



# User Manual

## Xtreme N<sup>®</sup> Gigabit 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
2.0	June 10, 2010	• New Revision
2.1	June 9, 2011	• Added IPv6 DDNS Support
2.2	September 6, 2011	• Added GNU GPL Statement
2.3	July 03, 2012	• Added IPv6 Routing and Firewall • Added QRS Mobile app

## Trademarks

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

Copyright ©2012 by D-Link Systems, Inc.

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

# Table of Contents

<b>Preface</b> .....	<b>i</b>	DS-Lite .....	25
Manual Revisions.....	i	Wireless Settings .....	26
Trademarks .....	i	Manual Wireless Settings .....	27
<b>Product Overview</b> .....	<b>1</b>	Wireless Security .....	28
Package Contents .....	1	What is WPA?.....	28
System Requirements.....	2	Wireless Network Setup Wizard .....	29
Introduction .....	3	Configure WPA-Personal (PSK).....	31
Features .....	4	Configure WPA-Enterprise (RADIUS) .....	32
Hardware Overview.....	5	Add Wireless Device with WPS Wizard.....	34
Connections.....	5	Network Settings.....	36
LEDs .....	6	Router Settings.....	36
<b>Installation</b> .....	<b>7</b>	DHCP Server Settings.....	37
Before you Begin .....	7	DHCP Reservation .....	38
Wireless Installation Considerations .....	8	USB Settings.....	39
<b>Configuration</b> .....	<b>9</b>	IPV6 .....	40
Quick Router Setup Wizard (CD) .....	9	IPv6 Internet Connection Setup Wizard.....	41
QRS Mobile App.....	10	IPv6 Manual Setup .....	46
Quick Setup Wizard .....	12	Advanced .....	55
Web-based Configuration Utility.....	18	Virtual Server .....	55
Internet Connection Setup.....	19	Port Forwarding.....	57
Static IP.....	20	Application Rules .....	58
Dynamic IP .....	21	QoS Engine.....	59
PPPoE (DSL) .....	22	Network Filters .....	60
PPTP .....	23	Access Control.....	61
L2TP.....	24	Access Control Wizard.....	61
		Website Filters .....	64
		Inbound Filters.....	65

## Table of Contents

---

Firewall Settings .....	66	IPv6 .....	89
Application Level Gateway Configuration .....	67	IPv6 Routing .....	89
Routing .....	68	Support.....	90
Advanced Wireless Settings .....	69	<b>Connect to a Wireless Network.....</b>	<b>91</b>
WISH Settings.....	70	WPS Button.....	91
Wi-Fi Protected Setup (WPS).....	71	Windows® 7 .....	92
Advanced Network Settings .....	72	Windows Vista® .....	95
Guest Zone .....	73	Configure Wireless Security.....	96
IPv6 Firewall .....	74	Using Windows® XP .....	98
IPv6 Routing.....	75	Configure Wireless Security.....	99
Tools.....	76	<b>Troubleshooting .....</b>	<b>101</b>
Administrator Settings.....	76	<b>Wireless Basics .....</b>	<b>105</b>
Time Settings.....	77	Tips .....	107
SysLog .....	78	Wireless Modes .....	108
Email Settings.....	79	<b>Networking Basics .....</b>	<b>109</b>
System Settings .....	80	Check your IP address.....	109
Update Firmware.....	81	<b>Technical Specifications .....</b>	<b>111</b>
DDNS .....	82	<b>Contacting Technical Support .....</b>	<b>112</b>
System Check .....	83	<b>GNU General Public License .....</b>	<b>113</b>
Schedules.....	84	<b>Warranty.....</b>	<b>124</b>
Status.....	85	<b>Registration .....</b>	<b>130</b>
Device Information.....	85		
Log.....	86		
Stats .....	87		
Active Sessions.....	87		
Routing .....	88		
Wireless.....	88		

# Package Contents



DIR-655 Xtreme N® Gigabit Router



Ethernet Cable



Three Detachable Antennas



Power Adapter



CD-ROM with Manual and Setup Wizard

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-655 will cause damage and void the warranty.

# System Requirements

<b>Network Requirements</b>	<ul style="list-style-type: none"><li>• An Ethernet-based Cable or DSL modem</li><li>• IEEE 802.11n or 802.11g wireless clients</li><li>• 10/100/1000 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 6.0 or higher</li><li>• Chrome 2.0 or higher</li><li>• Firefox 3.0 or higher</li><li>• Safari 3.0 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>CD Installation Wizard Requirements</b>	<p><b>Computer with the following:</b></p> <ul style="list-style-type: none"><li>• Windows® 7, Vista®, or XP with Service Pack 2</li><li>• An installed Ethernet adapter</li><li>• CD-ROM drive</li></ul>

# Introduction

## **TOTAL PERFORMANCE**

Combines award winning router features and 802.11n wireless technology to provide the best wireless performance.

## **TOTAL SECURITY**

The most complete set of security features including Active Firewall and WPA2™ to protect your network against outside intruders.

## **TOTAL COVERAGE**

Provides greater wireless signal rates even at farther distances for best-in-class Whole Home Coverage.

## **ULTIMATE PERFORMANCE**

The D-Link Xtreme N™ Router (DIR-655) is a 802.11n compliant device that delivers real world performance of up to 650% faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the Xtreme N™ Router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this Router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

## **EXTENDED WHOLE HOME COVERAGE**

Powered by Xtreme N™ technology, this high performance router provides superior Whole Home Coverage while reducing dead spots. The Xtreme N™ Router is designed for use in bigger homes and for users who demand higher performance networking. Add a Xtreme N™ notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

## **TOTAL NETWORK SECURITY**

The Xtreme N™ Router supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this Xtreme N™ Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

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

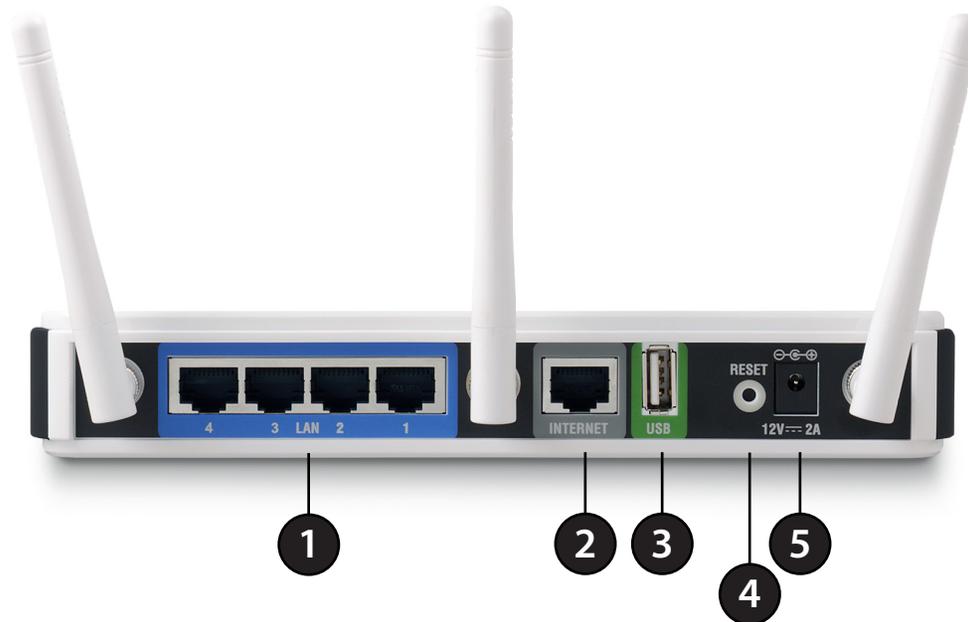
## Features

- **Faster Wireless Networking** - The DIR-655 provides up to 300Mbps\* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11n wireless router gives you the freedom of wireless networking at speeds 650% faster than 802.11g.
- **Compatible with 802.11g Devices** - The DIR-655 is still fully compatible with the IEEE 802.11g standard, so it can connect with existing 802.11g PCI, USB and FireWire 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-655 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-655 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-655 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 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

# Hardware Overview

## Connections



<b>1</b>	LAN Ports (1-4)	Connect Ethernet devices such as computers, switches, and hubs.
<b>2</b>	Internet Port	The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.
<b>3</b>	USB	Connect a USB 1.1 or 2.0 flash drive to configure the wireless settings using WCN.
<b>4</b>	Reset	Pressing the Reset button restores the router to its original factory default settings.
<b>5</b>	Power Receptor	Receptor for the supplied power adapter.

## LEDs



<b>1</b>	Power LED	A solid light indicates a proper connection to the power supply.
<b>2</b>	Internet LED	A solid light indicates connection on the Internet port. This LED blinks during data transmission. A solid blue light indicates that there is an Internet connection, an orange light indicates that there is none.
<b>3</b>	WLAN LED	A solid light indicates that the wireless segment is ready. This LED blinks during wireless data transmission.
<b>4</b>	Local Network's LED	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.
<b>5</b>	WCN LED	Insert a USB flash drive with WCN information. The LED will blink 3 times if it successfully transfers the wireless settings.

# 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. Also, 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 that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

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

# Configuration

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

- **Quick Router Setup Wizard** - Insert the supplied CD and launch the setup wizard (see below).
- **D-Link Setup Wizard** - This wizard will launch if you do not run the CD wizard and log into the router for the first time. Refer to page 12.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to page 18.
- **QRS Mobile app** - Download the QRS Mobile app on your iPhone, iPad, or Android mobile device and set up your router. Refer to the next page.

## Quick Router Setup Wizard (CD)

To run the **Quick Router Setup Wizard**, insert the CD in the CD-ROM drive. When the autorun screen appears, click **English** (or **French**), and then click the **Install** button.

**Note:** If the CD Autorun function does not automatically start on your computer, go to **Start** > **Run**. In the run box type **D:\autorun.exe** (where D: represents the drive letter of your CD-ROM drive).



When the Wizard appears, select your language from the drop-down menu and then click **Next** to continue. Follow the on-screen instructions to configure your router. Once you are finished, you may skip to page 18 and will be able to log into the web-based configuration utility and configure more advanced features.

**Note:** It is recommended to write down the SSID and Security Key, followed by the login password on the provided CD holder.

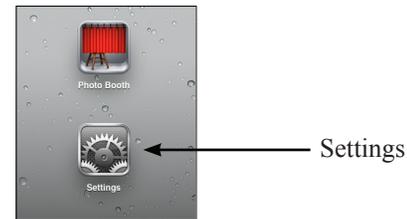
# QRS Mobile App

D-Link offers an app for your iPad, iPod Touch, or iPhone (iOS 4.3 or higher) to install and configure your router.

1. Scan the bar code to download “QRS Mobile” app from the app store to your iPhone or iPad.



2. From your mobile device, click Settings. Then, click **Wi-Fi**.



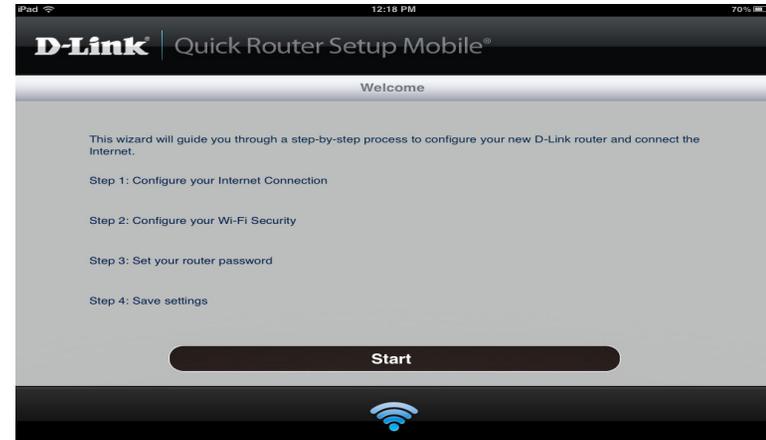
3. Select the default network “**dlink**”.



4. Once it connected, click on the **QRS Mobile** icon.



5. Click **Start** to continue.



6. Follow the instruction and click **Next** to continue.

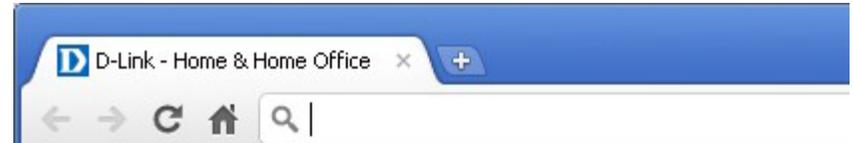
7. Once the Setup is complete, the following screen will show up. Then, select your new Wi-Fi Name and enter the password you just setup from your laptop or mobile device.



# 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**.

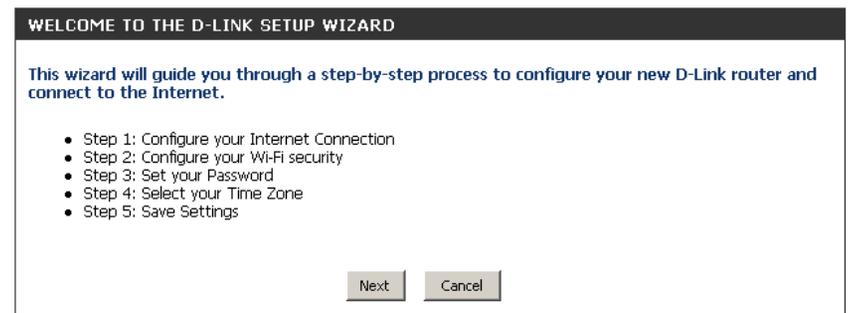
If you have already configured your settings and you would like to access the configuration utility, please refer to page 18.



If you did not run the setup wizard from the CD and this is the 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.

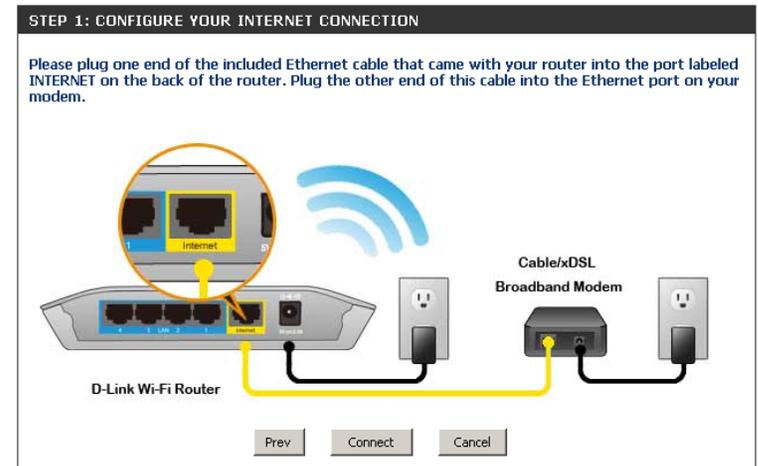
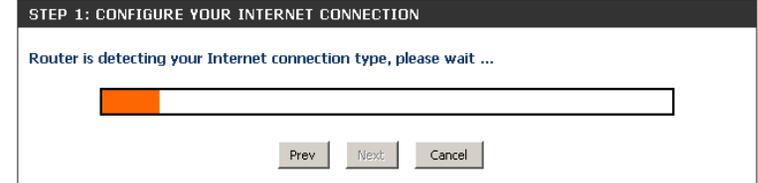


## Section 3 - Configuration

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.



## Section 3 - Configuration

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.

**STEP 1: CONFIGURE YOUR INTERNET CONNECTION**

Please select your Internet connection type below:

- 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 connection type of connection.
- Username / Password Connection (PPTP)**  
PPTP client.
- Username / Password Connection (L2TP)**  
L2TP client.
- Static IP Address Connection**  
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

Prev Next Cancel

**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

## Section 3 - Configuration

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 (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 :

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 :

## Section 3 - Configuration

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

Create a wireless security passphrase or key (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.

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.

Select your time zone from the drop-down menu and 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)

**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 :

**STEP 4: SELECT YOUR TIME ZONE**

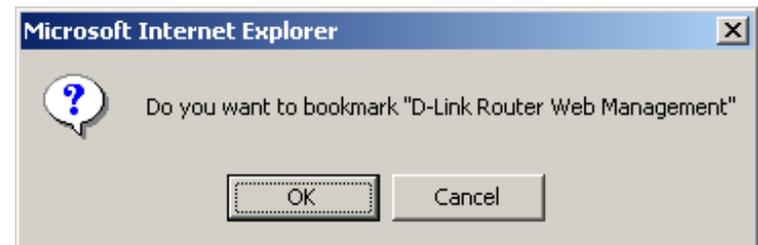
Select the appropriate time zone for your location. This information is required to configure the time-based options for the router.

## Section 3 - Configuration

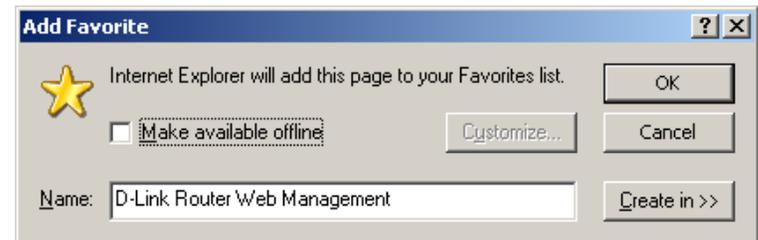
The Setup Complete window will display your wireless settings. Click **Save and Connect** to continue.



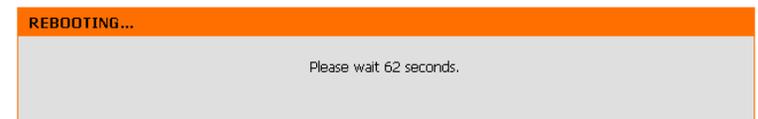
If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.



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



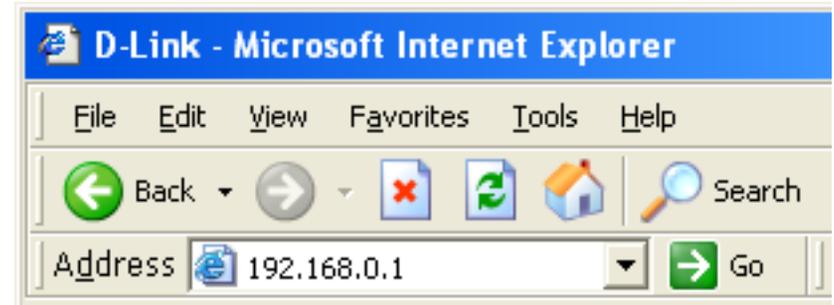
The router will now reboot. Please allow a minute or two. Click the **Continue** button once it is active.



# Web-based Configuration Utility

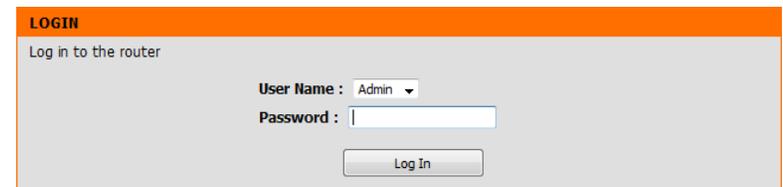
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.0.1).

You can also enter **http://dlinkrouter** to connect.



Select **Admin** from the drop-down menu and then enter your password. The password is left blank by default.

If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



# Internet Connection Setup

You may click **Internet Connection Setup Wizard** to quickly configure your router.

If you want to enter your settings without running the wizard, click **Manual Internet Configuration Setup** and skip to the next page.

The screenshot shows a web-based configuration interface for a D-Link router. It is divided into three main sections:

- INTERNET CONNECTION**: An orange header section containing the text: "There are two ways to set up your Internet connection: you can use the Web-based Internet Connection Setup Wizard, or you can manually configure the connection."
- INTERNET CONNECTION WIZARD**: A dark grey header section containing the text: "If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below." Below this text is a button labeled "Internet Connection Setup Wizard". A **Note** follows: "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 OPTIONS**: A dark grey header section containing the text: "If you would like to configure the Internet settings of your new D-Link Systems Router manually, then click on the button below." Below this text is a button labeled "Manual Internet Connection Setup".

# Manual Internet Setup

## Static IP

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.

**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.

**WAN**

Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

**Note:** If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

**INTERNET CONNECTION TYPE**

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

My Internet Connection is :

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

**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 :**   
**MTU :**  (bytes) MTU default = 1500  
**MAC Address :**

## Dynamic IP

**My Internet Connection:** Select **Dynamic IP (DHCP)** to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for cable modem services such as Comcast and Cox.

**Enable Advanced DNS Service:** Advanced Domain Name System (DNS) services enhances your Internet performance by getting you the information and web pages you are looking for faster and more reliably. In addition, it improves your overall Internet experience by correcting many common typo mistakes automatically, taking you where you intended to go and saving you valuable time.

**Disclaimer:** D-Link makes no warranty as to the availability, reliability, functionality and operation of the Advanced DNS service or its features.

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

**Use Unicasting:** Check the box if you are having problems obtaining an IP address from your ISP.

**Primary/Secondary DNS Server:** Enter the Primary and secondary DNS server IP addresses assigned by your ISP. These addresses are usually obtained automatically from your ISP. Leave at 0.0.0.0 if you did not specifically receive these from your ISP.

**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 :

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service :

---

**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 :

Use Unicasting :  (compatibility for some DHCP Servers)

Primary DNS Address :

Secondary DNS Address :

MTU :  (bytes) MTU default = 1500

MAC Address :

## 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:** 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 the Primary and Secondary DNS Server Addresses (Static PPPoE only).

**DNS Addresses:** Enter a maximum idle time during which the Internet connection is maintained during 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.

**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 :** PPPoE (Username / Password) ▼

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

**Enable Advanced DNS Service :**

---

**PPPOE :**

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

**Address Mode**  Dynamic IP  Static IP

**IP Address :**

**User Name :**

**Password :**

**Verify Password :**

**Service Name :**  (optional)

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

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

**Primary DNS Address :**  (optional)

**Secondary DNS Address :**  (optional)

**MTU :**  (bytes) MTU default = 1492

**MAC Address :**

## 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.

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

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

**PPTP Subnet Mask:** Enter the Primary and Secondary DNS Server Addresses (Static PPTP only).

**PPTP Gateway:** Enter the Gateway IP Address provided by your ISP.

**PPTP Server IP:** Enter the Server IP provided by your ISP (optional).

**Username:** Enter your PPTP username.

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

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

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

**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. 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.

**INTERNET CONNECTION TYPE**

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

**My Internet Connection is :** PPTP (Username / Password) ▾

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

**Enable Advanced DNS Service :**

---

**PPTP :**

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 on     On demand     Manual

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

**Primary DNS Address :**

**Secondary DNS Address :**

**MTU :**  (bytes) MTU default = 1400

**MAC Address :**

## 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.

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

**L2TP IP Address:** Enter the L2TP IP address supplied by your ISP (Static only).

**L2TP Subnet Mask:** Enter the Subnet Mask supplied by your ISP (Static only).

**L2TP Gateway:** Enter the Gateway IP Address provided by your ISP.

**L2TP Server IP:** Enter the Server IP provided by your ISP (optional).

**Username:** Enter your L2TP username.

**Password:** Enter your L2TP password and then retype the password in the next box.

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

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

**DNS Servers:** Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

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

**Clone 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 :** L2TP (Username / Password) ▼

---

**ADVANCED DNS SERVICE**

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

**Enable Advanced DNS Service :**

---

**L2TP :**

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 demand  Manual

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

**Primary DNS Address :**

**Secondary DNS Address :**

**MTU :**  (bytes) MTU default = 1400

**MAC Address :**

## DS-Lite

Another Internet Connection type is 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, 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.

**WAN**

Use this section to configure your Internet Connection type. There are several connection types to choose from Static IP, DHCP, PPPoE, PPTP, L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

**Note:** If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

Save Settings
Don't Save Settings
Reboot Now

**INTERNET CONNECTION TYPE**

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

My Internet Connection is : DS-Lite

**AFTR ADDRESS INTERNET CONNECTION TYPE :**

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

**DS-Lite Configuration**    DS-Lite DHCPv6 Option    Manual Configuration

**AFTR IPv6 Address :**

**B4 IPv4 Address :** 192.0.0. (optional)

**WAN IPv6 Address :**

**IPv6 WAN Default Gateway :**

# Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Connection Setup Wizard** and refer to page 29.

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 41.

If you want to manually configure the wireless settings on your router click **Manual Wireless Connection Setup** and refer to the next 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.

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

This wizard is designed to assist you in connecting your wireless device to your 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](#)

### MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

[Manual Wireless Connection Setup](#)

# Manual Wireless Settings

**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.

**Schedule:** The schedule of time when the wireless settings rules 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.

**Wireless Network Name:** 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 Scan:** The **Auto Channel Scan** setting can be selected to allow the DIR-655 to choose the channel with the least amount of interference.

**Wireless Channel:** Indicates the channel setting for the DIR-655. By default the channel is set to 6. 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 Scan**, this option will be greyed out.

**802.11 Mode:** Select one of the following:  
**802.11g Only** - Select if all of your wireless clients are 802.11g.  
**802.11n Only** - Select only if all of your wireless clients are 802.11n.  
**Mixed 802.11n and 802.11g** - Select if you are using a mix of 802.11n and 11g wireless clients.

**Channel Width:** Select the Channel Width:  
**Auto 20/40** - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.  
**20MHz** - Select if you are not using any 802.11n wireless clients.  
**40MHz** - Select if using only 802.11n wireless clients.

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

**Visibility Status:** Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-655. If Invisible is selected, the SSID of the DIR-655 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-655

**WIRELESS NETWORK SETTINGS**

**Enable Wireless :**  Always New Schedule

**Wireless Network Name :**  (Also called the SSID)

**802.11 Mode :**

**Enable Auto Channel Scan :**

**Wireless Channel :**

**Transmission Rate :**

**Channel Width :**

**Visibility Status :**  Visible  Invisible

---

**WIRELESS SECURITY MODE**

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

**Security Mode :**

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-655 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, or Wi-Fi Protected Access, is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?\*&\_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

# Wireless Network Setup Wizard

To run the security wizard, click on Setup at the top and then click **Wireless Network Setup Wizard**.

Click **Next** to continue.

**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 Network 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.

**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](#)

**MANUAL WIRELESS NETWORK SETUP**

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

[Manual Wireless Network Setup](#)

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

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

**Network Name (SSID) :**

- 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](#)

## Section 3 - Configuration

---

The following screen will show you your Pre-Shared Key to enter on your wireless clients.

Click **Save** to finish the Security Wizard.

**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 Network Name (SSID) :** dlink  
**Security Mode :** Auto (WPA or WPA2) - Personal  
**Cipher Type :** TKIP and AES  
**Pre-Shared Key :** 9fa2e46b5e9e860843fe7d22398faf16fab24d64d60eb406b0829101495d4939

If you selected WPA-Enterprise, the RADIUS information will be displayed. Click **Save** to finish the Security Wizard.

## Configure WPA-Personal (PSK)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Click on **Manual Wireless Connection Setup**.
3. Next to *Security Mode*, select **WPA-Personal**.
4. Next to *WPA Mode*, select **Auto, WPA2 Only, or WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
6. Next to *Pre-Shared Key*, enter a key (passphrase). The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.
7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

The screenshot shows the D-Link DIR-655 web-based configuration interface. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar lists configuration sections: 'INTERNET', 'WIRELESS SETTINGS', 'NETWORK SETTINGS', 'USB SETTINGS', and 'IPv6'. The main content area is titled 'WIRELESS :'. It contains a 'WIRELESS NETWORK SETTINGS' section with options for 'Enable Wireless' (checked), 'Wireless Network Name' (dlink), '802.11 Mode' (Mixed 802.11n, 802.11g and 802.11b), 'Enable Auto Channel Scan' (checked), 'Wireless Channel' (2.437 GHz - CH 6), 'Transmission Rate' (Best (automatic)), 'Channel Width' (20 MHz), and 'Visibility Status' (Visible). Below this is the 'WIRELESS SECURITY MODE' section, which includes a 'Security Mode' dropdown set to 'WPA-Personal'. The 'WPA' section explains the modes and provides options for 'WPA Mode' (Auto (WPA or WPA2)), 'Cipher Type' (TKIP and AES), and 'Group Key Update Interval' (3600 seconds). The 'PRE-SHARED KEY' section has a text input field for the key, currently showing asterisks. A 'Helpful Hints...' sidebar on the right provides additional information about network security and channel selection.

## Configure WPA-Enterprise (RADIUS)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Click on **Manual Wireless Connection Setup**.
3. Next to *Security Mode*, select **WPA-Enterprise**.
4. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
6. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).
7. Next to *RADIUS Server IP Address* enter the IP Address of your RADIUS server.
8. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
9. Next to *RADIUS Server Shared Secret*, enter the security key.

The screenshot shows the wireless security configuration interface. At the top, it explains that WPA-Enterprise provides a higher level of security but requires an external RADIUS server. The **Security Mode** is set to **WPA-Enterprise**. Below this, the **WPA** section is active, detailing that WPA or WPA2 mode is used for a balance of security and compatibility. It offers three options: **Auto** (WPA or WPA2), **WPA2 Only** (using AES/CCMP), and **WPA Only** (using TKIP). The **WPA Mode** is set to **Auto (WPA or WPA2)**, the **Cipher Type** is **TKIP and AES**, and the **Group Key Update Interval** is **3600** seconds. The **EAP (802.1X)** section is also visible, stating that the router uses EAP (802.1x) for authentication. Fields for **Authentication Timeout** (60 minutes), **RADIUS server IP Address** (0.0.0.0), **RADIUS server Port** (1812), and **RADIUS server Shared Secret** are present. The **MAC Address Authentication** checkbox is checked. An **Advanced >>** button is at the bottom of the configuration area. A sidebar on the right contains a warning about writing down the Key or Passphrase and a **More...** link.

9. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.
10. Click **Advanced** to enter settings for a secondary RADIUS Server.
11. Click **Apply Settings** to save your settings.

### EAP (802.1X)

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

**Authentication Timeout :**  (minutes)

**RADIUS server IP Address :**

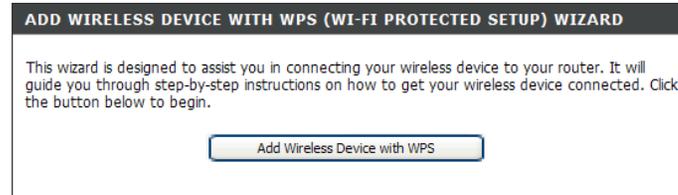
**RADIUS server Port :**

**RADIUS server Shared Secret :**

**MAC Address Authentication :**

## Add Wireless Device with WPS Wizard

From the **Setup > Wireless Settings** screen, click **Add Wireless Device with WPS**.



Select **Auto** to add a wireless client using WPS (Wi-Fi Protected Setup) and then click **Next**. Skip to the next page.



If you select **Manual**, a settings summary screen will appear. Write down the security key and enter this on your wireless clients. Click **OK** to finish.

**PIN:** Select this option to use PIN method. In order to use this method you must know the wireless client's 8 digit PIN and click **Connect**.

**PBC:** Select this option to use PBC (Push Button) method to add a wireless client. Click **Connect**.

Once you click **Connect**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.

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

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

**PBC**

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

### ADD WIRELESS DEVICE WITH WPS

Please press down the Push Button (physical or virtual) on the wireless device you are adding to your wireless network within **117** seconds ...

# Network Settings

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

## Router Settings

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

If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

**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 the 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 here, you may need to adjust your PC's network settings to access the network again.

---

**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 :**   
**Subnet Mask :**   
**Device Name :**   
**Local Domain Name :**   
**Enable DNS Relay :**

## DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-655 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 to be 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-655. 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** Check this box to enable the DHCP server on your router.

**Server:** Uncheck to disable this function.

**DHCP IP Address** Enter the starting and ending IP addresses for the DHCP server's

**Range:** 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:** Enable this feature to broadcast your networks DHCP server to LAN/WLAN clients.

**NetBIOS Announcement:** NetBIOS allows LAN hosts to discover all other computers within the network, enable this feature to allow the DHCP Server to offer NetBIOS configuration settings.

**Learn NetBIOS from WAN:** Enable this feature to allow WINS information to be learned from the WAN side, disable to allow manual configuration.

**NetBIOS Scope:** This feature allows the configuration of a NetBIOS 'domain' name under which network hosts operates. This setting has no effect if the 'Learn NetBIOS information from WAN' is activated."

**NetBIOS Mode Type:** Select the different type of NetBIOS node: **Broadcast only**, **Point-to-Point**, **Mixed-mode**, and **Hybrid**.

**Primary/Secondary WINS IP Address:** Enter your Primary (and Secondary) WINS IP address(es).

**DHCP SERVER SETTINGS**

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

**Enable DHCP Server :**

**DHCP IP Address Range :**  to

**DHCP Lease Time :**  (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.

**Copy 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.

**Save:** Click **Save** to save your entry. You must click **Save Settings** at the top to activate your reservations.

**Number of Dynamic DHCP Clients:** In this section you can see what LAN devices are currently leasing IP addresses.

**Revoke:** Click **Revoke** to cancel the lease for a specific LAN device and free an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.

**Note:** The Revoke option will not disconnect a PC with a current network session from the network; you would need to use MAC Address Filter to do that. Revoke will only free up a DHCP Address for the very next requester. If the previous owner is still available, those two devices may both receive an IP Address Conflict error, or the second device may still not receive an IP Address; in that case, you may still need to extend the "DHCP IP Address Range" to address the issue, it is located in the DHCP Server section.

**Reserve:** The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

**ADD DHCP RESERVATION**

**Enable :**

**Computer Name :**  << Computer Name ▾

**IP Address :**

**MAC Address :**

**DHCP RESERVATIONS LIST :**

Enable	Host Name	MAC Address	IP Address

**NUMBER OF DYNAMIC DHCP CLIENTS : 1**

Hardware Address	Assigned IP	Hostname	Expires	
00:16:17:45:11:af	192.168.0.100	pm1-PC	Tue Dec 1 16:51:49 2009	<a href="#">Revoke</a> <a href="#">Reserve</a>

# USB Settings

Use this section to configure your USB port. There are two configurations to choose from: Network USB and WCN Configuration.

**Note:** *If using the Network USB option, users will need to install the Network USB Utility into the computers to share the USB device through the router.*

**USB Settings:** Choose between these two configuration: Network USB and WCN Configuration.

**Network USB:** Please set the Network USB Detection interval time.

### USB SETTINGS

Use this section to configure your USB port. There are several configurations to choose from: Network USB and WCN Configuration.

If you have trouble accessing the Internet through the router. Double check the settings you entered on this page and verify with your Internet Service Provider (ISP) if needed.

### USB SETTINGS

Choose the type of USB device to be plugged into the USB port.

My USB type is :

### SHAREPORT FOR GUEST ZONE

Enable SharePort For Guest Zone :

**Note:** *Please see the SharePort Manual on the CD for more information.*

# 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.

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.

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

DIR-655	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
INTERNET	<b>IPv6 INTERNET CONNECTION</b>				<b>Helpful Hints...</b> If you are new to networking and have never configured a router before, click on <b>IPv6 Internet Connection Setup Wizard</b> and the router will guide you through a few simple steps to get your network up and running.  If you consider yourself an advanced user and have configured a router before, click <b>Manual IPv6 Internet Connection Setup</b> to input all the settings manually.  <a href="#">More...</a>
WIRELESS SETTINGS	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.				
NETWORK SETTINGS	<b>IPv6 INTERNET CONNECTION SETUP WIZARD</b> 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.  <div style="text-align: center;"> <input type="button" value="IPv6 Internet Connection Setup Wizard"/> </div>				
USB SETTINGS	<b>MANUAL IPv6 LOCAL CONNECTIVITY SETTINGS</b> If you would like to configure IPv6 local connectivity setting of your D-Link Router, then click on the button below  <div style="text-align: center;"> <input type="button" value="IPv6 Local Connectivity Settings"/> </div>				
IPv6	<b>MANUAL IPv6 INTERNET CONNECTION SETUP</b> If you would like to configure the IPv6 Internet settings of your new D-Link Systems Router manually, then click on the button below.  <div style="text-align: center;"> <input type="button" value="Manual IPv6 Internet Connection Setup"/> </div>				

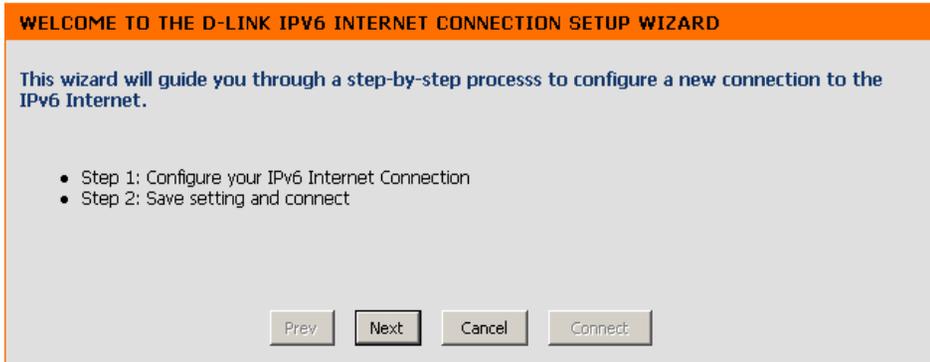
## IPv6 Internet Connection Setup Wizard

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.



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.

### STEP 1: CONFIGURE YOUR IPV6 INTERNET CONNECTION

Please select your IPv6 Internet Connection type

**IPv6 over PPPoE**

Choose this option if your IPv6 Internet 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 Internet Service Provider (ISP) provided you with IPv6 address information that has to be manually configured.

**Tunneling Connection (6rd)**

Choose this option if your Internet Service Provider (ISP) provided you a IPv6 Internet connection by using 6rd automatic tunneling mechanism.

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 LAN.)

**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::226:5AFF:FECC:F932

Subnet Prefix Length : 64

Default Gateway : \_\_\_\_\_

Primary IPv6 DNS Server : \_\_\_\_\_

Secondary IPv6 DNS Server : \_\_\_\_\_

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 : 192.168.0.100 Mask Length :

Assigned IPv6 Prefix : None

Tunnel Link-Local Address : FE80::COA8:0064/64

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 setting from your ISP.

The screenshot displays the IPv6 configuration interface. At the top, there is a header for 'IPv6' with a sub-instruction: 'Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.

The main configuration area is divided into several sections:

- IPv6 CONNECTION TYPE:** A section titled 'Choose the mode to be used by the router to the IPv6 Internet.' It features a dropdown menu labeled 'My IPv6 Connection is:' with 'Auto Detection' selected.
- IPv6 DNS SETTINGS:** A section titled 'Obtain a DNS server address automatically or enter a specific DNS server address.' It contains two radio buttons: 'Obtain a DNS server address automatically' (which is selected) and 'Use the following DNS address'. Below these are input fields for 'Primary IPv6 DNS Server:' and 'Secondary IPv6 DNS Server:'.
- LAN IPv6 ADDRESS SETTINGS:** A section titled '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.' It shows 'LAN IPv6 Address:' and 'LAN IPv6 Link-Local Address: FE80::226:5AFF:FECC:F931/64'.
- ADDRESS AUTOCONFIGURATION SETTINGS:** A section titled '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.' It includes several options: 'Enable automatic IPv6 address assignment:' (checked), 'Enable Automatic DHCP-PD in LAN:' (checked), 'Autoconfiguration Type:' (set to 'SLAAC + Stateless DHCPv6'), and 'Router Advertisement Lifetime:' (set to '1440' 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 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**

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

---

**IPv6 CONNECTION TYPE**

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

My IPv6 Connection is : Static IPv6

---

**WAN IPv6 ADDRESS SETTINGS**

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

Use Link-Local Address :

IPv6 Address :

Subnet Prefix Length :

Default Gateway :

Primary IPv6 DNS Server :

Secondary IPv6 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.

LAN IPv6 Address :  /64

LAN IPv6 Link-Local Address : FE80::226:5AFF:FECC:F931/64

---

**ADDRESS AUTOCONFIGURATION SETTINGS**

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable automatic IPv6 address assignment :

Autoconfiguration Type : SLAAC + Stateless DHCPv6

Router Advertisement Lifetime :  (minutes)

## 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 Autoconfiguration:** Check to enable the Autoconfiguration feature.

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

**Router Advertisement Lifetime:** Enter the IPv6 Address Lifetime (in minutes).

**IPv6**

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

**IPv6 CONNECTION TYPE**

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

**My IPv6 Connection is :**

**IPv6 DNS SETTINGS**

Obtain a DNS server address automatically or enter a specific DNS server address.

Obtain a DNS server address automatically  
 Use the following DNS address

**Primary IPv6 DNS Server :**

**Secondary IPv6 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 :**

**LAN IPv6 Address :**  /64

**LAN IPv6 Link-Local Address :** FE80::226:5AFF:FECC:F931/64

**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 :**

**Enable Automatic DHCP-PD in LAN :**

**Autoconfiguration Type :**

**Router Advertisement Lifetime:**  (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 during which the Internet connection is maintained during 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.

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

**IPv6**

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

---

**IPv6 CONNECTION TYPE**

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

My IPv6 Connection is : PPPoE

---

**PPPOE**

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

**PPPoE Session:**  Share with IPv4  Create a new session  
**Address Mode**  Dynamic IP  Static IP  
**IP Address :**   
**User Name :**   
**Password :**   
**Verify Password :**   
**Service Name :**  (optional)  
**Reconnect Mode :**  Always on  On demand  Manual  
**Maximum Idle Time :**  (minutes, 0=infinite)  
**MTU :**  (bytes) = 1492

---

**IPv6 DNS SETTINGS**

Obtain a DNS server address automatically or enter a specific DNS server address.

Obtain a DNS server address automatically  
 Use the following DNS address  
**Primary IPv6 DNS Server :**   
**Secondary IPv6 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 :**   
**LAN IPv6 Address :**  /64  
**LAN IPv6 Link-Local Address :** FE80::226:5AFF:FECC:F931/64

---

**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 :**   
**Enable Automatic DHCP-PD in LAN :**   
**Autoconfiguration Type :** SLAAC + Stateless DHCPv6  
**Router Advertisement Lifetime :**  (minutes)

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

**IPv6 Advertisement 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).

**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 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.

**Pv6 Address Lifetime:** Enter the Router Advertisement Lifetime (in minutes).

**IPv6**

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

---

**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 : 192.168.0.100

Local IPv6 Address :

---

**IPv6 DNS SETTINGS**

Obtain a DNS server address automatically or enter a specific DNS server address.

Obtain a DNS server address automatically  
 Use the following DNS address

Primary IPv6 DNS Server :

Secondary IPv6 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 :

LAN IPv6 Address :  /64

LAN IPv6 Link-Local Address : FE80::226:5AFF:FECC:F931/64

---

**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 :

Enable Automatic DHCP-PD in LAN :

Autoconfiguration Type : SLAAC + Stateless DHCPv6

Router Advertisement Lifetime :  (minutes)

## 6 to 4

**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 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**

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

**IPv6 CONNECTION TYPE**

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

My IPv6 Connection is :

**6to4 SETTINGS**

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

6to4 Address : 2002:COA8:0064::COA8:0064

6to4 Relay :

Primary IPv6 DNS Server :

Secondary IPv6 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.

LAN IPv6 Address : 2002:COA8:0064::0001 ::1/64

LAN IPv6 Link-Local Address : FE80::226:5AFF:FECC:F931/64

**ADDRESS AUTOCONFIGURATION SETTINGS**

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable automatic IPv6 address assignment :

Autoconfiguration Type :

Router Advertisement Lifetime :  (minutes)

## 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 Autoconfiguration:** Check to enable the Autoconfiguration feature.

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

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

**IPv6**

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

---

**IPv6 CONNECTION TYPE**

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

My IPv6 Connection is :

---

**6RD SETTINGS**

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

Enable Hub and Spoke Mode :

6rd Configuration :  6rd DHCPv4 Option  Manual Configuration

6rd IPv6 Prefix :  /

IPv4 Address : 192.168.0.100 Mask Length :

Assigned IPv6 Prefix : None

Tunnel Link-Local Address : FE80::C0A8:0064/64

6rd Border Relay IPv4 Address :

Primary IPv6 DNS Server :

Secondary IPv6 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.

LAN IPv6 Address : None

LAN IPv6 Link-Local Address : FE80::226:5AFF:FECC:F931/64

---

**ADDRESS AUTOCONFIGURATION SETTINGS**

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable automatic IPv6 address assignment :

Autoconfiguration Type :

Router Advertisement Lifetime :  (minutes)

## 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

Use this section to configure your IPv6 Connection type. If you are unsure of your connection method, please contact your Internet Service Provider.

Save Settings

Don't Save Settings

### IPv6 CONNECTION TYPE

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

My IPv6 Connection is :

### LAN IPv6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. The LAN IPv6 Link-Local Address is the IPv6 Address that you use to access the Web-based management interface

LAN IPv6 Link-Local Address : FE80::226:5AFF:FECC:F931/64

# Advanced Virtual Server

The DIR-655 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DIR-655 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-655 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-655 redirects the external service request to the appropriate server within the LAN network.

The DIR-655 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

For a list of ports for common applications, please visit [http://support.dlink.com/faq/view.asp?prod\\_id=1191](http://support.dlink.com/faq/view.asp?prod_id=1191).

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.

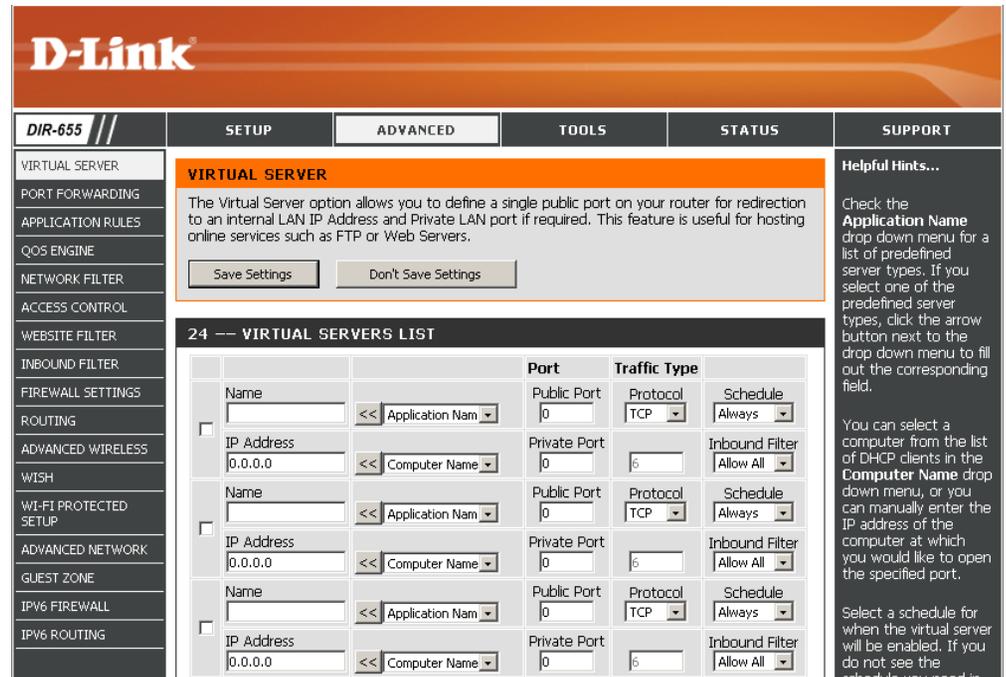
**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click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

**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.

**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.

**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.



**Helpful Hints...**

Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.

Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in

# 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), your 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

**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.

**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.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**PORT FORWARDING RULES :**

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 various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

Save Settings Don't Save Settings

**24 --- PORT FORWARDING RULES**

	Name	IP Address	Application Name	Computer Name	Ports to Open	Schedule	Inbound Filter
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	TCP 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	TCP 0	Always	Allow All
<input type="checkbox"/>		0.0.0.0	<< Application Name	<< Computer Name	UDP 0	Always	Allow All

**Helpful Hints...**

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the LAN computer to which you would like to open the specified port.

Select a schedule for when the rule will be enabled. If you do not see the schedule you need in the list of

# 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-655. 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-655 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 predefined 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.

**Helpful Hints...**

Use this feature if you are trying to execute one of the listed network applications and it is not communicating as expected.

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the [Tools → Schedules](#)

## 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.

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

**Dynamic Fragmentation:** This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones.

**Automatic Uplink Speed:** This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

**Measured Uplink Speed:** This displays the detected uplink speed.

**Manual 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 speed as a download/upload pair. For example, 1.5Mbits/284Kbits. 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).

**Connection Type:** By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either "Static" or "DHCP" in the Internet settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

**Detected xDSL:** When Connection Type is set to automatic, the automatically detected connection type is displayed here.

**QoS ENGINE**

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. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

Save Settings Don't Save Settings

**WAN TRAFFIC SHAPING**

Enable Traffic Shaping :

Automatic Uplink Speed :

Measured Uplink Speed : Not Estimated

Manual Uplink Speed : 128 kbps << Select Transmission Rate

Connection Type : Auto-detect

Detected Network type : Not detected

**QoS ENGINE SETUP**

Enable QoS Engine :

Automatic Classification :

Dynamic Fragmentation :

**Helpful Hints ...**

If the Measured Uplink Speed is known to be incorrect (that is, it produces suboptimal performance), disable Automatic Uplink Speed and enter the Manual Uplink Speed. Some experimentation and performance measurement may be required to converge on the optimal value.

More...

# 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 Broadband 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 section in this manual.

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

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**MAC ADDRESS FILTER**

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

Save Settings Don't Save Settings

**24 -- MAC FILTERING RULES**

Configure MAC Filtering below:  
Turn MAC Filtering OFF

MAC Address		DHCP Client List	
	<<	Computer Name	Clear
	<<	Computer Name	Clear
	<<	Computer Name	Clear
	<<	Computer Name	Clear
	<<	Computer Name	Clear
	<<	Computer Name	Clear

**Helpful Hints...**

Create a list of MAC addresses that you would either like to allow or deny access to your network.

Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu, then click the arrow to add that device's MAC address to the list.

Click the **Clear** button to remove the MAC address from the MAC Filtering list.

[More...](#)

# 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.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**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

**ENABLE**

Enable Access Control :

**Helpful Hints...**

Check **Enable Access Control** if you want to enforce rules that limit Internet access from specific LAN computers.

Click **Add Policy** to start the process of creating a rule. You can control the process at any time. When you are finished creating a rule it will be added to the **Policy Table** below.

Click the **Edit** icon to modify an existing rule using the **Policy Wizard**.

Click the **Delete** icon to permanently remove a rule.

## Access Control Wizard

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

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**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

## Section 3 - Configuration

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 :

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



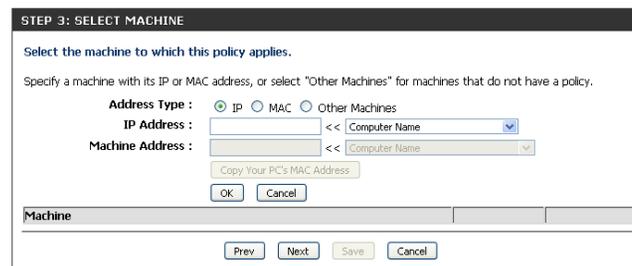
STEP 2: SELECT SCHEDULE

Choose a schedule to apply to this policy.

Details :

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.



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 :  <<

Machine Address :  <<

Machine

## Section 3 - Configuration

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.

**STEP 4: SELECT FILTERING METHOD**

Select the method for filtering.

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

Prev Next Save Cancel

# Website Filters

Website Filters are used to deny LAN computers from accessing specific web sites by the URL or domain. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display. To use this feature, enter the text string to be blocked and click **Save Settings**. The text to be blocked will appear in the list. To delete the text, click **Clear the List Below**.

**Website URL/ Domain:** Enter the keywords or URLs that you want to block (or allow). Any URL with the keyword in it will be blocked.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'WEBSITE FILTER' selected. The main content area is titled 'WEBSITE FILTER' and contains the following text: 'The Website Filter option allows you to set up a list of Web sites you would like to allow or deny through your network. To us this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. A section titled '40 - WEBSITE FILTERING RULES' contains the text 'Configure Website Filter below:' followed by a dropdown menu set to 'DENY computers access to ONLY these sites'. Below the dropdown is a 'Clear the list below...' button. At the bottom, there is a table with the header 'Website URL/Domain' and two columns of input fields for entering URLs or domains.

# 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.

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

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

**Save:** Click the **Save** 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.

**D-Link**

DIR-655

SETUP ADVANCED TOOLS STATUS SUPPORT

**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.

**Helpful Hints...**

Give each rule a **Name** that is meaningful to you.

Each rule can either **Allow** or **Deny** access from the WAN.

Up to eight ranges of WAN IP addresses can be controlled by each rule. The checkbox by each IP range can be used to disable ranges already defined.

The starting and ending IP addresses are WAN-side address.

Click the **Add** or **Update** button to store a finished rule in the Rules List below.

Click the **Edit** icon in the Rules List to change a rule.

Click the **Delete** icon in the Rules List to permanently remove a rule.

**More...**

**ADD INBOUND FILTER RULE**

Name :

Action :

Remote IP Range	Enable	Remote IP Start	Remote IP End
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="255.255.255.255"/>

**INBOUND FILTER RULES LIST**

Name	Action	Remote IP Range

**WIRELESS**

# Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-655 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.

**NAT Endpoint** Select one of the following for TCP and UDP ports:

**Filtering: Endpoint Independent** - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

**Address Restricted** - Incoming traffic must match the IP address of the outgoing connection.

**Address + Port Restriction** - Incoming traffic must match the IP address and port of the outgoing connection.

**Enable DMZ Host:** If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

**Note:** *Placing 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.*

**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 **Basic > DHCP** page so that the IP address of the DMZ machine does not change.

The screenshot shows the D-Link DIR-655 web interface. The 'ADVANCED' tab is selected, and the 'FIREWALL SETTINGS' section is active. The 'Enable SPI' checkbox is checked. Under 'NAT ENDPOINT FILTERING', 'UDP Endpoint Filtering' is set to 'Address Restricted' and 'TCP Endpoint Filtering' is set to 'Port And Address Restricted'. The 'ANTI-SPOOF CHECKING' section has 'Enable anti-spoof checking' unchecked. The 'DMZ HOST' section has 'Enable DMZ Host' unchecked, with the 'DMZ IP Address' field set to '0.0.0.0' and a 'Computer Name' dropdown menu. The 'APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION' section has 'PPTP', 'IPSec (VPN)', 'RTSP', and 'SIP' all checked.

## Application Level Gateway Configuration

Here you can enable or disable ALG's. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

**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.

**RTSP:** Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

**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.

# Routing

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

**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.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**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

**32 --ROUTE LIST**

	Name	Destination IP	Metric	Interface
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>
	Netmask	Gateway		
	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>		
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>
	Netmask	Gateway		
	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>		
<input type="checkbox"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="1"/>	<input type="text" value="WAN"/>
	Netmask	Gateway		
	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>		

**Helpful Hints...**

Each route has a check box next to it, check this box if you want the route to be enabled.

The name field allows you to specify a name for identification of this route, e.g. "Network 2"

The destination IP address is the address of the host or network you wish to reach.

The netmask field identifies the portion of the destination IP in use.

The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

More...

# Advanced Wireless Settings

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

**Beacon Period:** Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

**RTS Threshold:** This value should remain at its default setting of 2342. If inconsistent data flow is a problem, only a minor modification should be made.

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

**DTIM Interval:** (Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

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

**Short GI:** Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**ADVANCED WIRELESS**

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

Save Settings Don't Save Settings

**ADVANCED WIRELESS SETTINGS**

Transmit Power : High

Beacon Period : 100 (20..1000)

RTS Threshold : 2346 (0..2347)

Fragmentation : 2346 (256..2346)

DTIM Interval : 1 (1..255)

WLAN Partition :

WMM Enable :

Short GI :

**Helpful Hints...**

It is recommended that you leave these parameters at their default values. Adjusting them could limit the performance of your wireless network.

Use **802.11d** only for countries where it is required.

Enabling **WMM** can help control latency and jitter when transmitting multimedia content over a wireless connection.

[More...](#)

# WISH Settings

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

**Enable WISH:** Enable this option if you want to allow WISH to prioritize your traffic.

**HTTP:** Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

**Windows Media Center:** Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

**Automatic:** When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behavior that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

**WISH Rules:** A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

The screenshot shows the WISH settings interface for a D-Link DIR-655 router. The interface includes a navigation menu on the left with options like VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WISH, WI-FI PROTECTED SETUP, ADVANCED NETWORK, GUEST ZONE, IPV6 FIREWALL, and IPV6 ROUTING. The main content area is divided into several sections:

- WISH:** A section with a description: "WISH (Wireless Intelligent Stream Handling) prioritizes the traffic of various wireless applications." It contains "Save Settings" and "Don't Save Settings" buttons.
- WISH:** A section with the "Enable WISH" checkbox, which is currently unchecked.
- PRIORITY CLASSIFIERS:** A section with checkboxes for "HTTP" and "Windows Media Center", both of which are checked.
- 24 -- WISH RULES:** A table for defining WISH rules. The table has columns for Name, Priority (set to Background (BK)), Protocol (set to TCP), Host 1 IP Range (0.0.0.0 to 255.255.255.255), Host 1 Port Range (0 to 65535), Host 2 IP Range (0.0.0.0 to 255.255.255.255), and Host 2 Port Range (0 to 65535).

On the right side of the interface, there is a "Helpful Hints..." section with text: "Enable this option if you want to allow WISH to prioritize wireless traffic." and "For most applications, the priority classifiers ensure the right priorities, and specific WISH Rules are not required." Below this is a "More..." link.

# 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 depressing 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.

**Lock Wireless Security Settings:** Locking the wireless security settings prevents the settings from being changed by the Wi-Fi Protected Setup feature of the router. Devices can still be added to the network using Wi-Fi Protected Setup. However, the settings of the network will not change once this option is checked.

**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. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.

**Current PIN:** Shows the current value of the router’s 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 registrar. This Wizard helps you add wireless devices to the wireless network.

**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 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

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.

**Add Wireless Device Wizard:** Start the wizard.

**Device Wizard:**

The screenshot shows the D-Link DIR-655 router's web interface. The main content area is titled "WI-FI PROTECTED SETUP" and contains the following sections:

- WI-FI PROTECTED SETUP:** A section with a description: "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." Below this are two buttons: "Save Settings" and "Don't Save Settings".
- WI-FI PROTECTED SETUP:** A section with two checkboxes: "Enable" (checked) and "Disable WPS-PIN Method" (unchecked). Below the "Disable WPS-PIN Method" checkbox is a "Reset to Unconfigured" button.
- PIN SETTINGS:** A section showing the "Current PIN" as "56068078". Below this are two buttons: "Generate New PIN" and "Reset PIN to Default".
- ADD WIRELESS STATION:** A section with a single button: "Add Wireless Device with WPS".

The left sidebar contains a list of menu items: VIRTUAL SERVER, PORT FORWARDING, APPLICATION RULES, QOS ENGINE, NETWORK FILTER, ACCESS CONTROL, WEBSITE FILTER, INBOUND FILTER, FIREWALL SETTINGS, ROUTING, ADVANCED WIRELESS, WISH, WI-FI PROTECTED SETUP (highlighted), ADVANCED NETWORK, GUEST ZONE, IPV6 FIREWALL, and IPV6 ROUTING. The bottom of the page has a "WIRELESS" header.

The right sidebar contains "Helpful Hints..." with the following text:

- Enable** if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup.
- Only "Admin" account can change security settings.
- Lock Wireless Security Settings** after all wireless network devices have been configured.
- Click **Add Wireless Device Wizard** to use Wi-Fi Protected Setup to add wireless devices to the wireless network.
- More...**

# Advanced Network Settings

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

**Internet Ping:** Unchecking the box will not allow the DIR-655 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be “pinged”.

**Internet Port Speed:** You may set the port speed of the Internet port to 10Mbps, 100Mbps, 1000Mbps, or Auto 10/100/1000Mbps. Some older cable or DSL modems may require you to set the port speed to 10Mbps.

**Multicast** Check the box to allow multicast traffic to pass **streams:** through the router from the Internet.

**D-Link**

DIR-655 // SETUP **ADVANCED** TOOLS STATUS SUPPORT

**ADVANCED NETWORK**

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

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 :

**WAN PING**

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

Enable WAN Ping Respond :

WAN Ping Inbound Filter : Allow All

Details : Allow\_All

**WAN PORT SPEED**

WAN Port Speed : 10/100/1000Mbps Auto

**MULTICAST STREAMS**

Enable Multicast Streams :

**IPv6 MULTICAST STREAMS**

Enable IPv6 Multicast Streams :

**Helpful Hints...**

UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.

For added security, it is recommended that you disable the WAN Ping Respond option. Ping is often used by malicious Internet users to locate active networks or PCs.

The WAN speed is usually detected automatically. If you are having problems connecting to the WAN, try selecting the speed manually.

If you are having trouble receiving multicast streams from the Internet, make sure the Multicast Streams option is enabled.

[More...](#)

**WIRELESS**

# 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.

**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.

**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 displays the D-Link router's web interface for configuring the Guest Zone. The top navigation bar includes 'D-Link', 'DIR-655', and tabs for 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration categories, with 'GUEST ZONE' highlighted. The main content area is titled 'GUEST ZONE' and contains the following settings:

- Enable Guest Zone:** A checkbox that is currently unchecked. Next to it is a dropdown menu set to 'Always' and a 'New Schedule' button.
- Wireless Band:** A dropdown menu set to '2.4GHz Band'.
- Wireless Network Name:** A text input field containing 'dlink\_guest', with a note '(Also called the SSID)'.
- Enable Routing Between Zones:** A checkbox that is currently unchecked.

Below the settings are two buttons: 'Save Settings' and 'Don't Save Settings'. On the right side of the interface, there is a 'Helpful Hints...' section with a 'More...' link.

# IPv6 Firewall

The DIR-655's IPv6 Firewall feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-655'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.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The main content area is titled 'IPv6 FIREWALL RULES :'. Below this, there is a section for 'IPv6 SIMPLE SECURITY' with an 'Enable IPv6 Simple Security' checkbox. The 'IPv6 FIREWALL RULES' section contains a configuration table with the following structure:

Name	Schedule	Interface	IP Address Range	Protocol	Port Range
1.	Always	Source		TCP	1-65535
		Dest			

Helpful Hints...  
For each rule you can create a name and control the direction of traffic. You can also allow or deny a range of IP Addresses, the protocol and a port range.  
In order to apply a schedule to a firewall rule, you must first define a schedule on the [Tools -> Schedules](#) page.  
[More...](#)

# 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.

**D-Link**

DIR-655

SETUP ADVANCED TOOLS STATUS SUPPORT

**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**

Name	Metric	Interface	Destination IP/Prefix Length	Gateway
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> /64	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> /64	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> /64	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> /64	<input type="text"/>

**Helpful Hints...**

Each route has a check box next to it, check this box if you want the route to be enabled.

The name field allows you to specify a name for identification of this route, e.g. "Network 2".

The destination IP address is the address of the host or network you wish to reach.

The netmask field identifies the portion of the destination IP in use.

The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

[More...](#)

# Tools

## Administrator Settings

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 the DIR-655 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.

**Enable Remote Management:** Remote management allows the DIR-655 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

**Remote Admin Inbound Filter:** The port number used to access the DIR-655. Example: `http://x.x.x.x:8080` whereas x.x.x.x is the Internet IP address of the DIR-655 and 8080 is the port used for the Web Management interface. If you have enabled **HTTPS Server** and checked **Use HTTPS**, you must enter **https://** as part of the URL to access the router remotely.

**Details:** 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 screenshot shows the D-Link DIR-655 web management interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration categories like ADMIN, TIME, SYSLOG, etc. The main content area is titled "ADMINISTRATOR SETTINGS" and contains the following sections:

- ADMINISTRATOR SETTINGS:** A text box explaining that the "admin" and "user" accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access. A note states that by default there is no password configured, and it is highly recommended to create a password for security. There are "Save Settings" and "Don't Save Settings" buttons.
- ADMIN PASSWORD:** A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields for "Password" and "Verify Password".
- USER PASSWORD:** A section with the instruction "Please enter the same password into both boxes, for confirmation." It contains two input fields for "Password" and "Verify Password".
- SYSTEM NAME:** A section with a label "Gateway Name" and a text input field containing "DIR-655".
- ADMINISTRATION:** A section with several checkboxes and input fields:
  - Enable Graphical Authentication:
  - Enable HTTPS Server:
  - Enable Remote Management:
  - Remote Admin Port:  Use HTTPS
  - Remote Admin Inbound Filter:
  - Details:

On the right side of the interface, there is a "Helpful Hints ..." section with security advice and a "More ..." link.

# Time Settings

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

**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. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

**NTP Server Used:** Enter the 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**. You can also click **Copy Your Computer's Time Settings**.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADMIN  
TIME  
SYSLOG  
EMAIL SETTINGS  
SYSTEM  
FIRMWARE  
DYNAMIC DNS  
SYSTEM CHECK  
SCHEDULES

**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 NTP (Network Time Protocol) Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Save Settings Don't Save Settings

**TIME CONFIGURATION**

Current Router Time : Tuesday, November 24, 2009 5:13:47 PM  
Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana  
Enable Daylight Saving :   
Daylight Saving Offset : +1:00  
Daylight Saving Dates :  
DST Start : Mar 3rd Sun 1:00 AM  
DST End : Nov 2nd Sun 1:00 AM

**AUTOMATIC TIME CONFIGURATION**

Enable NTP Server :   
NTP Server Used : << Select NTP Server

**SET THE DATE A.D TIME MANUALLY**

Date And Time :  
Year 2009 Month Nov Day 24  
Hour 05 Minute 13 Second 40 PM  
Copy Your Computer's Time Settings

Helpful Hints ...  
Good timekeeping is important for accurate logs and scheduled firewall rules.  
More...

# 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).

The screenshot displays the D-Link DIR-655 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration sections: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSLOG' and contains the following text: 'The SysLog options allow you to send log information to a SysLog Server.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. A section titled 'SYLOG SETTINGS' contains the option 'Enable Logging To Syslog Server : '. On the right side, there is a 'Helpful Hints...' section with a text box explaining that a System Logger (syslog) is a server that collects logs from different sources and that if the LAN includes a syslog server, the user can use this option to send the router's logs to that server. A 'More...' link is also present.

# 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.

**Enable Email Notification:** When this option is enabled, router activity logs are e-mailed 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. If your SMTP server requires authentication, select this option.

**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 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**.

The screenshot shows the D-Link DIR-655 Web UI. The top navigation bar includes 'DIR-655 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS (selected), SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'EMAIL SETTINGS' and contains the following sections:

- EMAIL SETTINGS:** A message stating 'The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.' Below this are two buttons: 'Save Settings' and 'Don't Save Settings'.
- EMAIL NOTIFICATION:** A section with the label 'Enable Email Notification :
- EMAIL SETTINGS:** A section with the following fields:
  - From Email Address :
  - To Email Address :
  - SMTP Server Address :
  - Enable Authentication :
  - Account Name :
  - Password :
  - Verify Password :
- EMAIL LOG WHEN FULL OR ON SCHEDULE:** A section with the following options:
  - On Log Full :
  - On Schedule :
  - Schedule :
  - Detail :

On the right side of the page, there is a 'Helpful Hints...' section with the text: 'You may want to make the email settings similar to those of your email client program.' and a 'More...' link.

# System Settings

**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. You will then see a file dialog, where you can 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 control to find a previously save 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.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes the D-Link logo and tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM (highlighted), FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'SYSTEM SETTINGS' and contains the following text and buttons:

**SYSTEM SETTINGS**

The System Settings section allows you to reboot the device, or 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 have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

**Save To Local Hard Drive:**

**Load From Local Hard Drive:**

**Restore To Factory Default:**   
Restore all settings to the factory defaults.

**Reboots the Device:**

**Helpful Hints...**

Once your router is configured the way you want it, you can save the configuration settings to a configuration file.

You might need this file so that you can load your configuration later in the event that the router's default settings are restored.

To save the configuration, click the **Save Configuration** button.

[More...](#)

The bottom of the interface features the 'WIRELESS' logo.

# Update Firmware

You can upgrade the firmware of the Router 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 site for firmware updates at <http://support.dlink.com>. You can download firmware upgrades to your hard drive from the D-Link support site.

**Firmware Upgrade:** Click on **Check Online Now for Latest Firmware Version** to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

**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.

Check **Automatically Check Online for Latest Firmware Version** to have the router check automatically to see if there is a new firmware upgrade.

**Notifications Options:** Check **Email Notification of Newer Firmware Version** to have the router send an email when there is a new firmware available.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The left sidebar lists menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES. The main content area is titled 'FIRMWARE' and contains the following information:

**FIRMWARE INFORMATION**

- Current Firmware Version : 2.08NA
- Current Firmware Date : 18, Mar, 2012
- 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 from the [Tools → System](#) screen.

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.

Input fields and buttons:

**Helpful Hints...**

Firmware updates are released periodically to improve the functionality of your router and to add features. If you run into a problem with a specific feature of the router, check if updated firmware is available for your router.

[More...](#)

# DDNS

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.

**DDNS:** 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:** Choose your DDNS provider from the drop-down menu.

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

**Username or Key:** Enter the Username for your DDNS account.

**Password or Key:** Enter the Password for your DDNS account.

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

**Status:** Displays the status of your DDNS connection.

## DDNS for IPv6 Hosts

**Enable:** Check the box to enable DDNS for IPv6 Hosts.

**IPv6 Address:** Enter the IPv6 address of your computer/server in your local network. You can click the << button and select a computer/server from the drop-down list.

**Host Name:** Enter the IPv6 Host Name that you registered with your DDNS service provider.

**IPv6 DDNS List:** Once you save your entry, the IPv6 DDNS host information will be displayed here.

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

**Host Name:** Displays the name of your IPv6 DDNS host.

**IPv6 Address:** Displays the IPv6 address of your computer/server associated with the IPv6 DDNS host.

**Edit/Delete:** Click the edit icon to make changes to the entry or click the delete icon to remove the entry.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**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 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).

Save Settings Don't Save Settings

**DYNAMIC DNS SETTINGS**

Enable Dynamic DNS :

Server Address : dlinkddns.com(Free) << Select Dynamic DNS Server

Host Name :

Username or Key :

Password or Key :

Verify Password or Key :

Timeout : 576 (hours)

Status : Dynamic DNS service is not enabled.

**DYNAMIC DNS FOR IPV6 HOSTS**

Enable:

IPv6 Address:  << Computer Name

Host Name:  (e.g.: ipv6.mydomain.net)

Save Clear

**IPV6 DYNAMIC DNS LIST**

Enable	Host Name	IPv6 Address
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

WIRELESS

**Helpful Hints...**

To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu.

More...

# System Check

**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**.

**Ping Results:** The results of your ping attempts will be displayed here.

The screenshot displays the D-Link DIR-655 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar includes tabs for 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The 'TOOLS' tab is selected. On the left, a sidebar menu lists various system settings: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK (highlighted), and SCHEDULES. The main content area is titled 'PING TEST' and contains the following text: 'Ping Test sends "ping" packets to test a computer on the Internet.' Below this, there is a section for entering the target: 'Host Name or IP Address :' followed by a text input field, a 'Ping' button, and a 'Stop' button. A 'PING RESULT' section below that contains the instruction: 'Enter a host name or IP address above and click 'Ping''. To the right of the main content, there is a 'Helpful Hints...' section with explanatory text: 'Ping checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.' and a 'More...' link. The bottom of the page features a 'WIRELESS' logo.

# Schedules

**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.

**Save:** Click **Save** to save your schedule. You must click Save Settings at the top for your schedules to go into effect.

**Schedule Rules** The list of schedules will be listed here. Click the **List:** **Edit** icon to make changes or click the **Delete** icon to remove the schedule.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

ADMIN  
TIME  
SYSLOG  
EMAIL SETTINGS  
SYSTEM  
FIRMWARE  
DYNAMIC DNS  
SYSTEM CHECK  
SCHEDULES

**SCHEDULES**

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

**ADD SCHEDULE RULE**

Name :

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

Sun  Mon  Tue  Wed  Thu  Fri  Sat

All Day - 24 hrs :

Start Time :  :  :  AM (hour:minute, 12 hour time)

End Time :  :  :  AM (hour:minute, 12 hour time)

**SCHEDULE RULES LIST :**

Name :	Day(s) :	Time Frame :
--------	----------	--------------

**Helpful Hints...**

Schedules are used with a number of other features to define when those features are in effect.

Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

Click **Save** to add a completed schedule to the list below.

Click **Edit** icon to change an existing schedule.

Click **Delete** icon to permanently delete a schedule.

[More...](#)

**WIRELESS**

# Status

## Device Information

This page displays the current information for the DIR-655. 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 for the router.

**LAN:** Displays the MAC address and the private (local) IP settings for the router.

**Wireless LAN:** Displays the 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 the Multicast Group IP Address.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**DEVICE INFORMATION**  
All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

**GENERAL**  
Time : Friday, May 18, 2012 7:58:11 PM  
Firmware Version : 2.08NA , 18, Mar, 2012

**WAN**  
Connection Type : DHCP Client  
Cable Status : Disconnected  
Network Status : Disconnected  
StreamEngine : N/A  
Connection Up Time : N/A  
DHCP Release DHCP Renew  
MAC Address : 00:26:5A:CC:F9:32  
IP Address : 0.0.0.0  
Subnet Mask : 0.0.0.0  
Default Gateway : 0.0.0.0  
Primary DNS Server : 0.0.0.0  
Secondary DNS Server : 0.0.0.0  
Advanced DNS : Enabled

**LAN**  
MAC Address : 00:26:5A:CC:F9:31  
IP Address : 192.168.0.1  
Subnet Mask : 255.255.255.0  
DHCP Server : Enabled

**WIRELESS LAN**  
Wireless Radio : Enabled  
802.11 Mode : 11bgn  
Channel Width : 20 MHz  
Channel : 6  
WISH : Inactive  
Wi-Fi Protected Setup : Enabled/Not Configured

**SSID List:**

Network Name (SSID)	Guest	MAC Address	Security Mode
dlink	No	00:26:5A:CC:F9:31	disable

**LAN COMPUTERS**

IP Address	Name (if any)	MAC
192.168.0.100	PM_TEST01	00:04:23:2C:51:A3

**IGMP MULTICAST MEMBERSHIPS**

Multicast Group Address

**WIRELESS**

# Log

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.

**What to View:** You can select the types of messages that you want to display from the log. Firewall & Security, System, and Router Status messages can be selected.

**View Levels:** There are three levels of message importance: **Informational**, **Warning**, and **Critical**. Select the levels that you want displayed in the log.

**Apply Log Settings:** Will filter the log results so that only the selected options appear.

**Refresh:** Updates the log details on the screen so it displays any recent activity.

**Clear:** Clears all of the log contents.

**Email Now:** This option will send a copy of the router log to the email address configured in the Tools > Email screen.

**Save Log:** This option will save the router to a log file on your computer.

**D-Link**

DIR-655 // SETUP ADVANCED TOOLS STATUS SUPPORT

**LOGS**  
Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has internal syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

**LOG OPTIONS**

**Log Type :**  System Activity  
 Debug Information  
 Attacks  
 Dropped Packets  
 Notice

Apply Log Settings Now

**LOG DETAILS**

1 / 17

Priority	Time	Message
info	May 18 19:11:39	version 1.8.3 started
info	May 18 19:11:27	version 1.8.3 started
info	May 18 18:36:30	UDHCPD Inform: add_lease 192.168.0.100
info	May 18 18:36:26	UDHCPD Inform: add_lease 192.168.0.100
info	May 18 18:20:36	UDHCPD sending OFFER of 192.168.0.100
info	May 18 18:20:22	version 1.8.3 started
notice	May 18 18:20:20	HTTP listening on port 50353
notice	May 18 18:20:18	HTTP listening on port 65530
info	May 18 18:20:17	[ 30.090000] br0: port 2(ath0) entering forwarding state
info	May 18 18:20:17	[ 30.090000] br0: topology change detected, propagatin g

WIRELESS

**Helpful Hints...**  
Check the log frequently to detect unauthorized network usage.  
You can also have the log mailed to you periodically. Refer to [Tools → EMail](#).  
More...

# Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-655 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.

Category	Sent	Received	TX Packets	RX Packets	Dropped	Collisions	Errors
LAN STATISTICS	16112	4685	0	0	0	0	0
WAN STATISTICS	14	0	0	0	0	0	0
WIRELESS STATISTICS	2192	0	0	0	0	0	0

# Active Sessions

Local	NAT	Internet	Protocol	State	Dir	Time Out

# Routing

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'ROUTING' selected. The main content area is titled 'ROUTING' and contains a 'Routing Table' section. Below this, a 'ROUTING TABLE' is displayed as a table with the following data:

Destination IP	NetMask	Gateway	Metric	Interface	Type	Creator
192.168.0.0	255.255.255.0	0.0.0.0	0	LAN	INTRANET	System
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN	INTRANET	System
127.0.0.0	255.0.0.0	0.0.0.0	0	Local Loopback	LOCAL	System

# 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.

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options, with 'WIRELESS' selected. The main content area is titled 'WIRELESS' and contains a section for viewing wireless clients. Below this, a 'NUMBER OF WIRELESS CLIENTS : 0' is displayed. A table with the following columns is shown:

MAC Address	IP Address	Mode	Rate	Signal(%)
-------------	------------	------	------	-----------

On the right side of the interface, there is a 'Helpful Hints...' section with the text: 'This is a list of all wireless clients that are currently connected to your wireless router.' and a 'More...' link.

# IPV6

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various menu items, with 'IPV6 ROUTING' selected. The main content area is titled 'IPv6 Network Information' and contains the following details:

**IPv6 Network Information**  
All of your IPv6 Internet and network connection details are displayed on this page.

**IPv6 Connection Information**

- IPv6 Connection Type : PPPoE
- Network Status : Disconnected
- Connection Up Time : N/A
- 
- WAN IPv6 Address : None
- IPv6 Default Gateway : None
- LAN IPv6 Address : None
- LAN IPv6 Link-Local Address : fe80::226:5aff:fecc:f931/64
- Primary DNS Address : None
- Secondary DNS Address : None
- DHCP-PD : Enabled
- IPv6 network assigned by DHCP-PD: None

**LAN IPv6 Computers**

IPv6 Address	Name (if any)

Helpful Hints...  
All of your WAN and LAN connection details are displayed here.  
[More...](#)

# IPV6 Routing

The screenshot shows the D-Link DIR-655 web interface. The top navigation bar includes 'DIR-655', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various menu items, with 'IPV6 ROUTING' selected. The main content area is titled 'IPV6 ROUTING' and contains the following details:

**IPV6 ROUTING**

**IPv6 Routing Table**

This page displays the IPv6 routing details configured for your router

**IPV6 ROUTING TABLE**

Destination IP	Gateway	Metric	Interface

# Support

The screenshot displays the D-Link DIR-655 web interface. At the top, the D-Link logo is visible. Below it, a navigation bar contains tabs for SETUP, ADVANCED, TOOLS, STATUS, and SUPPORT. The SUPPORT tab is currently selected. On the left side, a vertical menu lists the main sections: MENU, SETUP, ADVANCED, TOOLS, and STATUS. The main content area is titled 'SUPPORT MENU' and contains several sub-sections, each with a list of links:

- SUPPORT MENU**
  - [Setup](#)
  - [Advanced](#)
  - [Tools](#)
  - [Status](#)
- SETUP HELP**
  - [Internet Connection](#)
  - [WAN](#)
  - [Wireless](#)
  - [Network Settings](#)
  - [USB Settings](#)
- ADVANCED HELP**
  - [Virtual Server](#)
  - [Port Forwarding](#)
  - [Application Rules](#)
  - [QoS Engine](#)
  - [Access Control](#)
  - [Website Filter](#)
  - [Network Filter](#)
  - [Firewall Settings](#)
  - [Routing](#)
  - [Inbound Filter](#)
  - [Advanced Wireless](#)
  - [WISH](#)
  - [Advanced Network](#)
  - [GUEST ZONE](#)
  - [IPv6](#)
- TOOLS HELP**
  - [Admin](#)
  - [Time](#)
  - [Syslog](#)
  - [Email Settings](#)
  - [System](#)
  - [Firmware](#)
  - [Dynamic DNS](#)
  - [System Check](#)
  - [Schedules](#)
- STATUS**
  - [Device Info](#)
  - [Logs](#)
  - [Statistics](#)
  - [Internet Sessions](#)

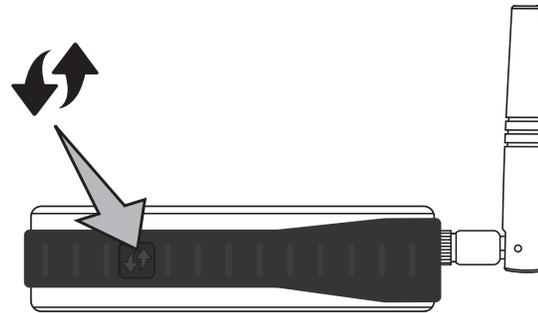
At the bottom of the interface, the word 'WIRELESS' is displayed in a dark bar.

# Connect to a Wireless Network

## 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-655 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-655 for about 1 second. The WPS button 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 WPS light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

# Windows® 7

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).



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



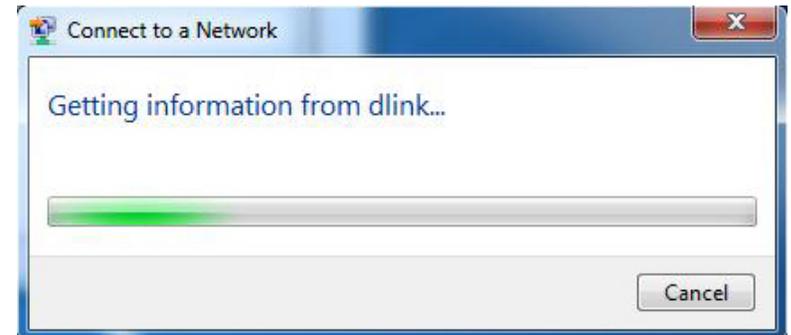
## Section 4 - Connecting to a Wireless Network

3. Highlight the wireless network (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.



## Section 4 - Connecting to a Wireless Network

5. Enter the same security key or passphrase that is on your router and click **Ok**.

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



# Windows Vista®

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

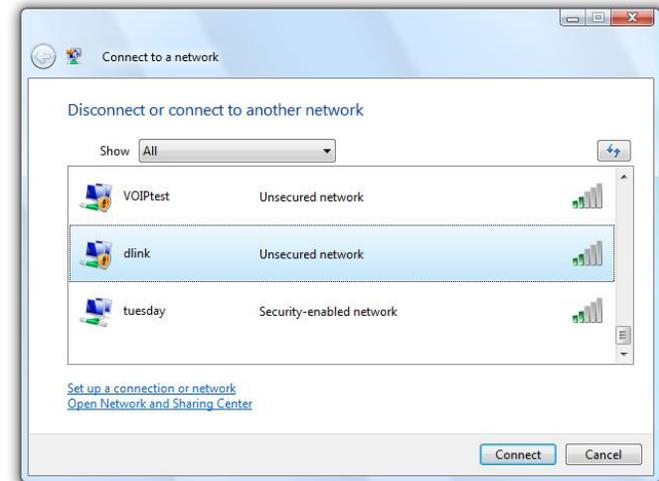
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

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



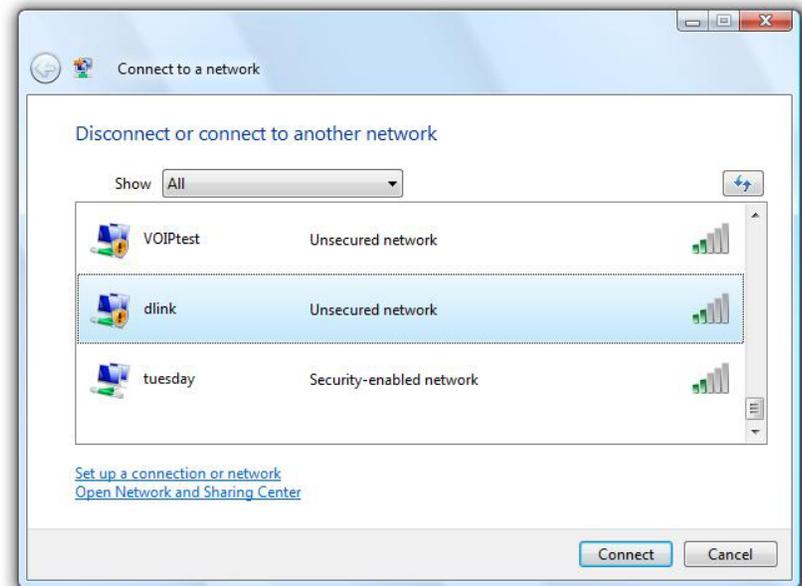
## Configure Wireless Security

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**.

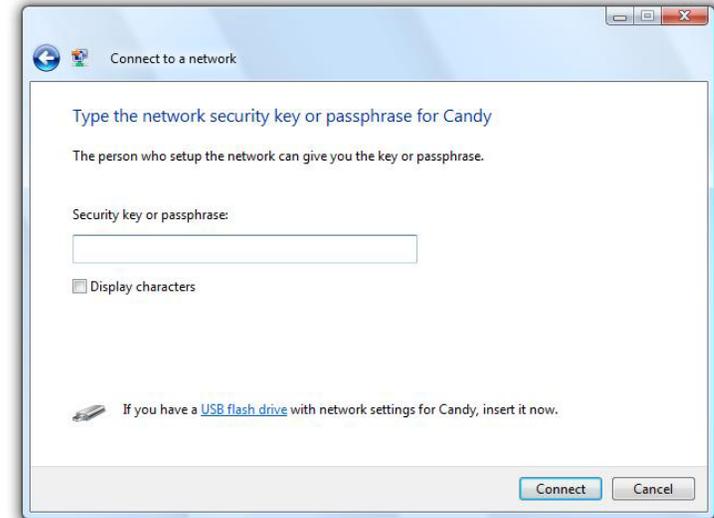


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase 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.



# Using 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.

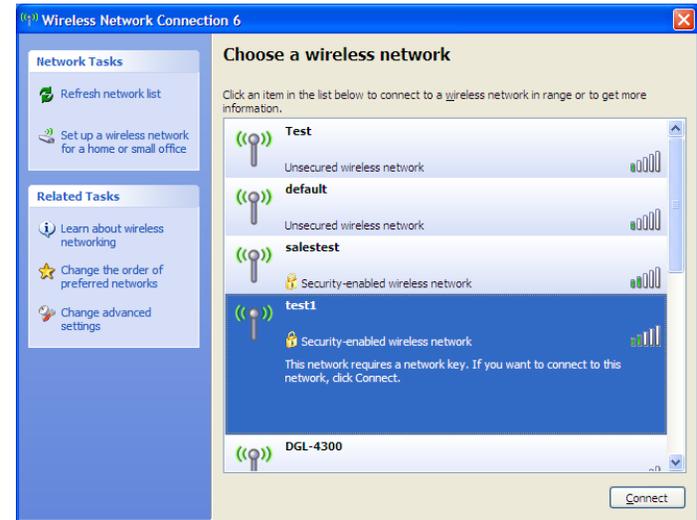
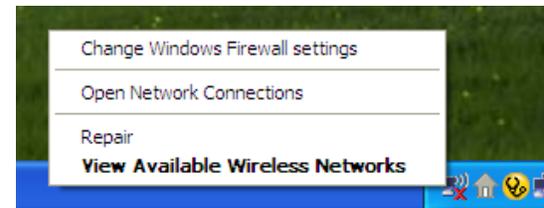
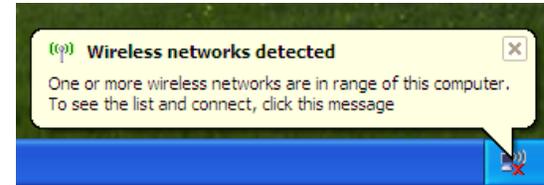
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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 network (displayed using the SSID) and click the **Connect** button.

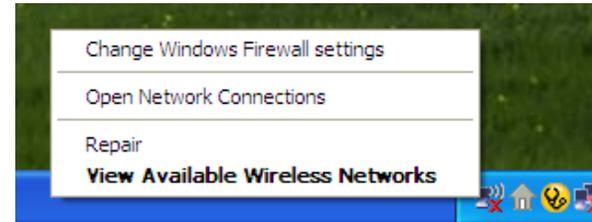
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



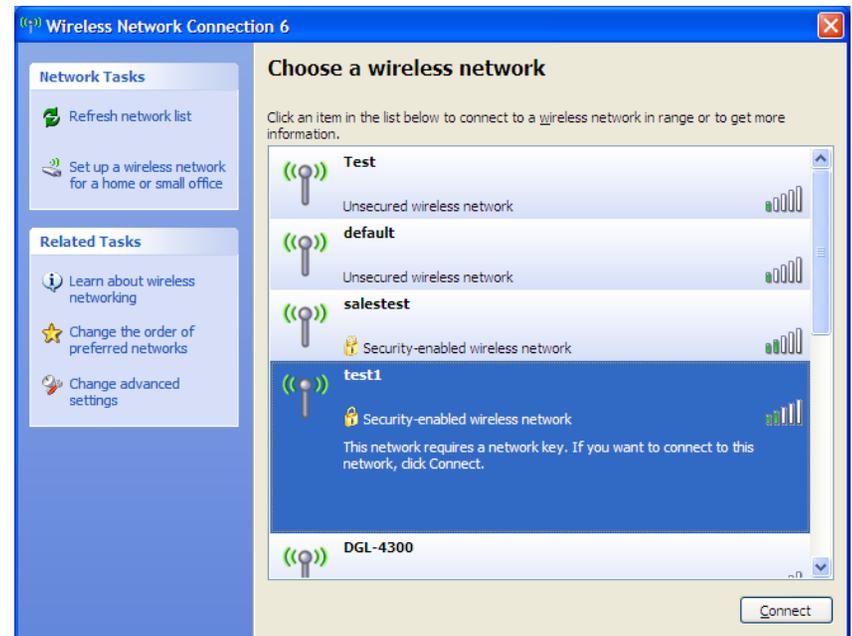
# Configure Wireless Security

It is recommended to enable encryption 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 passphrase 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**.

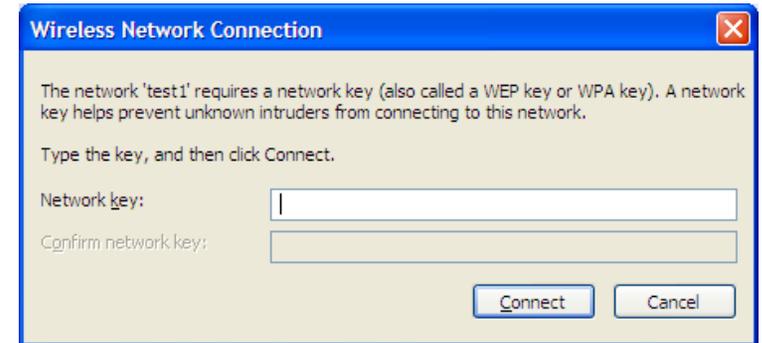


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK passphrase 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 WPA-PSK passphrase 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-655. 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 on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
  - Internet Explorer 6.0 or higher
  - Mozilla 1.7.12 (5.0) or higher
  - Opera 8.5 or higher
  - Safari 1.2 or higher (with Java 1.3.1 or higher)
  - Camino 0.8.4 or higher
  - Firefox 1.5 or higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
  - Go to **Start > Settings > Control Panel**. Double-click 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 the web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

To reset the router, locate the reset button (hole) on the rear panel of the unit. With the router powered on, use a paperclip to hold the button down for 10 seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. The default IP address is 192.168.0.1. 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).

**Note: AOL DSL+ users must use MTU of 1400.**

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.

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

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

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

C:\>
```

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

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

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

- Open your browser, enter the IP address of your router (192.168.0.1) 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, and 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 security feature on the router. Refer to product manual for detail information on how to set it up.

# Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-655 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.

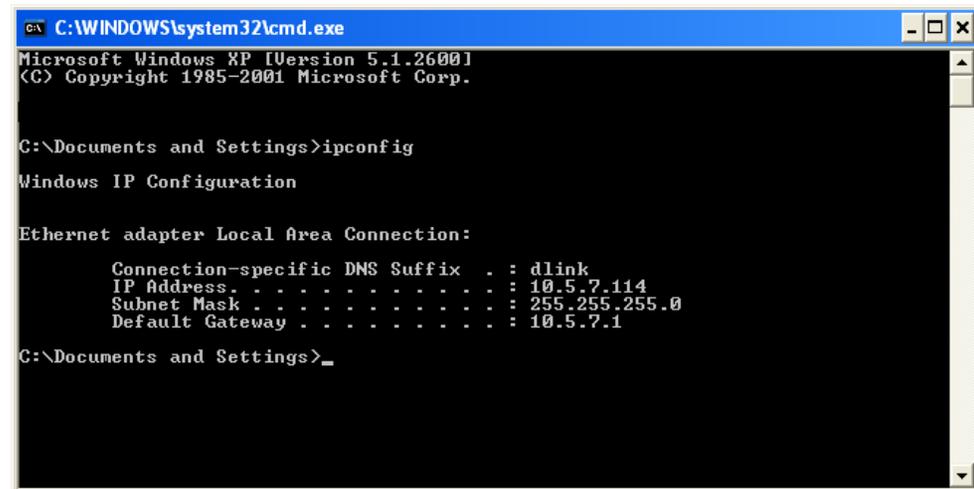
Click on **Start > Run**. In the run box type **cmd** and click **OK**. (Windows Vista® users type *cmd* in the **Start Search** box.)

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.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>_
```

## Statically Assign an IP address

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

### Step 1

Windows® 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 D-Link network adapter and select **Properties**.

### Step 3

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

### Step 4

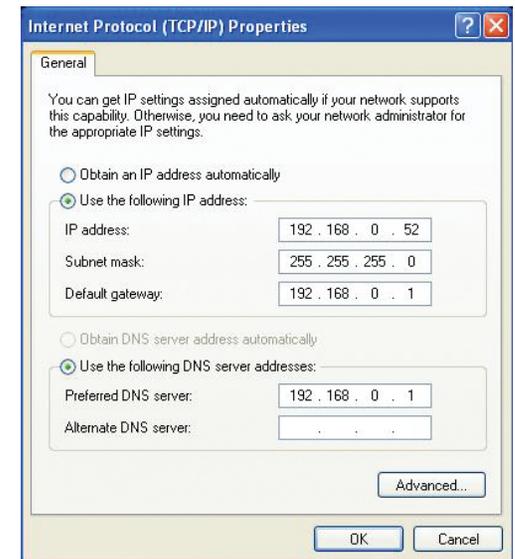
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

**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 Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

### Step 5

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



# Technical Specifications

## Standards

- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3u

## Security

- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise

## Wireless Signal Rates\*

- 300Mbps
- 108Mbps
- 54Mbps
- 48Mbps
- 36Mbps
- 24Mbps
- 18Mbps
- 12Mbps
- 11Mbps
- 9Mbps
- 6Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

## MSC (0-15)

- 130Mbps (270)
- 104Mbps (216)
- 66Mbps (135)
- 52Mbps (108)
- 26Mbps (54)
- 12Mbps (27)
- 117Mbps (243)
- 78Mbps (162)
- 58.5Mbps (121.5)
- 39Mbps (81)
- 19.5Mbps (40.5)
- 6.5Mbps (13.5)

## Frequency Range

- 2.4GHz to 2.483GHz

## Transmitter Output Power

- 15dBm  $\pm$  2dB

## External Antenna Type

- Three (3) detachable reverse SMA Antennas

## LEDs

- Power
- Internet
- Status
- WLAN
- LAN (10/100/1000)
- USB

## Operating Temperature

- 32°F to 131°F ( 0°C to 55°C)

## Humidity

- 95% maximum (non-condensing)

## Safety & Emissions

- FCC
- CE

## Dimensions

- L = 7.6 inches
- W = 4.6 inches
- H = 1.2inches

## Warranty

- 1 Year

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

# Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (e.g. DIR-655)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev B1))
- Serial Number (s/n number located on the label on the bottom of the router).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

## For customers within the United States:

**Phone Support:**

(877) 453-5465

**Internet Support:**

<http://support.dlink.com>

## For customers within Canada:

**Phone Support:**

(800) 361-5265

**Internet Support:**

<http://support.dlink.ca>

# GNU General Public License

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License ("GPL" or GNU Lesser General Public License ("LGPL"). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

<http://tsd.dlink.com.tw/GPL.asp>

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

## **WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE**

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPL source code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL

.  
Please direct all inquiries to:  
Email: [GPLCODE@DLink.com](mailto:GPLCODE@DLink.com)

Snail Mail:  
Attn: GPLSOURCE REQUEST  
D-Link Systems, Inc.  
17595 Mt. Herrmann Street  
Fountain Valley, CA 92708

## **GNU GENERAL PUBLIC LICENSE**

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

### TERMS AND CONDITIONS

#### 0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

#### 1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

### **2. Basic Permissions.**

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

### **3. Protecting Users' Legal Rights From Anti-Circumvention Law.**

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

### **4. Conveying Verbatim Copies.**

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

### **5. Conveying Modified Source Versions.**

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

### **6. Conveying Non-Source Forms.**

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

### **7. Additional Terms.**

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

### **8. Termination.**

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

### **9. Acceptance Not Required for Having Copies.**

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

### **10. Automatic Licensing of Downstream Recipients.**

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

### **11. Patents.**

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

### **12. No Surrender of Others' Freedom.**

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

### **13. Use with the GNU Affero General Public License.**

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

### **14. Revised Versions of this License.**

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

### **15. Disclaimer of Warranty.**

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

### **16. Limitation of Liability.**

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

### **17. Interpretation of Sections 15 and 16.**

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

# Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

## **Limited Warranty:**

D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

### **Limited Software Warranty:**

D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Software Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by DLink in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

### **Non-Applicability of Warranty:**

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link’s products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold “As-Is” without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

### **Submitting A Claim:**

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.
- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-800-361-5265, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization (“RMA”) number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.ca/>.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.
- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery (“COD”) is allowed. Products sent COD will be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link’s reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.
- RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

### **What Is Not Covered:**

The Limited Warranty provided herein by D-Link does not cover:

Products that, in D-Link’s judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

### **Disclaimer of Other Warranties:**

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED “AS-IS” WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

### **Limitation of Liability:**

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

### **Governing Law:**

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

### **Trademarks:**

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

### **Copyright Statement:**

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright ©2008-2011 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

### **CE Mark Warning:**

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

### **FCC Statement:**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. 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 or more 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 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.

### **IMPORTANT NOTICE:**

#### **FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

**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.

**IMPORTANT NOTE:**

**Radiation Exposure Statement:**

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device has been designed to operate with an antenna having a maximum gain of 2dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

# Registration

Register your product at [registration.dlink.com](http://registration.dlink.com)



Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 2.3  
July 3, 2012