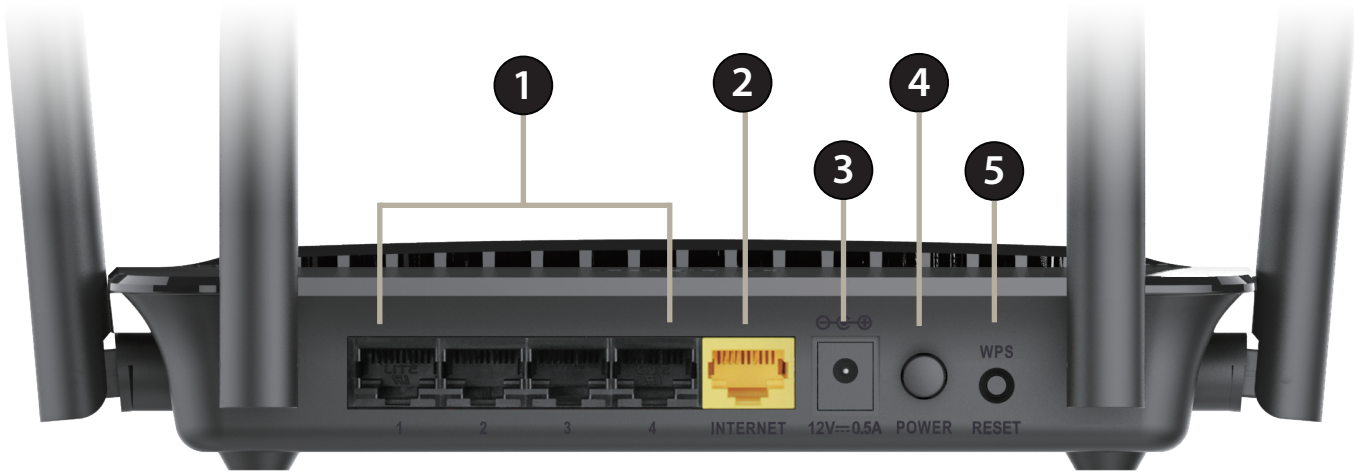
# Features

- **Ultimate Fast Wireless Networking** - The DIR-822 provides up to 300 Mbps wireless connection in 2.4 GHz band, and up to 867 Mbps wireless connection in 5 GHz with other 802.11ac and 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11ac wireless router gives you the freedom of wireless networking at speeds 3x faster than 802.11n.
- **Compatible with 802.11n/g/b/a Devices** - The DIR-822 is still fully compatible with the IEEE 802.11a, IEEE 802.11b, 802.11g and 802.11n, so it can connect with existing 802.11a, IEEE 802.11b, 802.11g and 802.11n PCI, USB, and CardBus adapters.
- **Advanced Firewall Features** - The web-based user interface displays a number of advanced network management features including:
  - **Content Filtering** - Easily applied content filtering based on MAC address, URL, and/or domain name.
  - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.
  - **Secure Multiple/Concurrent Sessions** - The DIR-822 can pass through VPN sessions. It supports multiple and concurrent IPsec and PPTP sessions, so users behind the DIR-822 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use web-based user interface, the DIR-822 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.

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

# Hardware Overview

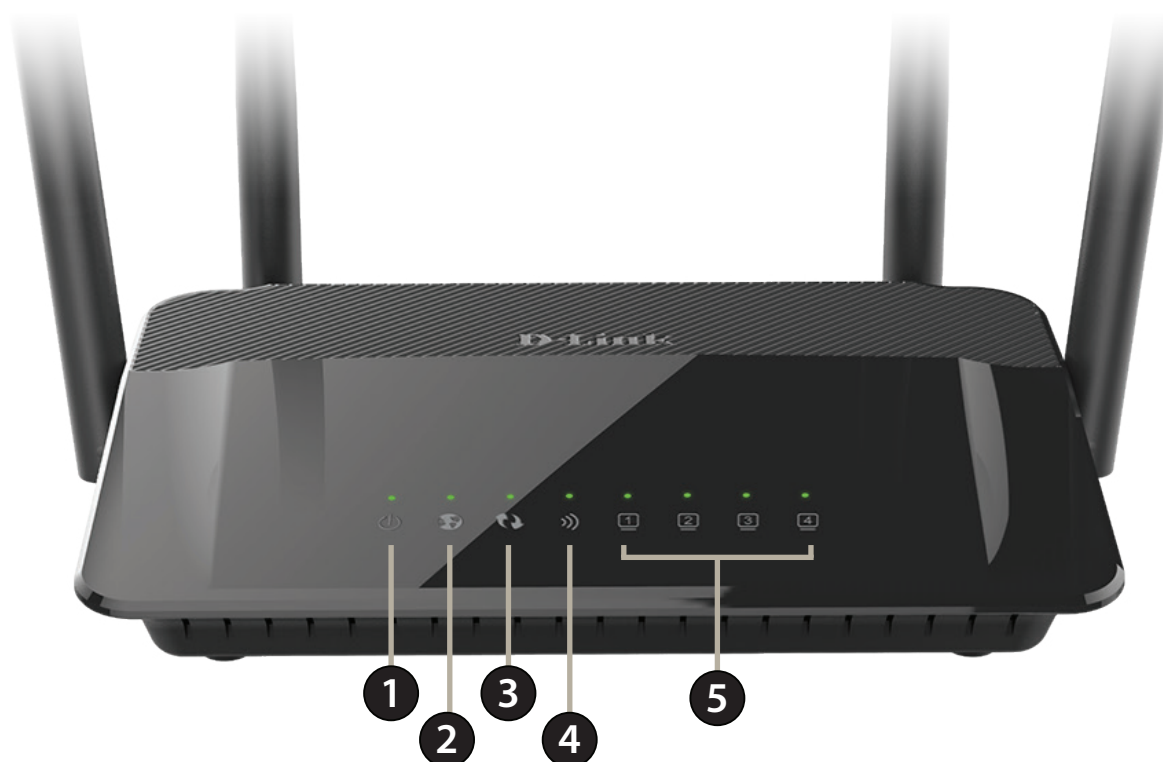
## Connections



|   |                    |  |
|---|--------------------|--|
| 1 | LAN Ports (1-4)    | Connect 10/100 Ethernet devices such as computers, switches, storage (NAS) devices and game consoles.    |
| 2 | Internet Port      | Using an Ethernet cable, connect your broadband modem to this port.                                      |
| 3 | Power Receptor     | Receptor for the supplied power adapter.   |
| 4 | Power Button       | Press the power button to power the DIR-822 on and off.  |
| 5 | WPS / Reset Button | Short press to start the WPS process. Long press for 10 seconds to reset the router to default settings. |

# Hardware Overview

## LEDs



|   |              |  |
|---|--------------|--|
| 1 | Power LED    | A solid light indicates that the device is powered on. The light will blink while the device is in recovery mode.              |
| 2 | Internet LED | A solid light indicates that an Internet link is established.  |
| 3 | WPS LED      | A solid light indicates that the WPS handshake has been completed. The light will blink while the WPS handshake is processing. |
| 4 | WLAN LED     | A solid light indicates that the wireless segment is ready.  |
| 5 | LAN LEDs 1-4 | A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4 respectively.                                |

# Installation

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

## Before you Begin

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

# Wireless Installation Considerations

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

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



# Manual Setup

1. Turn off and unplug your cable or DSL broadband modem. This is required.
2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.
3. Unplug the Ethernet cable from your modem (or existing router if upgrading) that is connected to your computer. Plug it into the LAN port labeled **1** on the back of your router. The router is now connected to your computer.
4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.
5. Reconnect the power adapter to your cable or DSL broadband modem and wait for two minutes.
6. Connect the supplied power adapter into the power port on the back of the router and then plug it into a power outlet or surge protector. Press the power button and verify that the power LED is lit. Allow 1 minute for the router to boot up.
7. If you are connecting to a broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser connecting to a website. If a solid light indicates a connection on the Internet port, then the router can connect to the Internet.

# Configuration

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

- **D-Link Setup Wizard** - This wizard will launch when you log into the router for the first time. Refer to page 11.
- **QRS Mobile App** - Use your iPhone, iPad, or iPod Touch to configure your router. Refer to page 16.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to page 20.

# Quick Setup Wizard

If this is your first time installing the router, open your web browser. You will automatically be directed to the **Wizard Setup Screen**. If not, enter **http://dlinkrouter.local**. Then, press Enter.

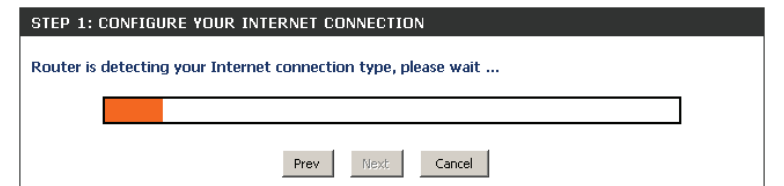
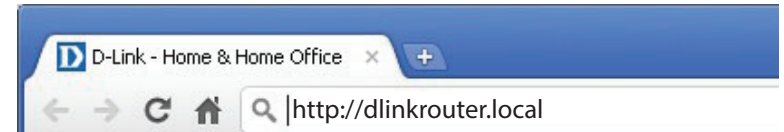
If you have already configured your settings and you would like to access the configuration utility, please refer to page 20.

If this is your first time logging into the router, this wizard will start automatically.

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

Click **Next** to continue.

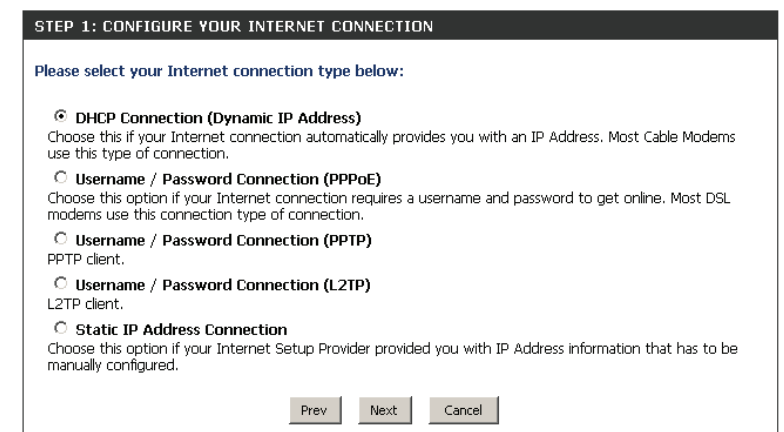
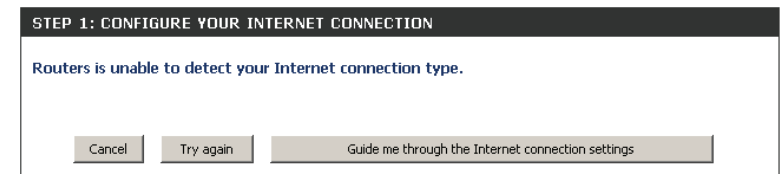
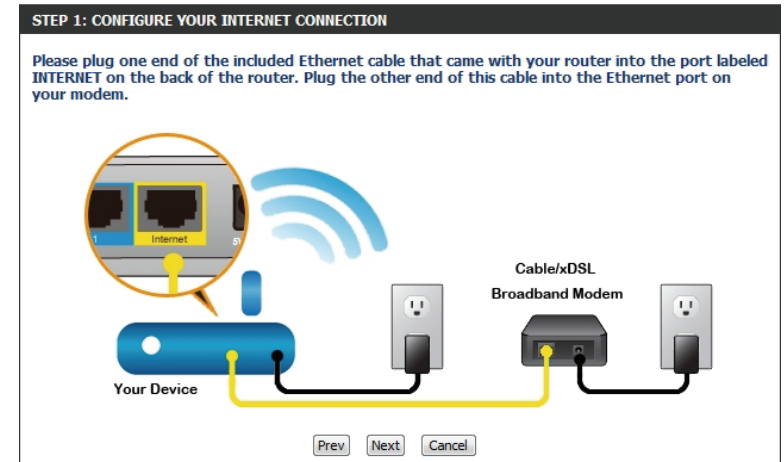
Please wait while your router detects your Internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password.



If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Connect your broadband modem to the Internet port and then click **Try Again**.

If the router detects an Ethernet connection but does not detect the type of Internet connection you have, this screen will appear. Click **Guide me through the Internet Connection Settings** to display a list of connection types to choose from.

Select your Internet connection type and click **Next** to continue.



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

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

If the router detected or you selected **PPTP**, enter your PPTP username, password, and other information supplied by your ISP. Click **Next** to continue.

If the router detected or you selected **L2TP**, enter your L2TP username, password, and other information supplied by your ISP. Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (PPPOE)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. If you do not have this information, please contact your ISP.

User Name :

Password :

Prev Next Cancel

SET USERNAME AND PASSWORD CONNECTION (PPTP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.

Address Mode : ☒ Dynamic IP ☐ Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

Prev Next Cancel

SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.

Address Mode : ☒ Dynamic IP ☐ Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address (may be same as gateway) :

User Name :

Password :

Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

Prev Next Cancel

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

SET STATIC IP ADDRESS CONNECTION

To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP.

IP Address :

Subnet Mask :

Gateway Address :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

Prev

Next

Cancel

For both the 2.4 GHz and 5 GHz segments, create a Wi-Fi network name (SSID) using up to 32 characters.

Create a Wi-Fi password (between 8-63 characters). Your wireless clients will need to have this passphrase or key entered to be able to connect to your wireless network.

Click **Next** to continue.

STEP 2: CONFIGURE YOUR WI-FI SECURITY

Give your Wi-Fi network a name and a password. (2.4GHz Band)

Wi-Fi Network Name (SSID) :  (Using up to 32 characters)

Wi-Fi Password :  (Between 8 and 63 characters)

Give your Wi-Fi network a name and a password. (5GHz Band)

Wi-Fi Network Name (SSID) :  (Using up to 32 characters)

Wi-Fi Password :  (Between 8 and 63 characters)

Prev

Next

Cancel

In order to secure your router, please enter a new password. Check the Enable Graphical Authentication box to enable CAPTCHA authentication for added security. Click **Next** to continue.

STEP 3: SET YOUR PASSWORD

By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below, and enabling CAPTCHA Graphical Authentication provides added security protection to prevent unauthorized online users and hacker software from accessing your network settings.

Password:

Verify Password :

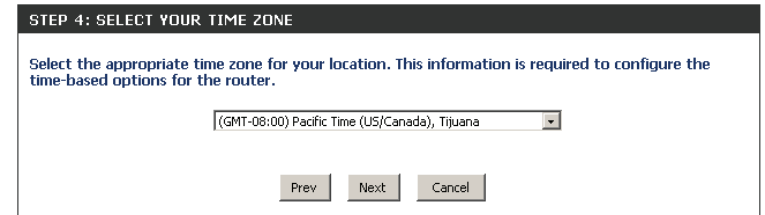
Enable Graphical Authentication : ☐

Prev

Next

Cancel

Select your time zone from the drop-down menu and click **Next** to continue.



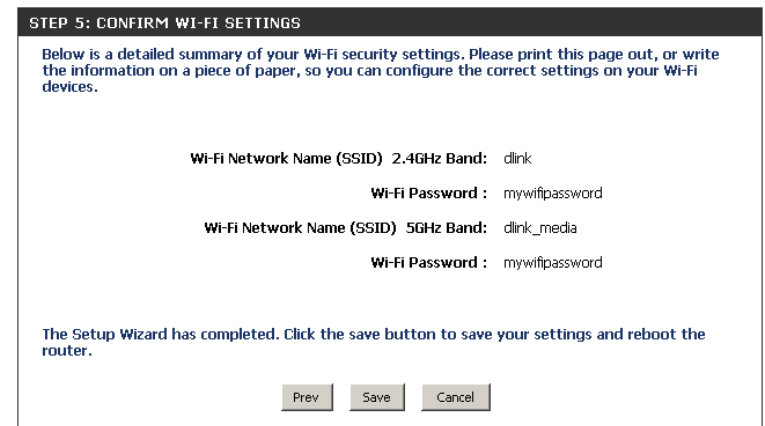
STEP 4: SELECT YOUR TIME ZONE

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

(GMT-08:00) Pacific Time (US/Canada), Tijuana

Prev Next Cancel

The Confirm Wi-Fi Settings window will display your Wi-Fi settings. Click **Save** to continue.



STEP 5: CONFIRM WI-FI SETTINGS

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

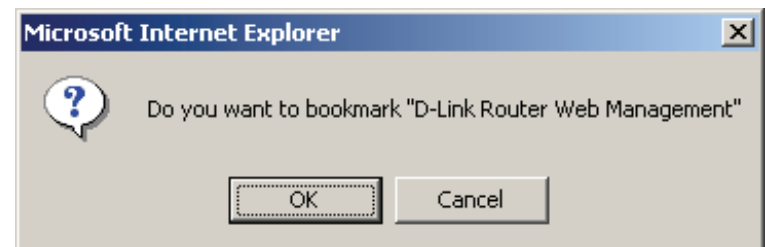
Wi-Fi Network Name (SSID) 2.4GHz Band: dlink  
Wi-Fi Password : mywifipassword

Wi-Fi Network Name (SSID) 5GHz Band: dlink\_media  
Wi-Fi Password : mywifipassword

The Setup Wizard has completed. Click the save button to save your settings and reboot the router.

Prev Save Cancel

If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.

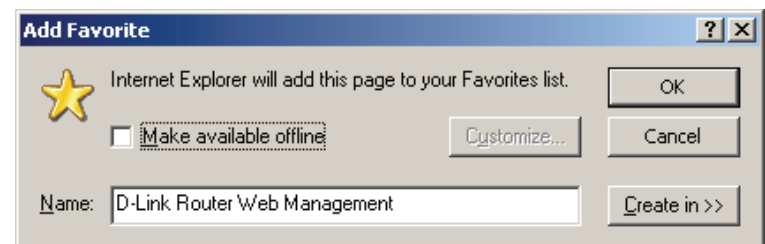


Microsoft Internet Explorer

Do you want to bookmark "D-Link Router Web Management"

OK Cancel

If you clicked **Yes**, a window may appear (depending on what web browser you are using) to create a bookmark.



Add Favorite

Internet Explorer will add this page to your Favorites list.

Make available offline

Name: D-Link Router Web Management

OK Cancel Create in >>

# QRS Mobile App

QRS Mobile app allows you to install and configure your router from your mobile device.

**Note:** The screenshots may be different depending on your mobile device's OS version.

## Step 1

Search for the free **QRS Mobile** App on the iTunes Store or Google Play.



## Step 2

Once your app is installed, you may now configure your router. Connect to the router wirelessly by going to your wireless utility on your device. Scan for the Wi-Fi name (SSID) as listed on the supplied info card. Select and then enter your Wi-Fi password.

| D-Link Wi-Fi Configuration Card  |   |
|--|---|
| <b>Default Configuration</b>   | Wi-Fi Name(SSID) 2.4GHz:                                    |
| Wi-Fi Name (SSID):<br>dlink-a8fa   | Wi-Fi Password:   |
| Wi-Fi Password:<br>akbdj19368  | Wi-Fi Name(SSID) 5GHz *:                                    |
|  | Wi-Fi Password *:   |
| To configure your router, go to:<br>http://dlinkrouter.local.<br>Or http://192.168.0.1<br>Username: "Admin"<br>Password: " (leave the field blank) | <b>Your configuration</b><br>Username: "Admin"<br>Password: |
|  | *For applicable models                                      |

## Step 3

Once you connect to the router, launch the QRS Mobile app from the Home screen of your device.

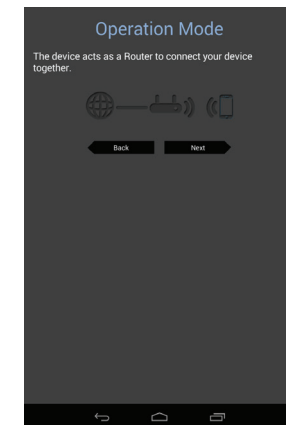
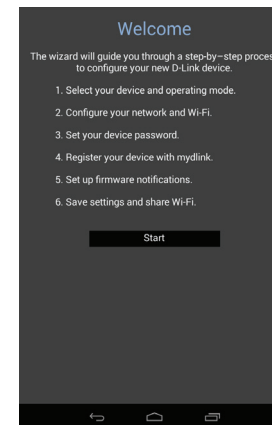
**Note:** The following steps show the Android interface of the QRS Mobile app. If you are using an iPhone, iPad, or iPod touch, the appearance may be different to that of the screenshots, but the process is the same.





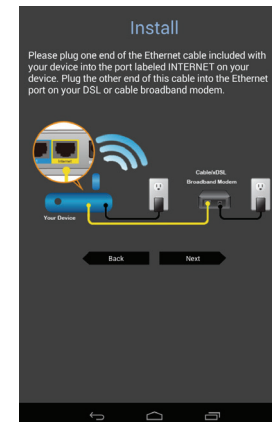
### Step 4

You will see the welcome screen. Tap **Start** to proceed, then enter your device password and tap **Log In**. Tap **Next** once the Operation Mode screen appears.



### Step 5

At this point, please ensure that your the router is connected to a modem. Plug one end of the provided Ethernet cable into your DSL or cable modem, and plug the other end into the port marked INTERNET on the DIR-822. Tap **Next** to automatically detect your Internet connection and proceed to the next step.



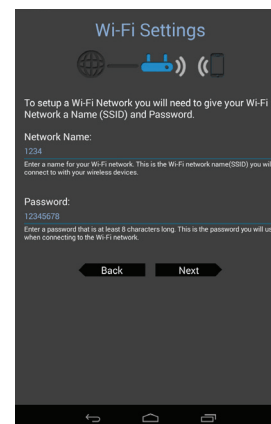
### Step 6

Firstly, enter a network name (SSID) of your choice, or leave it unchanged to accept the default SSID.

Secondly, choose a Wi-Fi password of at least 8 characters. Any device trying to connect to the router wirelessly will need to enter this password the first time it connects.

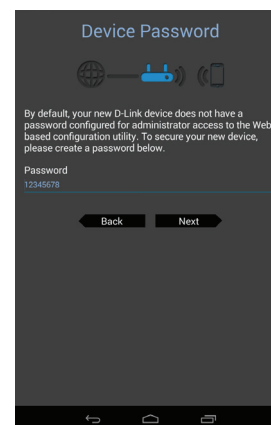
Finally, tap **Next** to proceed.

You will be asked to enter a SSID and password for your 5 GHz network. Repeat step 6 and tap **Next** to proceed.



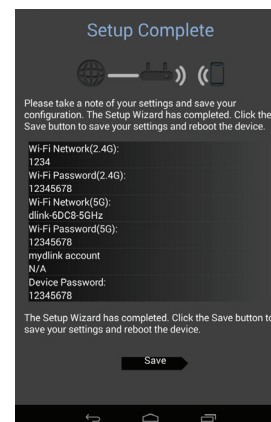
### Step 7

Enter the administrator password of your choice. Unlike the Wi-Fi password, this password is only required when you need to configure the router. See **“Web-based Configuration Utility” on page 20** for details of when this password is used. Tap **Next** to proceed.



## Step 8

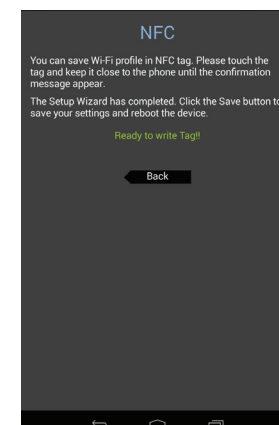
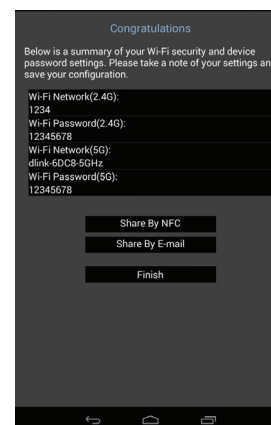
You will be presented with a summary of your chosen settings. Tap **Save** to complete the setup.



Congratulations, your device has been successfully configured! You can share this information by tapping **Share By NFC**, **Share By E-mail**, or tap **Finish** to exit the app.

If you tap **Share By NFC**, you can now touch the tag with your other device until the confirmation message appears.

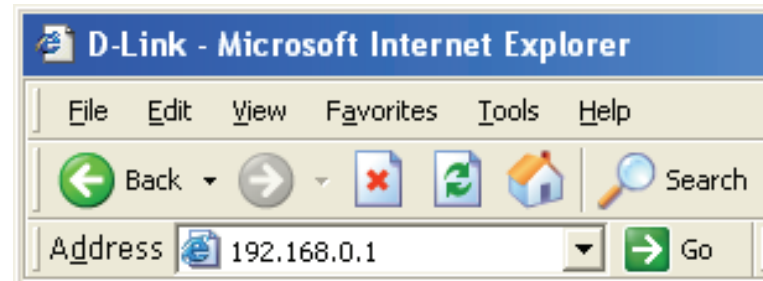
**Note:** *NFC is not supported by iPhone, iPad, and iPod touch devices.*



# Web-based Configuration Utility

To access the configuration utility, open a web browser such as Internet Explorer and enter the address of the router (**http://dlinkrouter.local or http://192.168.0.1**).

Non-Windows and non-Mac users may also connect by typing **http://192.168.0.1** in the address bar.



Leave the password blank by default.

A screenshot of the D-Link router's login page. The page has an orange header with the word "LOGIN" in white. Below the header, the text "Login to the router :" is displayed. There are two input fields: "User Name :" with the value "Admin" and "Password :". To the right of the password field is a "Login" button.

## Internet Connection Setup

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard**. You will be directed to the Quick Setup Wizard. See the next page for details.

Click **Manual Internet Connection Setup** to configure your connection manually. See “**Internet (Manual)**” on page 28 for details.

**INTERNET CONNECTION**

If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

**INTERNET CONNECTION SETUP WIZARD**

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.

[Internet Connection Setup Wizard](#)

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

**MANUAL INTERNET CONNECTION OPTION**

If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

[Manual Internet Connection Setup](#)

# Internet Connection Setup Wizard

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

At any time during the Internet Connection Setup Wizard, the user can click on the **Cancel** button to discard any changes and return to the main Internet page. Also the user can click on the **Prev** button, to return to the previous window for re-configuration.

## Welcome:

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

Click **Next** to continue.

## Step 1: Set Your Password

By default, the D-Link router does not have a password configured for administrator access to the web-based configuration pages. To secure your new networking device, please enter and verify a password in the spaces provided. The two passwords must match.

Click **Next** to continue.

### INTERNET CONNECTION

If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

### INTERNET CONNECTION SETUP WIZARD

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.

[Internet Connection Setup Wizard](#)

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

### WELCOME TO THE D-LINK INTERNET CONNECTION SETUP WIZARD

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

- Step 1: Set your Password
- Step 2: Select your Time Zone
- Step 3: Configure your Internet Connection
- Step 4: Save Settings and Connect

[Prev](#) [Next](#) [Cancel](#) [Connect](#)

### STEP 1: SET YOUR PASSWORD

By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

[Prev](#) [Next](#) [Cancel](#) [Connect](#)

### Step 2: Select Your Time Zone

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

Click **Next** to continue.

The screenshot shows a configuration window titled "STEP 2: SELECT YOUR TIME ZONE". Below the title, it says "Select the appropriate time zone for your location. This information is required to configure the time-based options for the router." There is a dropdown menu labeled "Time Zone :" with "(GMT+08:00) Taipei" selected. At the bottom, there are four buttons: "Prev", "Next", "Cancel", and "Connect".

### Step 3: Internet Connection

Here you will be able to configure the Internet connection used by this device. If your ISP connection is listed in the drop-down menu select it and click **Next**. If your ISP connection is not listed then you can proceed to select any of the other manual Internet connection methods listed below.

The following parameters will be available for configuration:

**Dynamic IP Address:** Choose this if your Internet connection automatically provides you with an IP address. Most cable modems use this type of connection.

**PPPoE:** Choose this option if your Internet connection requires a PPPoE username and password to get online. Most DSL modems use this type of connection.

**PPTP:** Choose this option if your Internet connection requires a PPTP username and password to get online.

**L2TP:** Choose this option if your Internet connection requires an L2TP username and password to get online.

**Static IP Address:** Choose this option if your Internet service provider provided you with IP address information that has to be manually configured.

The screenshot shows a configuration window titled "STEP 3: CONFIGURE YOUR INTERNET CONNECTION". Below the title, it says "Please select the Internet connection type below:". There are five radio button options:
 

- DHCP Connection (Dynamic IP Address)**: Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.
- Username / Password Connection (PPPoE)**: Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (PPTP)**: Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Username / Password Connection (L2TP)**: Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.
- Static IP Address Connection**: Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

 At the bottom, there are four buttons: "Prev", "Next", "Cancel", and "Connect".

### Step 3: Internet Connection (Dynamic IP Address)

After selecting the Dynamic IP Address Internet connection method, the following page will appear.

The following parameters will be available for configuration:

**MAC Address:** Enter the MAC address of the Internet gateway (plugged into the Internet port of this device) here.

**Clone Button:** If the configuration PC also acts as the Internet gateway, then click on the Clone Your PC's MAC Address button to copy the PC's MAC address into the space provided. If you're not sure, leave the MAC Address field blank.

**Host Name:** Enter the host name used here. If you do not have or know this information, please contact your ISP.

**Primary DNS Address:** Enter the Primary DNS IP address used here.

**Secondary DNS Address:** Enter the Secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

### Step 3: Internet Connection (PPPoE)

After selecting the PPPoE Internet connection method, the following page will appear:

The following parameters will be available for configuration:

**User Name:** Enter the PPPoE account user name used here. This information is given by the ISP.

**Password:** Enter the PPPoE account password used here. This information is given by the ISP.

Click **Next** to continue.



**Step 3: Internet Connection (PPTP)**

After selecting the PPTP Internet connection method, the following page will appear:

The following parameters will be available for configuration:

**Address Mode:** Here the user can specify whether this Internet connection requires the use of a Dynamic or Static IP address. PPTP usually requires a dynamic IP configuration.

**PPTP IP Address:** Enter the PPTP IP address used here. This option is only available if Static IP is selected.

**PPTP Subnet Mask:** Enter the PPTP subnet mask used here.

**PPTP Gateway IP Address:** Enter the PPTP gateway IP address used here.

**PPTP Server IP Address:** Enter the PPTP server IP address used here. This is normally the same as the PPTP gateway IP address.

**User Name:** Enter the PPTP username used here.

**Password:** Enter the PPTP password used here.

**Verify Password:** Re-enter the PPTP password used here.

**Primary DNS Address:** Enter the primary DNS IP address used here.

**Secondary DNS Address:** Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

### Step 3: Internet Connection (L2TP)

After selecting the L2TP Internet connection method, the following page will appear:

The following parameters will be available for configuration:

**Address Mode:** Here the user can specify whether this Internet connection requires the use of a dynamic or static IP address. L2TP usually requires a dynamic IP configuration.

**L2TP IP Address:** Enter the L2TP IP address used here. This option is only available if Static IP is selected.

**L2TP Subnet Mask:** Enter the L2TP subnet mask used here.

**L2TP Gateway IP Address:** Enter the L2TP gateway IP address used here.

**L2TP Server IP Address:** Enter the L2TP server IP address used here. This is normally the same as the L2TP gateway IP address.

**User Name:** Enter the L2TP username used here.

**Password:** Enter the L2TP password used here.

**Verify Password:** Re-enter the L2TP password used here.

**Primary DNS Address:** Enter the primary DNS IP address used here.

**Secondary DNS Address:** Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.

Address Mode : ☒ Dynamic IP ☐ Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :  (may be same as gateway)

User Name :

Password :

Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :  (optional)

Prev

Next

Cancel

Connect

### Step 3: Internet Connection (Static IP Address)

After selecting the Static IP Address Internet connection method, the following page will appear:

The following parameters will be available for configuration:

**IP Address:** Enter the static IP address provided by the ISP here.

**Subnet Mask:** Enter the subnet Mask provided by the ISP here.

**Gateway Address:** Enter the gateway IP address provided by the ISP here.

**Primary DNS Address:** Enter the primary DNS IP address used here.

**Secondary DNS Address:** Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

### Setup Complete!

This is the last page of the Internet Connection Setup Wizard.

Click the **Connect** button to save your settings.

**SET STATIC IP ADDRESS CONNECTION**

To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP.

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway Address : 0.0.0.0

**DNS SETTINGS**

Primary DNS Address : 0.0.0.0

Secondary DNS Address : 0.0.0.0 (optional)

Prev Next Cancel Connect

**SETUP COMPLETE!**

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings.

Prev Next Cancel Connect

## Internet (Manual)

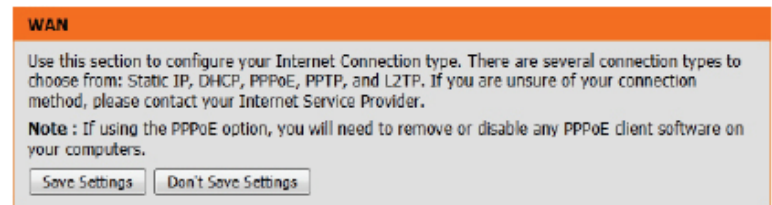
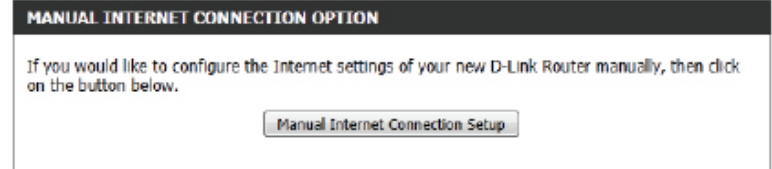
On this page the user can configure the Internet Connection settings manually. To access the Manual Internet Connection Setup page, click on the **Manual Internet Connection Setup** button. On this page there are multiple parameters that can be configured regarding the Internet connection setup.

At any given point the user can save the configuration done, on this page, by clicking on the **Save Settings** button. If you choose to discard the changes made, click on the **Don't Save Settings** button.

### Internet Connection Type

In this section, the user can select from a list of Internet connection types that can be configured and used on this router. Options to choose from are **Static IP, Dynamic IP, PPPoE, PPTP, L2TP, and DS-Lite**.

After selecting a specific Internet connection type, this page will automatically refresh to provide the relevant configuration options for the selected connection type.



### My Internet Connection is: Dynamic IP (DHCP)

The default WAN configuration for this router is Dynamic IP (DHCP). This option allows the router to obtain an IP address automatically from the device that is connected to the Internet port.

**Note:** If you're not sure about the type of Internet connection you have, please contact your Internet Service Provider (ISP) for assistance.

After selecting Dynamic IP, the following parameters will be available for configuration:

**Host Name:** The host name is optional but may be required by some ISPs. Leave blank if you are not sure.

**Use Unicasting:** Tick this option if your ISP uses the unicast method to provide IP addresses.

**Primary DNS:** Enter the primary DNS IP address used here.

**Secondary DNS:** Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

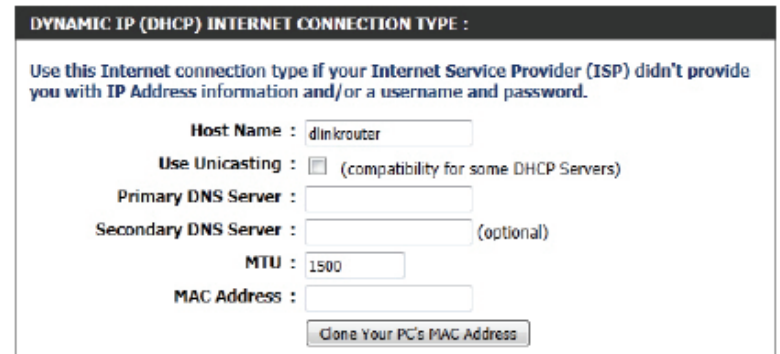
**MAC Address:** The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.



**INTERNET CONNECTION TYPE**

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : Dynamic IP (DHCP)



**DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :**

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name : dlinkrouter

Use Unicasting : ☐ (compatibility for some DHCP Servers)

Primary DNS Server :

Secondary DNS Server :  (optional)

MTU : 1500

MAC Address :

Clone Your PC's MAC Address

# Manual Internet Setup

## Static (assigned by ISP)

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format.

**My Internet Connection:** Select **Static IP** to manually enter the IP settings supplied by your ISP.

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

**Subnet Mask:** Enter the subnet mask assigned by your ISP.

**Default Gateway:** Enter the gateway assigned by your ISP.

**DNS Servers:** The DNS server information will be supplied by your ISP (Internet Service Provider.)

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1500 is the default MTU.

**MAC Address:** The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

**INTERNET CONNECTION TYPE**

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is :

**STATIC IP ADDRESS INTERNET CONNECTION TYPE :**

Enter the static address information provided by your Internet Service Provider (ISP).

IP Address :

Subnet Mask :

Default Gateway :

Primary DNS Server :

Secondary DNS Server :  (optional)

MTU :

MAC Address :

# Internet Setup

## PPPoE (DSL)

Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.

**My Internet Connection:** Select **PPPoE (Username/Password)** from the drop-down menu.

**Address Mode:** Here the user can specify whether this Internet connection requires the use of a **Dynamic** or **Static IP** address. PPPoE usually requires a Dynamic IP configuration.

**IP Address:** Enter the PPPoE IP address used here. This option is only available if Static IP is selected.

**Username:** Enter the PPPoE account username used here. This information is given by the ISP.

**Password:** Enter the PPPoE account password used here. This information is given by the ISP.

**Verify Password:** Re-enter the PPPoE account password used here.

**Service Name:** This optional field enables the user to enter a service name to identify this Internet connection here.

**Reconnect Mode:** Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : PPPoE (Username / Password)

PPPOE INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : ☒ Dynamic IP ☐ Static IP

IP Address :

Username :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : ☐ Always ☒ On demand ☐ Manual

Maximum Idle Time : (minutes, 0=infinite)

DNS Mode : ☒ Receive DNS from ISP ☐ Enter DNS Manually

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1492

MAC Address :

Clone Your PC's MAC Address

To create a new schedule, click the **New Schedule** button to open the Schedules page. Schedules will be discussed later.

**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity.

**DNS Mode:** This option allows the router to obtain the DNS IP addresses from the ISP, when **Receive DNS from ISP** is selected, or allows the user to enter DNS IP address manually, when **Enter DNS Manually** is selected.

**Primary DNS Server:** Enter the primary DNS IP address used here.

**Secondary DNS Server:** Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

**MAC Address:** The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

**PPPOE INTERNET CONNECTION TYPE :**

Enter the information provided by your Internet Service Provider (ISP).

**Address Mode :** ☒ Dynamic IP ☐ Static IP

**IP Address :**

**Username :**

**Password :**

**Verify Password :**

**Service Name :**  (optional)

**Reconnect Mode :** ☐ Always on  ☒ On demand ☐ Manual

**Maximum Idle Time :**  (minutes, 0=infinite)

**DNS Mode :** ☒ Receive DNS from ISP ☐ Enter DNS Manually

**Primary DNS Server :**

**Secondary DNS Server :**  (optional)

**MTU :**

**MAC Address :**



# Internet Setup

## PPTP

Choose PPTP (Point-to-Point-Tunneling Protocol ) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

**My Internet Connection:** Select **PPTP (Username/Password)** from the drop-down menu.

**Address Mode:** Here the user can specify whether this Internet connection requires the use of a **Dynamic** or **Static IP** address. PPTP usually requires a Dynamic IP configuration.

**PPTP IP Address:** Enter the PPTP IP address used here. This option is only available if Static IP is selected.

**PPTP Subnet Mask:** Enter the PPTP subnet mask used here.

**PPTP Gateway IP Address:** Enter the PPTP gateway IP address used here.

**PPTP Server IP Address:** Enter the PPTP server IP address used here. This is normally the same as the PPTP gateway IP address.

**Username:** Enter the PPTP username used here.

**Password:** Enter the PPTP password used here.

**Verify Password:** Re-enter the PPTP password used here.

**Reconnect Mode:** Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the **New Schedule** button to open the Schedules page. Schedules will be discussed later.

The screenshot shows the 'INTERNET CONNECTION TYPE' section of a router's configuration page. It prompts the user to 'Choose the mode to be used by the router to connect to the Internet.' The 'My Internet Connection is' dropdown menu is set to 'PPTP (Username / Password)'. Below this, the 'PPTP INTERNET CONNECTION TYPE' section asks the user to 'Enter the information provided by your Internet Service Provider (ISP)'. The configuration options include:
 

- Address Mode:** Radio buttons for 'Dynamic IP' (selected) and 'Static IP'.
- PPTP IP Address:** A text input field.
- PPTP Subnet Mask:** A text input field.
- PPTP Gateway IP Address:** A text input field.
- PPTP Server IP Address:** A text input field.
- Username:** A text input field.
- Password:** A text input field.
- Verify Password:** A text input field.
- Reconnect Mode:** Radio buttons for 'Always on' (selected), 'On demand', and 'Manual'. There is a 'New Schedule' button next to the 'Always on' option.
- Maximum Idle Time:** A text input field with '(minutes, 0=infinite)' as a hint.
- Primary DNS Server:** A text input field.
- Secondary DNS Server:** A text input field with '(optional)' as a hint.
- MTU:** A text input field with '1400' as the default value.
- MAC Address:** A text input field with a 'Clone Your PC's MAC Address' button next to it.

**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

**Primary DNS Server:** Enter the primary DNS IP address used here.

**Secondary DNS Server:** Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

**MAC Address:** The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

**PPTP INTERNET CONNECTION TYPE :**

Enter the information provided by your Internet Service Provider (ISP).

**Address Mode :** ☒ Dynamic IP ☐ Static IP

**PPTP IP Address :**

**PPTP Subnet Mask :**

**PPTP Gateway IP Address :**

**PPTP Server IP Address :**

**Username :**

**Password :**

**Verify Password :**

**Reconnect Mode :** ☒ Always ☐ New Schedule

☒ On demand ☐ Manual

**Maximum Idle Time :**  (minutes, 0=infinite)

**Primary DNS Server :**

**Secondary DNS Server :**  (optional)

**MTU :**  1400

**MAC Address :**

# Internet Setup

## L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.

**My Internet Connection:** Select **L2TP (Username/Password)** from the drop-down menu.

**Address Mode:** Here the user can specify whether this Internet connection requires the use of a dynamic or static IP address. L2TP usually requires a dynamic IP configuration.

**L2TP IP Address:** Enter the L2TP IP address used here. This option is only available if Static IP is selected.

**L2TP Subnet Mask:** Enter the L2TP subnet mask used here.

**L2TP Gateway IP Address:** Enter the L2TP gateway IP address used here.

**L2TP Server IP Address:** Enter the L2TP server IP address used here. This is normally the same as the L2TP gateway IP address.

**Username:** Enter the L2TP username used here.

**Password:** Enter the L2TP password used here.

**Verify Password:** Re-enter the L2TP password used here.

**Reconnect Mode:** Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the New Schedule button to open the Schedules page. Schedules will be discussed later.

INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : L2TP (Username / Password)

L2TP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : ☒ Dynamic IP ☐ Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : ☐ Always on ☒ On demand ☐ Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1400

MAC Address :

Clone Your PC's MAC Address

**Maximum Idle Time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

**Primary DNS Server:** Enter the primary DNS IP address used here.

**Secondary DNS Server:** Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1400 is the default MTU.

**MAC Address:** The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

**L2TP INTERNET CONNECTION TYPE :**

Enter the information provided by your Internet Service Provider (ISP).

**Address Mode :** ☒ Dynamic IP ☐ Static IP

**L2TP IP Address :**

**L2TP Subnet Mask :**

**L2TP Gateway IP Address :**

**L2TP Server IP Address :**

**Username :**

**Password :**

**Verify Password :**

**Reconnect Mode :** ☐ Always on ☒ On demand ☐ Manual

**Maximum Idle Time :**  (minutes, 0=infinite)

**Primary DNS Server :**

**Secondary DNS Server :**  (optional)

**MTU :**

**MAC Address :**

## Internet Setup

### DS-Lite

DS-Lite is an IPv6 connection type. After selecting DS-Lite, the following parameters will be available for configuration:

**DS-Lite Configuration:** Select the **DS-Lite DHCPv6 Option** to let the router allocate the AFTR IPv6 address automatically. Select the **Manual Configuration** to enter the AFTR IPv6 address in manually.

**AFTR IPv6 Address:** After selecting the Manual Configuration option above, the user can enter the AFTR IPv6 address used here.

**B4 IPv4 Address:** Enter the B4 IPv4 address value used here.

**WAN IPv6 Address:** Once connected, the WAN IPv6 address will be displayed here.

**IPv6 WAN Default Gateway** Once connected, the IPv6 WAN default gateway address will be displayed here.

Click on the **Save Settings** button to accept the changes made.

Click on the **Don't Save Settings** button to discard the changes made.

The screenshot shows the 'INTERNET CONNECTION TYPE' configuration page. The first section, 'INTERNET CONNECTION TYPE', prompts the user to 'Choose the mode to be used by the router to connect to the Internet.' and shows 'My Internet Connection is : DS-Lite' selected in a dropdown menu. The second section, 'AFTR ADDRESS INTERNET CONNECTION TYPE', prompts the user to 'Enter the AFTR address information provided by your Internet Service Provider (ISP)'. It contains two radio buttons for 'DS-Lite Configuration': 'DS-Lite DHCPv6 Option' (which is selected) and 'Manual Configuration'. Below these are four fields: 'AFTR IPv6 Address' (empty), 'B4 IPv4 Address' (pre-filled with '192.0.0.' and an '(optional)' label next to an empty box), 'WAN IPv6 Address' (empty), and 'IPv6 WAN Default Gateway' (empty).

# Wireless Connection Setup Wizard

On this page the user can configure the wireless settings for this device. There are 3 ways to configure wireless using this router. Firstly, the user can choose the quick and easy **Wireless Connection Setup Wizard**. Secondly, the user can choose to make use of Wi-Fi Protected Setup. Lastly, the user can configure the wireless settings manually.

## Wireless Settings: Wireless Connection Setup Wizard

The Wireless Connection Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to configure the wireless settings of this router. It is highly recommended to customize the wireless network settings to fit into your environment and to add higher security.

To initiate the **Wireless Connection Setup Wizard** click on the Wireless Connection Setup Wizard button.

**Step 1:** In this step, the user must enter a custom Wireless Network Name or SSID. Enter the new **Network Name (SSID)** in the appropriate space provided.

There are separate spaces provided for a **2.4 GHz** Network Name and a **5 GHz** Network Name.

Secondly the user can choose between two wireless security wizard configurations. The user can select **Automatically assign a network key**, by which the router will automatically generate a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods; or the user can select **Manually assign a network key**, by which the user will be prompted to manually enter a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

**WIRELESS SETTINGS**

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

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

**WIRELESS NETWORK SETUP WIZARD**

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Wireless Connection Setup Wizard

**Note:** Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

**STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD**

Give your network a name, using up to 32 characters.

Network Name (SSID) 2.4GHz :

Network Name (SSID) 5GHz :

☒ **Automatically assign a network key (Recommended)**  
To prevent outsiders from accessing your network, the router will automatically assign a security (also called WEP or WPA key) to your network.

☐ **Manually assign a network key**  
Use this options if you prefer to create our own key.

**Note:** All D-Link wireless adapters currently support WPA.

Prev Next Cancel Save



**Step 2:** This step will only be available if the user selected **Manually assign a network key** in the previous step. Here the user can manually enter the WPA/WPA2 pre-shared key in the **Wireless Security Password** space provided. The key entered must be between 8 and 63 characters long. Remember, this key will be used when wireless clients want to connect to this device. So please remember this key to prevent future troubleshooting. If you want to use the same Wireless Security Password for both 2.4 GHz and 5 GHz bands, **tick** the option provided. If not selected, you need to input two separate Wireless Security Passwords for each individual Wireless band.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

**Setup Complete:** On this page the user can view the configuration made and verify whether they are correct.

Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard the changes made and return to the main wireless page. Click on the **Save** button to accept the changes made.

**STEP 2: SET YOUR WIRELESS SECURITY PASSWORD**

You have selected your security level - you will need to set a wireless security password.

The WPA (Wi-Fi Protected Access) key must meet one of following guidelines:

- Between 8 and 63 characters (A longer WPA key is more secure than a short one)
- Exactly 64 characters using 0-9 and A-F

☐ Use the same Wireless Security Password on both 2.4GHz and 5GHz band

2.4Ghz Wireless Security Password :

5Ghz Wireless Security Password :

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

**SETUP COMPLETE!**

Below is a detailed summary of your wireless security 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.

**Wireless Band :** 2.4GHz Band

**Wireless Network Name (SSID) :** dlink-ecb8

**Security Mode :** Auto (WPA or WPA2) - Personal

**Cipher Type :** TKIP and AES

**Pre-Shared Key :** 2c2dbdb54

**Wireless Band :** 5GHz Band

**Wireless Network Name (SSID) :** dlink-media-ecba

**Security Mode :** Auto (WPA or WPA2) - Personal

**Cipher Type :** TKIP and AES

**Pre-Shared Key :** 2c2dbdb54

After clicking the **Save** button the device will save the settings made and return to the main wireless page.

**End of Wizard.**





# Wi-Fi Protected Setup Wizard

## Wireless Settings: Wi-Fi Protected Setup Wizard

If your Wireless Clients support the WPS connection method, this Wi-Fi Protected Setup Wizard can be used to initiate a wireless connection between this device and Wireless clients with a simple click of the WPS button. The Wi-Fi Protected Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to connect wireless clients to this router using the WPS method.

To initiate the Wi-Fi Protected Setup Wizard click on the **Add Wireless Device with WPS** button.

**Step 1:** In this step the user have two options to choose from. You can choose **Auto** if the wireless client supports WPS, or **Manual** if the wireless client does not support WPS.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

**Step 2:** After selecting **Auto**, the following page will appear. There are two ways to add a wireless device, that supports WPS. Firstly, there is the Personal Identification Number (**PIN**) method. Using this method will prompt the user to enter a PIN code. This PIN code should be identical on the wireless client. Secondly, there is the Push Button Configuration (**PBC**) method. Using this method will allow the wireless client to connect to this device by similarly pressing the PBC button on it.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page.

**ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD**

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

**Add Wireless Device with WPS**

**STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK**

Please select one of following configuration methods and click next to continue.

**Auto** ☒ Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

**Manual** ☐ Select this option will display the current wireless settings for you to configure the wireless device manually

**Prev** **Next** **Cancel** **Connect**

**STEP 2: CONNECT YOUR WIRELESS DEVICE**

There are two ways to add wireless device to your wireless network:  
 -PIN (Personal Identification Number)  
 -PBC (Push Button Configuration)

**PIN** ☒

please enter the PIN from your wireless device and click the below "Connect" Button within 120 seconds

**PBC** ☐

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

**Prev** **Next** **Cancel** **Connect**

**Step 2:** After selecting Manual, the following page will appear. On this page to user can view the wireless configuration of this router. The wireless clients should configure their wireless settings to be identical to the settings displayed on this page for a successful connection. This option is for wireless clients that can't use the WPS method to connect to this device.

Click on the **Prev** button to return to the previous page. Click on the **Next** button to continue to the next page. Click on the **Cancel** button to discard the changes made and return to the main wireless page. Click on the **Wireless Status** button to navigate to the Status > Wireless page to view what wireless client are connected to this device.

### End of Wizard.

**STEP 2: CONNECT YOUR WIRELESS DEVICE**

Below is a detailed summary of your wireless security 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.

**2.4 Ghz Frequency**  
SSID: dlink-ecb8  
Security Mode: Auto (WPA or WPA2) - Personal  
Cipher Type: TKIP and AES  
Pre-shared Key: 24key24key

**5 Ghz Frequency**  
SSID: dlink-media-ecba  
Security Mode: Auto (WPA or WPA2) - Personal  
Cipher Type: TKIP and AES  
Pre-shared Key: 50key50key

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-822 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 - generally missing in WEP - is made stronger using 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.

# Manual Wireless Network Setup

## Wireless Settings: Manual Wireless Network Setup

The manual wireless network setup option allows users to configure the wireless settings of this device manually. This option is for the more advanced users and includes all parameters that can be configured for wireless connectivity.

To initiate the Manual Wireless Setup page, click on the **Manual Wireless Connection Setup** button.

On this page the user can configure all the parameters related to the wireless connectivity of this router.

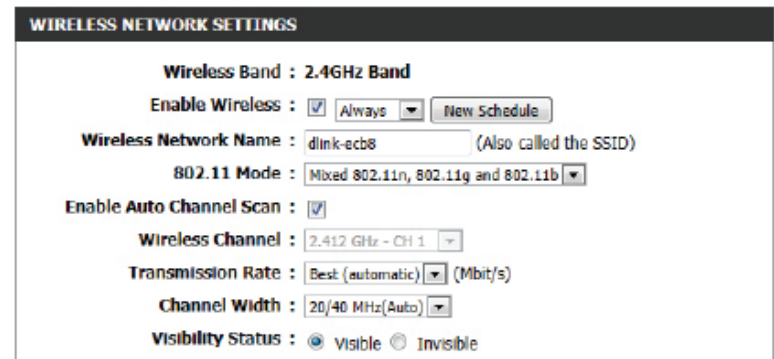
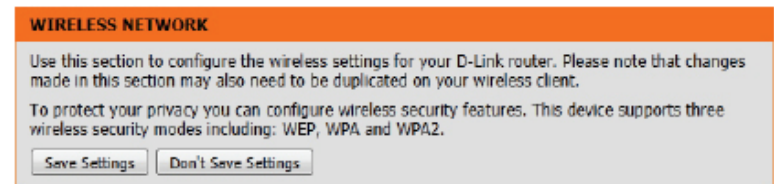
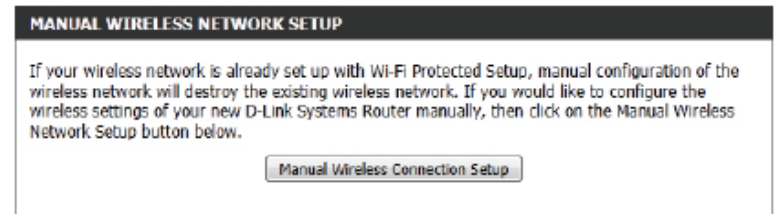
The following parameters will be available for configuration:

**Wireless Band:** Displays the wireless band being configured. In this option we find that the following parameters will be regarding the 2.4 GHz band.

**Enable Wireless:** Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click New Schedule to create a new schedule.

**Wireless Network Name:** The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive. Enable Auto Channel

**802.11 Mode:** Here the user can manually select the preferred frequency band to use for this wireless network.



**Enable Auto Channel Scan:** The auto channel selection setting can be selected to allow this device to choose the channel with the least amount of interference.

**Wireless Channel:** By default the channel is set to 1. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.

**Transmission Rate:** Select the transmit rate. It is strongly suggested to select Best (Automatic) for best performance.

**Channel Width:** When using the 802.11n frequency band, the user has an option to choose between a 20 MHz or 20/40 MHz bandwidth.

**Visibility Status:** The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually to connect to the network.

By default the wireless security of this router will be disabled. In this next option the user can enable or disable wireless security for the frequency band 2.4 GHz. There are two types of encryption that can be used. WEP or WPA/WPA2.

### Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. Even though it is known as a 'weak' security method, it is better than no security at all. Older wireless adapter sometimes only supports WEP encryption and thus we still find this encryption method used today.

The following parameters will be available for configuration:

**WEP Key Length:** Here the user can specify to either use a 64 bit or a 128 bit encrypted key.

**Authentication:** Authentication is a process by which the router verifies the identity of a network device that is attempting to join the wireless network. There are two types authentication for this device when using WEP. **Open System** allows all wireless devices to communicate with the router before they are required to provide the encryption key needed to gain access to the network. **Shared Key** requires any wireless device attempting to communicate with the router to provide the encryption key needed to access the network before they are allowed to communicate with the router.

**WEP Key 1:** Enter the WEP key used here. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WIRELESS SECURITY MODE

Security Mode : None

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP Key Length : 64 bit (10 hex digits) (length applies to all keys)

Authentication : Both

WEP Key 1 :

**Wireless Security Mode: WPA-Personal**

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a pass-phrase (Shared Secret) for security.

The following parameters will be available for configuration:

**WPA Mode:** WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the “WPA2” option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the “WPA2 Only” option, the router associates only with clients that also support WPA2 security.

**Cipher Type:** Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES).

**Group Key Update Interval:** Enter the amount of time before the group key used for broadcast and multicast data is changed.

**Pre-Shared Key:** Enter the shared secret phrase used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

| WIRELESS SECURITY MODE   |                      |
|--|----------------------|
| Security Mode :  | WPA-Personal ▼       |
| <b>WPA</b><br>Use <b>WPA</b> or <b>WPA2</b> mode to achieve a balance of strong security and best compability. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use <b>WPA2 Only</b> mode. This mode uses AES(CCM) cipher and legacy stations are not allowed access with WPA security. For maximum compability, use <b>WPA Only</b> . This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.<br><br>To achieve better wireless performance use <b>WPA2 Only</b> security mode (or in other words AES cipher). |                      |
| WPA Mode :   | Auto(WPA or WPA2) ▼  |
| Cipher Type :  | TKIP and AES ▼       |
| Group Key Update Interval :  | 3600 (seconds)       |
| <b>PRE-SHARED KEY</b><br>Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.   |                      |
| Pre-Shared Key :   | <input type="text"/> |



**Wireless Security Mode: WPA-Enterprise**

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a pass-phrase (Shared Secret) for security.

The following parameters will be available for configuration:

**WPA Mode:** WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the “WPA2” option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the “WPA2 Only” option, the router associates only with clients that also support WPA2 security.

**Cipher Type:** Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES).

**Group Key Update Interval:** Enter the amount of time before the group key used for broadcast and multicast data is changed.

**RADIUS Server IP Address:** When the user chooses to use the EAP authentication framework, the RADIUS server’s IP address can be entered here.

**RADIUS Server Port:** When the user chooses to use the EAP authentication framework, the RADIUS server’s port number can be entered here.

**RADIUS Server Shared Secret:** Enter the shared secret used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

WPA

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

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

WPA Mode : Auto(WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

EAP (802.1X)

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

RADIUS server IP Address :

RADIUS server Port : 1812

RADIUS server Shared Secret :

Advanced >>



The following parameters will be available for configuration:

**Wireless Band:** Displays the wireless band being configured. In this option we find that the following parameters will be regarding the 5 GHz band.

**Enable Wireless:** Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions. Select the time frame that you would like your wireless network enabled. The schedule may be set to Always. Any schedule you create will be available in the drop-down menu. Click New Schedule to create a new schedule.

**Wireless Network Name:** The Service Set Identifier (SSID) is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive. Enable Auto Channel

**802.11 Mode:** Here the user can manually select the preferred frequency band to use for this wireless network.

**Enable Auto Channel Scan:** The auto channel selection setting can be selected to allow this device to choose the channel with the least amount of interference.

**Wireless Channel:** By default the channel is set to 36. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable Auto Channel Selection, this option will be greyed out.

**Transmission Rate:** Select the transmit rate. It is strongly suggested to select Best (Automatic) for best performance.

**Channel Width:** When using the 802.11n frequency band, the user has an option to choose between a 20 MHz, 20/40 MHz, or 20/40/80 MHz bandwidth.

**Visibility Status:** The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) on the client manually, to connect to the network.

**WIRELESS NETWORK SETTINGS**

Wireless Band : 5GHz Band

Enable Wireless : ☒ Always

Wireless Network Name : dlink-media-ecba (Also called the SSID)

802.11 Mode : Mixed 802.11ac

Enable Auto Channel Scan : ☒

Wireless Channel : 5.180 GHz - CH 36

Transmission Rate : Best (automatic) (Mbit/s)

Channel Width : 20/40/80 MHz(Auto)

Visibility Status : ☒ Visible ☐ Invisible

By default the wireless security of this router will be disabled. In this next option the user can enable or disable wireless security for the frequency band 5 GHz. There are two types of encryption that can be used. WEP or WPA/WPA2.

### Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption used for wireless networks. If you have an older wireless adapter that only supports WEP encryption, please select this option.

The following parameters will be available for configuration:

**WEP Key Length:** Here the user can specify to either use a 64 bit or a 128 bit encrypted key.

**Authentication:** Authentication is a process by which the router verifies the identity of a network device that is attempting to join the wireless network. There are two types authentication for this device when using WEP. **Open System** allows all wireless devices to communicate with the router before they are required to provide the encryption key needed to gain access to the network. **Shared Key** requires any wireless device attempting to communicate with the router to provide the encryption key needed to access the network before they are allowed to communicate with the router.

**WEP Key 1:** Enter the WEP key used here. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

WIRELESS SECURITY MODE

Security Mode : None

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.

WEP Key Length :

64 bit (10 hex digits)

(length applies to all keys)

Authentication :

Both

WEP Key 1 :

**Wireless Security Mode: WPA-Personal**

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP).

The following parameters will be available for configuration:

**WPA Mode:** WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the “WPA2” option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the “WPA2 Only” option, the router associates only with clients that also support WPA2 security.

**Cipher Type:** Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES).

**Group Key Update Interval:** Enter the amount of time before the group key used for broadcast and multicast data is changed.

**Pre-Shared Key:** Enter the shared secret phrase used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

| WIRELESS SECURITY MODE   |  |
|--|--|
| Security Mode : <input type="text" value="WPA-Personal"/>  |  |
| <b>WPA</b>   |  |
| <p>Use <b>WPA or WPA2</b> mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use <b>WPA2 Only</b> mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use <b>WPA Only</b>. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.</p> <p>To achieve better wireless performance use <b>WPA2 Only</b> security mode (or in other words AES cipher).</p> |  |
| <p>WPA Mode : <input type="text" value="Auto(WPA or WPA2)"/></p> <p>Cipher Type : <input type="text" value="TKIP and AES"/></p> <p>Group Key Update Interval : <input type="text" value="3600"/> (seconds)</p>   |  |
| <b>PRE-SHARED KEY</b>  |  |
| <p>Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.</p> <p>Pre-Shared Key : <input type="text"/></p>  |  |

### Wireless Security Mode: WPA-Enterprise

Wi-Fi Protected Access (WPA) is the most advanced and up to date wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP).

The following parameters will be available for configuration:

**WPA Mode:** WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. With the “WPA2” option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the “WPA2 Only” option, the router associates only with clients that also support WPA2 security.

**Cipher Type:** Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (TKIP), Advanced Encryption Standard (AES), and Both (TKIP and AES).

**Group Key Update Interval:** Enter the amount of time before the group key used for broadcast and multicast data is changed.

**RADIUS Server IP Address:** If you choose to use the EAP authentication framework, the RADIUS server’s IP address can be entered here.

**RADIUS Server Port:** If you choose to use the EAP authentication framework, the RADIUS server’s port number can be entered here.

**RADIUS Server Shared Secret:** Enter the shared secret used here. This secret phrase needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

WPA

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

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

WPA Mode : Auto(WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)

EAP (802.1X)

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

RADIUS server IP Address :

RADIUS server Port : 1812

RADIUS server Shared Secret :

Advanced >>

# Network Settings

This section will allow you to change the local network settings of the router and to configure the DHCP settings.

## Router Settings

**Router IP Address:** Enter the IP address of the router. The default IP address is **192.168.0.1**.

**Note:** *If you change the IP address, once you click **Save Settings**, 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**.

**Device Name:** Enter a name for the router.

**Local Domain:** Enter the domain name (Optional).

**Enable DNS Relay:** Uncheck the box to transfer the DNS server information from your ISP to your computers. If checked, your computers will use the router for a DNS server.

**NETWORK SETTINGS**

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP server to assign IP addresses to computers on your network. The 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 in this section, you may need to adjust your PC's network settings to access the network again.

**Please note that this section is optional and you do not need to change any of the settings here to get your network up and running.**

**ROUTER SETTINGS**

Use this section to configure the internal network settings of your router. The 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 :**

**Default Subnet Mask :**

**Host Name :**

**Local Domain Name :**  (optional)

**Enable DNS Relay :** ☒

## DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-822 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers as DHCP clients by setting their TCP/IP settings to **Obtain an IP Address Automatically**. When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-822. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

**Enable DHCP Server:** Check this box to enable the DHCP server on your router.  
**Server:** Uncheck to disable this function.

**DHCP IP Address Range:** Enter the starting and ending IP addresses for the DHCP server's IP assignment.

**Note:** If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.

**DHCP Lease Time:** The length of time for the IP address lease. Enter the Lease time in minutes.

**Always Broadcast:** If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

**NetBIOS Announcement:** Check this box to allow the DHCP Server to offer NetBIOS configuration settings to the LAN hosts. NetBIOS allow LAN hosts to discover all other computers within the network, e.g. within network neighborhood.

The screenshot shows the 'DHCP SERVER SETTINGS' page. At the top, it says 'Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.' The settings are as follows:

- Enable DHCP Server :** ☒ (checked)
- DHCP IP Address Range :** 100 to 199 (addresses within the LAN subnet)
- DHCP Lease Time :** 10080 (minutes)
- Always broadcast :** ☒ (compatibility for some DHCP Clients)
- NetBIOS announcement :** ☐ (unchecked)
- Learn NetBIOS from WAN :** ☐ (unchecked)
- NetBIOS Scope :** (empty field) (optional)
- NetBIOS node type :**
  - ☐ Broadcast only (use when no WINS servers configured)
  - ☐ Point-to-Point (no broadcast)
  - ☒ Mixed-mode (Broadcast then Point-to-Point)
  - ☐ Hybrid (Point-to-Point then Broadcast)
- Primary WINS IP Address :** (empty field)
- Secondary WINS IP Address :** (empty field)



**Learn NetBIOS from WAN:** If NetBIOS announcement is switched on, it will cause WINS information to be learned from the WAN side, if available. Turn this setting off to configure manually.

**NetBIOS Scope:** This is an advanced setting and is normally left blank. This allows the configuration of a NetBIOS 'domain' name under which network hosts operate. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

**NetBIOS Node:** This field indicates how network hosts are to perform NetBIOS name registration and discovery. **Hybrid** or H-Node, this indicates a Hybrid-State of operation. First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers. **Mixed-mode** or M-Node (default), this indicates a Mixed-Mode of operation. First Broadcast operation is performed to register hosts and discover other hosts, if broadcast operation fails, WINS servers are tried, if any. This mode favours broadcast operation which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN. **Point-to-point** or P-Node, this indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operation to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server. **Broadcast only** or B-Node, this indicates to use local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is preferred you try M-Node operation first. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated.

#### WINS IP

**Address:** Enter your WINS Server IP address(es).

**DHCP SERVER SETTINGS**

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

**Enable DHCP Server :** ☒

**DHCP IP Address Range :** 100 to 199 (addresses within the LAN subnet)

**DHCP Lease Time :** 10080 (minutes)

**Always broadcast :** ☒ (compatibility for some DHCP Clients)

**NetBIOS announcement :** ☐

**Learn NetBIOS from WAN :** ☐

**NetBIOS Scope :**  (optional)

**NetBIOS node type :**

- ☐ Broadcast only (use when no WINS servers configured)
- ☐ Point-to-Point (no broadcast)
- ☒ Mixed-mode (Broadcast then Point-to-Point)
- ☐ Hybrid (Point-to-Point then Broadcast)

**Primary WINS IP Address :**

**Secondary WINS IP Address :**

## DHCP Reservation

If you want a computer or device to always have the same IP address assigned, you can create a DHCP reservation. The router will assign the IP address only to that computer or device.

**Note:** This IP address must be within the DHCP IP Address Range.

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

**Computer Name:** Enter the computer name or select from the drop-down menu and click <<.

**IP Address:** Enter the IP address you want to assign to the computer or device. This IP Address must be within the DHCP IP Address Range.

**MAC Address:** Enter the MAC address of the computer or device.

**Clone Your PC's MAC Address:** If you want to assign an IP address to the computer you are currently on, click this button to populate the fields.

**DHCP Reservations List:** Displays any reservation entries. Displays the host name (name of your computer or device), MAC address, and IP address.

**Enable:** Check to enable the reservation.

**Edit:** Click the edit icon to make changes to the reservation entry.

**Delete:** Click to remove the reservation from the list.

**Revoke:** Click to revoke the assigned IP address.

**Reserve:** Click to reserve the IP address.

ADD DHCP RESERVATION

Enable : ☐

Computer Name :  << Computer Name ▼

IP Address :

MAC Address :

Clone Your PC's MAC Address

Add / Update Clear



DHCP RESERVATIONS LIST

| Enable | Host Name | IP Address | MAC Address |
|--------|-----------|------------|-------------|
|--------|-----------|------------|-------------|

NUMBER OF DYNAMIC DHCP CLIENTS

| Host Name     | IP Address    | MAC Address       | Expired Time               |
|---------------|---------------|-------------------|----------------------------|
| Windows-Phone | 192.168.0.136 | 54:79:75:fe:77:ac | 6 Days 23 Hours 53 Minutes |

DHCP RESERVATIONS LIST

| Enable                              | Host Name | MAC Address       | IP Address    |   |
|-------------------------------------|-----------|-------------------|---------------|---|
| <input checked="" type="checkbox"/> | PM_test01 | 00:04:23:2c:51:a3 | 192.168.0.112 |   |

NUMBER OF DYNAMIC DHCP CLIENTS : 1

| Hardware Address  | Assigned IP   | Hostname  | Expires                 |  |
|-------------------|---------------|-----------|-------------------------|--|
| 00:04:23:2c:51:a3 | 192.168.0.112 | PM_test01 | Thu Sep 1 19:49:06 2011 | <a href="#">Revoke</a> <a href="#">Reserve</a> |



# IPv6

On this page, the user can configure the IPv6 Connection type. There are two ways to set up the IPv6 Internet connection. You can use the web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

For the beginner user that has not configured a router before, click on the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.

To configure the IPv6 local settings, click on the **IPv6 Local Connectivity Setup** button.

For the advanced user that has configured a router before, click on the **Manual IPv6 Internet Connection Setup** button to input all the settings manually.

**IPv6 INTERNET CONNECTION**

There are two ways to set up your IPv6 Internet connection. You can use the Web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

**IPv6 INTERNET CONNECTION SETUP WIZARD**

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the IPv6 Internet, click on the button below.

[IPv6 Internet Connection Setup Wizard](#)

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

**MANUAL IPv6 LOCAL CONNECTIVITY SETUP**

If you would like to configure the IPv6 local connectivity settings of your D-Link Router, then click on the button below.

[IPv6 Local Connectivity Settings](#)

**MANUAL IPv6 INTERNET CONNECTION SETUP**

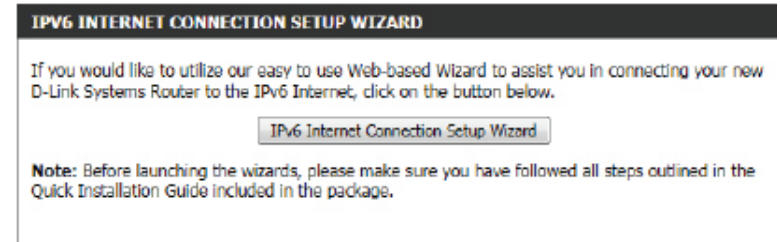
If you would like to configure the IPv6 Internet settings of your new D-Link Router manually, then click on the button below.

[Manual IPv6 Internet Connection Setup](#)

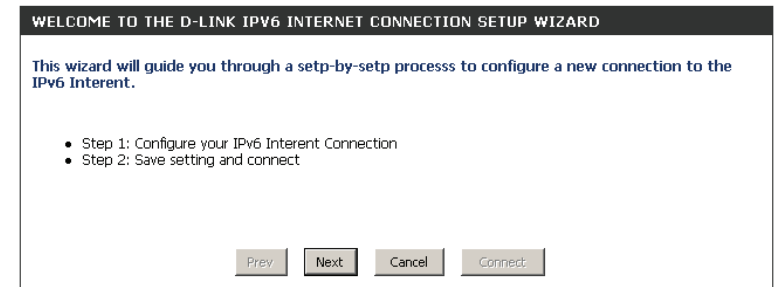
## IPv6 Internet Connection Setup Wizard

On this page, the user can configure the IPv6 Connection type using the IPv6 Internet Connection Setup Wizard.

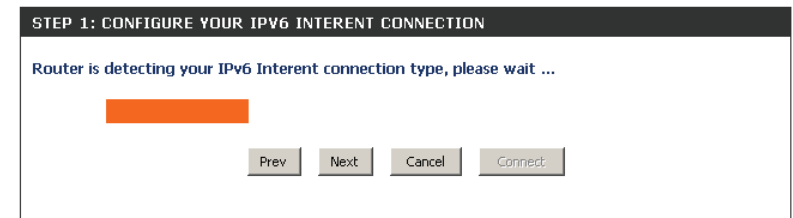
Click the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.



Click **Next** to continue to the next page. Click **Cancel** to discard the changes made and return to the main page.



The router will try to detect whether its possible to obtain the IPv6 Internet connection type automatically. If this succeeds then the user will be guided through the input of the appropriate parameters for the connection type found.



However, if the automatic detection fails, the user will be prompt to either **Try again** or to click on the **Guide me through the IPv6 settings** button to initiate the manual continual of the wizard.

There are several connection types to choose from. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

**Note:** If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled. The 3 options available on this page are **IPv6 over PPPoE**, **Static IPv6 address and Route**, and **Tunneling Connection**.

Choose the required IPv6 Internet Connection type and click on the **Next** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

Click on the **Next** button to continue. Click on the **Prev** button to return to the previous page.

Click on the **Cancel** button to discard all the changes made and return to the main page.

STEP 1: CONFIGURE YOUR IPV6 INTERENT CONNECTION

Router is unable detect your IPv6 Internet connection type

Buttons: Cancel, Try again, Guide me through the IPv6 setting

STEP 1: CONFIGURE YOUR IPV6 INTERENT CONNECTION

Please select your IPv6 Interent Connection type

- ☒ **IPv6 over PPPoE**  
Choose this option if your IPv6 Interent connection requires a username and password to get online. Most DSL modems use this type of connection.
- ☐ **Static IPv6 address and Route**  
Choose this option if your Interent Service Provider (ISP) provided you with IPv6 address information that has to be manually configured.
- ☐ **Tunneling Connection (6rd)**  
Choose this option if your Interent Service Provider (ISP) provided you a IPv6 Internet connection by using 6rd automatic tunneling mechanism.

Buttons: Prev, Next, Cancel, Connect

### IPv6 over PPPoE

After selecting the IPv6 over PPPoE option, the user will be able to configure the IPv6 Internet connection that requires a username and password to get online. Most DSL modems use this type of connection.

The following parameters will be available for configuration:

**PPPoE Session:** Select the PPPoE Session value used here. This option will state that this connection shares its information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.

**User Name:** Enter the PPPoE username used here. If you do not know your user name, please contact your ISP.

**Password:** Enter the PPPoE password used here. If you do not know your password, please contact your ISP.

**Verify Password:** Re-enter the PPPoE password used here.

**Service Name:** Enter the service name for this connection here. This option is optional.

**SET USERNAME AND PASSWORD CONNECTION (PPPOE)**

To set up this connection you will need to have a Username and Password from your IPv6 Internet Service Provider. If you do not have this information, please contact your ISP.

PPPoE Session: ☒ Share with IPv4 ☐ Create a new session

Username :

Password :

Verify Password :

Service Name :  (Optional)

Note: You may also need to provide a Service Name. If you do not have or know this information, please contact your ISP.

## Static IPv6 Address Connection

This mode is used when your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings. You must enter the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server, and Secondary DNS Server. Your ISP provides you with all this information.

**Use Link-Local Address:** The Link-local address is used by nodes and routers when communicating with neighboring nodes on the same link. This mode enables IPv6-capable devices to communicate with each other on the LAN side.

**IPv6 Address:** Enter the WAN IPv6 address for the router here.

**Subnet Prefix Length:** Enter the WAN subnet prefix length value used here.

**Default Gateway:** Enter the WAN default gateway IPv6 address used here.

**Primary IPv6 DNS Address:** Enter the WAN primary DNS server address used here.

**Secondary IPv6 DNS Address:** Enter the WAN secondary DNS server address used here.

**LAN IPv6 Address:** These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 address configuration is based on the IPv6 address and subnet assigned by your ISP. (A subnet with prefix /64 is supported in here.)

**SET STATIC IPV6 ADDRESS CONNECTION**

To set up this connection you will need to have a complete list of IPv6 information provided by your IPv6 Internet Service Provider. If you have a Static IPv6 connection and do not have this information, please contact your ISP.

Use Link-Local Address : ☒

IPv6 Address : FE80::218:E7FF:FE95:689F

Subnet Prefix Length : 64

Default Gateway :

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 Address : /64

Prev Next Cancel Connect

## Tunneling Connection (6rd)

After selecting the Tunneling Connection (6rd) option, the user can configure the IPv6 6rd connection settings.

The following parameters will be available for configuration:

**6rd IPv6 Prefix:** Enter the 6rd IPv6 address and prefix value used here.

**IPv4 Address:** Enter the IPv4 address used here.

**Mask Length:** Enter the IPv4 mask length used here.

**Assigned IPv6 Prefix:** Displays the IPv6 assigned prefix value here.

**6rd Border Relay IPv4 Address:** Enter the 6rd border relay IPv4 address used here.

**IPv6 DNS Server:** Enter the primary DNS server address used here.

SET UP 6RD TUNNELING CONNECTION

To set up this 6rd tunneling connection you will need to have the following information from your IPv6 Internet Service Provider. If you do not have this information, please contact your ISP.

6rd IPv6 Prefix :  /

IPv4 Address : 192.168.1.2 Mask Length :

Assign IPv6 Prefix : None

Tunnel Link-Local Address : FE80::C0A8:0102/64

6rd Border Relay IPv4 Address :

IPv6 DNS Server :

The IPv6 Internet Connection Setup Wizard is complete.

Click on the **Connect** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

SETUP COMPLETE!

The IPv6 Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

## IPv6 Manual Setup

There are several connection types to choose from: Auto Detection, Static IPv6, Autoconfiguration (SLAAC/DHCPv6), PPPoE, IPv6 in IPv4 Tunnel, 6to4, 6rd, and Link-local. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

**Note:** If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled.

### Auto Detection

Select **Auto Detection** to have the router detect and automatically configure your IPv6 settings from your ISP.

| IPv6 CONNECTION TYPE  |
|---|
| Choose the mode to be used by the router to the IPv6 Internet.  |
| My IPv6 Connection is : <span>Auto Detection</span>   |
| IPv6 DNS SETTINGS   |
| Obtain a DNS server address automatically or enter a specific DNS server address.   |
| <input checked="" type="radio"/> Obtain a DNS server address automatically<br><input type="radio"/> Use the following DNS address   |
| Primary DNS Server : <input type="text"/>   |
| Secondary DNS Server : <input type="text"/>   |
| LAN IPv6 ADDRESS SETTINGS   |
| Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again. |
| Enable DHCP-PD : <input checked="" type="checkbox"/>  |
| LAN IPv6 Address : <input type="text"/> /64   |
| LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64   |
| ADDRESS AUTOCONFIGURATION SETTINGS  |
| Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.                |
| Enable automatic IPv6 address assignment : <input checked="" type="checkbox"/>  |
| Enable Automatic DHCP-PD in LAN : <input checked="" type="checkbox"/>   |
| Autoconfiguration Type : <span>SLAAC + Stateless DHCPv6</span>  |
| Router Advertisement Lifetime: <input type="text"/> (minutes)   |

## Static IPv6

**My IPv6 Connection:** Select **Static IPv6** from the drop-down menu.

**WAN IPv6 Address Settings:** Enter the address settings supplied by your Internet provider (ISP).

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the router's LAN link-local address.

**Enable automatic IPv6 address assignment:** Check to enable the autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 address for the DHCPv6 range for your local computers.

**IPv6 Address Lifetime:** Enter the IPv6 address lifetime (in minutes).

| IPv6 CONNECTION TYPE  |
|---|
| <p>Choose the mode to be used by the router to the IPv6 Internet.</p> <p>My IPv6 Connection is : <input type="text" value="Static IPv6"/></p>   |
| WAN IPv6 ADDRESS SETTINGS   |
| <p>Enter the IPv6 address information provided by your Internet Service Provider (ISP).</p> <p>Use Link-Local Address : <input checked="" type="checkbox"/></p> <p>IPv6 Address : <input type="text" value="FE80::218:E7FF:FE95:689F"/></p> <p>Subnet Prefix Length : <input type="text" value="64"/></p> <p>Default Gateway : <input type="text"/></p> <p>Primary DNS Server : <input type="text"/></p> <p>Secondary DNS Server : <input type="text"/></p> |
| LAN IPv6 ADDRESS SETTINGS   |
| <p>Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.</p> <p>LAN IPv6 Address : <input type="text"/> /64</p> <p>LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64</p>  |
| ADDRESS AUTOCONFIGURATION SETTINGS  |
| <p>Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.</p> <p>Enable automatic IPv6 address assignment : <input checked="" type="checkbox"/></p> <p>Autoconfiguration Type : <input type="text" value="SLAAC + Stateless DHCPv6"/></p> <p>Router Advertisement Lifetime : <input type="text" value="1440"/> (minutes)</p>   |



## Autoconfiguration

**My IPv6 Connection:** Select **Autoconfiguration (Stateless/DHCPv6)** from the drop-down menu.

**IPv6 DNS Settings:** Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

**Primary/Secondary DNS Address:** Enter the primary and secondary DNS server addresses.

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the router's LAN link-local address.

### Enable Automatic IPv6

**Address Assignment:** Click to enable Automatic IPv6 Address Assignment.

### Enable Automatic

**DHCP-PD in LAN:** Click to enable Automatic DHCP-PD in LAN.

**Enable Autoconfiguration:** Check to enable the autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 address for the DHCPv6 range for your local computers.

**IPv6 Address Lifetime:** Enter the IPv6 address lifetime (in minutes).

| IPv6 CONNECTION TYPE  |
|---|
| Choose the mode to be used by the router to the IPv6 Internet.<br><br>My IPv6 Connection is : <span>Autoconfiguration (SLAAC/DHCPv6)</span>   |
| IPv6 DNS SETTINGS   |
| Obtain a DNS server address automatically or enter a specific DNS server address.<br><br><div> <input checked="" type="radio"/> Obtain a DNS server address automatically             <input type="radio"/> Use the following DNS address           </div> Primary DNS Server : <input type="text"/><br>Secondary DNS Server : <input type="text"/>   |
| LAN IPv6 ADDRESS SETTINGS   |
| Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.<br><br>Enable DHCP-PD : <input checked="" type="checkbox"/><br>LAN IPv6 Address : <input type="text"/> /64<br>LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64   |
| ADDRESS AUTOCONFIGURATION SETTINGS  |
| Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.<br><br>Enable automatic IPv6 address assignment : <input checked="" type="checkbox"/><br>Enable Automatic DHCP-PD in LAN : <input checked="" type="checkbox"/><br>Autoconfiguration Type : <span>SLAAC + Stateless DHCPv6</span><br>Router Advertisement Lifetime : <input type="text"/> (minutes) |

## PPPoE

**My IPv6 Connection:** Select **PPPoE** from the drop-down menu.

**PPPoE:** Enter the PPPoE account settings supplied by your Internet provider (ISP).

**Address Mode:** Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

**IP Address:** Enter the IP address (Static PPPoE only).

**User Name:** Enter your PPPoE user name.

**Password:** Enter your PPPoE password and then retype the password in the next box.

**Service Name:** Enter the ISP service name (optional).

**Reconnection Mode:** Select either **Always-on**, **On-Demand**, or **Manual**.

**Maximum Idle Time:** Enter a maximum idle time after which the Internet connection will be dropped due to inactivity. To disable this feature, enable Auto-reconnect.

**MTU:** Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

**IPv6 DNS Settings:** Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

**Primary/Secondary DNS Address:** Enter the primary and secondary DNS server addresses.

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the router's LAN link-local address.

| IPv6 CONNECTION TYPE  |
|---|
| <p>Choose the mode to be used by the router to the IPv6 Internet.</p> <p>My IPv6 Connection is : <input type="text" value="PPPoE"/></p>   |
| PPPoE   |
| <p>Enter the information provided by your Internet Service Provider (ISP).</p> <p>PPPoE Session: <input checked="" type="radio"/> Share with IPv4 <input type="radio"/> Create a new session</p> <p>Address Mode: <input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP</p> <p>IP Address: <input type="text"/></p> <p>Username: <input type="text"/></p> <p>Password: <input type="text"/></p> <p>Verify Password: <input type="text"/></p> <p>Service Name: <input type="text"/> (Optional)</p> <p>Reconnect Mode: <input checked="" type="radio"/> Always on <input type="radio"/> On demand <input type="radio"/> Manual</p> <p>Maximum Idle Time: <input type="text" value="5"/> (minutes, 0=infinite)</p> <p>MTU: <input type="text" value="1492"/> (bytes)MTU default = 1492</p> |
| IPv6 DNS SETTINGS   |
| <p>Obtain a DNS server address automatically or enter a specific DNS server address.</p> <p><input checked="" type="radio"/> Obtain a DNS server address automatically</p> <p><input type="radio"/> Use the following DNS address</p> <p>Primary DNS Server: <input type="text"/></p> <p>Secondary DNS Server: <input type="text"/></p>   |
| LAN IPv6 ADDRESS SETTINGS   |
| <p>Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.</p> <p>Enable DHCP-PD: <input checked="" type="checkbox"/></p> <p>LAN IPv6 Address: <input type="text" value="FE80::218:E7FF:FE95:689E"/> /64</p> <p>LAN IPv6 Link-Local Address: FE80::218:E7FF:FE95:689E/64</p>  |
| ADDRESS AUTOCONFIGURATION SETTINGS  |
| <p>Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.</p> <p>Enable automatic IPv6 address assignment: <input checked="" type="checkbox"/></p> <p>Enable Automatic DHCP-PD in LAN: <input checked="" type="checkbox"/></p> <p>Autoconfiguration Type: <input type="text" value="SLAAC + Stateless DHCPv6"/></p> <p>Router Advertisement Lifetime: <input type="text" value="1440"/> (minutes)</p>   |

**Enable Automatic IPv6 Address Assignment:** Check to enable automatic IPv6 address assignment.

**Enable Automatic DHCP-PD in LAN:** Check to enable automatic DHCP-PD in LAN.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 address for the DHCPv6 range for your local computers.

**IPv6 Address Lifetime:** Enter the IPv6 address lifetime (in minutes).

## IPv6 in IPv4 Tunneling

**My IPv6 Connection:** Select **IPv6 in IPv4 Tunnel** from the drop-down menu.

**IPv6 in IPv4 Tunnel Settings:** Enter the settings supplied by your Internet provider (ISP).

**IPv6 DNS Settings:** Enter the settings supplied by your Internet provider (ISP) or check **Obtain a DNS Server address automatically**.

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the router's LAN link-local address.

**Enable Automatic IPv6 Address Assignment:** Check to enable automatic IPv6 address assignment.

**Enable Automatic DHCP-PD in LAN:** Check to enable automatic DHCP-PD in LAN.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range Start:** Enter the start IPv6 Address for the DHCPv6 range for your local computers.

**IPv6 Address Range End:** Enter the end IPv6 Address for the DHCPv6 range for your local computers.

**Pv6 Address Lifetime:** Enter the router advertisement lifetime (in minutes).

| IPv6 CONNECTION TYPE  |                                     |
|---|-------------------------------------|
| Choose the mode to be used by the router to the IPv6 Internet.  |                                     |
| My IPv6 Connection is :   | IPv6 in IPv4 Tunnel                 |
| IPv6 in IPv4 TUNNEL SETTINGS  |                                     |
| Enter the IPv6 in IPv4 Tunnel information provided by your Tunnel Broker.   |                                     |
| Remote IPv4 Address :   |                                     |
| Remote IPv6 Address :   |                                     |
| Local IPv4 Address :  | 192.168.1.2                         |
| Local IPv6 Address :  |                                     |
| IPv6 DNS SETTINGS   |                                     |
| Obtain a DNS server address automatically or enter a specific DNS server address.   |                                     |
| <input checked="" type="radio"/> Obtain a DNS server address automatically<br><input type="radio"/> Use the following DNS address   |                                     |
| Primary DNS Server :  |                                     |
| Secondary DNS Server :  |                                     |
| LAN IPv6 ADDRESS SETTINGS   |                                     |
| Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again. |                                     |
| Enable DHCP-PD :  | <input checked="" type="checkbox"/> |
| LAN IPv6 Address :  | /64                                 |
| LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64   |                                     |
| ADDRESS AUTOCONFIGURATION SETTINGS  |                                     |
| Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.                |                                     |
| Enable automatic IPv6 address assignment :  | <input checked="" type="checkbox"/> |
| Enable Automatic DHCP-PD in LAN :   | <input checked="" type="checkbox"/> |
| Autoconfiguration Type :  | SLAAC + Stateless DHCPv6            |
| Router Advertisement Lifetime :   | 1440 (minutes)                      |

## 6 to 4 Tunneling

**My IPv6 Connection:** Select **6 to 4** from the drop-down menu.

**6 to 4 Settings:** Enter the IPv6 settings supplied by your Internet provider (ISP).

**Primary/Secondary**

**DNS Address:** Enter the primary and secondary DNS server addresses.

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local**

**Address:** Displays the router's LAN link-local address.

**Enable Automatic**

**IPv6 Address** Check to enable automatic IPv6 address assignment.

**Assignment:**

**Autoconfiguration** Select **Stateful (DHCPv6)**, **SLAAC + RDNSS**  
**Type:** or **SLAAC + Stateless DHCPv6**.

**IPv6 Address Range** Enter the start IPv6 address for the DHCPv6 range for your  
**Start:** local computers.

**IPv6 Address Range** Enter the end IPv6 address for the DHCPv6 range for your  
**End:** local computers.

**IPv6 Address** Enter the IPv6 address lifetime (in minutes).  
**Lifetime:**

| IPv6 CONNECTION TYPE   |
|--|
| <p>Choose the mode to be used by the router to the IPv6 Internet.</p> <p>My IPv6 Connection is : <input type="text" value="6to4"/></p>   |
| 6to4 SETTINGS  |
| <p>Enter the IPv6 address information provided by your Internet Service Provider (ISP).</p> <p>6to4 Address : 2002:C0A8:0102::C0A8:0102</p> <p>6to4 Relay : <input type="text" value="192.88.99.1"/></p> <p>Primary DNS Server : <input type="text"/></p> <p>Secondary DNS Server : <input type="text"/></p>   |
| LAN IPv6 ADDRESS SETTINGS  |
| <p>Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.</p> <p>LAN IPv6 Address : 2002:C0A8:0102::0001 ::1/64</p> <p>LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64</p>  |
| ADDRESS AUTOCONFIGURATION SETTINGS   |
| <p>Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.</p> <p>Enable automatic IPv6 address assignment : <input checked="" type="checkbox"/></p> <p>Autoconfiguration Type : <input type="text" value="SLAAC + Stateless DHCPv6"/></p> <p>Router Advertisement Lifetime: <input type="text" value="60"/> (minutes)</p> |

## 6rd

**My IPv6 Connection:** Select **6rd** from the drop-down menu.

**6RD Settings:** Enter the address settings supplied by your Internet provider (ISP).

**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

**LAN Link-Local Address:** Displays the router's LAN link-local address.

**Enable Automatic IPv6 Address Assignment:** Check to enable automatic IPv6 address assignment.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)**, **SLAAC+RDNSS** or **SLAAC + Stateless DHCPv6**.

**Router Advertisement Lifetime:** Enter the router advertisement lifetime (in minutes).

| IPv6 CONNECTION TYPE   |
|--|
| <p>Choose the mode to be used by the router to the IPv6 Internet.</p> <p>My IPv6 Connection is : <input type="text" value="6rd"/></p>  |
| 6RD SETTINGS   |
| <p>Enter the IPv6 address information provided by your Internet Service Provider (ISP).</p> <p>6rd Configuration : <input checked="" type="radio"/> 6rd DHCPv4 Option <input type="radio"/> Manual Configuration</p> <p>6rd IPv6 Prefix : <input type="text" value=""/> / <input type="text" value="32"/></p> <p>IPv4 Address : 192.168.1.2 Mask Length : <input type="text" value="0"/></p> <p>Assign IPv6 Prefix : None</p> <p>Tunnel Link-Local Address : FE80::C0A8:0102/64</p> <p>6rd Border Relay IPv4 Address : <input type="text" value=""/></p> <p>Primary DNS Server : <input type="text" value=""/></p> <p>Secondary DNS Server : <input type="text" value=""/></p> |
| LAN IPv6 ADDRESS SETTINGS  |
| <p>Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.</p> <p>LAN IPv6 Address : None</p> <p>LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64</p>   |
| ADDRESS AUTOCONFIGURATION SETTINGS   |
| <p>Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.</p> <p>Enable automatic IPv6 address assignment : <input checked="" type="checkbox"/></p> <p>Autoconfiguration Type : <input type="text" value="SLAAC + Stateless DHCPv6"/></p> <p>Router Advertisement Lifetime : <input type="text" value="60"/> (minutes)</p>  |

# Link-Local Connectivity

**My IPv6 Connection:** Select **Link-Local Only** from the drop-down menu.

**LAN IPv6 Address Settings:** Displays the IPv6 address of the router.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is : 

Local Connectivity Only

LAN IPv6 ADDRESS SETTINGS

LAN IPv6 address for local IPv6 communications.

LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64

## Advanced Virtual Server

This will allow you to open a single port. If you would like to open a range of ports, refer to the next page.

**Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

**Private Port/**

**Public Port:** Enter the port that you want to open next to Private Port and Public Port. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

**Protocol Type:** Select **TCP**, **UDP**, or **Both** from the drop-down menu.

**Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

### VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings Don't Save Settings

### 24 - VIRTUAL SERVERS LIST

Remaining number of rules that can be created: 24

|                          |            |                       | Port         | Traffic Type    |                            |
|--------------------------|------------|-----------------------|--------------|-----------------|----------------------------|
| <input type="checkbox"/> | Name       | << Application name ▼ | Public Port  | Protocol Both ▼ | Schedule Always ▼          |
|                          | IP Address | << Computer Name ▼    | Private Port |                 | Inbound Filter Allow All ▼ |
| <input type="checkbox"/> | Name       | << Application name ▼ | Public Port  | Protocol Both ▼ | Schedule Always ▼          |
|                          | IP Address | << Computer Name ▼    | Private Port |                 | Inbound Filter Allow All ▼ |
| <input type="checkbox"/> | Name       | << Application name ▼ | Public Port  | Protocol Both ▼ | Schedule Always ▼          |



# Port Forwarding

This will allow you to open a single port or a range of ports.

- Name:** Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.
- IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the “Computer Name” drop-down menu. Select your computer and click <<.
- TCP/UDP:** Enter the TCP and/or UDP port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a common.  
  
Example: 24,1009,3000-4000
- Schedule:** The schedule of time when the Virtual Server Rule will be enabled. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.
- Inbound Filter:** Select **Allow All** (most common) or a created Inbound filter. You may create your own inbound filters in the **Advanced > Inbound Filter** page.

**PORT FORWARDING**

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in the format, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689). This option is only applicable to the INTERNET session.

Save Settings

Don't Save Settings

**24 -- PORT FORWARDING RULES**

Remaining number of rules that can be created: 24

|                          |   |                                      |   |
|--------------------------|---|--------------------------------------|---|
| <input type="checkbox"/> | <div><div>Name</div><div><div>&lt;&lt;</div><div>Application Name</div><div></div></div></div>    | <div><div>TCP</div><div></div></div> | <div><div>Schedule</div><div>Always</div><div></div></div>          |
|                          | <div><div>IP Address</div><div><div>&lt;&lt;</div><div>Computer Name</div><div></div></div></div> | <div><div>UDP</div><div></div></div> | <div><div>Inbound Filter</div><div>Allow All</div><div></div></div> |
| <input type="checkbox"/> | <div><div>Name</div><div><div>&lt;&lt;</div><div>Application Name</div><div></div></div></div>    | <div><div>TCP</div><div></div></div> | <div><div>Schedule</div><div>Always</div><div></div></div>          |
|                          | <div><div>IP Address</div><div><div>&lt;&lt;</div><div>Computer Name</div><div></div></div></div> | <div><div>UDP</div><div></div></div> | <div><div>Inbound Filter</div><div>Allow All</div><div></div></div> |
| <input type="checkbox"/> | <div><div>Name</div><div><div>&lt;&lt;</div><div>Application Name</div><div></div></div></div>    | <div><div>TCP</div><div></div></div> | <div><div>Schedule</div><div>Always</div><div></div></div>          |
|                          | <div><div>IP Address</div><div><div>&lt;&lt;</div><div>Computer Name</div><div></div></div></div> | <div><div>UDP</div><div></div></div> | <div><div>Inbound Filter</div><div>Allow All</div><div></div></div> |
| <input type="checkbox"/> | <div><div>Name</div><div><div>&lt;&lt;</div><div>Application Name</div><div></div></div></div>    | <div><div>TCP</div><div></div></div> | <div><div>Schedule</div><div>Always</div><div></div></div>          |
|                          | <div><div>IP Address</div><div><div>&lt;&lt;</div><div>Computer Name</div><div></div></div></div> | <div><div>UDP</div><div></div></div> | <div><div>Inbound Filter</div><div>Allow All</div><div></div></div> |
| <input type="checkbox"/> | <div><div>Name</div><div><div>&lt;&lt;</div><div>Application Name</div><div></div></div></div>    | <div><div>TCP</div><div></div></div> | <div><div>Schedule</div><div>Always</div><div></div></div>          |
|                          | <div><div>IP Address</div><div><div>&lt;&lt;</div><div>Computer Name</div><div></div></div></div> | <div><div>UDP</div><div></div></div> | <div><div>Inbound Filter</div><div>Allow All</div><div></div></div> |

## Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DIR-822. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-822 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

**Name:** Enter a name for the rule. You may select a pre-defined application from the drop-down menu and click <<.

**Trigger:** This is the port used to trigger the application. It can be either a single port or a range of ports.

**Traffic Type:** Select the protocol of the trigger port (TCP, UDP, or Both).

**Firewall:** This is the port number on the Internet side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

**Traffic Type:** Select the protocol of the firewall port (TCP, UDP, or Both).

**Schedule:** The schedule of time when the Application Rule will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**APPLICATION RULES**

The Application Rules option is used to open single or multiple ports in your firewall when the router senses data sent to the Internet on an outgoing "Trigger" port or port range. Special Application rules apply to all computers on your internal network.

**24 -- APPLICATION RULES**

Remaining number of rules that can be created: 24

|                          | Name                 | Application           | Port  | Traffic Type                      | Schedule                                |
|--------------------------|----------------------|-----------------------|---|-----------------------------------|---|
| <input type="checkbox"/> | <input type="text"/> | << Application Name ▾ | <input type="text" value="Trigger"/><br><input type="text" value="Firewall"/> | <div>All ▾</div> <div>All ▾</div> | <div>Always ▾</div> <div>Always ▾</div> |
| <input type="checkbox"/> | <input type="text"/> | << Application Name ▾ | <input type="text" value="Trigger"/><br><input type="text" value="Firewall"/> | <div>All ▾</div> <div>All ▾</div> | <div>Always ▾</div> <div>Always ▾</div> |
| <input type="checkbox"/> | <input type="text"/> | Application           | <input type="text" value="Trigger"/><br><input type="text" value="Firewall"/> | <div>All ▾</div> <div>All ▾</div> | <div>Always ▾</div> <div>Always ▾</div> |

## QoS Engine

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically. The QoS section contains a queuing mechanism, traffic shaping and classification. It supports two kinds of queuing mechanisms. Strict Priority Queue (SPQ) and Weighted Fair Queue (WFQ). SPQ will process traffic based on traffic priority. Queue1 has the highest priority and Queue4 has the lowest priority. WFQ will process traffic based on the queue weight. Users can configure each queue's weight. The sum of all the queues' weight must be 100. When surfing the Internet, the system will do traffic shaping based on the uplink and downlink speed. The classification rules can be used to classify traffic to different queues, then SPQ or WFQ will do QoS based on the queue's priority or weight.

The following parameters will be available for configuration:

**Enable QoS:** This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

**Uplink Speed:** The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5 Mbits/284 Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as [www.dslreports.com](http://www.dslreports.com).

**Downlink Speed:** The speed at which data can be transferred from the ISP to the router. This is determined by your ISP. ISP's often define speed as a download/upload pair. For example, 1.5 Mbits/284 Kbits. Using this example, you would enter 1500. Alternatively you can test your downlink speed with a service such as [www.dslreports.com](http://www.dslreports.com).

**Queue Type:** Here the user can specify the queue type used. When choosing the option Strict Priority Queue, the router will apply QoS based on the internal specification for the queue ID's listed. When choosing the option Weight Fair Queue, the router will apply QoS based on the user defined percentage in the Queue Weight column.

**Queue ID:** In this column the Queue ID used will be displayed.

**Queue Priority:** In this column the Queue Priority used will be displayed.

**Queue Weight:** After choosing to use the Weight Fair Queue option, under Queue Type, the user will be able to manual enter the Queue Weight for each individual Queue ID.

**QOS SETTINGS**

Use this section to configure D-Link's QoS Engine powered by QoS Engine Technology. This QoS Engine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.

Save Settings
Don't Save Settings

**QOS SETUP**

**Enable QoS :** ☐

**Uplink Speed :**  kbps << Select Transmission Rate ▼

**Downlink Speed :**  kbps << Select Transmission Rate ▼

**Queue Type :** ☐ Strict Priority Queue ☒ Weighted Fair Queue

| Queue ID | Queue Weight                      |
|----------|-----------------------------------|
| 1        | <input type="text" value="40"/> % |
| 2        | <input type="text" value="30"/> % |
| 3        | <input type="text" value="20"/> % |
| 4        | <input type="text" value="10"/> % |

After specifying the QoS framework used, in the QoS setup section, the user can now create individual rules for scenarios that require the use of traffic control and data priority manipulation.

The following parameters will be available for configuration:

**Checkbox:** Tick this option to enable the rule specified.

**Name:** Enter a custom name for the rule being created here. This name is used for identification.

**Queue ID:** Select the appropriate priority requirement from the drop-down menu that will be applied to this rule. Option to choose from are Highest, Higher, Normal, and Best Effort.

**Protocol:** Select the protocol used for the application for in the drop-down menu and it will automatically place it in the Protocol field.

**Local IP Range:** Enter the local IP range used here. This is the IP range of your Local Area Network. The router's IP cannot be included in this range.

**Remote IP Range:** Enter the remote IP range used here. This is the IP range of the public network from the Internet Port side. To apply this rule to any IP addresses from the public side, enter the range 0.0.0.1 to 255.255.255.254.

**Application Port:** Enter the application port number used here.

**32 -- CLASSIFICATION RULES**

Remaining number of rules that can be created: 18

|                                     |                      |                         |                                       |
|-------------------------------------|----------------------|-------------------------|---------------------------------------|
| <input type="checkbox"/>            | Name<br>Youtube      | Queue ID<br>1 - Highest | Protocol<br>TCP << ALL                |
| <input checked="" type="checkbox"/> | Local IP Range<br>to | Remote IP Range<br>to   | Application Port<br>YOUTUBE << ALL    |
| <input type="checkbox"/>            | Name<br>Google_talk  | Queue ID<br>1 - Highest | Protocol<br>TCP << ALL                |
| <input checked="" type="checkbox"/> | Local IP Range<br>to | Remote IP Range<br>to   | Application Port<br>VOICE << ALL      |
| <input type="checkbox"/>            | Name<br>Web_audio    | Queue ID<br>1 - Highest | Protocol<br>TCP << ALL                |
| <input checked="" type="checkbox"/> | Local IP Range<br>to | Remote IP Range<br>to   | Application Port<br>HTTP_AUDIO << ALL |
| <input type="checkbox"/>            | Name<br>Web_video    | Queue ID<br>2 - Higher  | Protocol<br>TCP << ALL                |
| <input checked="" type="checkbox"/> | Local IP Range<br>to | Remote IP Range<br>to   | Application Port<br>HTTP_VIDEO << ALL |

## Network Filters

Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the router.

**Configure MAC Filtering:** Select **Turn MAC Filtering Off, Allow MAC addresses listed below**, or **Deny MAC addresses listed below** from the drop-down menu.

**MAC Address:** Enter the MAC address you would like to filter.

To find the MAC address on a computer, please refer to the **Networking Basics** on page 137 section in this manual.

**DHCP Client:** Select a DHCP client from the drop-down menu and click << to copy that MAC address.

24 -- MAC FILTERING RULES

Configure MAC Filtering below:

Turn MAC Filtering OFF

Remaining number of rules that can be created: 24

|                          | MAC Address          |    | DHCP Client List | Schedule                       |
|--------------------------|----------------------|----|------------------|--------------------------------|
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |
| <input type="checkbox"/> | <input type="text"/> | << | Computer Name    | Always <div>New Schedule</div> |

# Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

**Add Policy:** Click the **Add Policy** button to start the Access Control Wizard.

**ACCESS CONTROL**

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

Save Settings

Don't Save Settings

**ACCESS CONTROL**

Enable Access Control: ☒

Add Policy

**POLICY TABLE**

|               |         |           |        |          |  |
|---------------|---------|-----------|--------|----------|--|
| Enable Policy | Machine | Filtering | Logged | Schedule |  |
|---------------|---------|-----------|--------|----------|--|

# Access Control Wizard

Click **Next** to continue with the wizard.

**ADD NEW POLICY**

This wizard will guide you through the following steps to add a new policy for Access Control.

Step 1 - Choose a unique name for your policy

Step 2 - Select a schedule

Step 3 - Select the machine to which this policy applies

Step 4 - Select filtering method

Step 5 - Select filters

Step 6 - Configure Web Access Logging

Prev

Next

Save

Cancel

Enter a name for the policy and then click **Next** to continue.

**STEP 1: CHOOSE POLICY NAME**

Choose a unique name for your policy.

Policy Name :

Prev

Next

Save

Cancel

Select a schedule (I.E. Always) from the drop-down menu and then click **Next** to continue.

**STEP 2: SELECT SCHEDULE**

Choose a schedule to apply to this policy.

Details : Always

Prev Next Save Cancel

Enter the following information and then click **Next** to continue.

- **Address Type** - Select IP address, MAC address, or Other Machines.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.
- **Machine Address** - Enter the PC MAC address (i.e. 00:00.00.00.00).

**STEP 3: SELECT MACHINE**

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

Address Type : ☒ IP ☐ MAC ☐ Other Machines

IP Address : 192.168.0.112 << RM-Test01 (192.168.0.112) >>

Machine Address : << Computer Name >>

Copy Your PC's MAC Address

OK Clear

| Machine       |
|---------------|
| 192.168.0.112 |

Prev Next Save Cancel

Select the filtering method and then click **Next** to continue.

**STEP 4: SELECT FILTERING METHOD**

Select the method for filtering.

Method : ☐ Log Web Access Only ☐ Block All Access ☒ Block Some Access

Apply Web Filter : ☐

Apply Advanced Port Filters : ☐

Prev Next Save Cancel

Enter the rule:

- Enable** - Check to enable the rule.
- Name** - Enter a name for your rule.
- Dest IP Start** - Enter the starting IP address.
- Dest IP End** - Enter the ending IP address.
- Protocol** - Select the protocol.
- Dest Port Start** - Enter the starting port number.
- Dest Port End** - Enter the ending port number.

**STEP 5: PORT FILTER**

Add Port Filters Rules.

Specify rules to prohibit access to specific IP addresses and ports.

| Enable                   | Name | Dest IP Start | Dest IP End     | Protocol | Dest Port Start | Dest Port End |
|--------------------------|------|---------------|-----------------|----------|-----------------|---------------|
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |
| <input type="checkbox"/> |      | 0.0.0.0       | 255.255.255.255 | Any      | 0               | 65535         |

Prev Next Save Cancel

To enable web logging, click **Enable**.

Click **Save** to save the access control rule.

Your newly created policy will now show up under **Policy Table**.

STEP 6: CONFIGURE WEB ACCESS LOGGING

Web Access Logging : ☐ Disabled  
☒ Enable

PrevNextSaveCancel

ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

Save SettingsDon't Save SettingsReboot Now

ENABLE

Enable Access Control : ☒

Add Policy

POLICY TABLE

| Enable                              | Policy | Machine       | Filtering         | Logged | Schedule |  |  |
|-------------------------------------|--------|---------------|-------------------|--------|----------|--|--|
| <input checked="" type="checkbox"/> | dlink  | 192.168.0.106 | Block Some Access | No     | Always   |  |  |



# Website Filters

Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section.

**Add Website** Select either **DENY computers access to ONLY these sites** or **Filtering Rule: ALLOW computers access to ONLY these sites**.

**Website URL/ Domain:** Enter the keywords or URLs that you want to allow or block.  
**Domain:** Click **Save Settings**.

40 -- WEBSITE FILTERING RULES

Configure Website Filter below:

DENY computers access to ONLY these sites

Clear the list below...

| Website URL/Domain |  |
|--------------------|--|
|                    |  |
|                    |  |
|                    |  |
|                    |  |
|                    |  |
|                    |  |
|                    |  |
|                    |  |
|                    |  |

# Inbound Filters

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound Filters can be used with Virtual Server, Port Forwarding, or Remote Administration features.

**Name:** Enter a name for the inbound filter rule.

**Action:** Select **Allow** or **Deny**.

**Enable:** Check to enable rule.

**Remote IP Start:** Enter the starting IP address. Enter 0.0.0.0 if you do not want to specify an IP range.

**Remote IP End:** Enter the ending IP address. Enter 255.255.255.255 if you do not want to specify an IP range.

**Add:** Click the **Add** button to apply your settings. You must click **Save Settings** at the top to save the settings.

**Inbound Filter Rules List:** This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule.

INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.

ADD INBOUND FILTER RULE

Name :

Action :

Allow

Remote IP Range :

Enable

Remote IP Start

Remote IP End

☐

0.0.0.0

255.255.255.255

☐

0.0.0.0

255.255.255.255

☐

0.0.0.0

255.255.255.255

☐

0.0.0.0

255.255.255.255

☐

0.0.0.0

255.255.255.255

☐

0.0.0.0

255.255.255.255

☐

0.0.0.0

255.255.255.255

☐

0.0.0.0

255.255.255.255



☐

0.0.0.0

255.255.255.255

Add

Cancel

| INBOUND FILTER RULES LIST |        |                           |   |   |
|---------------------------|--------|---------------------------|---|---|
| Name                      | Action | Remote IP Range           |   |   |
| Inbound1                  | allow  | 192.168.1.0-192.168.1.254 |  |  |

## Firewall Settings

A firewall protects your network from the outside world. The DIR-822 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

**Enable SPI:** SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

**Anti-Spoof Check:** Enable this feature to protect your network from certain kinds of “spoofing” attacks.

**DMZ IP Address:** Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its IP address automatically using DHCP, be sure to make a static reservation on the **Setup > Network Settings** page so that the IP address of the DMZ machine does not change.

**PPTP:** Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

**IPSEC (VPN):** Allows multiple VPN clients to connect to their corporate network using IPsec. Some VPN clients support traversal of IPsec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

**SIP:** Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

**FIREWALL & DMZ SETTINGS**

DMZ means "Demilitarized Zone". DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers and others.

Save Settings
Don't Save Settings

**FIREWALL SETTINGS**

Enable SPI : ☐

**ANTI-SPOOF CHECKING**

Enable anti-spoof checking : ☐

**DMZ HOST**

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

**Note:** Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ : ☐

DMZ IP Address :  << Computer Name ▼

**APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION**

PPTP : ☒

IPSec (VPN) : ☒

SIP : ☒

Save Settings
Don't Save Settings

# Routing

The Routing option is an advanced method of customizing specific routes of data through your network.

- Name:** Enter a name for your route.
- Destination IP:** Enter the IP address of packets that will take this route.
- Netmask:** Enter the netmask of the route, please note that the octets must match your destination IP address.
- Gateway:** Enter your next hop gateway to be taken if this route is used.
- Metric:** The route metric is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.
- Interface:** Select the interface that the IP packet must use to transit out of the router when this route is used.

ROUTING

The Routing option allows you to define static routes to specific destinations.

Save SettingsDon't Save Settings

32 -- ROUTE LIST

Remaining number of rules that can be created: 32

|                          |                                 |  | Metric                         | Interface           |
|--------------------------|---------------------------------|--|--------------------------------|---------------------|
| <input type="checkbox"/> | Name<br><input type="text"/>    | Destination IP<br><input type="text"/> | <input type="text" value="1"/> | WAN (172.17.5.44) ▼ |
| <input type="checkbox"/> | Netmask<br><input type="text"/> | Gateway<br><input type="text"/>        |                                |                     |
| <input type="checkbox"/> | Name<br><input type="text"/>    | Destination IP<br><input type="text"/> | <input type="text" value="1"/> | WAN (172.17.5.44) ▼ |
| <input type="checkbox"/> | Netmask<br><input type="text"/> | Gateway<br><input type="text"/>        |                                |                     |
| <input type="checkbox"/> | Name<br><input type="text"/>    | Destination IP<br><input type="text"/> | <input type="text" value="1"/> | WAN (172.17.5.44) ▼ |
| <input type="checkbox"/> | Netmask<br><input type="text"/> | Gateway<br><input type="text"/>        |                                |                     |

## Advanced Wireless

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

**WLAN Partition:** This enables 802.11d operation. 802.11d is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it.

**WMM Enable:** WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

**HT20/40 Coexistence:** Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40 MHz and there is another wireless network's channel over-lapping and causing interference, the router will automatically change to 20 MHz.

**ADVANCED WIRELESS SETTINGS**

These options are for users that wish to change the behavior of their 802.11n wireless radio from the standard settings. We do not recommend changing these settings from the factory defaults. Incorrect settings may impact the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

**ADVANCED WIRELESS SETTINGS**

**Wireless Band :** 2.4GHz Band  
**Transmit Power :** High ▾  
**WLAN Partition :** ☐  
**WMM Enable :** ☒  
**HT 20/40 Coexistence :** ☒ Enable ☐ Disable

**ADVANCED WIRELESS SETTINGS**

**Wireless Band :** 5GHz Band  
**Transmit Power :** High ▾  
**WLAN Partition :** ☐  
**WMM Enable :** ☒

## Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) System is a simplified method for securing your wireless network during the “Initial setup” as well as the “Add New Device” processes. The Wi-Fi Alliance (WFA) has certified it across different products as well as manufactures. The process is just as easy as pressing a button for the Push-Button Method or correctly entering the 8-digit code for the Pin Code Method. The time reduction in setup and ease of use are quite beneficial, while the highest wireless Security setting of WPA2 is automatically used.

**Enable:** Enable the Wi-Fi Protected Setup feature.

**Note:** *if this option is unchecked, the WPS button on the side of the router will be disabled.*

**Lock Wireless Security Settings:** Tick this option to lock the configured wireless security settings.

**PIN Settings:** A PIN is a unique number that can be used to add the router to an existing network or to create a new network. Only the Administrator (“admin” account) can change or reset the PIN.

**Current PIN:** Shows the current PIN.

**Reset PIN to Default:** Restore the default PIN of the router.

**Generate New PIN:** Create a random number that is a valid PIN. This becomes the router’s PIN. You can then copy this PIN to the user interface of the wireless client. This wizard helps you add wireless devices to the wireless network.

**WI-FI PROTECTED SETUP**

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

Save Settings Don't Save Settings

---

**WI-FI PROTECTED SETUP**

Enable : ☒

WiFi Protected Setup : Enable/Configured

Lock WPS-PIN Setup : ☐

---

**PIN SETTINGS**

PIN : 33401027

Reset PIN to Default Generate New PIN

---

**ADD WIRELESS STATION**

Connect your Wireless Device

Save Settings Don't Save Settings

**Add Wireless Station:** The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 120 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

**Add Wireless Device Wizard:** There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar for the network, although other devices may act as a registrar as well.

Click to start the wizard and refer to page 41.

### WPS Button

You can also simply press the WPS button on the side of the router, and then press the WPS button on your wireless client to automatically connect without logging into the router.

Refer to page 111 for more information.



## Advanced Network Settings

**Enable UPnP:** To use the Universal Plug and Play (UPnP™) feature click on **Enabled**. UPnP provides compatibility with networking equipment, software and peripherals.

**WAN Ping:** Checking the box will allow the DIR-822 to respond to pings. Unchecking the box may provide some extra security from hackers.

**WAN Port Speed:** You may set the port speed of the Internet port to 10 Mbps, 100 Mbps, or Auto (recommended).

**Enable IPV4 Multicast Streams:** Check the box to allow multicast traffic to pass through the router from the Internet (IPv4).

**Enable IPV6 Multicast Streams:** Check the box to allow multicast traffic to pass through the router from the Internet (IPv6).

**ADVANCED NETWORK SETTINGS**

These options are for users that wish to change the LAN settings. We do not recommend changing these settings from factory default. Changing these settings may affect the behavior of your network.

Save Settings Don't Save Settings

**UPNP**

Universal Plug and Play(UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP IGD : ☒

**WAN PING**

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Response : ☐

**WAN PORT SPEED**

WAN Port Speed : Auto 10/100Mbps

**MULTICAST STREAMS**

Enable Multicast Streams : ☐

**IPV6 MULTICAST STREAMS**

Enable IPv6 Multicast Streams : ☒

Save Settings Don't Save Settings



## Guest Zone

The Guest Zone feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network. You may configure different zones for the 2.4 GHz and 5 GHz wireless bands.

**Enable Guest Zone:** Check to enable the Guest Zone feature.

**Schedule:** The schedule of time when the Guest Zone will be active. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section or click **Add New**.

**Wireless Network Name:** Enter a wireless network name (SSID) that is different from your main wireless network.

**Enable Routing Between Zones:** Check to allow network connectivity between the different zones created.

**Security Mode:** Select the type of security or encryption you would like to enable for the guest zone.

The screenshot shows the 'GUEST ZONE' configuration page. At the top, there's an orange header with the title 'GUEST ZONE'. Below it, a grey box contains instructions: 'Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.' There are two buttons: 'Save Settings' and 'Don't Save Settings'. Below this is a section titled 'GUEST ZONE' with a checkbox for 'Enable Routing Between Zones'. The page is divided into two main sections: 'SESSION 2.4GHZ' and 'SESSION 5GHZ'. Each session has its own settings: 'Enable Guest Zone' (checkbox), 'Wireless Band' (dropdown), 'Wireless Network Name' (text input), and 'Security Mode' (dropdown). The 2.4GHz session shows 'Always' for the enable checkbox, '2.4GHz Band' for the band, 'dlink-guest' for the SSID, and 'None' for security. The 5GHz session shows 'Always' for the enable checkbox, '5GHz Band' for the band, 'dlink-5GHz-guest' for the SSID, and 'None' for security. At the bottom, there are 'Save Settings' and 'Don't Save Settings' buttons.

**GUEST ZONE**

Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.

Save Settings Don't Save Settings

**GUEST ZONE**

Enable Routing Between Zones : ☐

**SESSION 2.4GHZ**

Enable Guest Zone : ☒ Always

Wireless Band : 2.4GHz Band

Wireless Network Name : dlink-guest (Also called the SSID)

Security Mode : None

**SESSION 5GHZ**

Enable Guest Zone : ☒ Always

Wireless Band : 5GHz Band

Wireless Network Name : dlink-5GHz-guest (Also called the SSID)

Security Mode : None

Save Settings Don't Save Settings

## IPv6 Firewall

The DIR-822's IPv6 Firewall feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-822's IPv6 Firewall functions in a similar way to the IP Filters feature.

**Enable Checkbox:** Check the box to enable the IPv6 firewall simple security.

**Configure IPv6 Firewall:** Select an action from the drop-down menu.

**Name:** Enter a name to identify the IPv6 firewall rule.

**Schedule:** Use the drop-down menu to select the time schedule that the IPv6 Firewall Rule will be enabled on. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools > Schedules** section.

**Source:** Use the **Source** drop-down menu to specify the interface that connects to the source IPv6 addresses of the firewall rule.

**IP Address Range:** Enter the source IPv6 address range in the adjacent **IP Address Range** field.

**Dest:** Use the **Dest** drop-down menu to specify the interface that connects to the destination IP addresses of the firewall rule.

**Protocol:** Select the protocol of the firewall port (**All, TCP, UDP, or ICMP**).

**Port Range:** Enter the first port of the range that will be used for the firewall rule in the first box and enter the last port in the field in the second box.

### IPv6 FIREWALL

The firewall settings section is an advance feature used to allow or deny traffic from passing through the device. It works in the same way as IP Filters with additional settings. You can create more detailed rules for the device.

Save Settings
Don't Save Settings

### IPv6 SIMPLE SECURITY

Enable IPv6 Simple Security : ☐

### 20 -- IPv6 FIREWALL RULES

Remaining number of rules that can be created: 20

Configure IPv6 Filtering below:  
Turn IPv6 Filtering OFF

|        |           |                  |            |
|--------|-----------|------------------|------------|
| Name   | Schedule  |                  |            |
|        | Always    |                  |            |
| Source | Interface | IP Address Range | Protocol   |
|        |           |                  | ALL        |
| Dest   | Interface | IP Address Range | Port Range |
|        |           |                  |            |
| Name   | Schedule  |                  |            |
|        |           |                  |            |

# IPv6 Routing

This page allows you to specify custom routes that determine how data is moved around your network.

**Route List:** Check the box next to the route you wish to enable.

**Name:** Enter a specific name to identify this route.

**Destination IP/Prefix Length:** This is the IP address of the router used to reach the specified destination or enter the IPv6 address prefix length of the packets that will take this route.

**Metric:** Enter the metric value for this rule here.

**Interface:** Use the drop-down menu to specify if the IP packet must use the WAN or LAN interface to transit out of the router.

**Gateway:** Enter the next hop that will be taken if this route is used.

ROUTING

This Routing page allows you to specify custom routes that determine how data is moved around your network.

Save Settings

Don't Save Settings

10 -- ROUTE LIST

|                          |   |   |
|--------------------------|---|---|
| <input type="checkbox"/> | <div><div>Name</div><div></div></div>   | <div><div>Destination IPv6 / Prefix Length</div><div>64 /</div></div> |
|                          | <div><div>Metric</div><div></div></div> | <div><div>Interface</div><div>NULL</div></div>                        |
|                          |   | <div><div>Gateway</div><div></div></div>                              |
| <input type="checkbox"/> | <div><div>Name</div><div></div></div>   | <div><div>Destination IPv6 / Prefix Length</div><div>64 /</div></div> |
|                          | <div><div>Metric</div><div></div></div> | <div><div>Interface</div><div>NULL</div></div>                        |
|                          |   | <div><div>Gateway</div><div></div></div>                              |
| <input type="checkbox"/> | <div><div>Name</div><div></div></div>   | <div><div>Destination IPv6 / Prefix Length</div><div>64 /</div></div> |

# Tools

## Admin

This page will allow you to change the Administrator and User passwords. You can also enable Remote Management. There are two accounts that can access the management interface through the web browser. The accounts are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes. Only the admin account has the ability to change both admin and user account passwords.

**Admin Password:** Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

**User Password:** Enter the new password for the User login. If you login as the User, you cannot change the settings (you can only view them).

**Gateway name:** Enter a name for your router.

**Enable Graphical Authentication:** Enables a challenge-response test to require users to type letters or numbers from a distorted image displayed on the screen to prevent online hackers and unauthorized users from gaining access to your router's network settings.

**Enable HTTPS Server:** Check to enable HTTPS to connect to the router securely. This means to connect to the router, you must enter **https://192.168.0.1** (forexample) instead of **http://192.168.0.1**.

**Enable Remote Management:** Remote management allows the DIR-822 to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

**Remote Admin Port:** The port number used to access the DIR-822 is used in the URL. Example: **http://x.x.x.x:8080** whereas **x.x.x.x** is the Internet IP address of the DIR-822 and **8080** is the port used for the Web Management interface.

**ADMINISTRATOR SETTINGS**

The 'admin' account can access the management interface. The admin has read/write access and can change password.

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

Save Settings
Don't Save Settings

**ADMIN PASSWORD**

Please enter the same password into both boxes, for confirmation.

Password :
Verify Password :

**SYSTEM NAME**

Gateway Name : DIR-822

**ADMINISTRATION**

Enable Graphical Authentication :
Enable HTTPS Server :
Enable Remote Management :

Remote Admin Port : 8080
Use HTTPS:

Remote Admin Inbound Filter : Allow All
Details : Allow All

Save Settings
Don't Save Settings

**Remote Admin** Inbound Filter: If you have enabled HTTPS Server, you must enter https:// as part of the URL to access the router remotely.

**Inbound Filter:**

This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule. The current status will be displayed in the details section.

## Time

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 Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

**Time:** Displays the current date and time of the router.

**Time Zone:** Select your Time Zone from the drop-down menu.

**Enable Daylight Saving:** To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

**Enable NTP Server:** NTP is short for Network Time Protocol. A NTP server will synch the time and date with your router. This will only connect to a server on the Internet, not a local server. Check the box to enable this feature.

**NTP Server Used:** Enter the IP address of a NTP server or select one from the drop-down menu.

**Manual:** To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Set Time**.

**TIME AND DATE**

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

Save Settings
Don't Save Settings

**TIME AND DATE CONFIGURATION**

Time : 01/01/2000 01:03:11
Time Zone : (GMT+08:00) Taipei

Enable Daylight Saving : ☐
Daylight Saving Offset : +01:00

Daylight Saving Dates :

|           | Month | Week | Day of Week | Time     |
|-----------|-------|------|-------------|----------|
| DST Start | Jan   | 1st  | Sun         | 12:00 AM |
| DST End   | Jan   | 1st  | Sun         | 12:00 AM |

**AUTOMATIC TIME AND DATE CONFIGURATION**

☒ Automatically synchronize with D-Link's Internet time server

NTP Server Used : ntp1.dlink.com
Update Now

**SET THE TIME AND DATE MANUALLY**

|      |      |        |     |        |    |
|------|------|--------|-----|--------|----|
| Year | 2009 | Month  | Jan | Day    | 1  |
| Hour | 1    | Minute | 3   | Second | 11 |

# SysLog

The broadband router keeps a running log of events and activities occurring on the router. You may send these logs to a SysLog server on your network.

**Enable Logging to SysLog Server:** Check this box to send the router logs to a SysLog Server.

**SysLog Server IP Address:** The address of the SysLog server that will be used to send the logs. You may also select your computer from the drop-down menu (only if receiving an IP address from the router via DHCP).

SYSLOG

The SysLog options allow you to send log information to a Syslog Server.

Save SettingsDon't Save Settings

SYSLOG SETTINGS

Enable Logging To SysLog : ☐  
Server

Save SettingsDon't Save Settings

## Email Settings

The Email feature can be used to send the system log files, router alert messages, and firmware update notifications to your email address.

**Enable Email Notification:** When this option is enabled, router activity logs are emailed to a designated email address.

**From Email Address:** This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

**To Email Address:** Enter the email address where you want the email sent.

### SMTP Server

**Address:** Enter the SMTP server address for sending email.

**SMTP Server Port:** Enter the SMTP port used on the server.

**Enable Authentication:** Check this box if your SMTP server requires authentication.

**Account Name:** Enter your account for sending email.

**Password:** Enter the password associated with the account. Re-type the password associated with the account.

**On Log Full:** When this option is selected, logs will be sent via email to your account when the log is full.

**On Schedule:** Selecting this option will send the logs via email according to schedule.

**Schedule:** This option is enabled when **On Schedule** is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to **Tools > Schedules**.

**Detail:** Your Schedule details will be displayed here.

**EMAIL SETTINGS**

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

Save Settings
Don't Save Settings

**EMAIL NOTIFICATION**

Enable Email Notification : ☐

**EMAIL SETTINGS**

From Email Address :

To Email Address :

Email Subject :

SMTP Server Address :

SMTP Server Port :

Enable Authentication : ☐

Account Name :

Password :

Verify Password :

**EMAIL LOG WHEN FULL OR ON SCHEDULE**

On Log Full : ☐

On Schedule : ☐

Schedule :

Detail :

Save Settings
Don't Save Settings



## System

This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

**Save Settings to Local Hard Drive:** Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. A file dialog will appear, allowing you to select a location and file name for the settings.

**Load Settings from Local Hard Drive:** Use this option to load previously saved router configuration settings. First, use the **Browse** option to find a previously saved file of configuration settings. Then, click the **Load** button to transfer those settings to the router.

**Restore to Factory Default Settings:** This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the **Save** button above.

**Reboot Device:** Click to reboot the router.

**Clear Language Pack:** Click **Clear** to remove your router's current language pack.

**SAVE AND RESTORE SETTINGS**

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings, or restore the factory default settings.

**SAVE AND RESTORE SETTINGS**

**Save Settings To Local Hard Drive :**

**Load Settings From Local Hard Drive :**

**Restore To Factory Default Settings :**

**Reboot The Device :**

**Clear Language Pack :**

## Firmware

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.

**Browse:** After you have downloaded the new firmware, click **Browse** to locate the firmware update on your hard drive. Click **Upload** to complete the firmware upgrade.

**Upload:** Once you have a firmware update on your computer, use this option to browse for the file and then upload the information into the access point.

## Language Pack

You can change the language of the web UI by uploading available language packs.

**Browse:** After you have downloaded the new language pack, click **Browse** to locate the language pack file on your hard drive. Click **Upload** to complete the language pack upgrade.

**FIRMWARE UPDATE**

There may be new firmware for your router to improve functionality and performance. [Click here to check for an upgrade on our support site.](#)

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the firmware upgrade.

The language pack allows you to change the language of the user interface on the router. We suggest that you upgrade your current language pack if you upgrade the firmware. This ensures that any changes in the firmware are displayed correctly.

To upgrade the language pack, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the language pack upgrade.

**FIRMWARE INFORMATION**

Current Firmware Version : 1.00

Current Firmware Time : 07/08/2013 16:37:00

Check Online Now for Latest Firmware Version

**FIRMWARE UPGRADE**

**Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.**

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

**LANGUAGE PACK UPGRADE**

Upload :

## Dynamic DNS

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

**Enable Dynamic DNS:** Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP address. Check the box to enable DDNS.

**Server Address:** Select your DDNS provider from the drop-down menu or enter the DDNS server address.

**Host Name:** Enter the host name that you registered with your DDNS service provider.

**Username or**

**Key:** Enter the username or key for your DDNS account.

**Password or**

**Key:** Enter the password or key for your DDNS account.

**Timeout:** Enter a timeout time (in hours).

**Status:** Displays the current connection status.

### Dynamic DNS for IPv6 Hosts

**Enable:** Click **Enable** to active Dynamic DNS for IPv6 hosts on your router.

**IP Address:** Enter the IPv6 address here.

**Host Name:** Enter your host name here.

#### DYNAMIC DNS

The Dynamic DNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.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 in your host name to connect to your game server no matter what your IP address is.

[Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.](http://www.DLinkDDNS.com)

#### DYNAMIC DNS SETTINGS

Enable Dynamic DNS : ☐

Server Address :

Host Name :

Username or Key :

Password or Key :

Verify Password or Key :

Timeout :  (hours)

Status : Disconnected

#### DYNAMIC DNS FOR IPV6 HOSTS

Enable : ☐

IPv6 Address :

Host Name :  (e.g.: ipv6.mydomain.net)

#### IPV6 DYNAMIC DNS LIST

| Enable                   | Host Name | IPv6 Address |
|--------------------------|-----------|--------------|
| <input type="checkbox"/> |           |              |

# Ping Test

**Ping Test:** The Ping Test is used to send ping packets to test if a computer is on the Internet. Enter the IP address that you wish to Ping and click **Ping**.

**IPv6 Ping Test:** Enter the IPv6 address that you wish to ping and click **Ping**.

**Ping Results:** The results of your ping attempts will be displayed here.

PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Host Name or IP Address :

IPv6 PING TEST

Host Name or IPv6 Address :

PING RESULT

Enter a host name or IP address above and click 'Ping'

# Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

- Name:** Enter a name for your new schedule.
  - Days:** Select a day, a range of days, or All Week to include every day.
  - Time:** Check **All Day - 24hrs** or enter a start and end time for your schedule.
  - Add:** You must click **Add** for your schedule to go into effect.
- Schedule Rules** The list of schedules will be listed here. Click the **Edit** icon to **List:** make changes or click the **Delete** icon to remove the schedule.

SCHEDULES

The Schedule configuration option is used to manage schedule rules for "WAN", "Wireless", "Virtual Server", "Port Forwarding", "Applications" and "Network Filter".

10 -- ADD SCHEDULE RULE

Name :

Day(s) : ☐ All Week ☒ Select Day(s)  
☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat

All Day - 24 hrs : ☐

Time Format :

Start Time :  :   (hour:minute)

End Time :  :   (hour:minute)

SCHEDULE RULES LIST

| Name | Day(s) | Time Frame |  |  |
|------|--------|------------|--|--|
|------|--------|------------|--|--|

# Status Device Info

This page displays the current information for the DIR-822. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

**General:** Displays the router’s time and firmware version.

**WAN:** Displays the MAC address and the public IP settings

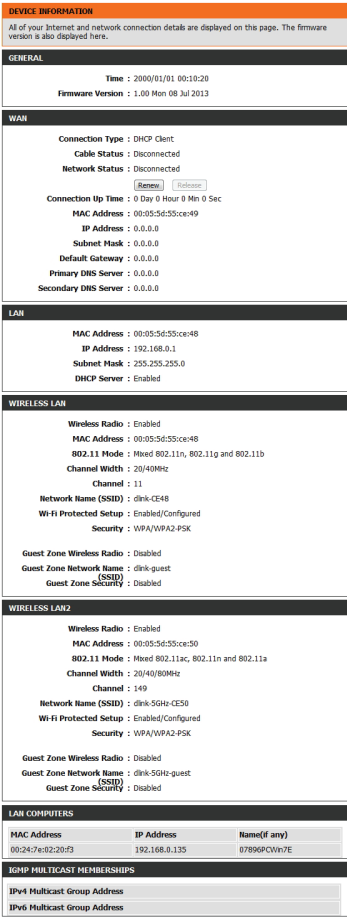
**LAN:** Displays the MAC address and the private (local) IP settings for the router.

**Wireless LAN1:** Displays the 2.4 GHz wireless MAC address and your wireless settings such as SSID and Channel.

**Wireless LAN2:** Displays the 5 GHz wireless MAC address and your wireless settings such as SSID and Channel.

**LAN Computers:** Displays computers and devices that are connected to the router via Ethernet and that are receiving an IP address assigned by the router (DHCP).

**IGMP Multicast Memberships:** Displays a list of IGMP multicast memberships that your router is currently subscribed to.



## Logs

The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest 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. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

**Save Log File:** This option will save the router log to a file on your computer.

**Log Type and Level:** You can select the types of messages that you want to receive from the log. System, Firewall and Security, and Router Status can be selected. Define the importance of the log in Log level by choosing from Critical, Warning, and Information.

**First Page:** Click to go to the first page.

**Last Page:** Click to go to the last page.

**Previous:** Click to go back one page.

**Next:** Click to go to the next page.

**Clear:** Clears all of the log contents.

**Link To Email** This option will send a copy of the router log to your email  
**Log Settings:** address configured in the **Tools > Email Settings** screen.

**VIEW LOG**

The View Log displays the activities occurring on the router.

Save Settings
Don't Save Settings

**SAVE LOG FILE**

Save Log File To Local Hard Drive.

**LOG TYPE & LEVEL**

Log Type: ☒ System ☐ Firewall & Security ☐ Router Status

Log Level: ☐ Critical ☐ Warning ☒ Information

**LOG FILES**

1/5

| Time                    | Message                     |
|-------------------------|-----------------------------|
| Sat Jan 1 00:19:18 2000 | DHCP: Client send DISCOVER. |
| Sat Jan 1 00:19:02      | DHCP: Client send DISCOVER. |

## Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-822 on both the WAN, LAN ports and the wireless segments. The traffic counter will reset if the device is rebooted.

TRAFFIC STATISTICS

Traffic Statistics displays Receive and Transmit packets passing through the device.

Refresh Statistics

Reset Statistics

LAN STATISTICS

Sent :6304

TX Packets Dropped :0

Collisions :0

Received :6683

RX Packets Dropped :0

Errors :0

WAN STATISTICS

Sent :0

TX Packets Dropped :0

Collisions :0

Received :0

RX Packets Dropped :0

Errors :0

WIRELESS STATISTICS - 2.4GHZ BAND

Sent :816

TX Packets Dropped :0

Collisions :0

Received :9767

RX Packets Dropped :0

Errors :6

WIRELESS STATISTICS - 5GHZ BAND

Sent :2158

TX Packets Dropped :0

Collisions :0

Received :45268

RX Packets Dropped :0

Errors :0



# Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

INTERNET SESSIONS

This page displays Source and Destination sessions passing through the device.

Refresh

| IP | TCP Count | UDP Count |
|----|-----------|-----------|
|----|-----------|-----------|

# Wireless

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.

|   |            |      |             |            |
|---|------------|------|-------------|------------|
| CONNECTED WIRELESS CLIENT LIST  |            |      |             |            |
| View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.) |            |      |             |            |
| NUMBER OF WIRELESS CLIENTS - 2.4GHZ BAND : 0  |            |      |             |            |
| MAC Address   | IP Address | Mode | Rate (Mbps) | Signal (%) |
|   |            |      |             |            |
| NUMBER OF WIRELESS CLIENTS - 5GHZ BAND : 0  |            |      |             |            |
| MAC Address   | IP Address | Mode | Rate (Mbps) | Signal (%) |
|   |            |      |             |            |

# Routing

This page will display your current routing table.

| ROUTING  |         |               |        |       |         |
|--|---------|---------------|--------|-------|---------|
| Routing Table  |         |               |        |       |         |
| This page displays the routing details configured for your router. |         |               |        |       |         |
| ROUTING TABLE  |         |               |        |       |         |
| Destination  | Gateway | Genmask       | Metric | Iface | Creator |
| 192.168.7.0  | 0.0.0.0 | 255.255.255.0 | 0      | LAN   | SYSTEM  |
| 192.168.0.0  | 0.0.0.0 | 255.255.255.0 | 0      | LAN   | SYSTEM  |
| 239.0.0.0  | 0.0.0.0 | 255.0.0.0     | 0      | LAN   | SYSTEM  |

# IPv6

The IPv6 page displays a summary of the router’s IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

IPv6 NETWORK INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

IPv6 CONNECTION INFORMATION

IPv6 Connection Type : Link-Local

IPv6 Default Gateway : None

LAN IPv6 Link-Local Address : fe80::bef6:85ff:fed2:4a35 /64

LAN IPV6 COMPUTERS

| IPv6 Address | Name(if any) |
|--------------|--------------|
|--------------|--------------|

# IPv6 Routing

This page displays the IPv6 routing details configured for your router.

| IPv6 ROUTING   |         |        |           |
|--|---------|--------|-----------|
| IPv6 Routing Table   |         |        |           |
| This page displays the routing details configured for your router. |         |        |           |
| IPv6 ROUTING TABLE   |         |        |           |
| Destination IP   | Gateway | Metric | Interface |

# Support

|   |
|---|
| <b>SUPPORT MENU</b> <ul style="list-style-type: none"><li>• <a href="#">Setup</a></li><li>• <a href="#">Advanced</a></li><li>• <a href="#">Tools</a></li><li>• <a href="#">Status</a></li></ul>   |
| <b>SETUP HELP</b> <ul style="list-style-type: none"><li>• <a href="#">Internet</a></li><li>• <a href="#">Wireless Settings</a></li><li>• <a href="#">Network Settings</a></li><li>• <a href="#">IPv6</a></li></ul>  |
| <b>ADVANCED HELP</b> <ul style="list-style-type: none"><li>• <a href="#">Virtual Server</a></li><li>• <a href="#">Port Forwarding</a></li><li>• <a href="#">Application Rules</a></li><li>• <a href="#">QoS Engine</a></li><li>• <a href="#">Network Filter</a></li><li>• <a href="#">Access Control</a></li><li>• <a href="#">Website Filter</a></li><li>• <a href="#">Inbound Filter</a></li><li>• <a href="#">Firewall Settings</a></li><li>• <a href="#">Routing</a></li><li>• <a href="#">Advanced Wireless</a></li><li>• <a href="#">Wi-Fi Protected Setup</a></li><li>• <a href="#">Advanced Network</a></li><li>• <a href="#">Guest Zone</a></li><li>• <a href="#">IPv6 Firewall</a></li><li>• <a href="#">IPv6 Routing</a></li></ul> |
| <b>TOOLS HELP</b> <ul style="list-style-type: none"><li>• <a href="#">Device Administration</a></li><li>• <a href="#">Time</a></li><li>• <a href="#">Syslog</a></li><li>• <a href="#">Email Settings</a></li><li>• <a href="#">System</a></li><li>• <a href="#">Firmware</a></li><li>• <a href="#">Dynamic DNS</a></li><li>• <a href="#">System Check</a></li><li>• <a href="#">Schedules</a></li></ul>   |
| <b>STATUS HELP</b> <ul style="list-style-type: none"><li>• <a href="#">Device Info</a></li><li>• <a href="#">Logs</a></li><li>• <a href="#">Statistics</a></li><li>• <a href="#">Internet Sessions</a></li><li>• <a href="#">Wireless</a></li><li>• <a href="#">Routing</a></li><li>• <a href="#">IPv6</a></li><li>• <a href="#">IPv6 Routing</a></li></ul>   |

# Connect a Wireless Client to your Router

## WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DIR-822 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 DIR-822 for about 1 second. The Internet LED on the front will start to blink.



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

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

# Windows® 8

## WPA/WPA2

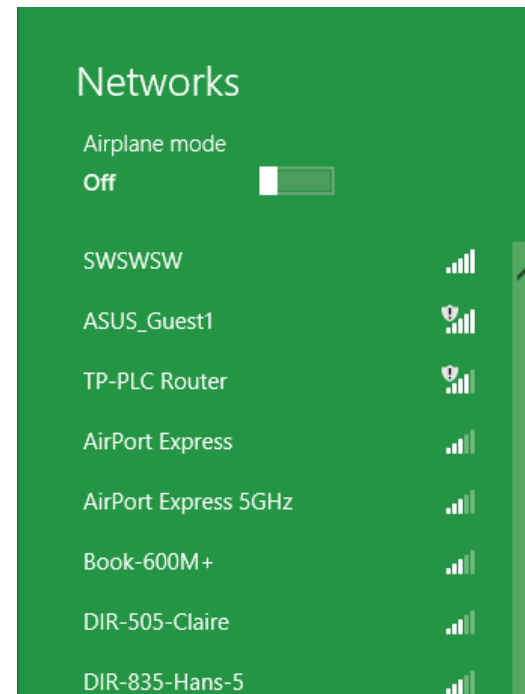
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key (Wi-Fi password) being used.

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



Wireless Icon

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

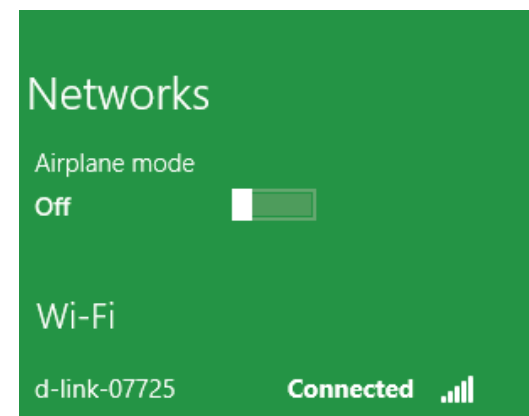
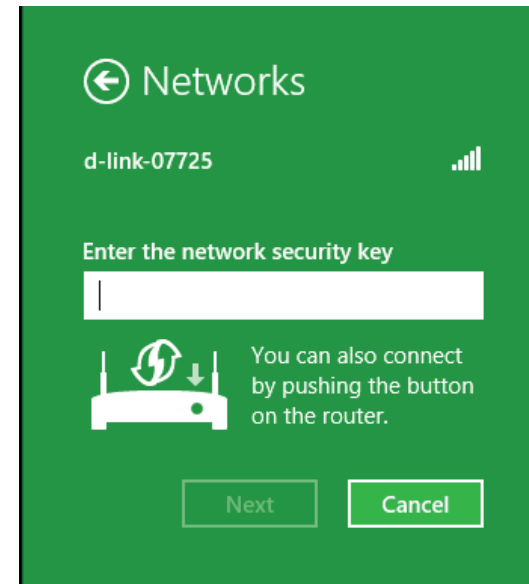




You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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

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

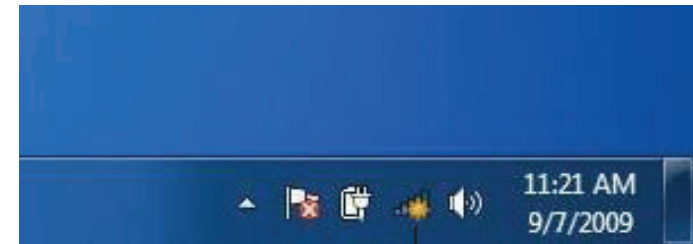


# Windows® 7

## WPA/WPA2

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

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



Wireless Icon

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

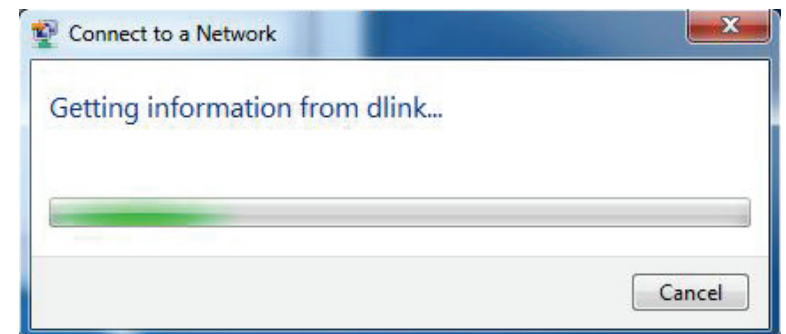


3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

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

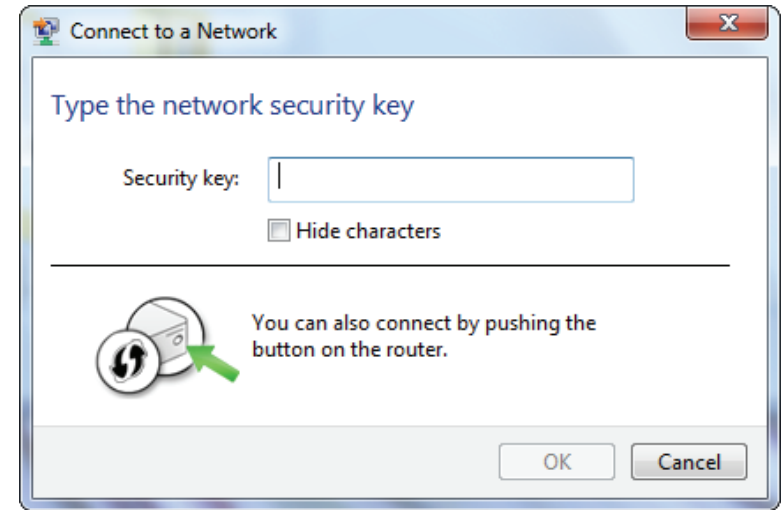


4. The following window appears while your computer tries to connect to the router.



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

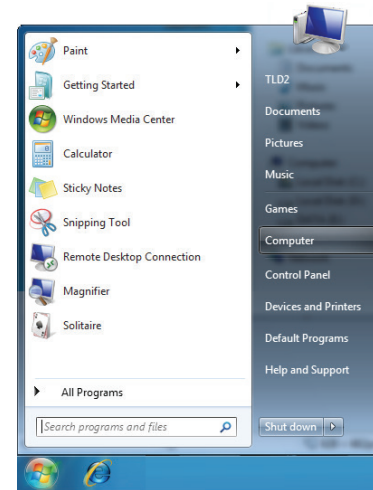
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



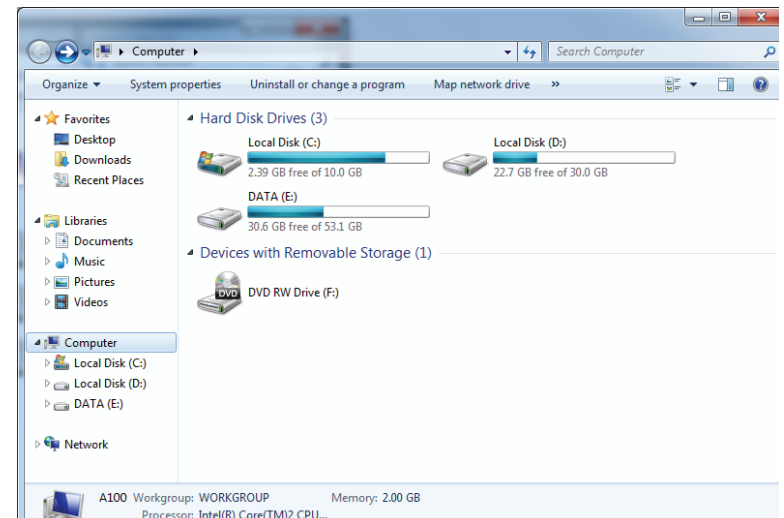
## WPS

The WPS feature of the DIR-822 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

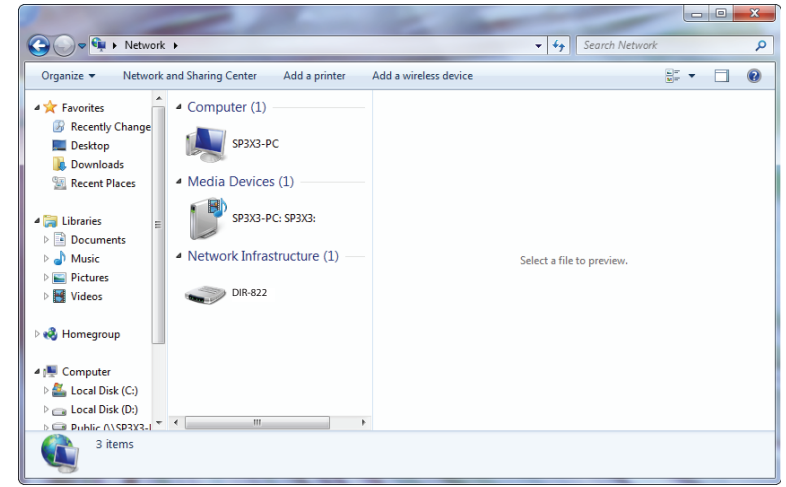
1. Click the **Start** button and select **Computer** from the Start menu.



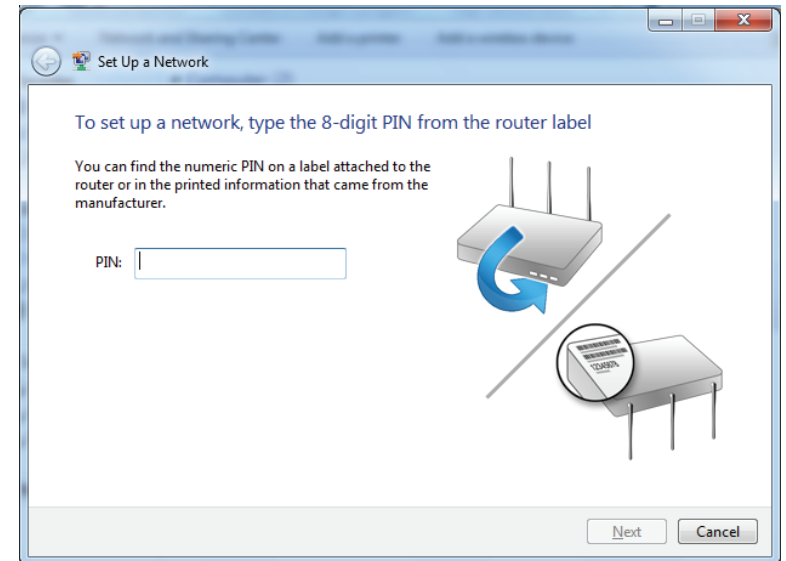
2. Click **Network** on the left side.



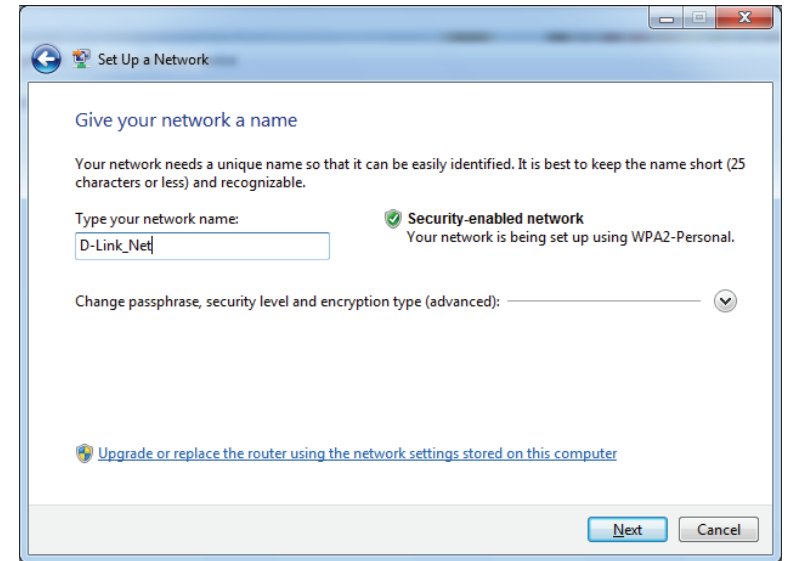
3. Double-click the DIR-822.



4. Input the WPS PIN number (on the router label) in the **Setup** > **Wireless Setup** menu in the router's web UI) and click **Next**.

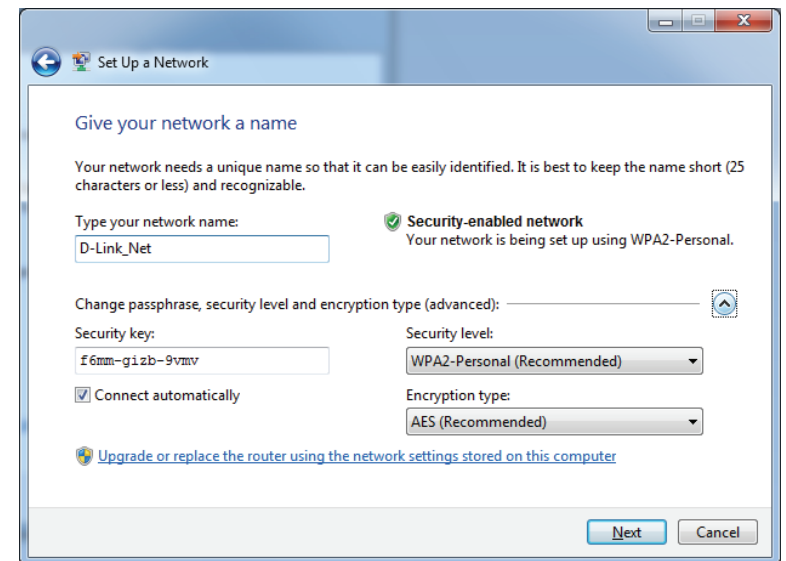


5. Type a name to identify the network.



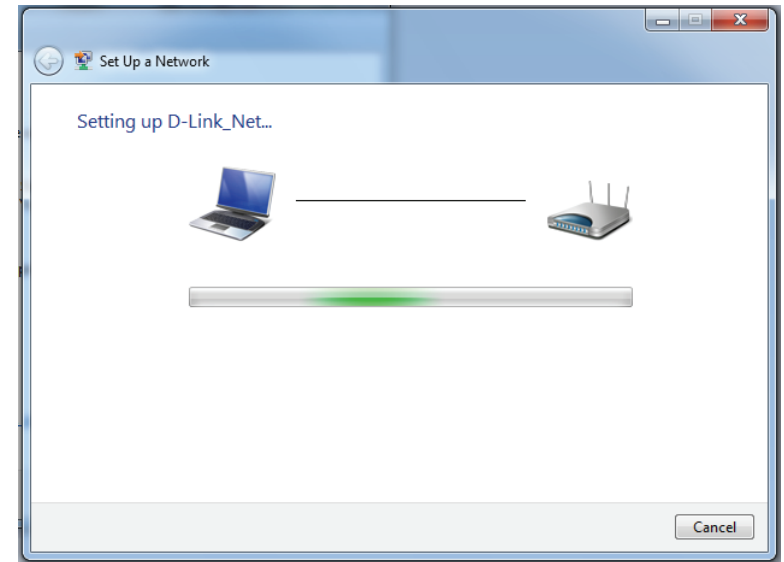
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



7. The following window appears while the router is being configured.

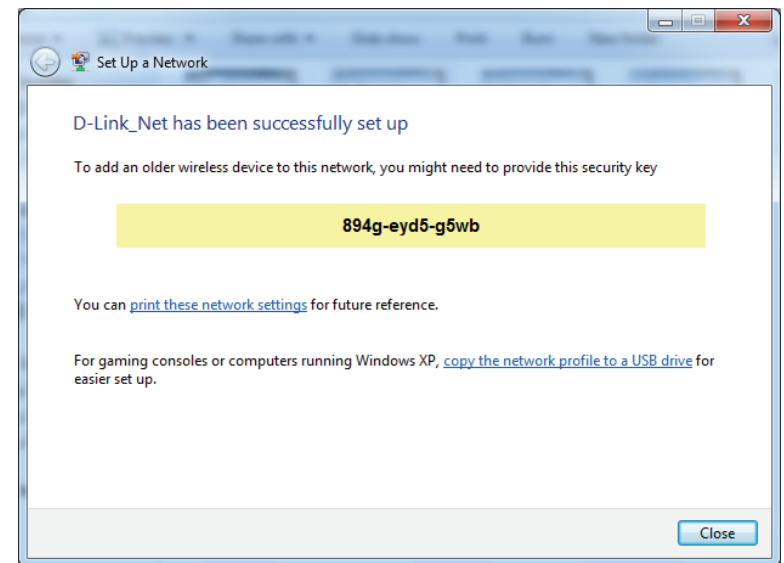
Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been setup successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click **Close** to complete WPS setup.





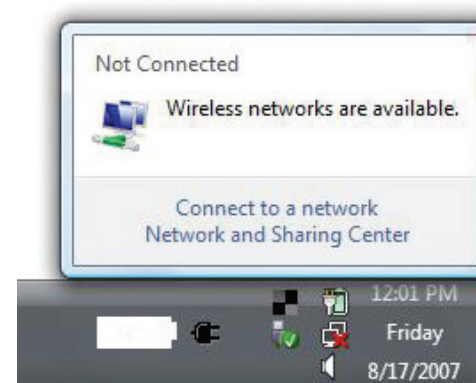
# Windows Vista®

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

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

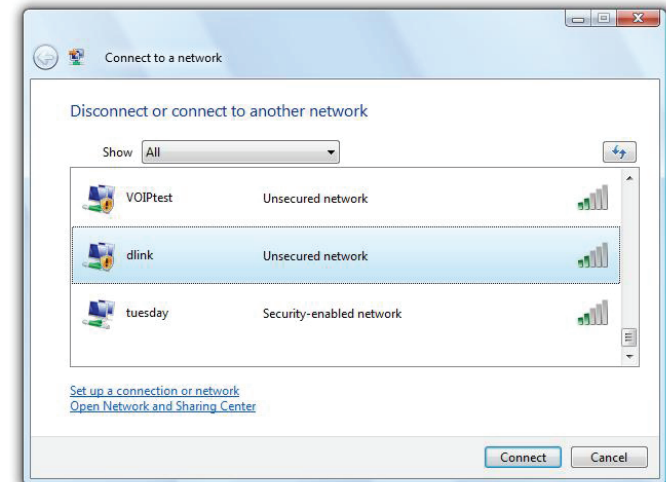
or

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



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

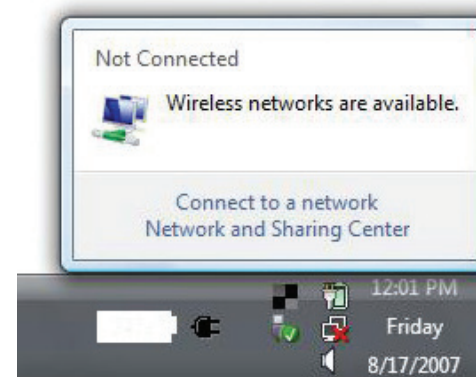
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



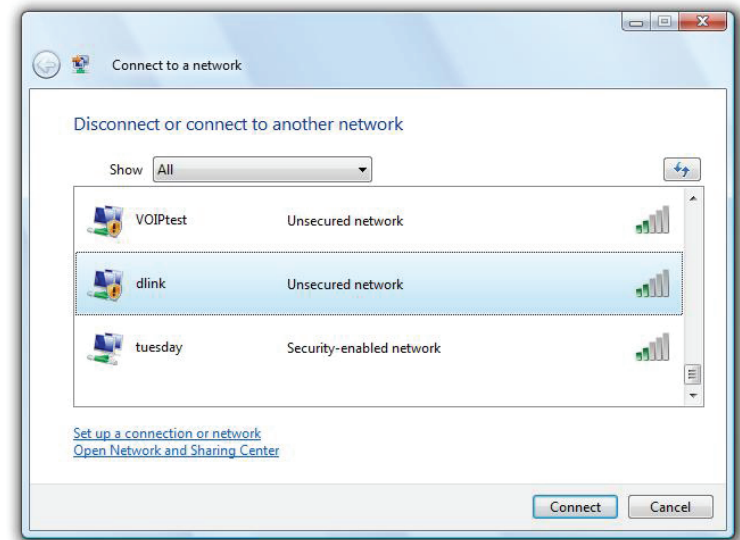
## WPA/WPA2

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

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



2. Highlight the Wi-Fi name (SSID) you would like to connect to and click **Connect**.



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

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



## WPS/WCN 2.0

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and unconfigured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the **Enable** checkbox in the **Basic > Wireless** section. Use the Current PIN that is displayed on the **Advanced > Wi-Fi Protected Setup** section or choose to click the **Generate New PIN** button or **Reset PIN to Default** button.



If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

# Windows® XP

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

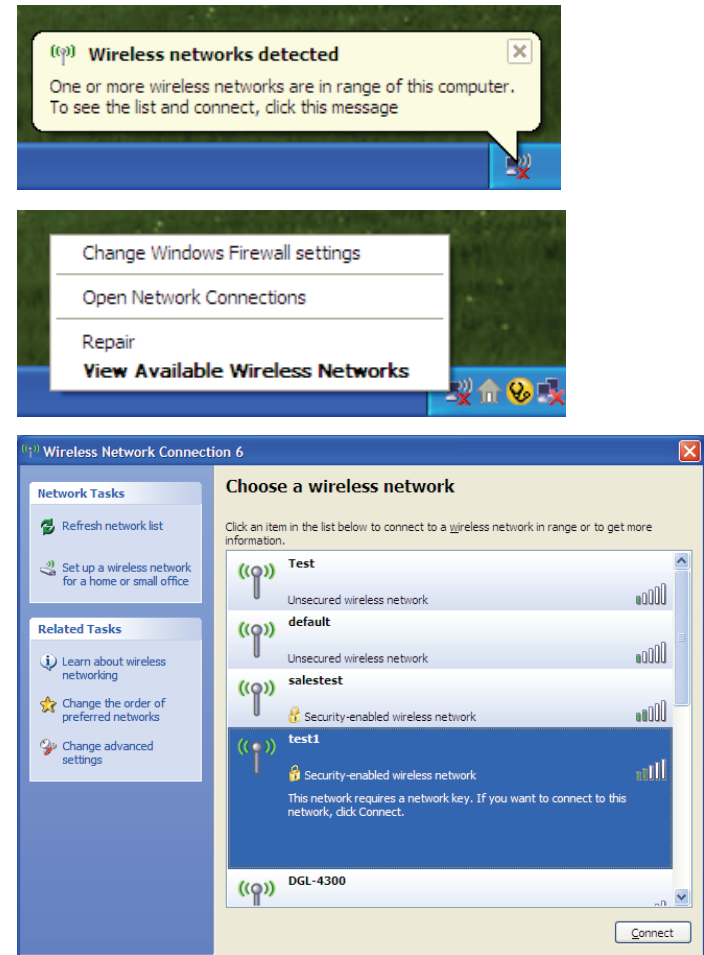
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

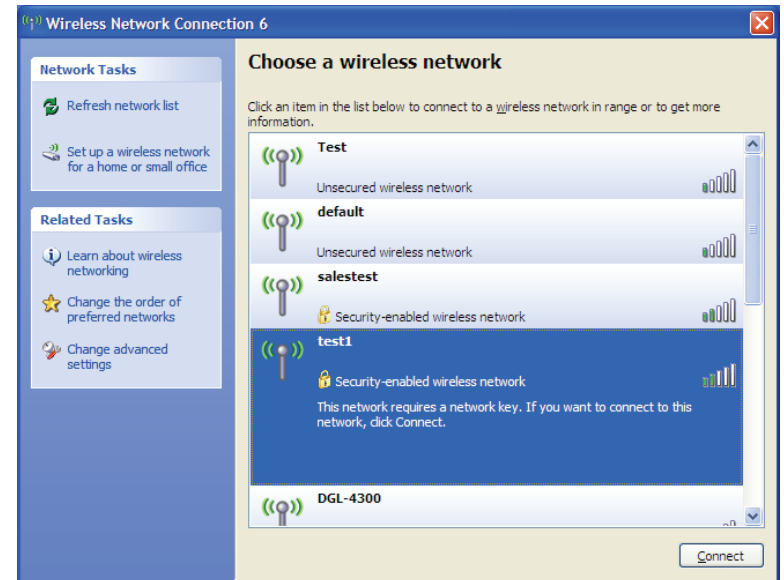
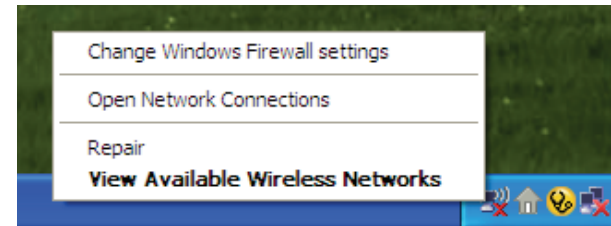
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



## WPA/WPA2

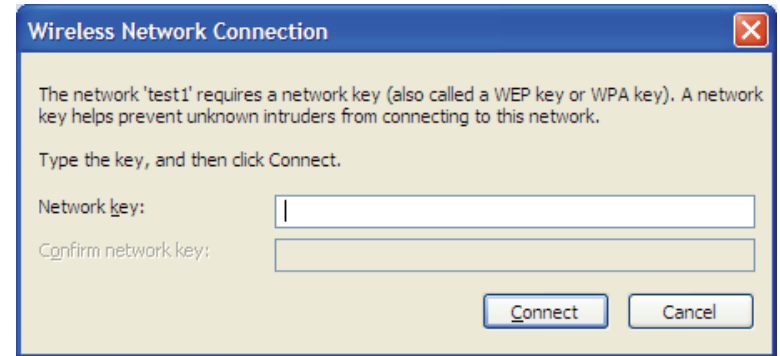
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

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



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

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



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-822. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

When entering the IP address of the D-Link router (192.168.0.1 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® 9 and higher
  - Mozilla Firefox 20 and higher
  - Google™ Chrome 25 and higher
  - Apple Safari 5.1 and higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.



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

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

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

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. When logging in, the username is **admin** and leave the password box empty.

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

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

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

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

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

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

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms
C:\>
```

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

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

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

- Open your browser, enter the IP address of your router (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

# Wireless Basics

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

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

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

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

## **What is Wireless?**

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

## **Why D-Link Wireless?**

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

## **How does wireless work?**

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

### **Wireless Local Area Network (WLAN)**

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

## **Wireless Personal Area Network (WPAN)**

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

## **Who uses wireless?**

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

### **Home**

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

### **Small Office and Home Office**

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

## **Where is wireless used?**

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

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

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

## **Tips**

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

### **Centralize your router or access point**

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

### **Eliminate Interference**

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

## Security

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

# Wireless Modes

There are basically two modes of networking:

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

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

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



# Networking Basics

## Check your IP address

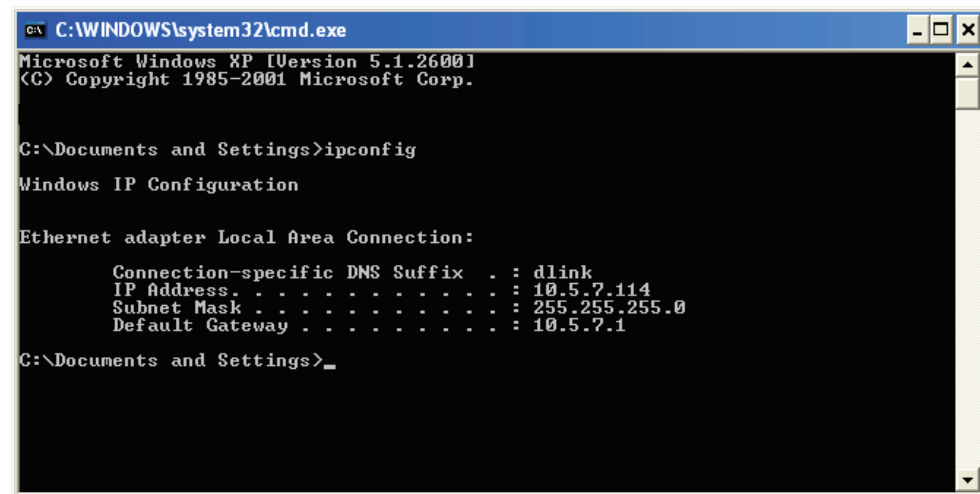
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(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

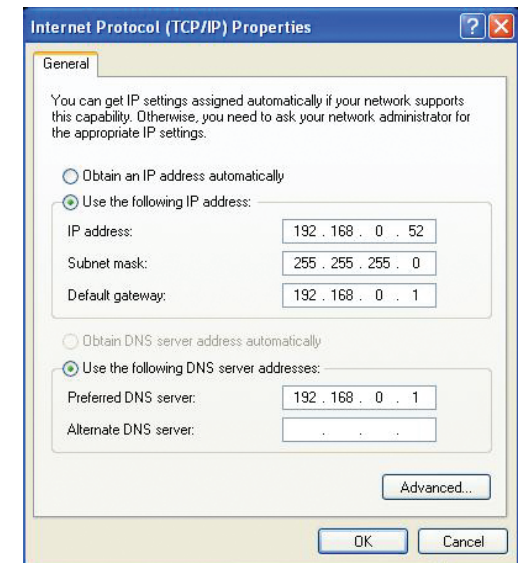
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.0.1).

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

### Step 5

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



# Technical Specifications

## Hardware Specifications

- LAN Interface: Four 10/100 Mbps LAN ports
- WAN Interface: One 10/100 Mbps Internet port
- Wireless Interface (2.4 GHz): IEEE 802.11b/g/n
- Wireless Interface (5 GHz): IEEE 802.11a/n/ac

## Operating Voltage

- Input: 100~240 V AC, 50~60 Hz
- Output: 12 V DC, 0.5 A

## Temperature

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

## Humidity

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

## Wireless Frequency Range

- IEEE 802.11a: 5180 MHz~5240 MHz, 5745 MHz~5825 MHz
- IEEE 802.11b: 2400 MHz~2483 MHz
- IEEE 802.11g: 2400 MHz~2484 MHz
- IEEE 802.11n: 2400 MHz~2484 MHz, 5180 MHz~5240 MHz, 5745 MHz~5825 MHz
- IEEE 802.11ac: 5180 MHz~5240 MHz, 5745 MHz~5825 MHz

## Wireless Bandwidth Rate

- IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11b: 11, 5.5, 2, and 1 Mbps

- IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11n: 6.5 to 300 Mbps
- IEEE 802.11ac: 6.5 to 867 Mbps

## Antenna Type

- Four external antennas

## Wireless Security

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

## Certifications

- CE
- RoHS
- LVD
- BSMI
- NCC
- FCC
- D-Link Green
- CSA
- CCC

## Dimensions & Weight

- 190 x 133 x 38 mm (7.48 x 5.23 x 1.49 inches)
- 263.1 g (9.28 oz)

# Regulatory Information

## Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

For operation within 5.15 ~ 5.25 GHz frequency range, it is restricted to indoor environment.

This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

### **Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 24cm between the radiator & your body.

**Note:** The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only. The product must be used with the power adapter included with the device.

### **Industry Canada statement:**

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.  
Caution :

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

Avertissement:

(i) les dispositifs fonctionnant dans la bande 5 150-5 250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

### **Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator & your body.

### **Déclaration d'exposition aux radiations:**

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 24 cm de distance entre la source de rayonnement et votre corps.

Le produit doit être utilisé avec l'adaptateur secteur fourni avec le périphérique.

### **Power management**

#### **1.1 For all equipment other than networked equipment:**

Equipment shall, unless inappropriate for the intended use, offer a power management function or a similar function. When equipment is not providing the main function, and other energy-using product(s) are not dependent on its functions, the power management function shall switch equipment after the shortest possible period of time appropriate for the intended use of the equipment, automatically into:

- standby mode, or
- off mode, or
- another condition which does not exceed the applicable power consumption requirements for off mode and/or standby mode when the equipment is connected to the mains power source. The power management function shall be activated.

#### **1.2 For networked equipment:**

Equipment shall, unless inappropriate for the intended use, offer a power management function, or a similar function. When equipment is not providing the main function, and other energy-using product(s) are not dependent on its functions, the power management function shall switch equipment after the shortest possible period of time appropriate for the intended use of the equipment, automatically into a condition having networked standby.