

User Manual

All-in-One Mobile Companion

Preface

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

Manual Revisions

Revision	Date	Description
1.0	January 11, 2012	• Initial release for Revision A1

Trademarks

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

Copyright © 2011 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

Preface	i	Dynamic (Cable)	27
Manual Revisions	i	Internet Setup	28
Trademarks	i	PPPoE	28
Product Overview	1	Wireless Settings	29
Package Contents	1	Wireless Security Setup Wizard	30
System Requirements	2	Manual Configuration	32
Introduction	3	Wireless Settings	32
Features	4	Access Point Mode	33
Hardware Overview	5	Wireless Security	35
Connections	5	What is WEP?	35
LEDs	6	Configure WEP	36
Installation	7	Configure WPA/WPA2 Personal	37
Operation Modes	7	Configure WPA Enterprise	38
Access Point Mode	8	Network Settings	39
Repeater Mode	9	Router Settings	39
Hot Spot Mode	10	DHCP Reservation	40
Wireless Installation Considerations	11	Storage	41
Manual Setup	12	Advanced	42
Connect to an Existing Router	14	Virtual Server	42
Configuration	16	Application Rules	43
Quick Router Setup Wizard (CD)	16	MAC Address Filter	44
Quick Setup Wizard	18	Website Filters	45
Web-based Configuration Utility	21	Firewall Settings	46
Internet Connection Setup	22	Advanced Wireless	47
Manual Internet Setup	27	Wi-Fi Protected Setup (WPS)	48
		UPnP Settings	50

Guest Zone.....	51	Configure WPA/WPA2 Personal	74
DMZ	52	LAN Settings	75
Maintenance.....	53	Static IP	76
Admin	53	Advanced	77
Time	54	Advanced Wireless	77
System	55	Wi-Fi Protected Setup	78
Firmware	56	Maintenance	79
Dynamic DNS	57	Admin	79
System Check.....	58	System	80
Schedules	59	Language Pack.....	81
Status	60	Firmware	81
Device Info	60	Time	82
Logs	61	Status	83
Statistics	62	Device Info	83
Internet Sessions.....	63	Logs	84
Wireless	64	Statistics	85
Help	65	Quick Setup Wizard.....	86
Quick Setup Wizard.....	66	WiFi Hot Spot.....	86
Repeater Mode	66	Setup.....	90
Setup Wizard	68	Wi-Fi Hot Spot Setup	90
To start the Setup Wizard click Next.	68	Configure WPA/WPA2 Personal	92
Manual Configuration.....	70	WAN Settings	93
Wireless Settings.....	70	Wireless Setup.....	94
Repeater Mode	71	Manual Wireless Settings.....	95
Wireless Security.....	72	LAN Setup.....	96
What is WEP?	72	Advanced	97
Configure WEP	73	Advanced Wireless	97
		Maintenance.....	98
		Admin	98

System	99	Technical Specifications.....	132
Language Pack.....	100	Contacting Technical Support.....	133
Firmware	100	GPL Code Statement.....	134
Time	101	Warranty.....	149
Status	102	Registration.....	156
Device Info	102		
Logs	103		
Statistics	104		
Help	105		
Connect a Wireless Client to your Router	106		
WPS Button.....	106		
Windows® 7.....	107		
WPA/WPA2	107		
WPS.....	110		
Windows Vista®	114		
WPA/WPA2	115		
WPS/WCN 2.0	117		
Windows® XP	118		
WPA/WPA2	119		
Troubleshooting	121		
Wireless Basics	125		
What is Wireless?	126		
Tips.....	128		
Wireless Modes.....	129		
Networking Basics	130		
Check your IP address	130		
Statically Assign an IP address	131		

Package Contents



DIR-505 All-in-One Mobile Companion



Ethernet Cable



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-505 will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n or 802.11g wireless clients • IEEE 802.11a wireless clients • 10/100/1000 Ethernet
Web-based Configuration Utility Requirements	Computer with the following: • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter Browser Requirements: • Internet Explorer 6 or higher • Firefox 3.0 or higher • Safari 3.0 or higher • Chrome 2.0 or higher Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	Computer with the following: • Windows® 7, Vista®, or XP (Service Pack 2 or higher) • An installed Ethernet adapter • CD-ROM drive

Introduction

TOTAL PERFORMANCE

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

TOTAL SECURITY

The most complete set of security features including Active Firewall and WPA/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 All-in-One Mobile Companion (DIR-505) is a 802.11n/802.11a compliant device that delivers real world performance of up to 14x 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 DIR-505 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 Wireless N technology, this high performance router provides superior Whole Home Coverage while reducing dead spots. The router is designed for use in bigger homes and for users who demand higher performance networking. Add a Wireless N notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

TOTAL NETWORK SECURITY

The Wireless 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/WPA2 standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

* Maximum wireless signal rate derived from IEEE Standard 802.11a, 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.

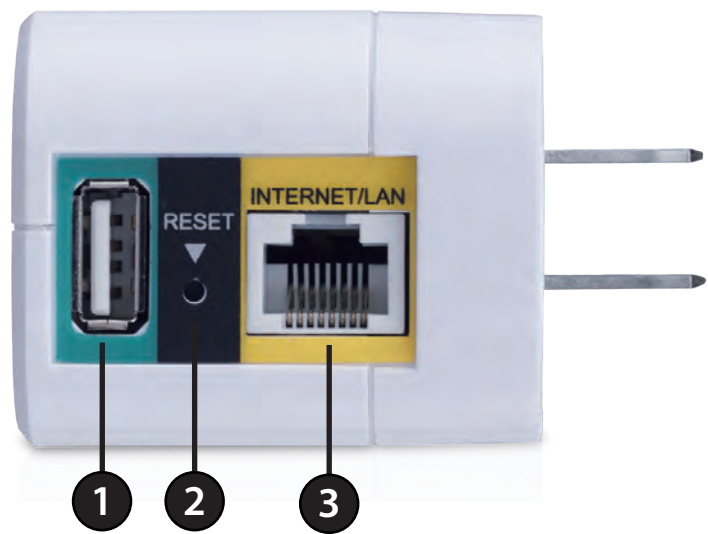
Features

- **Faster Wireless Networking** - The DIR-505 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 14x faster than 802.11g.
- **Compatible with 802.11a/g Devices** - The DIR-505 is still fully compatible with the IEEE 802.11g and 802.11a standards, so it can connect with existing 802.11g and 802.11a PCI, USB, and Cardbus adapters.
- **Advanced Firewall Features** - The Web-based user interface displays a number of advanced network management features including:
 - **Content Filtering** - Easily applied content filtering based on MAC Address, URL, and/or Domain Name.
 - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.
 - **Secure Multiple/Concurrent Sessions** - The DIR-505 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-505 can securely access corporate networks.
- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-505 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, 802.11a, 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



1	USB Port	Connect a USB 1.1 or 2.0 flash drive to configure the wireless settings using WCN and SharePort. SharePort allows you to share a printer or storage device with your local network.
2	Reset Button	Pressing the Reset button restores the router to its original factory default settings.
3	Ethernet Port	The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.

Hardware Overview

LEDs



LED Indicator	Color	Status	Description
Power/Status	Green	Solid Green	The device is powered ON and operating properly
		Blinking Green	The device is processing WPS
		Light off	The device is off
	Red	Solid Red	During Power ON or system is defective
		Blinking Red	The device is under recovery mode
		Light off	The device is powered off

Installation

Please configure the DIR-505 with a computer connected directly to the AP. The next few pages will explain the different operational modes you can use.

Operation Modes

Depending on how you want to use your DIR-505 will determine which mode you use. This section will help you figure out which setting works with your setup.

- Access Point mode - page 13
- Wireless Client mode - page 14
- Range Extender Mode - page 15
- Bridge mode - page 16
- Bridge with AP mode - page 17
- WISP Client Router mode - page 18
- WISP Range Extender Mode - page 19

Access Point Mode

In the Access Point mode, the DIR-505 acts as a central connection point for any computer (client) that has a 802.11n or backward-compatible 802.11g wireless network interface and is within range of the AP. Clients must use the same SSID (wireless network name) and channel as the AP in order to connect. If wireless security is enabled on the AP, the client will need to enter a password to connect to the AP. In Access Point mode, multiple clients can connect to the AP at the same time.

Repeater Mode

In the Wireless Client mode, the DIR-505 acts as a wireless network adapter for your Ethernet-enabled device (such as a game console or a TV set-top box). Connect your Ethernet-enabled device to the AP using an Ethernet cable. The AP Client mode can support multiple wired clients.

If you are going to connect several Ethernet-enabled devices to your DIR-505, connect the LAN port of the DIR-505 to an Ethernet switch, then connect your devices to this switch.

Example: Connect a gaming console using an ethernet cable to the DIR-505. The unit is set to Wireless Client mode which will wirelessly connect to a wireless router on your network.

Hot Spot Mode

In Range Extender Mode, the DIR-505 increases the range of your wireless network by extending the wireless coverage of another AP or wireless router. The APs and wireless router (if used) must be within range of each other. Make sure that all clients, APs, and the wireless router all use the same SSID (wireless network name), channel, and security settings.

Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.
5. If you are using 2.4GHz 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.

Manual Setup

Important: for best results, insert the Installation CD and follow the on-screen instructions. If you are unable to use the CD or are using Mac or Linux, please use the following installation steps:

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

4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.
5. Reconnect the power adapter to your cable or DSL broadband modem and wait for two minutes.
6. Connect the supplied power adapter into the power port on the back of the router and then plug it into a power outlet or surge protector. Press the power button and verify that the power LED is lit. Allow 1 minute for the router to boot up.
7. If you are connecting to a Broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser and enter a web site. If you connect, you are finished with your Internet setup. Please skip to page 13 to configure your router and use the manual setup procedure to configure your network and wireless settings. If you did not connect to the Internet, use the D-Link Setup Wizard (refer to page 15).

Connect to an Existing Router

Note: *It is strongly recommended to replace your existing router with the DIR-505 instead of using both. If your modem is a combo router, you may want to contact your ISP or manufacturer's user guide to put the router into Bridge mode, which will 'turn off' the router (NAT) functions.*

If you are connecting the DIR-505 router to an existing router to use as a wireless access point and/or switch, you will have to do the following to the DIR-505 before connecting it to your network:

- Disable UPnP™
- Disable DHCP
- Change the LAN IP address to an available address on your network. The LAN ports on the router cannot accept a DHCP address from your other router.

To connect to another router, please follow the steps below:

1. Plug the power into the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). Please see the **Networking Basics** section for more information. If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.
2. Open a web browser, enter **http://192.168.0.1** and press **Enter**. When the login window appears, set the user name to **Admin** and leave the password box empty. Click **Log In** to continue.
3. Click on **Advanced** and then click **Advanced Network**. Uncheck the **Enable UPnP** checkbox. Click **Save Settings** to continue.
4. Click **Setup** and then click **Network Settings**. Uncheck the **Enable DHCP Server** checkbox. Click **Save Settings** to continue.

5. Under Router Settings, enter an available IP address and the subnet mask of your network. Click **Save Settings** to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 1.
6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.
7. Connect an Ethernet cable in one of the **LAN** ports of the router and connect it to your other router. Do not plug anything into the Internet (WAN) port of the D-Link router.
8. You may now use the other 3 LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the **Configuration** and **Wireless Security** sections for more information on setting up your wireless network.

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 15.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to page 21.

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).*

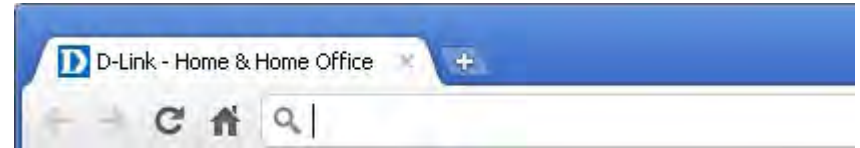
When the Wizard appears, select your language from the drop-down menu and then click **Next** to continue. Follow the on-screen instructions to configure your router.

Once you are finished, you may skip to page 21 and will be able to log into the web-based configuration utility and configure more advanced features.

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**.

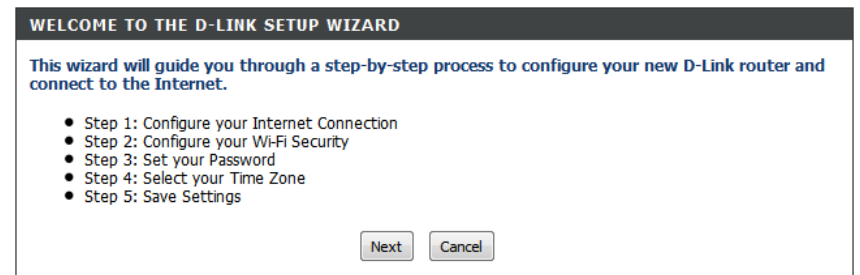
If you have already configured your settings and you would like to access the configuration utility, please refer to page 20.



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.



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.

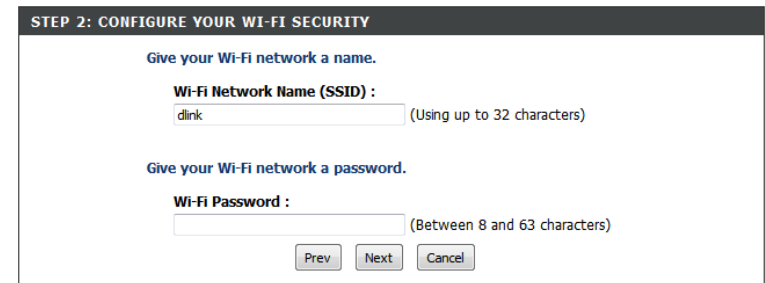


STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Router is detecting your Internet connection type, please wait ...

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.



STEP 2: CONFIGURE YOUR WI-FI SECURITY

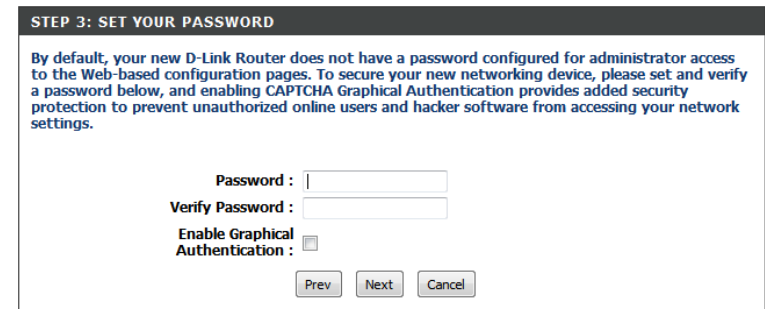
Give your Wi-Fi network a name.

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

Give your Wi-Fi network a password.

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

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



STEP 3: SET YOUR PASSWORD

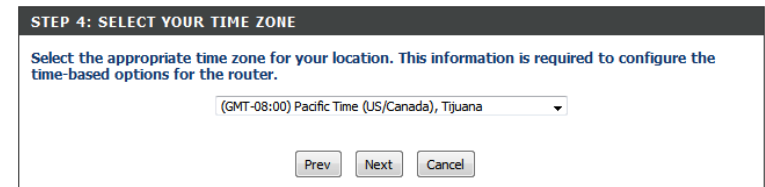
By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below, and enabling CAPTCHA Graphical Authentication provides added security protection to prevent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

Password :

Verify Password :

Enable Graphical Authentication : ☐

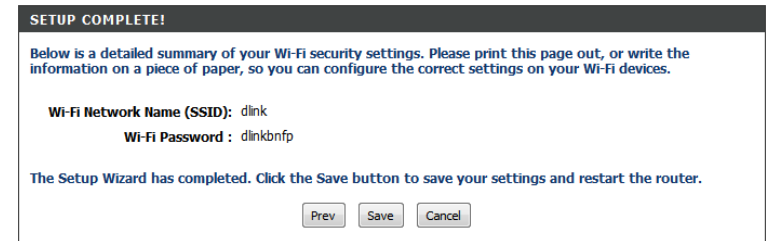
Select your time zone from the drop-down menu and click **Next** to continue.



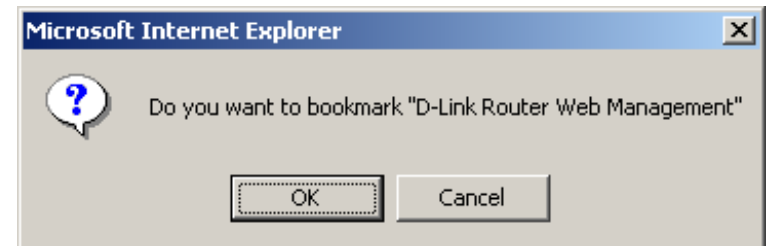
STEP 4: SELECT YOUR TIME ZONE

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

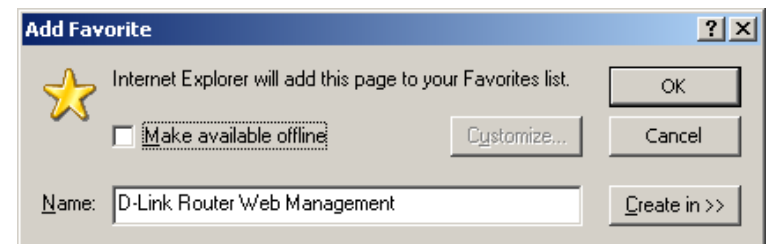
The Setup Complete window will display your wireless settings. Click **Save** to continue.



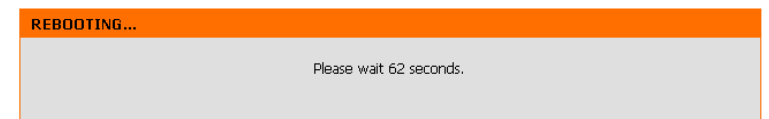
If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.



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 (**http://192.168.0.1**).

Windows and Mac users may also connect by typing **http://dlinkrouter** or **http://dlinkrouter.local** in the address bar.



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

A screenshot of the D-Link router's login page. The page has an orange header with the word "LOGIN" in white. Below the header, it says "Log in to the router:". There are two input fields: "User Name" with a dropdown menu showing "Admin" and "Password" with a text box. A "Log In" button is located below the password field.

Internet Connection Setup

Click **Manual Internet Connection Setup** to configure your connection manually and continue to the next page.

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard**. You will be directed to the Quick Setup Wizard. Please skip to page 24.

DIR-505

Router

Internet Settings

Wireless Settings

Network Settings

Storage

Setup

Advanced

Maintenance

Status

Help

Internet Connection

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 Setup Wizard

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.

Internet Connection Setup Wizard

Note:

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

Manual Internet Connection Options

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

Manual Internet Connection Setup

Helpful Hints...

If you are new to networking and have never configured a router before, click on **Internet Connection Setup Wizard** 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 **Manual Internet Connection Setup** to input all the settings manually.

More...

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.

WELCOME TO THE D-LINK INTERNET CONNECTION SETUP WIZARD

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

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

Prev Next Cancel Connect

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

STEP 1: SET YOUR PASSWORD

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

Password :

Verify Password :

Prev Next Cancel Connect

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

STEP 2: SELECT YOUR TIME ZONE

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

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

Prev Next Cancel Connect

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

Verify that you are connected to the D-Link Router with the PC that was originally connected to your broadband connection, and if you are, then click the **Clone MAC button** to copy your computer's MAC Address.

Click **Next** to continue.

Your setup is complete. Click **Connect** to save your settings and reboot your router.

STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Your Internet Connection could not be detected, please select your Internet Service Provider (ISP) from the list below. If your ISP is not listed, select the "Not Listed or Don't Know" option to manually configure your connection.

Comcast ▼

If your Internet Service Provider was not listed or you don't know who it is, please select the 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 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

Connect

DHCP CONNECTION (DYNAMIC IP ADDRESS)

To set up this connection, please make sure that you are connected to the D-Link Router with the PC that was originally connected to your broadband connection. If you are, then click the **Clone MAC button** to copy your computer's MAC Address to the D-Link Router.

MAC Address : 00:16:ea:61:54:76 (optional)

Clone Your PC's MAC address

Host Name :

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

Prev

Next

Cancel

Connect

SETUP COMPLETE!

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

Prev

Next

Cancel

Connect

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.

SET USERNAME / 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.

Address Mode : ☒ Dynamic IP ☐ Static IP

IP Address :

User Name :

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.

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

Prev Next Cancel Connect

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

SET USERNAME / 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 :

User Name :

Password :

Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

Prev Next Cancel Connect

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 / 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 :

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 :

Primary DNS Address :

Secondary DNS Address :

Manual Internet Setup

Dynamic (Cable)

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.

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 **Copy 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, L2TP, and Usb3g. 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

INTERNET CONNECTION TYPE

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

My Internet Connection is : Dynamic IP (DHCP)

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

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

Host Name :

Use Unicasting : ☒ (compatibility for some DHCP Servers)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1500

MAC Address :

Clone Your PC's MAC address

Internet Setup

PPPoE

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 IP** 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).

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.

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

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 **Copy 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, L2TP, and Usb3g. 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

INTERNET CONNECTION TYPE

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

My Internet Connection is : PPTP (Username / Password)

PPTP INTERNET CONNECTION TYPE :

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

Address Mode : ☐ Dynamic IP ☒ Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : ☐ Always on ☒ On demand ☐ Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server :

MTU : (bytes) MTU default = 1492

MAC Address :

Clone Your PC's MAC address

D-Link DIR-505 User Manual

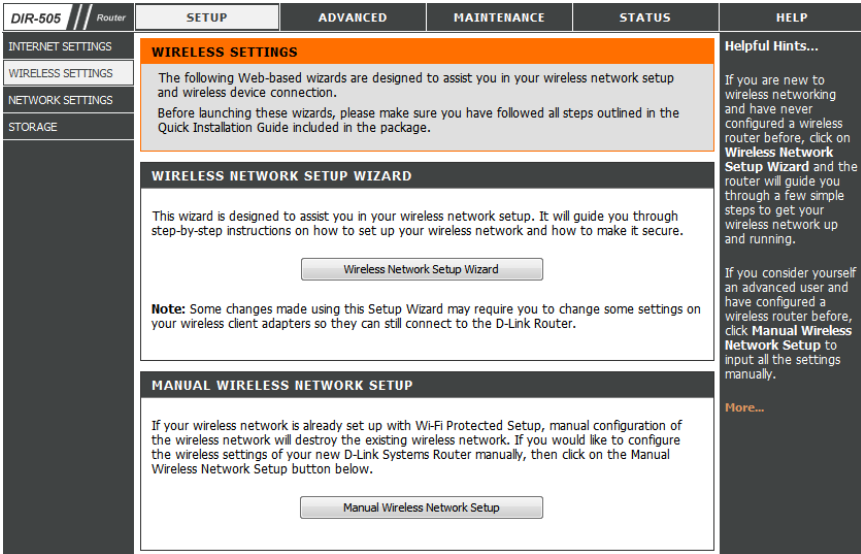
28

Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Security Setup Wizard** and refer to page 38.

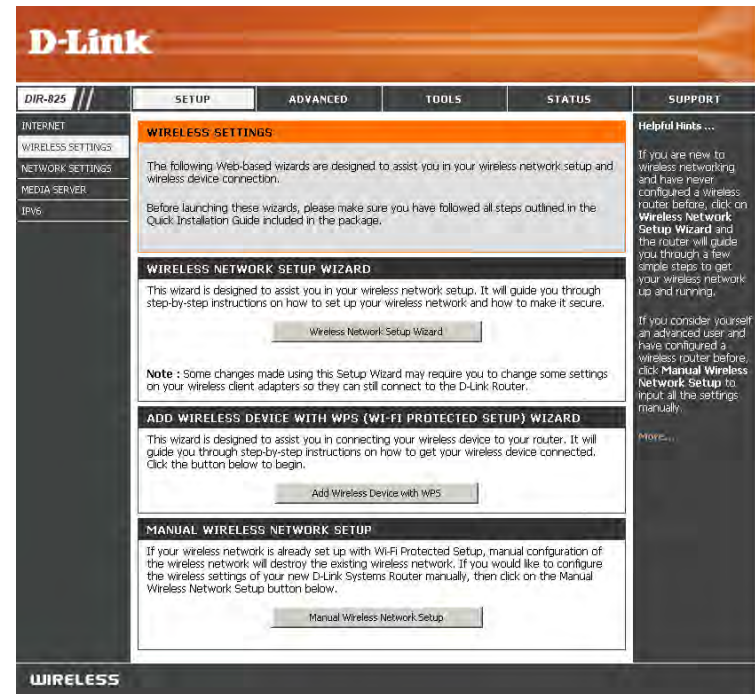
Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 41.

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



Wireless Security Setup Wizard

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



Check the **Manually set 5GHz band Network Name...** box to manually set your desired wireless network name for the 5GHz band.

Type your desired wireless network name (SSID).

Automatically: Select this option to automatically generate the router's network key and click **Next**.

Manually: Select this option to manually enter your network key and click **Next**.

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 to your network.

☐ Manually assign a network key

Use this options if you prefer to create our own key.

☐ Use WPA encryption instead of WEP (WPA is stronger than WEP and all D-Link wireless client adapters support WPA)

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

If you selected **Automatically**, the summary window will display your settings. Write down the security key and enter this on your wireless clients. Click **Save** to save your settings.

Select **Manually** to manually enter your network key and click **Next**.

If you selected **Manually**, the following screen will appear once the setup is complete.

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.

Network Name (SSID): DIR505

WEP Key Length : 128 bit

Default WEP Key to Use : 1

Authentication : Both

WEP Key : 44A8C62AD0635678E1673C6988

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 to your network.

☒ Manually assign a network key

Use this options if you prefer to create our own key.

☒ Use WPA encryption instead of WEP (WPA is stronger than WEP and all D-Link wireless client adapters support WPA)

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

Prev

Next

Cancel

Save

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.

Network Name (SSID): DIR505

Security Mode : Auto (WPA or WPA2) - Personal

Cipher Type TKIP and AES

Pre-Shared Key : 12345678

Manual Configuration

Wireless Settings

DIR-505 Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
INTERNET SETTINGS	WIRELESS				Helpful Hints... Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information. Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on. Visibility Status is another way to secure your network. With invisible option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.
WIRELESS SETTINGS	Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client. Save Settings Don't Save Settings				
NETWORK SETTINGS	WIRELESS NETWORK SETTINGS				
STORAGE	Enable Wireless : ☒ Always Add New Wireless Mode : Router Wireless Network Name : DIR505 (Also called the SSID) Wireless Band : 2.4GHz 802.11 Mode : Mixed 802.11n, 802.11g and 802.11b Enable Auto Channel Scan : ☒ Wireless Channel : 2.437 GHz - CH 6 (Domain:United States) Channel Width : Auto 20/40 MHz Visibility Status : ☒ Visible ☐ Invisible WIRELESS SECURITY MODE Security Mode : None None WEP WPA-Personal WPA-Enterprise				

Access Point Mode

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. You may also set up a specific time range (schedule). Select a schedule from the drop-down menu or click **Add New** to create a new schedule.

Wireless Mode: Select **Access Point** from the drop-down menu.

Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the default network name.

802.11 Mode: Select one of the following:

- 802.11b Only** - Select if you are only using 802.11b wireless clients.
- 802.11g Only** - Select if you are only using 802.11g wireless clients.
- 802.11n Only** - Select if you are only using 802.11n wireless clients.
- Mixed 802.11g and 802.11b** - Select if you are using a mix of 802.11g and 11b wireless clients.
- Mixed 802.11n and 802.11g** - Select if you are using a mix of 802.11n and 11g wireless clients.
- Mixed 802.11n, 802.11g and 802.11b** - Select if you are using a mix of 802.11n, 11g, and 11b wireless clients.

Wireless Channel: Indicates the channel setting for the DIR-505. 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 grayed out.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DIR-505 to choose the channel with the least amount of interference.

DIR-505 // Router

INTERNET SETTINGS

WIRELESS SETTINGS

NETWORK SETTINGS

STORAGE

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

WIRELESS

Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

Save Settings

Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒ Always

Add New

Wireless Mode : Access Point

Wireless Network Name : DIR505 (Also called the SSID)

Wireless Band : 2.4GHz

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan : ☒

Wireless Channel : 2.437 GHz - CH 6 (Domain:United Status)

Channel Width : Auto 20/40 MHz

Visibility Status : ☒ Visible ☐ Invisible

WIRELESS SECURITY MODE

Security Mode : None

Helpful Hints...

Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

Enable Auto Channel Scan so that the router can select the best possible channel for your wireless network to operate on.

Visibility Status is another way to secure your network. With invisible option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name.

Channel Width: Select the Channel Width:

Auto 20/40 - 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.

Visibility Status: Check the box if you do not want the SSID of your wireless network to be broadcasted by the DIR-505. If checked, the SSID of the DIR-505 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-505 in order to connect to it.

Security Mode: Refer to page 30 for more information regarding the wireless security.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-605L offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

Configure WEP

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 Wireless Setup on the left side.

2. In the **Security Mode** section, select **WEP** from the drop-down menu.

3. In **WEP Key Length**, select either 64Bit or 128Bit encryption from the drop-down menu.

5. Next to **WEP Key 1**, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using Hex or ASCII. Hex is recommended (letters A-F and numbers 0-9 are valid). In ASCII all numbers and letters are valid.

6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

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

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

WEP Key 1 : ••••••••

Authentication : Both

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless access point 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 access point (192.168.0.50). Click on Setup and then click Wireless Settings on the left side.

2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *Cipher Type*, select **TKIP**, **AES**, or **Auto**.

4. Next to *Passphrase*, enter a key. The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The passphrase must be between 8-63 characters.

6. Click **Save Settings** at the top of the window to save your settings.

If you are configuring the access point 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 access point.

WIRELESS SECURITY MODE

Security Mode :

WPA

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

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

WPA Mode :

Cipher Type :

PRE-SHARED KEY

Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

Configure WPA Enterprise

It is recommended to enable encryption on your wireless access point 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 access point (192.168.0.50). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WPA-Enterprise**.
3. Next to *WPA Mode* select **Auto (WPA or WPA2)**.
4. Next to *Cipher Mode*, select **TKIP**, **AES**, or **Auto**.
5. Next to *RADIUS Server*, enter the IP Address of your RADIUS server.
6. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
7. Next to *Shared Secret*, enter the security key.
8. Click **Save Settings** to save your settings.

WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

WPA

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

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

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

EAP (802.1X)

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

RADIUS Server IP Address : 0.0.0.0

RADIUS Server Port : 1812

RADIUS Server Shared Secret :

Advanced

Optional backup RADIUS server :

Second RADIUS Server IP Address : 0.0.0.0

Second RADIUS Server Port : 1812

Second RADIUS Server Shared Secret :

Network Settings

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

Router Settings

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

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

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

Device Name: Enter a name for the router.

Local Domain: Enter the Domain name (Optional).

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

The screenshot shows the 'DIR-505 Router' configuration interface. The 'SETUP' tab is selected, and the 'NETWORK SETTINGS' section is highlighted. The 'NETWORK SETTINGS' section contains instructions and two buttons: 'Save Settings' and 'Don't Save Settings'. Below this is the 'ROUTER SETTINGS' section, which also contains instructions and several input fields: 'Router IP Address' (192.168.0.1), 'Subnet Mask' (255.255.255.0), 'Device Name' (dlinkrouter), 'Local Domain Name' (optional), and 'Enable DNS Relay' (checked). A 'Helpful Hints...' sidebar on the right provides additional guidance.

DIR-505 Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
INTERNET SETTINGS	NETWORK SETTINGS				Helpful Hints... If you already have a DHCP server on your network or are using static IP addresses on all the devices on your network, uncheck Enable DHCP Server to disable this feature. If you have devices on your network that should always have fixed IP addresses, add a DHCP Reservation for each such device. More...
WIRELESS 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. Save Settings Don't Save Settings				
NETWORK SETTINGS	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 : 192.168.0.1 Subnet Mask : 255.255.255.0 Device Name : dlinkrouter Local Domain Name : (optional) Enable DNS Relay : ☒				
STORAGE					

DHCP Reservation

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

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

Enable: Check this box to enable the reservation.

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

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

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

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

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

DHCP Reservations List

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

Enable: Check to enable the reservation.

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

Delete: Click to remove the reservation from the list.

ADD DHCP RESERVATION

Enable : ☐

Computer Name : << Computer Name ▼

IP Address :

MAC Address :

DHCP RESERVATIONS LIST			
Enable	Computer Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS:					
Hardware Address	Assigned IP	Hostname	Expires		
00:16:ea:61:54:76	192.168.0.100	Lifbook	Sun Jan 2 00:35:39 2011	Revoke	Reserve

DHCP RESERVATIONS LIST				
Enable	Host Name	MAC Address	IP Address	
☒	PM_test01	00:04:23:2c:51:a3	192.168.0.112	 

NUMBER OF DYNAMIC DHCP CLIENTS : 1					
Hardware Address	Assigned IP	Hostname	Expires		
00:04:23:2c:51:a3	192.168.0.112	PM_test01	Thu Sep 1 19:49:06 2011	Revoke	Reserve

Storage

This page will allow you to access files from a USB external hard drive or thumb drive that is plugged into the router from your local network or from the Internet using either a web browser or an app for your smartphone or tablet. You can create users to be allowed to access these files.

Enable Web File Check to enable sharing files on your USB storage device
Access: that is plugged in your router.

Enable HTTP Check to enable HTTP access to your router's storage. You
Storage Remote will have to type HTTP in the URL.
Access:

Remote Access Enter a port (8181 is default). You will have to enter this port
Port: in the URL when connecting to the shared files. For example:
(http://192.168.0.1:8181).

Enable HTTPS Check to enable HTTPS (secure) access to your router's
Storage Remote storage. You will have to type HTTPS in the URL.
Access:

Remote HTTPS Enter a port (4433 is default). You will have to enter this port
Port: in the URL when connecting to the shared files. For example:
(https://192.168.0.1:8181).

User Name: To create a new user, enter a user name.

Password: Enter a password for this account.

Verify Password: Re-enter the password. Click **Add/Edit** to create the user.

User List: Displays the accounts. The Admin and Guest accounts are built-in to the router.

Number of Displays the USB device plugged into the router.
Devices:

The screenshot shows the 'STORAGE' configuration page of a D-Link DIR-505 Router. The page has a sidebar with navigation links: INTERNET SETTINGS, WIRELESS SETTINGS, NETWORK SETTINGS, and STORAGE (selected). The main content area is titled 'STORAGE' and contains several sections:

- STORAGE**: A section with a description of Web File Access and two buttons: 'Save Settings' and 'Don't Save Settings'.
- HTTP STORAGE**: A section with checkboxes for 'Enable Web File Access', 'Enable HTTP Storage Remote Access', and 'Enable HTTPS Storage Remote Access'. It also includes input fields for 'Remote Access Port' (default 8181) and 'Remote HTTPS Port' (default 4433).
- 10 -- USER CREATION**: A section for creating a new user, with fields for 'User Name', 'Password', and 'Verify Password', and buttons for 'Add/Edit' and 'Delete'.
- USER LIST**: A table displaying the list of users. The table has columns for 'No.', 'User Name', 'Access Path', and 'Permission'. It shows two users: 'Admin' (Read/Write) and 'Guest' (Read Only). There are icons for 'Modify' and 'Delete' next to each user.
- NUMBER OF DEVICES : 0**: A section showing the number of USB devices plugged into the router. It includes a table with columns for 'Device', 'Total Space', and 'Free Space'.
- HTTP STORAGE LINK**: A section with a description of the link used to connect to the drive remotely.

On the right side of the page, there is a 'Helpful Hints...' section with a 'More...' link.

Advanced Virtual Server

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

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

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

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

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

DIR-505 Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP																																																						
VIRTUAL SERVER	VIRTUAL SERVER The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers. Save Settings Don't Save Settings				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. More...																																																						
APPLICATION RULES	8--VIRTUAL SERVERS LIST <table border="1"> <thead> <tr> <th></th> <th>Name</th> <th></th> <th>Port</th> <th>Traffic Type</th> </tr> </thead> <tbody> <tr> <td>☐</td> <td>Name</td> <td><< Application Name</td> <td>Public 0</td> <td>Protocol TCP</td> </tr> <tr> <td></td> <td>IP Address</td> <td><< Computer Name</td> <td>Private 0</td> <td>6</td> </tr> <tr> <td>☐</td> <td>Name</td> <td><< Application Name</td> <td>Public 0</td> <td>Protocol TCP</td> </tr> <tr> <td></td> <td>IP Address</td> <td><< Computer Name</td> <td>Private 0</td> <td>6</td> </tr> <tr> <td>☐</td> <td>Name</td> <td><< Application Name</td> <td>Public 0</td> <td>Protocol TCP</td> </tr> <tr> <td></td> <td>IP Address</td> <td><< Computer Name</td> <td>Private 0</td> <td>6</td> </tr> <tr> <td>☐</td> <td>Name</td> <td><< Application Name</td> <td>Public 0</td> <td>Protocol TCP</td> </tr> <tr> <td></td> <td>IP Address</td> <td><< Computer Name</td> <td>Private 0</td> <td>6</td> </tr> <tr> <td>☐</td> <td>Name</td> <td><< Application Name</td> <td>Public 0</td> <td>Protocol TCP</td> </tr> <tr> <td></td> <td>IP Address</td> <td><< Computer Name</td> <td>Private 0</td> <td>6</td> </tr> </tbody> </table>						Name		Port	Traffic Type	☐	Name	<< Application Name	Public 0	Protocol TCP		IP Address	<< Computer Name	Private 0	6	☐	Name	<< Application Name	Public 0	Protocol TCP		IP Address	<< Computer Name	Private 0	6	☐	Name	<< Application Name	Public 0	Protocol TCP		IP Address	<< Computer Name	Private 0	6	☐	Name	<< Application Name	Public 0	Protocol TCP		IP Address	<< Computer Name	Private 0	6	☐	Name	<< Application Name	Public 0	Protocol TCP		IP Address	<< Computer Name	Private 0
	Name		Port	Traffic Type																																																							
☐	Name	<< Application Name	Public 0	Protocol TCP																																																							
	IP Address	<< Computer Name	Private 0	6																																																							
☐	Name	<< Application Name	Public 0	Protocol TCP																																																							
	IP Address	<< Computer Name	Private 0	6																																																							
☐	Name	<< Application Name	Public 0	Protocol TCP																																																							
	IP Address	<< Computer Name	Private 0	6																																																							
☐	Name	<< Application Name	Public 0	Protocol TCP																																																							
	IP Address	<< Computer Name	Private 0	6																																																							
☐	Name	<< Application Name	Public 0	Protocol TCP																																																							
	IP Address	<< Computer Name	Private 0	6																																																							
MAC ADDRESS FILTER																																																											
WEBSITE FILTER																																																											
FIREWALL SETTINGS																																																											
ADVANCED WIRELESS																																																											
WIFI PROTECTED SETUP																																																											
UPNP SETTINGS																																																											
GUEST ZONE																																																											
DMZ																																																											

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-505. 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-505 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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

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

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

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

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

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

DIR-505 Router

SETUP **ADVANCED** **MAINTENANCE** **STATUS** **HELP**

VIRTUAL SERVER
APPLICATION RULES
MAC ADDRESS FILTER
WEBSITE FILTER
FIREWALL SETTINGS
ADVANCED WIRELESS
WI-FI PROTECTED SETUP
UPNP SETTINGS
GUEST ZONE
DMZ

APPLICATION RULES

This option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

Save Settings Don't Save Settings

8 -- APPLICATION RULES

	Name	Application	Trigger	Firewall	Traffic Type
☐		<< Application Name	0	0	TCP
☐		<< Application Name	0	0	TCP
☐		<< Application Name	0	0	TCP
☐		<< Application Name	0	0	TCP
☐		<< Application Name	0	0	TCP

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.

More...

MAC Address Filter

The MAC address filter section can be used to filter network access by machines based on the unique MAC addresses of their network adapter(s). It is most useful to prevent unauthorized wireless devices from connecting to your network. A MAC address is a unique ID assigned by the manufacturer of the network adapter.

Configure When you **Turn MAC Filtering OFF** is selected, MAC **MAC Filtering:** addresses are not used to control network access. When **Turn MAC Filtering ON and ALLOW computers listed to access the network** is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When **Turn MAC Filtering ON and DENY computers listed to access the network** is selected, any computer with a MAC address listed in the MAC Address List is refused access to the network.

Add MAC Filtering This parameter allows you to manually add a MAC filtering rule. Click the **Add** button to add the new MAC filtering rule **Rule:** to the MAC Filtering Rules list at the bottom of this screen.

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP																																				
VIRTUAL SERVER	MAC ADDRESS FILTER				Helpful Hints... Create a list of MAC address that you would either like to allow or deny access to your network. Select a MAC address from the drop down menu, then click the arrow to add that MAC address to the list. Click the Clear button to remove the MAC address from the MAC Filtering list.																																				
APPLICATION RULES	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																																								
MAC ADDRESS FILTER	WIRELESS ACCESS SETTINGS Configure MAC Filtering below: Turn MAC Filtering ON and ALLOW computers listed to access the network ▼																																								
WEBSITE FILTER	<table border="1"> <thead> <tr> <th>MAC Address</th> <th></th> <th>Wireless Client List</th> <th></th> </tr> </thead> <tbody> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> <tr> <td>00:00:00:00:00:00</td> <td><<</td> <td>MAC Address ▼</td> <td> Clear </td> </tr> </tbody> </table>				MAC Address		Wireless Client List		00:00:00:00:00:00	<<	MAC Address ▼	Clear	00:00:00:00:00:00	<<	MAC Address ▼	Clear	00:00:00:00:00:00	<<	MAC Address ▼	Clear	00:00:00:00:00:00	<<	MAC Address ▼	Clear	00:00:00:00:00:00	<<	MAC Address ▼	Clear	00:00:00:00:00:00	<<	MAC Address ▼	Clear	00:00:00:00:00:00	<<	MAC Address ▼	Clear	00:00:00:00:00:00	<<	MAC Address ▼	Clear	
MAC Address		Wireless Client List																																							
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
00:00:00:00:00:00	<<	MAC Address ▼	Clear																																						
FIREWALL SETTINGS																																									
ADVANCED WIRELESS																																									
WI-FI PROTECTED SETUP																																									
UPNP SETTINGS																																									
GUEST ZONE																																									
DMZ																																									

Website Filters

Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section (page 33).

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

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

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP										
VIRTUAL SERVER	WEBSITE FILTER 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 use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section. Save Settings Don't Save Settings				Helpful Hints... Create a list of Web Sites to which you would like to deny or allow through the network. More...										
APPLICATION RULES	8 -- WEBSITE FILTERING RULES Configure Website Filter below: DENY computers access to ONLY these sites ▼ Clear the list below...														
MAC ADDRESS FILTER	<table border="1"> <thead> <tr> <th colspan="2">Website URL/Domain</th> </tr> </thead> <tbody> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> <tr><td></td><td></td></tr> </tbody> </table>					Website URL/Domain									
Website URL/Domain															
WEBSITE FILTER															
FIREWALL SETTINGS															
ADVANCED WIRELESS															
WI-FI PROTECTED SETUP															
UPNP SETTINGS															
GUEST ZONE															
DMZ															

Firewall Settings

A firewall protects your network from the outside world. The DIR-505 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

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

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

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
VIRTUAL SERVER	FIREWALL SETTINGS				Helpful Hints... ALGs provide special handling of the IP payload for some protocols and applications to make them work with network address translation (NAT). More...
APPLICATION RULES	The Firewall Settings allow you to set a single computer on your network outside of the router. Save Settings Don't Save Settings				
MAC ADDRESS FILTER	FIREWALL SETTINGS				
WEBSITE FILTER	Enable SPI : ☒				
FIREWALL SETTINGS	ANTI-SPOOF CHECKING				
ADVANCED WIRELESS	Enable anti-spoof checking : ☐				
WI-FI PROTECTED SETUP					
UPNP SETTINGS					
GUEST ZONE					
DMZ					

Advanced Wireless

Transmit Power: Set the transmit power of the antennas.

WMM Enable: 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.

IGMP Snooping: Check to enable this feature.

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

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
VIRTUAL SERVER	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				Helpful Hints... Advanced Wireless: It is recommended that you leave these options at their default values. Adjusting them could negatively impact the performance of your wireless network. The options on this page should be changed by advanced users or if you are instructed to by one of our support personnel, as they can negatively affect the performance of your Access Point if configured improperly.
APPLICATION RULES					
MAC ADDRESS FILTER					
WEBSITE FILTER					
FIREWALL SETTINGS					
ADVANCED WIRELESS	ADVANCED WIRELESS SETTINGS Transmit Power : 100% ▾ WMM Enable : ☒ Short GI : ☒ IGMP Snooping : ☒ WLAN Partition : ☐				
WI-FI PROTECTED SETUP					
UPNP SETTINGS					
GUEST ZONE					
DMZ					

Wi-Fi Protected Setup (WPS)

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

Enable: Enable the Wi-Fi Protected Setup feature.

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

Lock Wireless Security Settings: 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. Only the Administrator (“admin” account) can change or reset the PIN.

Current PIN: Shows the current PIN.

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

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

DIR-505 Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
VIRTUAL SERVER	WI-FI PROTECTED SETUP				Helpful Hints... 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. Click Add Wireless Device Wizard to use Wi-Fi Protected Setup to add wireless devices to the wireless network. More...
APPLICATION RULES	Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method. If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on “Don’t Save Settings” button will not reset the PIN. However, if the new PIN is not saved, it will get lost when the device reboots or loses power.				
MAC ADDRESS FILTER	Save Settings Don't Save Settings				
WEBSITE FILTER	WI-FI PROTECTED SETUP				
FIREWALL SETTINGS	Enable : ☒ Lock Wireless Security Settings : ☐ Reset to Unconfigured				
ADVANCED WIRELESS	PIN SETTINGS				
WI-FI PROTECTED SETUP	Current PIN: 69740909 Reset PIN to Default Generate New PIN				
UPNP SETTINGS	ADD WIRELESS STATION				
GUEST ZONE	Add Wireless Device With WPS				
DMZ					

Add Wireless Station: This Wizard helps you add wireless devices to the wireless network.

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.

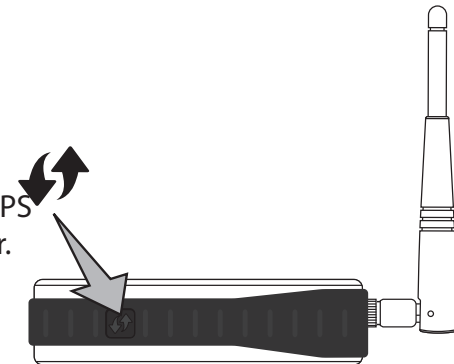
There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar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

Add Wireless Device Wizard: Click to start the wizard.

WPS Button

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

Refer to page 106 for more information.



UPnP Settings

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

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
VIRTUAL SERVER	UPNP SETTINGS				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. More...
APPLICATION RULES	Universal Plug and Play (UPnP) supports peer-to-peer Plug and Play functionality for network devices.				
MAC ADDRESS FILTER	Save Settings Don't Save Settings				
WEBSITE FILTER					
FIREWALL SETTINGS	UPNP SETTINGS				
ADVANCED WIRELESS	Enable UPnP : ☒				
WI-FI PROTECTED SETUP					
UPNP SETTINGS					
GUEST ZONE					
DMZ					

Guest Zone

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

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

Add New 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.

DIR-505 Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
VIRTUAL SERVER	GUEST ZONE				Helpful Hints... Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet. More...
APPLICATION RULES	Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet. Save Settings Don't Save Settings				
MAC ADDRESS FILTER	GUEST ZONE SELECTION				
WEBSITE FILTER	Enable Guest Zone : ☒ Always Add New Schedule Wireless Band : 2.4GHz Band Wireless Network Name : dlink_guest (Also called the SSID) Enable Routing Between Zones : ☐ Security Mode : WPA-Personal				
FIREWALL SETTINGS	WPA Use WPA or WPA2 mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use WPA2 Only mode. This mode uses AES(COMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use WPA Only . This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode. To achieve better wireless performance use WPA2 Only security mode (or in other words AES cipher). WPA Mode : Auto (WPA or WPA2) Cipher Type : TKIP and AES				
ADVANCED WIRELESS	PRE-SHARED KEY Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase. Pre-Shared Key :				
WI-FI PROTECTED SETUP					
UPNP SETTINGS					
GUEST ZONE					
DMZ					

DMZ

This feature allows you to set a single computer from your network to outside of the router and get unrestricted Internet access.

- Enable DMZ: Check the box to enable DMZ.
- DMZ IP Address: Enter the DMZ IP Address.

DIR-505Router

VIRTUAL SERVER

APPLICATION RULES

MAC ADDRESS FILTER

WEBSITE FILTER

FIREWALL SETTINGS

ADVANCED WIRELESS

WI-FI PROTECTED SETUP

UPNP SETTINGS

GUEST ZONE

DMZ

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

DMZ SETTINGS

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.
Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Save SettingsDon't Save Settings

DMZ HOST

Enable DMZ : ☒

DMZ IP Address : 0.0.0.0 << Computer Name

Helpful Hints...

Enable the DMZ option only as a last resort. If you are having trouble using an application from a computer behind the router, first try opening ports associated with the application in the Virtual Server sections.
[More...](#)

Maintenance Admin

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

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

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

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

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

Enable Remote Management: Remote management allows the DIR-505 to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

Remote Admin Port: The port number used to access the DIR-505 is used in the URL. Example: **http://x.x.x.x:8080** whereas x.x.x.x is the Internet IP address of the DIR-505 and 8080 is the port used for the Web Management interface.

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

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	ADMINISTRATOR SETTINGS The 'admin' account can access the management interface. The admin has read/write access and can change passwords. By default there is no password configured. It is highly recommended that you create a password to keep your router secure. Save Settings Don't Save Settings				Helpful Hints... For security reasons, it is recommended that you change the password for the Admin account. Be sure to write down the new passwords to avoid having to reset the router in case they are forgotten. Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet. Choose a port to open for remote management. More...
TIME	ADMIN PASSWORD Please enter the same password into both boxes, for confirmation. Password : Verify Password :				
SYSTEM	ADMINISTRATION Enable Graphical Authentication : ☐ Enable HTTPS Server : ☐ Enable Remote Management : ☐ Remote Admin Port : 8080				
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 Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

Current Router Time: Displays the current date and time of the router.

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

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

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

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

Set the Date and Time Manually: 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** to synch the date and time with the computer you are currently on.

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	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				Helpful Hints... Good timekeeping is important for accurate logs and scheduled firewall rules. More...
TIME					
SYSTEM					
FIRMWARE					
DYNAMIC DNS					
SYSTEM CHECK					
SCHEDULES					
TIME CONFIGURATION Current Router Time : Jan/01/2011 04:16:53 Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana Enable Daylight Saving : ☒ Daylight Saving Dates : DST start: Mar 3rd Sun 1 am DST End: Nov 2nd Sun 1 am					
AUTOMATIC TIME CONFIGURATION Enable NTP Server : ☒ NTP Server Used : << Select NTP Server					
SET THE DATE AND TIME MANUALLY Date And Time : Year 2011 Month Jan Day 01 Hour 00 Minute 00 Second 00 Copy Your Computer's Time Settings					

System

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

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

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

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

Reboot Device: Click to reboot the router.

Clear Language Pack: If you previously installed a language pack and want to revert all the menus on the Router interface back to the default language settings, click the **Clear** button.

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	SYSTEM SETTINGS				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...
TIME	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.				
SYSTEM	SYSTEM SETTINGS				
FIRMWARE	Save Settings To Local Hard Drive : Save Configuration				
DYNAMIC DNS	Load Settings From Local Hard Drive : Browse... Restore Configuration from File				
SYSTEM CHECK	Restore To Factory Default Settings : Restore Factory Defaults Restore all settings to the factory defaults.				
SCHEDULES	Reboot The Device : Reboot The Device Remove Language Pack : Remove				

Firmware

Use the Firmware window to upgrade the firmware of the Router and install language packs. If you plan to install new firmware, make sure the firmware you want to use is on the local hard drive of the computer. If you want to install a new language pack, make sure that you have the language pack available. 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 Information: This section displays information about the firmware that is loaded on the Router. Click the **Check Now** button to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

Firmware Upgrade: 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.

Language Pack Upgrade: If you want to change the Router's language pack, click **Browse** to locate the language pack. Click **Upload** to complete the load the new language pack.

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	FIRMWARE There may be new firmware for your DIR-505 to improve functionality and performance. Click here to check for an upgrade on our support site. After you have download the new firmware file from our support site, click the Browse button below to find the firmware file on your local hard drive. Click the Upload button to update the firmware on the DIR-505. Do not update firmware through wireless network!!				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...
TIME					
SYSTEM					
FIRMWARE					
DYNAMIC DNS					
SYSTEM CHECK					
SCHEDULES	FIRMWARE AND LANGUAGE PACK INFORMATION Current Firmware Version : 1.00betaNA Date : 2011/11/25 Current Language Pack Version : No Language pack Check Online Now for Latest Firmware and Language pack Version : Check Now				
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 Maintenance -> System screen To upgrade the firmware, your PC must have a wired connection to the access point. Enter the name of the firmware upgrade file, and click on the Upload button. Upload : Browse... Upload					
LANGUAGE PACK UPGRADE Upload : Browse... Upload					

Dynamic DNS

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

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

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

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

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

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

Timeout: Enter a timeout time (in hours).

Status: Displays the current connection status.

DIR-505

Router

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

ADMIN

TIME

SYSTEM

FIRMWARE

DYNAMIC DNS

SYSTEM CHECK

SCHEDULES

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

Save Settings

Don't Save Settings

DYNAMIC DNS

Enable Dynamic DNS : ☒

Server Address : << Select Dynamic DNS Server

Host Name :

Username or Key :

Password or Key :

Verify Password or Key :

Timeout : (hours)

Status : Disconnected

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**.

IPv6 Ping Test: Enter the IPv6 address that you wish to Ping and click **Ping**.

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

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	PING TEST				Helpful Hints... "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. More...
TIME	Ping Test sends "ping" packets to test a computer on the Internet.				
SYSTEM	PING TEST				
FIRMWARE	Host Name or IP Address: Ping				
DYNAMIC DNS	PING RESULT				
SYSTEM CHECK					
SCHEDULES					

Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

- Name:** Enter a name for your new schedule.
- Days:** Select a day, a range of days, or All Week to include every day.
- Time format:** Check **All Day - 24hrs** or enter a start and end time for your schedule.
- Save:** 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.

DIR-505Router

ADMIN

TIME

SYSTEM

FIRMWARE

DYNAMIC DNS

SYSTEM CHECK

SCHEDULES

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

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 :

Time format :

24-hour

Start Time :

00

:

00

AM

(hour:minute)

End Time :

00

:

00

AM

(hour:minute)

Save

Clear

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

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

More...

D-Link DIR-505 User Manual

59

Status Device Info

This page displays the current information for the DIR-505. 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.

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP								
DEVICE INFO LOGS STATISTICS INTERNET SESSIONS WIRELESS	DEVICE INFORMATION All of your wireless and network connection details are displayed on this page. The firmware version is also displayed here.				Helpful Hints... All of your WAN and LAN connection details are displayed here. More...								
GENERAL Time : Jan/01/2011 04:43:57 System Up Time : 0 Day, 04:44:20 Firmware Version : 1.00beta1A, Fri, 25 Nov 2011													
WAN Connection Type : DHCP client Cable Status : Disconnected Network Status : Disconnected DHCP Renew DHCP Release Connection Up Time : N/A MAC Address : 00:18:e7:95:6a:7f 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													
LAN MAC Address : 00:18:e7:95:6a:7e IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0 DHCP Server : Enabled													
WIRELESS LAN Wireless Radio : Enable Wireless Mode : Mixed 802.11n, 802.11g and 802.11b Channel Width : Auto 20/40 MHz Channel : 0 Wi-Fi Protected Setup : Enable / Configured													
SSID List <table border="1"> <thead> <tr> <th>Network Name (SSID)</th> <th>Guest</th> <th>MAC Address</th> <th>Security Mode</th> </tr> </thead> <tbody> <tr> <td>DIR505</td> <td>No</td> <td>00:18:e7:95:6a:7e</td> <td>None</td> </tr> </tbody> </table>						Network Name (SSID)	Guest	MAC Address	Security Mode	DIR505	No	00:18:e7:95:6a:7e	None
Network Name (SSID)	Guest	MAC Address	Security Mode										
DIR505	No	00:18:e7:95:6a:7e	None										
LAN COMPUTERS <table border="1"> <thead> <tr> <th>IP Address</th> <th>Name(If Any)</th> <th>MAC</th> </tr> </thead> <tbody> <tr> <td>192.168.0.100</td> <td>Lifebook</td> <td>00:16:ea:61:54:76</td> </tr> </tbody> </table>						IP Address	Name(If Any)	MAC	192.168.0.100	Lifebook	00:16:ea:61:54:76		
IP Address	Name(If Any)	MAC											
192.168.0.100	Lifebook	00:16:ea:61:54:76											

Logs

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.

Log Type: Use the radio buttons to select the types of messages that you want to display from the log. **System, Firewall & Security**, and **Router Status** messages can be selected.

Log Level: There are three levels of message importance: **Critical**, **Warning**, and **Information**. Select the levels that you want displayed in the log.

Log Files: Use this section to view and manage the Router's log entries.

First Page: Click this button to view the first page of the Router logs.

Last Page: Click this button to view the last page of the Router logs.

Previous: Click this button to view the previous page of the Router logs.

Next: Click this button to view the next page of the Router logs.

Clear: Clears all of the log contents.

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP																						
DEVICE INFO LOGS STATISTICS INTERNET SESSIONS WIRELESS	LOGS Use this option to view the device logs. You can define what types of events you want to view and the event levels to view. LOG OPTIONS Log Type : ☒ System Activity ☒ Debug Information ☒ Attacks ☒ Dropped Packets ☒ Notice Apply Log Settings Now LOG DETAILS First Page Last Page Previous Next Save Log Refresh Clear 1/7 <table border="1"> <thead> <tr> <th>Time</th> <th>Message</th> </tr> </thead> <tbody> <tr><td>Jan 1 04:16:29</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 03:24:56</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 03:19:48</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 03:18:12</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 03:16:30</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 02:16:31</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 01:23:26</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 00:35:39</td><td>UDHCPD Inform: add_lease 192.168.0.100</td></tr> <tr><td>Jan 1 00:35:33</td><td>UDHCPD sending ACK to 192.168.0.100</td></tr> <tr><td>Jan 1 00:35:33</td><td>UDHCPD sending OFFER of 192.168.0.100</td></tr> </tbody> </table>				Time	Message	Jan 1 04:16:29	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 03:24:56	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 03:19:48	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 03:18:12	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 03:16:30	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 02:16:31	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 01:23:26	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 00:35:39	UDHCPD Inform: add_lease 192.168.0.100	Jan 1 00:35:33	UDHCPD sending ACK to 192.168.0.100	Jan 1 00:35:33	UDHCPD sending OFFER of 192.168.0.100	Helpful Hints... Check the log frequently to detect unauthorized network usage. More...
Time	Message																										
Jan 1 04:16:29	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 03:24:56	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 03:19:48	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 03:18:12	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 03:16:30	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 02:16:31	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 01:23:26	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 00:35:39	UDHCPD Inform: add_lease 192.168.0.100																										
Jan 1 00:35:33	UDHCPD sending ACK to 192.168.0.100																										
Jan 1 00:35:33	UDHCPD sending OFFER of 192.168.0.100																										

Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-505 on both the WAN, LAN ports and both the 802.11n/g (2.4GHz) and 802.11n/a (5GHz) wireless bands. The traffic counter will reset if the device is rebooted.

Refresh: Click the **Refresh** button to refresh the Router's traffic statistics.

Reset: Click the **Reset** button to reset the Router's traffic statistics.

DIR-505 // Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
DEVICE INFO	TRAFFIC STATISTICS				Helpful Hints... This is a summary of the number of packets that have passed between the WAN and the LAN since the router was last initialized. More...
LOGS	Traffic Statistics display Receive and Transmit packets passing through your router.				
STATISTICS	Refresh Statistics Clear Statistics				
INTERNET SESSIONS					
WIRELESS					
	LAN STATISTICS				
	Sent : 80837 Received : 47738 TX Packets Dropped : 0 RX Packets Dropped : 0 Collisions : 0 Errors : 0				
	WAN STATISTICS				
	Sent : 0 Received : 0 TX Packets Dropped : 0 RX Packets Dropped : 0 Collisions : 0 Errors : 0				
	WIRELESS STATISTICS				
	Sent : 97592 Received : 47736 TX Packets Dropped : 1015 RX Packets Dropped : 0 Collisions : 0 Errors : 0				

Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer.

DIR-505 // Router

DEVICE INFO

LOGS

STATISTICS

INTERNET SESSIONS

WIRELESS

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

Helpful Hints...
This is a list of all active conversations between WAN computers and LAN computers.
[More...](#)

INTERNET SESSIONS

This page displays the full details of active internet sessions to your router.

INTERNET SESSIONS

Local

NAT

Internet

Protocol

State

Dir

Time-Out

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.

DIR-505 // Router		SETUP	ADVANCED	MAINTENANCE	STATUS	HELP									
DEVICE INFO		WIRELESS				Helpful Hints... This is a list of all wireless clients that are currently connected to your wireless router. More...									
LOGS		Use this option to view the wireless clients that are connected to your wireless router.													
STATISTICS															
INTERNET SESSIONS		NUMBER OF WIRELESS CLIENTS : 1													
WIRELESS		<table><tr><th>MAC Address</th><th>IP Address</th><th>Mode</th><th>Rate (Mbps)</th><th>Signal (%)</th></tr><tr><td>00:16:ea:61:54:76</td><td>192.168.0.100</td><td>802.11n (2.4GHz)</td><td>66M</td><td>94</td></tr></table>					MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)	00:16:ea:61:54:76	192.168.0.100	802.11n (2.4GHz)	66M
MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)											
00:16:ea:61:54:76	192.168.0.100	802.11n (2.4GHz)	66M	94											

Help

DIR-505	Router	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
MENU	SUPPORT MENU • Setup • Advanced • Maintenance • Status					Helpful Hints... Click on the links for more informations of each section in the GUI.
SETUP	SETUP HELP • Internet Connection • Internet Settings • Wireless Settings • Network Settings					
ADVANCED	ADVANCED HELP • Virtual Server • Application Rules • MAC Address Filter • Website Filter • Firewall Settings • Advanced Wireless • Wi-Fi Protected Setup • UPNP Settings • Guest Zone • DMZ					
MAINTENANCE	MAINTENANCE HELP • Admin • Time • System • Firmware • Schedules					
STATUS	STATUS HELP • Device Info • Logs • Statistics • Internet Sessions • Wireless					

Quick Setup Wizard

Repeater Mode

This Wizard is designed to assist you in configuring your DIR-505 as an repeater.

To start the Setup Wizard click **Next**.

WI-FI CONNECTION SETUP WIZARD

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

Select **WPS** as the configuration method only if your wireless device supports Wi-Fi Protected Setup (WPS). For **Manual** setup, skip to page 67.

Click **Next** to continue.

SELECT CONFIGURATION METHOD

Please select one of the following configuration methods. Click **Next** to continue.

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

☐ **Manual** -- Select this option if you want to setup your network manually.

Press down the **Push Button** on the Wireless device you are adding to your wireless network.

VIRTUAL PUSH BUTTON

Please press the Push Button (physical or virtual) on the AP or Router you are connecting to within **120** seconds...

Select **Manual** as the configuration method to set up your network manually.

Click **Next** to continue.

Please wait while your device scans for available Wi-Fi networks.

Select the network you would like your device to connect to.

SELECT CONFIGURATION METHOD

Please select one of the following configuration methods. Click **Next** to continue.

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

☒ **Manual** -- Select this option if you want to setup your network manually.

Prev

Next

Cancel

SELECT WI-FI NETWORK

Scanning for available Wi-Fi network...

Prev

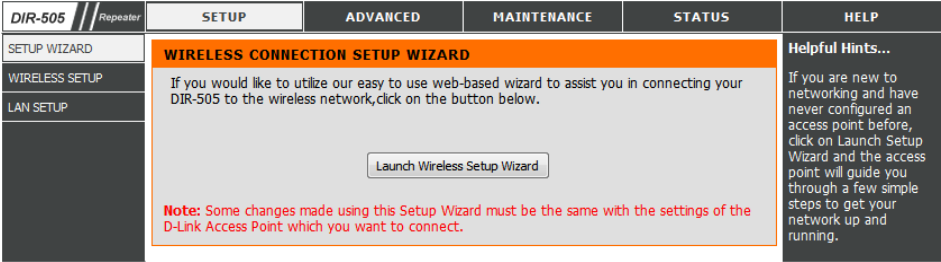
Next

Cancel

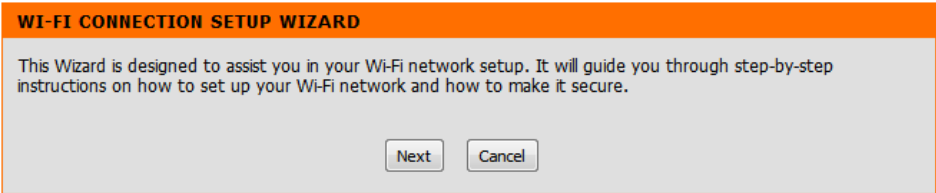
SELECT WI-FI NETWORK					
ID	Wi-Fi Network Name	Encrypt	Channel	Signal(%)	Select
1	Linksys Staples	WPA2-PSK	3	94	☐
2	00265a493e08	WPA2-PSK	1	94	☐
3	Cisco Staples	WPA/WPA2-PSK(auto)	1	94	☐
4	CAMERA432	WPA/WPA2-PSK(auto)	3	94	☐
5	DSR-500N_1	WPA2-PSK	6	94	☐
6	mywirelessnetwork	WPA/WPA2-PSK(auto)	11	94	☐
7	00265a493e1e	WPA2-PSK	11	94	☐
8	neopolitan	WPA/WPA2-PSK(auto)	6	94	☐
9	Strawberry	WPA/WPA2-PSK(auto)	9	94	☐
10	Firefly	WPA/WPA2-PSK(auto)	9	94	☐
11	vanilla	WEP	1	94	☐
12	vanilla	WEP	1	94	☐
13	vanilla	WEP	1	94	☐
14	7245 6100	WEP	6	94	☐
15	vanilla	WEP	6	94	☐
16	vanilla	WEP	6	94	☐
17	vanilla	WEP	6	94	☐
18	TheRack	WEP	6	94	☐
19	vanilla	WEP	11	94	☐
20	vanilla	WEP	11	94	☐
21	vanilla	WEP	11	94	☐
22	Chocolate	None	9	94	☐
23	vanilla	WEP	6	94	☐
24	dlink	None	10	94	☐
25	fc75164f587b	WPA2-PSK	11	93	☐
26	vanilla	WEP	1	93	☐

Setup Wizard

Click **Launch Wireless Setup Wizard** to begin the Setup Wizard.

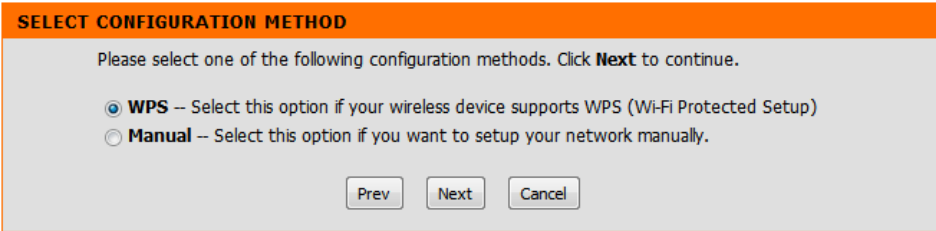


To start the Setup Wizard click **Next**.

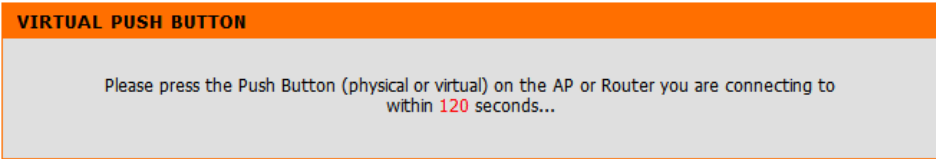


Select **WPS** as the configuration method only if your wireless device supports Wi-Fi Protected Setup (WPS).

Click **Next** to continue.



Press down the **Push Button** on the Wireless device you are adding to your wireless network.



Select **Manual** as the configuration method to set up your network manually.

Click **Next** to continue.

SELECT CONFIGURATION METHOD

Please select one of the following configuration methods. Click **Next** to continue.

☐ WPS – Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

☒ **Manual** – Select this option if you want to setup your network manually.

Prev

Next

Cancel

SELECT WI-FI NETWORK

Scanning for available Wi-Fi network...

Prev

Next

Cancel

Select the network you would like your device to connect to.

SELECT WI-FI NETWORK					
ID	Wi-Fi Network Name	Encrypt	Channel	Signal(%)	Select
1	Linksys Staples	WPA2-PSK	3	94	☐
2	00265a493e08	WPA2-PSK	1	94	☐
3	Cisco Staples	WPA/WPA2-PSK(auto)	1	94	☐
4	CAMERA432	WPA/WPA2-PSK(auto)	3	94	☐
5	DSR-500N_1	WPA2-PSK	6	94	☐
6	mywirelessnetwork	WPA/WPA2-PSK(auto)	11	94	☐
7	00265a493e1e	WPA2-PSK	11	94	☐
8	neopolitan	WPA/WPA2-PSK(auto)	6	94	☐
9	Strawberry	WPA/WPA2-PSK(auto)	9	94	☐
10	Firefly	WPA/WPA2-PSK(auto)	9	94	☐
11	vanilla	WEP	1	94	☐
12	vanilla	WEP	1	94	☐
13	vanilla	WEP	1	94	☐
14	7245 6100	WEP	6	94	☐
15	vanilla	WEP	6	94	☐

Manual Configuration

Wireless Settings

DIR-505 Repeater		SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
SETUP WIZARD		WIRELESS				Helpful Hints... Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information. Enable Auto Channel Scan so that the Access Point can select the best possible channel for your wireless network to operate on. Visibility Status is another way to secure your network. With invisible option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device. If you have enabled Wireless Security, make
WIRELESS SETUP		Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC. Save Settings Don't Save Settings				
LAN SETUP		WIRELESS NETWORK SETTINGS				
		Enable Wireless : ☒ Wireless Mode : Repeater Mode Site Survey Wireless Network Name : dlink (Also called the SSID) Channel Width : Auto 20/40 MHz				
		WIRELESS SECURITY MODE				
		Security Mode : None				
		WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)				
		Enable : ☒ Current PIN: 86844840 Reset PIN to Default Generate New PIN Process WPS				

Repeater Mode

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. You may also set up a specific time range (schedule). Select a schedule from the drop-down menu or click **Add New** to create a new schedule.

Wireless Mode: Select **Repeater Mode** from the drop-down menu.

Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the default network name.

Channel Width: Select the appropriate channel width between **20MHz** or **Auto 20/40MHz** from the drop-down menu.

Security Mode: Select **WEP** or **WPA Personal**.

The screenshot displays the configuration interface for a wireless repeater. It is divided into three main sections:

- WIRELESS NETWORK SETTINGS:** This section includes an "Enable Wireless" checkbox which is checked. Below it, the "Wireless Mode" is set to "Repeater Mode", with a "Site Survey" button to its right. The "Wireless Network Name" is set to "dlink" (noted as also called the SSID). The "Channel Width" is set to "Auto 20/40 MHz".
- WIRELESS SECURITY MODE:** This section shows the "Security Mode" dropdown menu, which is currently open, displaying options: "None", "WEP", and "WPA Personal".
- WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA):** This section has an "Enable" checkbox checked. It shows the "Current PIN" as "86844840". At the bottom, there are three buttons: "Reset PIN to Default", "Generate New PIN", and "Process WPS".

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-605L offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

Configure WEP

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 Wireless Setup on the left side.

2. In the **Security Mode** section, select **WEP** from the drop-down menu.

3. In **WEP Key Length**, select either 64Bit or 128Bit encryption from the drop-down menu.

5. Next to **WEP Key 1**, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using Hex or ASCII. Hex is recommended (letters A-F and numbers 0-9 are valid). In ASCII all numbers and letters are valid.

6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.

The screenshot shows the 'WIRELESS SECURITY MODE' configuration page. At the top, 'Security Mode' is set to 'WEP'. Below this, the 'WEP' section provides detailed instructions: 'WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.' It also states: 'You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.' A warning follows: 'If you choose the WEP security option this device will **ONLY** operate in **Legacy Wireless mode (802.11B/G)**. This means you will **NOT** get 11N performance due to the fact that WEP is not supported by the Draft 11N specification.' The configuration fields show 'WEP Key Length' set to '64 bit (10 hex digits)', 'WEP Key 1' as an empty text box, and 'Authentication' set to 'Both'. At the bottom, the 'WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)' section has 'Enable' checked, 'Current PIN' as '86844840', and three buttons: 'Reset PIN to Default', 'Generate New PIN', and 'Process WPS'.

WIRELESS SECURITY MODE

Security Mode : WEP

WEP

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

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

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

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

WEP Key 1 :

Authentication : Both

WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN: 86844840

Reset PIN to Default Generate New PIN Process WPS

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless access point 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 access point (192.168.0.50). Click on Setup and then click Wireless Settings on the left side.
2. Next to *Security Mode*, select **WPA-Personal**.
3. Next to *Cipher Type*, select **TKIP**, **AES**, or **Auto**.
4. Next to *Passphrase*, enter a key. The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The passphrase must be between 8-63 characters.
6. Click **Save Settings** at the top of the window to save your settings. If you are configuring the access point 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 access point.

WIRELESS SECURITY MODE

Security Mode : WPA-Personal ▼

WPA

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

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

WPA Mode : Auto (WPA or WPA2) ▼

Cipher Type : TKIP and AES ▼

PRE-SHARED KEY

Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN: 86844840

Reset PIN to Default

Generate New PIN

Process WPS

LAN Settings

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

Device Name: Enter the Device Name of the AP. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.

LAN Connection Type: Use the drop-down menu to select Dynamic IP (DHCP) to automatically obtain an IP address on the LAN/private network.

My IPv6 Connection Type: Select from the drop-down menu the type of IPv6 connection you would like to use.

IP Address: Enter the IP address of the access point. The default IP address is 192.168.0.50. 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 assigned by your ISP.

Gateway Address: Enter the Gateway assigned by your ISP.

DIR-505 // Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
SETUP WIZARD WIRELESS SETUP LAN SETUP	NETWORK SETTINGS Use this section to configure the internal network settings of your AP. Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. Recommend to change the device name if there're more than one D-Link devices within the subnet. Save Settings Don't Save Settings				Helpful Hints... Device Name: Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the device configuration. Recommend to change the device name if there're more than one D-Link devices within the network. LAN Settings: Also referred as private settings. LAN settings allow you to configure LAN interface of DIR-505. LAN IP address is private to your internal network and is not visible to Internet. The factory default setting is Dynamic IP(DHCP).
DEVICE NAME Device Name : dlinkrouter					
LAN IPV4 CONNECTION TYPE Choose the IPv4 mode to be used by the Access Point. My LAN Connection is : Dynamic IP (DHCP)					
DYNAMIC IP(DHCP) LAN IPV4 CONNECTION TYPE Enter the IPv4 Address Information. IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0 Gateway Address : 0.0.0.0 Primary DNS Server : 0.0.0.0 Secondary DNS Server : 0.0.0.0					

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 Access point will not accept the IP address if it is not in this format.

Device Name: Enter the Device Name of the AP. It recommended to change the Device Name if there is more than one D-Link device within the subnet. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. If you are using the device name to connect, ensure that your PC and your DIR-505 are on the same network.

LAN Connection Type: Select Static IP from the drop-down menu.

IP Address: Enter the IP address of the access point. The default IP address is 192.168.0.50. 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 assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

DIR-505 // Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
SETUP WIZARD WIRELESS SETUP LAN SETUP	NETWORK SETTINGS Use this section to configure the internal network settings of your AP. Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. Recommend to change the device name if there're more than one D-Link devices within the subnet. Save Settings Don't Save Settings				Helpful Hints... Device Name: Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the device configuration. Recommend to change the device name if there're more than one D-Link devices within the network. LAN Settings: Also referred as private settings. LAN settings allow you to configure LAN interface of DIR-505. LAN IP address is private to your internal network and is not visible to Internet. The factory default setting is Dynamic IP (DHCP).
DEVICE NAME Device Name : linkrouter					
LAN IPV4 CONNECTION TYPE Choose the IPV4 mode to be used by the Access Point. My LAN Connection is : Static IP					
STATIC IP ADDRESS LAN IPV4 CONNECTION TYPE Enter the static address Information. IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0 Gateway Address : 0.0.0.0 Primary DNS Server : 0.0.0.0 Secondary DNS Server : 0.0.0.0					

Advanced

Advanced Wireless

Transmit Power: Sets the transmit power of the antennas.

HT 20/40 Coexistence: Check to enable or disable this feature.

DIR-505 Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADVANCED WIRELESS	ADVANCED WIRELESS				Helpful Hints... Advanced Wireless: It is recommended that you leave these options at their default values. Adjusting them could negatively impact the performance of your wireless network. The options on this page should be changed by advanced users or if you are instructed to by one of our support personnel, as they can negatively
WI-FI PROTECTED SETUP	These options are for users that wish to change the behaviour of their 802.11n wireless radio from the standard setting. D-link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments. Save Settings Don't Save Settings ADVANCED WIRELESS SETTINGS Transmit Power : 100% HT20/40 Coexistence : ☒ Enable ☐ Disable				

Wi-Fi Protected Setup

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: Check this box to enable the function

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: Press the button to generate a new PIN or Reset to Default.

Current PIN: Shows the current value of the router’s PIN.

Reset PIN to Default: Restore the default PIN of the access point.

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.

Add Wireless Station: Press the button to start with the wizard to setup the WPS.

DIR-505 // Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADVANCED WIRELESS	WI-FI PROTECTED SETUP Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method. If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN. However, if the new PIN is not saved, it will get lost when the device reboots or loses power. Save Settings Don't Save Settings				Helpful Hints... Enable if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup. Click Add Wireless Device Wizard to use Wi-Fi Protected Setup to add wireless devices to the wireless network.
WI-FI PROTECTED SETUP	WI-FI PROTECTED SETUP Enable : ☒ Lock Wireless Security Settings : ☐ Reset to Unconfigured				
	PIN SETTINGS Current PIN: 86844840 Reset PIN to Default Generate New PIN				
	ADD WIRELESS STATION Add Wireless Device With WPS				

Maintenance Admin

This page will allow you to change the Administrator password. The administrator password has read/write access.

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

Confirm Password: Enter the same password that you entered in the previous textbox in order to confirm its accuracy.

Enable Graphical Authentication: Check to enable this feature.

DIR-505 // Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	ADMINISTRATOR SETTINGS Enter the new password in the "New Password" field and again in the next field to confirm. Click on "Save Settings" to execute the password change. The Password is case-sensitive, and can be made up of any keyboard characters. The new password must be between 0 and 15 characters in length. Save Settings Don't Save Settings				Helpful Hints... Passwords: For security reasons, is recommended that you change the Password for the Administrator account. Be sure to write down the Passwords to avoid having to reset the in the event that they are forgotten.
SYSTEM	PASSWORD Please enter the same password into both boxes, for confirmation. New Password : Verify Password :				
FIRMWARE	ADMINISTRATION Enable Graphical Authentication : ☐				
TIME					

System

- Save to Local Hard Drive:

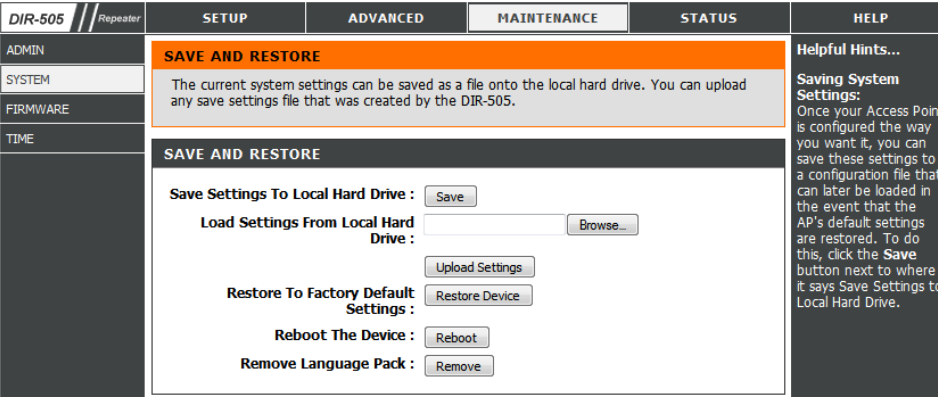
Use this option to save the current access point configuration settings to a file on the hard disk of the computer you are using. Click the **Save** button. You will then see a file dialog where you can select a location and file name for the settings.
- Upload from Local Hard Drive:

Use this option to load previously saved access point configuration settings. Click **Browse** to find a previously saved configuration file. Then, click the **Upload Settings** button to transfer those settings to the access point.
- Restore to Factory Default:

This option will restore all configuration settings back to the settings that were in effect at the time the access point 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 access point configuration settings, use the **Save** button above.
- Reboot the Device:

Click to reboot the access point.
- Note:

Restoring the factory default settings will not reset the Wi-Fi Protected Status to Not Configured.



Firmware

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

Firmware Upgrade: Click on **Check Now 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.

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

Language Pack

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

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

DIR-505 // Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	FIRMWARE There may be new firmware for your DIR-505 to improve functionality and performance. Click here to check for an upgrade on our support site. After you have download the new firmware file from our support site, click the Browse button below to find the firmware file on your local hard drive. Click the Upload button to update the firmware on the DIR-505. Do not update firmware through wireless network!!				Helpful Hints... Firmware Updates: Firmware updates are released periodically to improve the functionality of your Access Point and also to add features. If you run into a problem with a specific feature of the Access Point, check our support site by clicking on the Click here to check for an upgrade on our support site link and see if an updated firmware is available for your Access Point.
SYSTEM					
FIRMWARE					
TIME					
FIRMWARE AND LANGUAGE PACK INFORMATION Current Firmware Version : 1.00beta Date : 2011/12/12 Current Language Pack Version : No Language pack Check Online Now for Latest Firmware and Language pack Version : Check Now					
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 Maintenance -> System screen To upgrade the firmware, your PC must have a wired connection to the access point. Enter the name of the firmware upgrade file, and click on the Upload button. Upload : Browse... Upload					
LANGUAGE PACK UPGRADE Upload : Browse... Upload					

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. 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, click the **Enable Daylight Saving** check box. Next use the drop-down menu to select a Daylight Saving Offset and then 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.

Date and Time: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Save Settings**. You can also click the **Copy Your Computer's Time Settings** button at the bottom of the screen.

DIR-505 // Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	TIME				Helpful Hints... System Time Settings: This section allows admins to configure, update, and maintain the correct time on the Access Point's internal system clock.
SYSTEM	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				
FIRMWARE	TIME CONFIGURATION Current Time : Jan/01/2011 00:20:35 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 am DST End : Nov 2nd Sun 1 am				
TIME	AUTOMATIC TIME CONFIGURATION Enable NTP Server : ☐ NTP Server Used : << Select NTP Server >>				
SET THE DATE AND TIME MANUALLY Date And Time : Year 2011 Month Jan Day 01 Hour 00 Minute 00 Second 00 Copy Your Computer's Time Settings					

Status

Device Info

This page displays the current information for the DIR-505. It will display the LAN and wireless LAN information.

General: Displays the access point's time and firmware version.

LAN: Displays the MAC address and the private (local) IP settings for the access point.

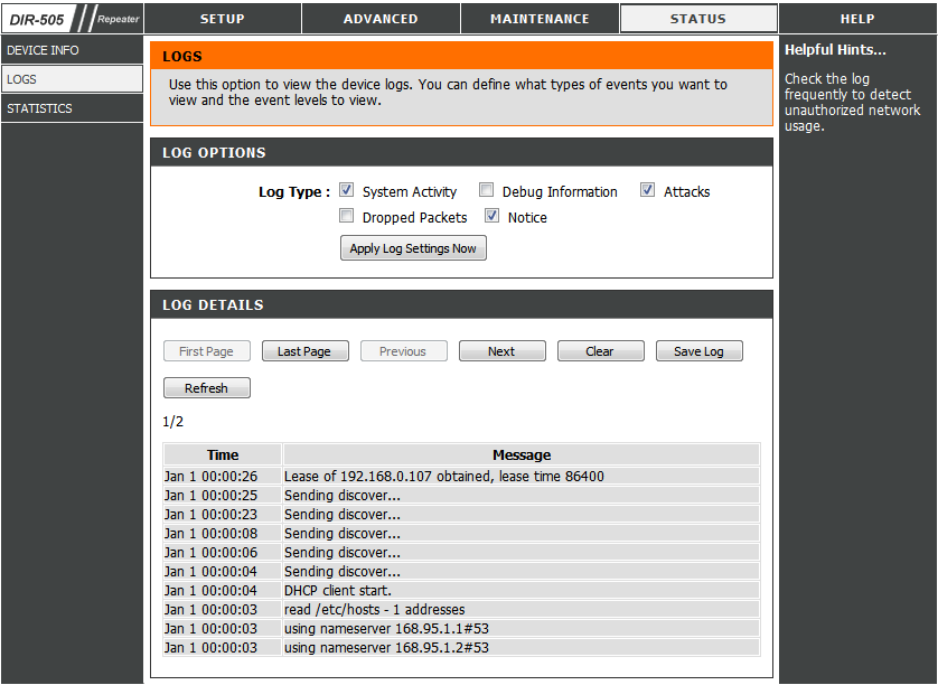
Wireless LAN: Displays the wireless MAC address and your wireless settings such as SSID and Channel.

DIR-505 // Repeater	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
DEVICE INFO	DEVICE INFORMATION				Helpful Hints... All of your LAN and Wireless connection details are displayed here.
LOGS	All of your wireless and network connection details are displayed on this page. The firmware version is also displayed here.				
STATISTICS					
	GENERAL				
	Time : Jan/01/2011 00:21:06 Firmware Version : 1.00beta, Mon, 12 Dec 2011				
	LAN				
	MAC Address : 00:18:e7:95:6d:d0 Connection : Dynamic IP IP Address : 192.168.0.107 Subnet Mask : 255.255.255.0 Gateway Address : 192.168.0.1 Primary DNS Server : 192.168.0.1 Secondary DNS Server : 0.0.0.0				
	WIRELESS LAN				
	MAC Address : 00:18:e7:95:6d:d0 Network Name (SSID) : dlink Security Mode : Disable				

Logs

The DIR-505 keeps a running log of events and activities occurring on the AP. If the AP is rebooted, the logs are automatically cleared. You can save the log files under Log Setting.

- Log Options:** There are several types of logs that can be viewed: **System Activity, Debug Information, Attacks, Dropped Packets** and **Notice**.
- First Page:** This button directs you to the first page of the log.
- Last Page:** This button directs you to the last page of the log.
- Previous Page:** This button directs you to the previous page of the log.
- Next Page:** This button directs you to the next page of the log.
- Clear Log:** This button clears all current log content.
- Log Settings:** This button opens a new menu where you can configure the log settings.
- Refresh:** This button refreshes the log.



Statistics

The DIR-505 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the access point is rebooted.

DIR-505 // Repeater

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

DEVICE INFO

LOGS

STATISTICS

TRAFFIC STATISTICS

Traffic Statistics display Receive and Transmit packets passing through your router.

Refresh Statistics

Clear Statistics

LAN STATISTICS

Sent : 329	Received : 249
TX Packets Dropped : 0	RX Packets Dropped : 0
Collisions : 0	Errors : 0

WIRELESS STATISTICS

Sent : 34	Received : 0
TX Packets Dropped : 31	RX Packets Dropped : 0
Collisions : 0	Errors : 0

Helpful Hints...

This is a summary of the number of packets that have passed between the Wireless and the LAN since the device was last initialized.

Quick Setup Wizard

WiFi Hot Spot

If this is your first time using this device, you will be directed to the Pre-Setup Wizard. If you have already completed the Pre-Setup Wizard, please continue to page 88.

Enter **Admin** in the User Name field. Leave the password blank by default.

Click Next to continue.

Please wait while your device scans for an available Wi-Fi Network.

LOGIN

Log in to the HotSpot:

User Name :

Admin

Password :

Login

WI-FI CONNECTION SETUP WIZARD

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

Next

Cancel

SELECT WI-FI NETWORK

Scanning for available Wi-Fi network...

Prev

Next

Cancel

Select the Network you would like your device to connect to and click **Connect**.

SELECT WI-FI HOTSPOT

ID	Wi-Fi Network Name	Encrypt	Channel	Signal(%)	Select
1	DHP-W306AV	WPA/WPA2-PSK(auto)	8	94	☐
2	dlink_DHP-1565	WPA/WPA2-PSK(auto)	6	94	☐
3	LoudFish	WPA/WPA2-PSK(auto)	11	94	☐
4	LoudFish-guest	None	11	94	☐
5	irvine2	WPA/WPA2-PSK(auto)	6	82	☐
6	ATT720	WPA/WPA2-PSK(auto)	1	3	☐

Rescan
Connect
Cancel

Enter the Wi-Fi password and click **Next** to continue.

ENTER WI-FI PASSWORD

Please enter Wi-Fi Password to establish wireless connection

Wi-Fi Password:

Prev
Next
Cancel

Select **Use the same Wi-Fi Network name for the extended Network** and click **Next**.

PLEASE ENTER THE SETTINGS FOR THE EXTENDER NETWORK

☒ Use the same Wi-Fi Network Name for the Extended Network

Wi-Fi Network Name (SSID): DHP-W306AV

Prev
Next
Cancel

Your setup is now complete. Click **Save** to finish.

SETUP COMPLETE!

Please take a note of the following summary of your Wi-Fi Security settings for future reference.

Wi-Fi Network Name (SSID) : DHP-W306AV

Wi-Fi Password : dlink1234

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

Prev
Save
Cancel

To start the Wizard, click **Next** to continue.

WI-FI CONNECTION SETUP WIZARD

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

Next

Cancel

Please wait while your device scans for an available Wi-Fi Network.

SELECT WI-FI NETWORK

Scanning for available Wi-Fi network...

Prev

Next

Cancel

Select the Network you would like your device to connect to and click **Connect**.

SELECT WI-FI HOTSPOT

ID	Wi-Fi Network Name	Encrypt	Channel	Signal(%)	Select
1	DHP-W306AV	WPA/WPA2-PSK(auto)	8	94	☐
2	dlink_DHP-1565	WPA/WPA2-PSK(auto)	6	94	☐
3	LoudFish	WPA/WPA2-PSK(auto)	11	94	☐
4	LoudFish-guest	None	11	94	☐
5	irvine2	WPA/WPA2-PSK(auto)	6	82	☐
6	ATT720	WPA/WPA2-PSK(auto)	1	3	☐

Rescan

Connect

Cancel

Enter the Wi-Fi password and click **Next** to continue.

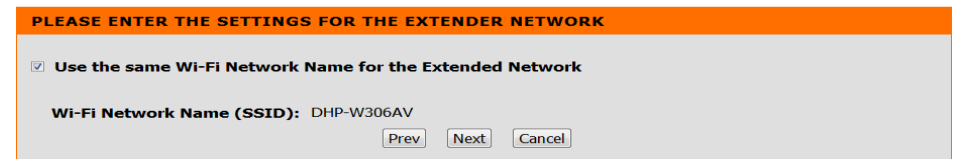


ENTER WI-FI PASSWORD

Please enter Wi-Fi Password to establish wireless connection

Wi-Fi Password:

Select **Use the same Wi-Fi Network name for the extended Network** and click **Next**.

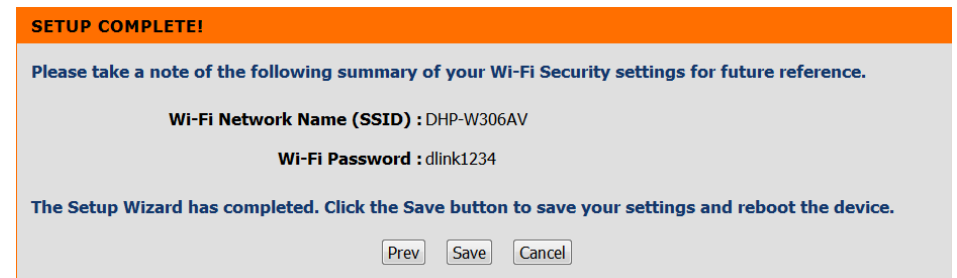


PLEASE ENTER THE SETTINGS FOR THE EXTENDER NETWORK

☒ **Use the same Wi-Fi Network Name for the Extended Network**

Wi-Fi Network Name (SSID): DHP-W306AV

Your setup is now complete. Click **Save** to finish.



SETUP COMPLETE!

Please take a note of the following summary of your Wi-Fi Security settings for future reference.

Wi-Fi Network Name (SSID) : DHP-W306AV

Wi-Fi Password : dl1nk1234

The Setup Wizard has completed. Click the **Save** button to save your settings and reboot the device.

Setup

Wi-Fi Hot Spot Setup

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. You may also set up a specific time range (schedule). Select a schedule from the drop-down menu or click **Add New** to create a new schedule.

Wireless Mode: Select **Wi-Fi Hot Spot Mode** from the drop-down menu.

Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID. For security purposes, it is highly recommended to change from the default network name.

Channel Width: Select the appropriate channel width between **20MHz** or **Auto 20/40MHz** from the drop-down menu.

Security Mode: Select **WEP** or **WPA Personal**.

DIR-505

HotSpot

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

SETUP WIZARD

WI-FI HOTSPOT SETUP

WIRELESS SETUP

LAN SETUP

WIRELESS

Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC.

Save Settings

Don't Save Settings

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Mode : Wi-Fi HotSpot Mode

Site Survey

Wireless Network Name : dlink (Also called the SSID)

Channel Width : Auto 20/40 MHz

WIRELESS SECURITY MODE

Security Mode : None

WAN SETTINGS

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

My Internet Connection is : Dynamic IP (DHCP)

Host Name : DIR-505

MTU : 1500

☒ Attain DNS Automatically

☐ Set DNS Manually

MAC Address : 00:00:00:00:00:00

Clone Your PC's MAC address

WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN : 69747786

Reset PIN to Default

Generate New PIN

Process WPS

Helpful Hints...

Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

Enable Auto Channel Scan so that the Access Point can select the best possible channel for your wireless network to operate on.

Visibility Status is another way to secure your network. With invisible option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device.

If you have enabled Wireless Security, make sure you write down the Key or Passphrase that you have configured. You will need to enter this information on any wireless device that you connect to your wireless network.

D-Link DIR-505 User Manual

90

Please Select the Wi-Fi Hotspot you would like to connect to with your device.

SELECT WI-FI HOTSPOT

ID	SSID	Encrypt	Channel	Signal(%)	Select
1	DHP-W306AV	WPA/WPA2-PSK(auto)	8	94	☐
2	dlink_DHP-1565	WPA/WPA2-PSK(auto)	6	94	☐
3	LoudFish	WPA/WPA2-PSK(auto)	11	94	☐
4	LoudFish-guest	None	11	94	☐
5	irvine2	WPA/WPA2-PSK(auto)	6	88	☐
6	Express Network	WPA/WPA2-PSK(auto)	11	87	☐
7	ATT720	WPA/WPA2-PSK(auto)	1	4	☐

Cancel

Connect

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless access point 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 access point (192.168.0.50). Click on Setup and then click Wireless Settings on the left side.
2. Next to *Security Mode*, select **WPA-Personal**.
3. Next to WPA Mode, select **Auto (WPA or WPA2)**.
4. Next to *Cipher Type*, select **TKIP, AES, or Auto**.
5. Next to *Passphrase*, enter a key. The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The passphrase must be between 8-63 characters.
7. Click **Save Settings** at the top of the window to save your settings. If you are configuring the access point 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 access point.

WIRELESS NETWORK SETTINGS

Enable Wireless : ☒

Wireless Mode : **Wi-Fi HotSpot Mode** [Site Survey](#)

Wireless Network Name : (Also called the SSID)

Channel Width :

WIRELESS SECURITY MODE

Security Mode :

WPA

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

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

WPA Mode :

Cipher Type :

PRE-SHARED KEY

Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

WAN Settings

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

My Internet Connection is: Use the drop-down menu to select Dynamic IP (DHCP) to automatically obtain an IP address on the LAN/private network.

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

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 SETTINGS

This page is used to configure the parameters for Internet network which connects to the WAN port of your Access Point. Here you may change the access method to Static IP, DHCP, PPPoE or PPTP by click the item value of WAN Access type.

My Internet Connection is :

Host Name :

MTU :

☒ **Attain DNS Automatically**

☐ **Set DNS Manually**

MAC Address :

WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN : 69747786

Wireless Setup

Extended SSID: Use the drop-down menu to select Dynamic IP (DHCP) to automatically obtain an IP address on the LAN/private network.

Channel Width: **20MHz** - Select if you are not using any 802.11n wireless clients.
40MHz - Select if you are using 802.11n wireless clients only.

Security Mode: Select from the drop-down menu the type of security mode you would like to use.

DIR-505 // HotSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
SETUP WIZARD WI-FI HOTSPOT SETUP WIRELESS SETUP LAN SETUP	WIRELESS Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made on this section will also need to be duplicated to your wireless clients and PC. Save Settings Don't Save Settings WIRELESS NETWORK SETTINGS Extended SSID : ☐ Remain the same as SSID ☒ Create Extended SSID dlink_hotspot Wireless Network Name : dlink Channel Width : Auto 20/40 MHz WIRELESS SECURITY MODE Security Mode : None WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA) Enable : ☒ Current PIN : 69747786 Reset PIN to Default Generate New PIN Process WPS				Helpful Hints... Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information. Enable Auto Channel Scan so that the Access Point can select the best possible channel for your wireless network to operate on. Visibility Status is another way to secure your network. With invisible option enabled, no wireless clients will be able to see your wireless network when they perform scan to see what's available. In order for your wireless devices to connect to your AP, you will need to manually enter the Wireless Network Name on each device. If you have enabled

Manual Wireless Settings

Extended SSID: Select **Remain the same as SSID** or **Create Extended SSID**.

Channel Width: **20MHz** - Select if you are not using any 802.11n wireless clients.

40MHz - Select if you are using 802.11n wireless clients only.

Security Mode: Select from the drop-down menu the type of security mode you would like to use.

WPA Mode: Select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

Cipher Type: Select **TKIP and AES**, **TKIP**, or **AES**.

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.

WIRELESS NETWORK SETTINGS

Extended SSID : ☐ Remain the same as SSID
☒ Create Extended SSID

dlink_hotspot

Wireless Network Name : dlink

Channel Width : Auto 20/40 MHz

WIRELESS SECURITY MODE

Security Mode : WPA-Personal

WPA

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

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

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

PRE-SHARED KEY

Enter an 8 to 63 character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key :

WIFI PROTECTED SETUP (ALSO CALLED WCN 2.0 IN WINDOWS VISTA)

Enable : ☒

Current PIN : 69747786

Reset PIN to Default

Generate New PIN

Process WPS

LAN Setup

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

Device Name: Enter the Device Name of the AP. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.

LAN Connection Type: Use the drop-down menu to select Dynamic IP (DHCP) to automatically obtain an IP address on the LAN/private network.

IP Address: Enter the IP address of the access point. The default IP address is 192.168.0.50. 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 assigned by your ISP.

Gateway Address: Enter the Gateway assigned by your ISP.

DIR-505 HotSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
SETUP WIZARD	NETWORK SETTINGS Use this section to configure the internal network settings of your AP. Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. Recommend to change the device name if there're more than one D-Link devices within the subnet. Save Settings Don't Save Settings				Helpful Hints... Device Name: Device Name allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the device configuration. Recommend to change the device name if there're more than one D-Link devices within the network. LAN Settings: Also referred as private settings. LAN settings allow you to configure LAN interface of DIR-505. LAN IP address is private to your internal network and is not visible to Internet. The factory default setting is Dynamic IP(DHCP).
WI-FI HOTSPOT SETUP					
WIRELESS SETUP					
LAN SETUP					
DEVICE NAME Device Name allows you to configure this device more easily. You can enter "http://device name" into your web browser instead of IP address for configuration. (Default: http://dlinkap) Device Name : dlinkrouter					
LAN IPV4 CONNECTION TYPE Choose the IPv4 mode to be used by the Access Point. My LAN Connection is : Static IP					
DYNAMIC IP (DHCP) LAN CONNECTION TYPE Enter the IPv4 Address Information. IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0 Gateway Address : 192.168.0.1 Primary DNS Server : 0.0.0.0 Secondary DNS Server : 0.0.0.0					
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 : 192.168.0.100 to 192.168.0.199 DHCP Lease Time : 1440 (minutes)					

Advanced

Advanced Wireless

Transmit Power: Sets the transmit power of the antennas.

HT 20/40 Coexistence: Check to enable or disable this feature.

DIR-505HotSpot

SETUPADVANCEDMAINTENANCESTATUSHELP

ADVANCED WIRELESS

ADVANCED WIRELESS

These options are for users that wish to change the behaviour of their 802.11n wireless radio from the standard setting. D-link does not recommend changing these settings from the factory default. Incorrect settings may impair the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

Save SettingsDon't Save Settings

ADVANCED WIRELESS SETTINGS

Transmit Power : 100%

HT20/40 Coexistence : ☒ Enable ☐ Disable

Helpful Hints...

Advanced Wireless:

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

The options on this page should be changed by advanced users or if you are instructed to by one of our support personnel, as they can negatively affect the performance of your Access Point if configured improperly.

Transmit Power:

You can lower the output power of the DIR-505 by selecting lower percentage Transmit Power values from the drop down. Your choices are: 100%, 75%, 50%, and 25%.

Maintenance Admin

This page will allow you to change the Administrator password. The administrator password has read/write access.

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

Confirm Password: Enter the same password that you entered in the previous textbox in order to confirm its accuracy.

Enable Check to enable this feature.

**Graphical
Authentication:**

DIR-505 // HotSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	ADMINISTRATOR SETTINGS Enter the new password in the "New Password" field and again in the next field to confirm. Click on "Save Settings" to execute the password change. The Password is case-sensitive, and can be made up of any keyboard characters. The new password must be between 0 and 15 characters in length. Save Settings Don't Save Settings				Helpful Hints... Passwords: For security reasons, it is recommended that you change the Password for the Administrator accounts. Be sure to write down the Passwords to avoid having to reset the AP in the event that they are forgotten.
SYSTEM	PASSWORD Please enter the same password into both boxes, for confirmation. New Password : Verify Password :				
FIRMWARE	ADMINISTRATION Enable Graphical Authentication : ☐				
TIME					

System

Save to Local Hard Drive: Use this option to save the current access point configuration settings to a file on the hard disk of the computer you are using. Click the **Save** button. You will then see a file dialog where you can select a location and file name for the settings.

Upload from Local Hard Drive: Use this option to load previously saved access point configuration settings. Click **Browse** to find a previously saved configuration file. Then, click the **Upload Settings** button to transfer those settings to the access point.

Restore to Factory Default: This option will restore all configuration settings back to the settings that were in effect at the time the access point 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 access point configuration settings, use the **Save** button above.

Note: Restoring the factory default settings will not reset the Wi-Fi Protected Status to Not Configured.

Reboot the Device: Click to reboot the access point.

DIR-505 // HotSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	SAVE AND RESTORE				Helpful Hints... Saving System Settings: Once your Access Point is configured the way you want it, you can save these settings to a configuration file that can later be loaded in the event that the AP's default settings are restored. To do this, click the Save button next to where it says Save Settings to Local Hard Drive.
SYSTEM	The current system settings can be saved as a file onto the local hard drive. You can upload any save settings file that was created by the DIR-505.				
FIRMWARE	SAVE AND RESTORE				
TIME	Save Settings To Local Hard Drive : Save Load Settings From Local Hard Drive : Choose File No file chosen Upload Settings Restore To Factory Default Settings : Restore Device Reboot The Device : Reboot Remove Language Pack : Remove				

Firmware

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

Firmware Upgrade: Click on **Check Now 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.

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

Language Pack

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

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

DIR-505 // HotSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	FIRMWARE				Helpful Hints... Firmware Updates: Firmware updates are released periodically to improve the functionality of your Access Point and also to add features. If you run into a problem with a specific feature of the Access Point, check our support site by clicking on the Click here to check for an upgrade on our support site link and see if an updated firmware is available for your Access Point.
SYSTEM	There may be new firmware for your DIR-505 to improve functionality and performance. Click here to check for an upgrade on our support site. After you have download the new firmware file from our support site, click the Browse button below to find the firmware file on your local hard drive. Click the Upload button to update the firmware on the DIR-505. Do not update firmware through wireless network!!				
FIRMWARE	FIRMWARE AND LANGUAGE PACK INFORMATION Current Firmware Version : 1.00beta Date : 2011/12/12 Current Language Pack Version : No Language pack Check Online Now for Latest Firmware and Language pack Version : Check Now				
TIME	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 Maintenance -> System screen To upgrade the firmware, your PC must have a wired connection to the access point. Enter the name of the firmware upgrade file, and click on the Upload button. Upload : Choose File No file chosen Upload				

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. 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, click the **Enable Daylight Saving** check box. Next use the drop-down menu to select a Daylight Saving Offset and then 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.

Date and Time: To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Save Settings**. You can also click the **Copy Your Computer's Time Settings** button at the bottom of the screen.

DIR-505 // NoSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
ADMIN	TIME				Helpful Hints... System Time Settings: This section allows admins to configure, update, and maintain the correct time on the Access Point's internal system clock.
SYSTEM	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				
FIRMWARE	TIME CONFIGURATION Current Time : Jan/01/2011 01:02:48 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 am DST End : Nov 2nd Sun 1 am				
TIME	AUTOMATIC TIME CONFIGURATION Enable NTP Server : ☐ NTP Server Used : << Select NTP Server >>				
SET THE DATE AND TIME MANUALLY Date And Time : Year 2011 Month Jan Day 01 Hour 00 Minute 00 Second 00 Copy Your Computer's Time Settings					

Status

Device Info

This page displays the current information for the DIR-505. 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.

DIR-505 // HotSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP
DEVICE INFO LOGS STATISTICS	DEVICE INFORMATION All of your wireless and network connection details are displayed on this page. The firmware version is also displayed here.				Helpful Hints... All of your LAN and Wireless connection details are displayed here.
	GENERAL Time : Jan/01/2011 01:03:32 Firmware Version : 1.00beta, Mon, 12 Dec 2011				
	WI-FI HOTSPOT MAC Address : 02:18:e7:95:6d:ce Connection : DHCP 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				
	LAN MAC Address : 00:18:e7:95:6d:ce Connection : Static IP / DHCP Server IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0				
	WIRELESS LAN MAC Address : 00:18:e7:95:6d:ce Network Name (SSID) : dlink Extended Network Name : dlink_hotspot Security Mode : None Channel Width : Auto 20/40 MHz Channel : 1 Wi-Fi Protected Setup : Enable / Not Configured				

Logs

The DIR-505 keeps a running log of events and activities occurring on the AP. If the AP is rebooted, the logs are automatically cleared. You can save the log files under Log Setting.

Log Type: Use the radio buttons to select the types of messages that you want to display from the log. **System, Firewall & Security**, and **Router Status** messages can be selected.

Log Level: There are three levels of message importance: **Critical**, **Warning**, and **Information**. Select the levels that you want displayed in the log.

Log Files: Use this section to view and manage the Router's log entries.

First Page: Click this button to view the first page of the Router logs.

Last Page: Click this button to view the last page of the Router logs.

Previous: Click this button to view the previous page of the Router logs.

Next: Click this button to view the next page of the Router logs.

Clear: Clears all of the log contents.

DIR-505 // HotSpot	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP		
DEVICE INFO LOGS STATISTICS	LOGS Use this option to view the device logs. You can define what types of events you want to view and the event levels to view. LOG OPTIONS Log Type : ☒ System Activity ☒ Debug Information ☒ Attacks ☒ Dropped Packets ☒ Notice Apply Log Settings Now LOG DETAILS First Page Last Page Previous Next Clear Save Log Refresh 0/0 <table border="1"> <thead> <tr> <th>Time</th> <th>Message</th> </tr> </thead> <tbody> </tbody> </table>				Time	Message	Helpful Hints... Check the log frequently to detect unauthorized network usage.
Time	Message						

Statistics

The DAP-505 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network.

DIR-505

HotSpot

SETUP

ADVANCED

MAINTENANCE

STATUS

HELP

DEVICE INFO

LOGS

STATISTICS

TRAFFIC STATISTICS

Traffic Statistics display Receive and Transmit packets passing through your router.

Refresh Statistics

Clear Statistics

LAN STATISTICS

Sent : 3557

TX Packets Dropped : 0

Collisions : 0

Received : 4799

RX Packets Dropped : 0

Errors : 0

WIRELESS STATISTICS

Sent : 5248

TX Packets Dropped : 0

Collisions : 0

Received : 4798

RX Packets Dropped : 0

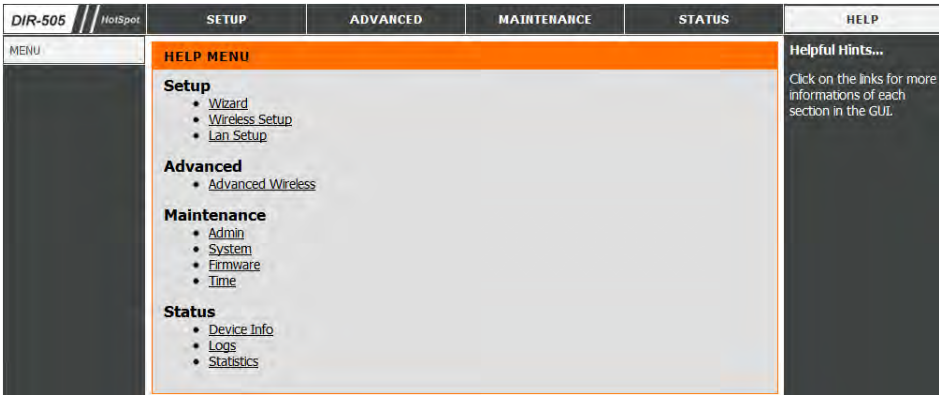
Errors : 0

Helpful Hints...

This is a summary of the number of packets that have passed between the Wireless and the LAN since the device was last initialized.

Help

Click the desired hyperlink to get more information about how to use the Router.



Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DIR-505 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-505 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

WPA/WPA2

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

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



Wireless Icon

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

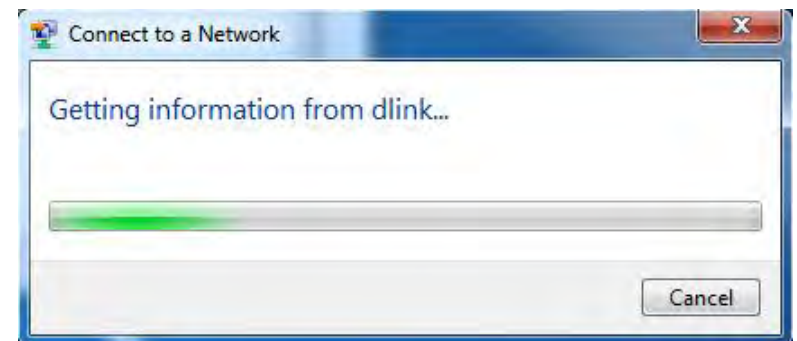


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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.



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

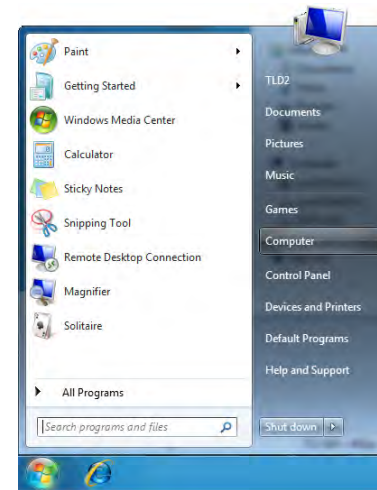
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



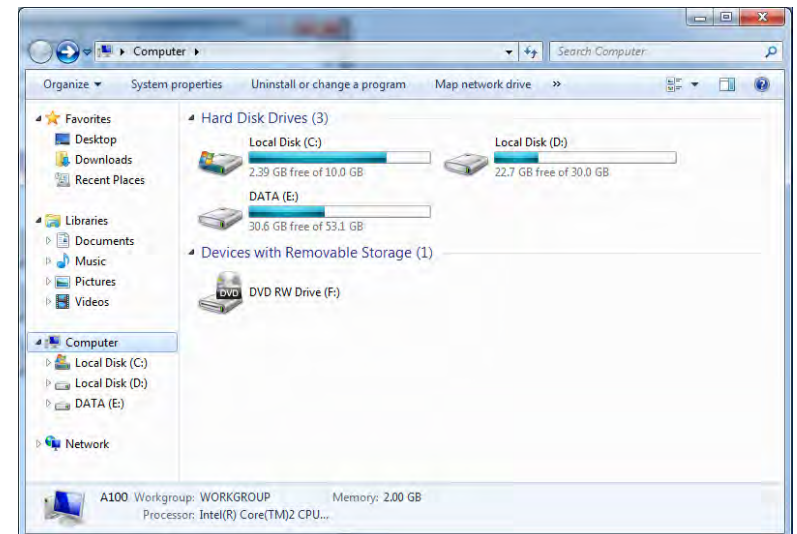
WPS

The WPS feature of the DIR-505 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

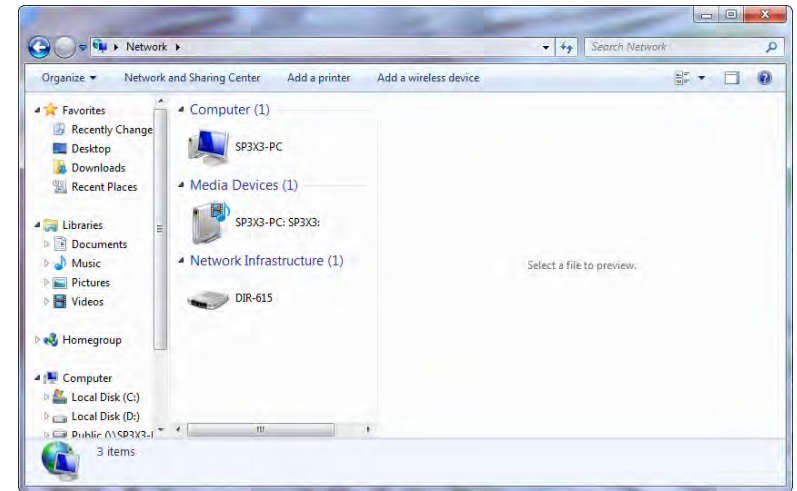
1. Click the **Start** button and select **Computer** from the Start menu.



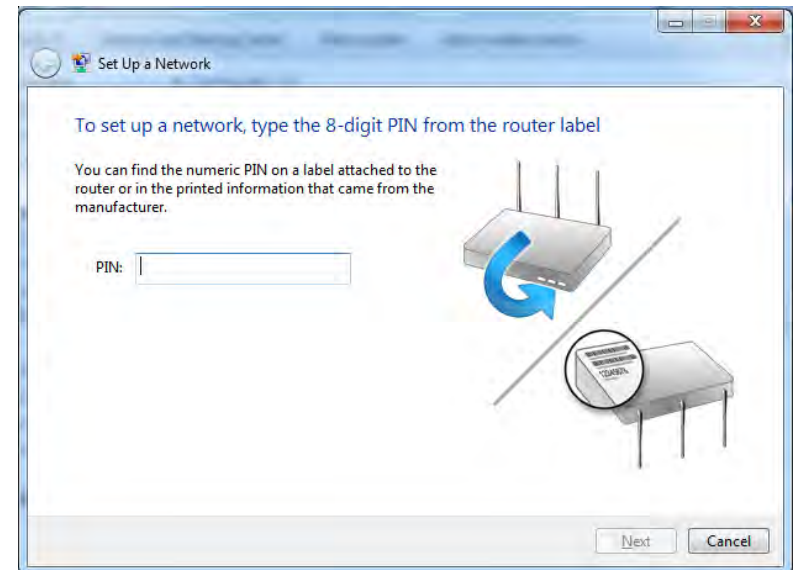
2. Click **Network** on the left side.



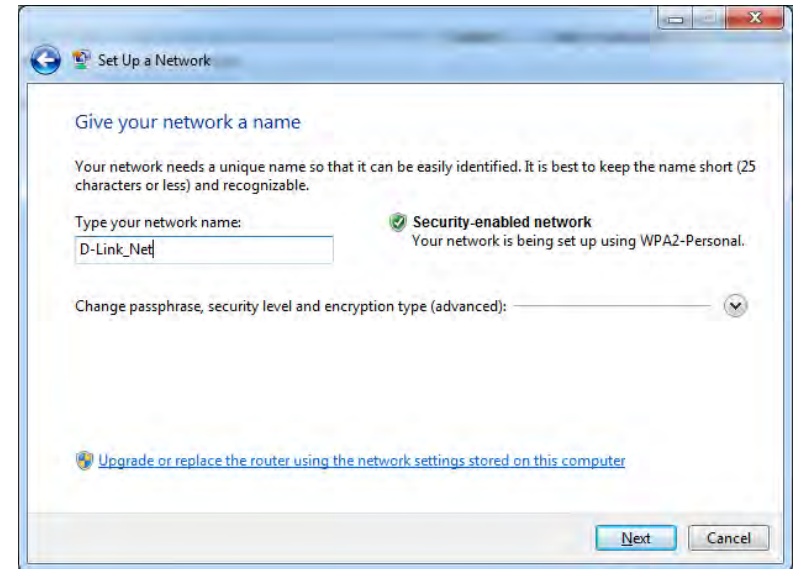
3. Double-click the DIR-505.



4. Input the WPS PIN number (displayed in the WPS window on the Router's LCD screen or in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.

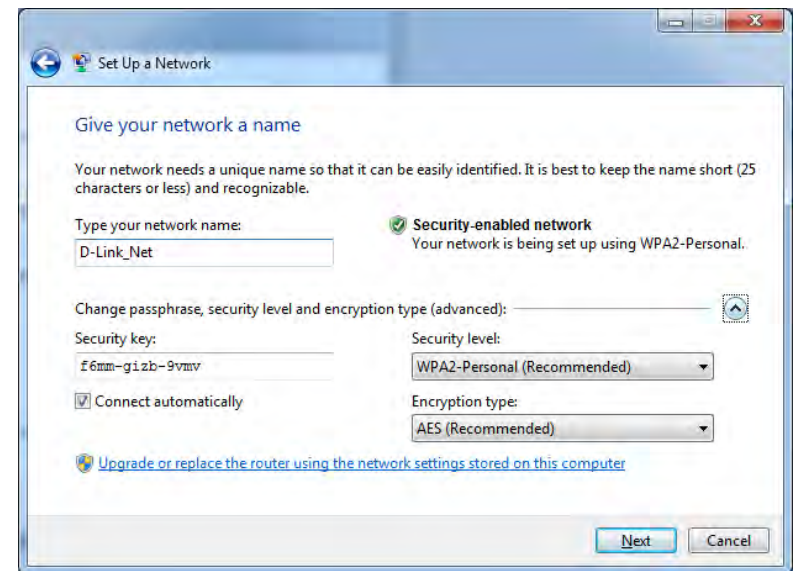


5. Type a name to identify the network.



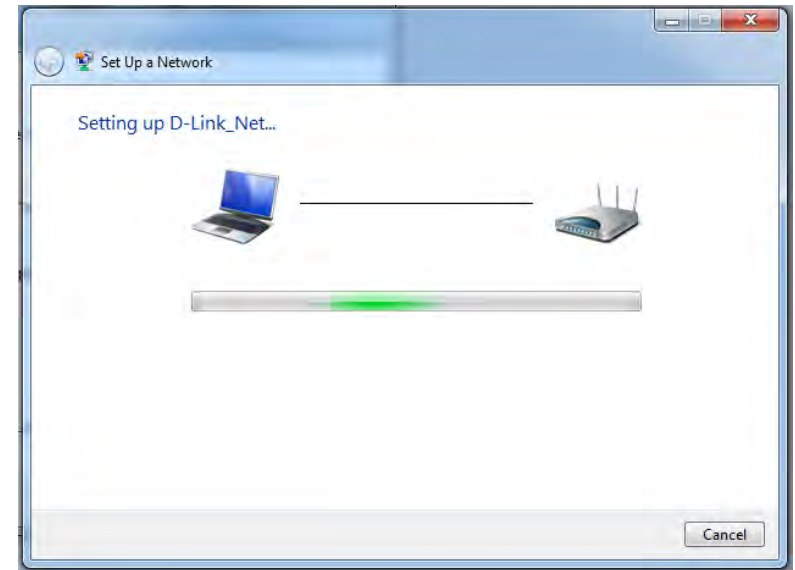
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



7. The following window appears while the Router is being configured.

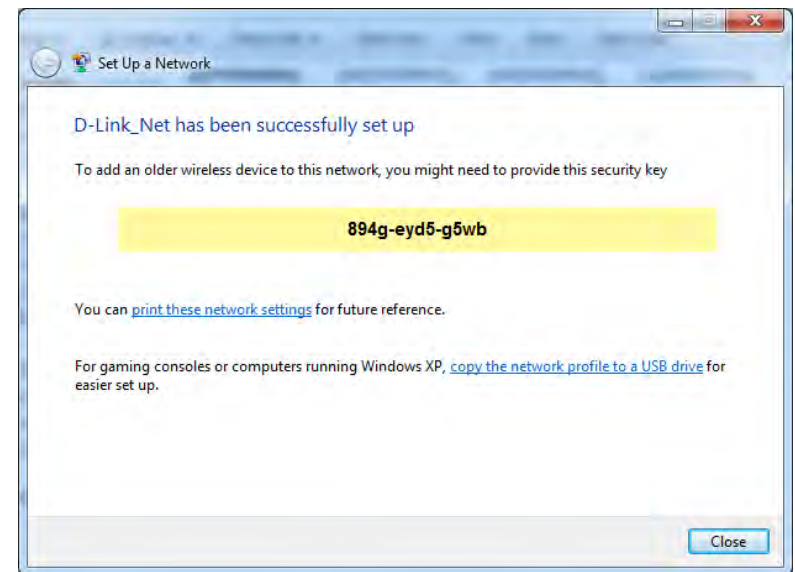
Wait for the configuration to complete.



8. The following window informs you that WPS on the router has been setup successfully.

Make a note of the security key as you may need to provide this security key if adding an older wireless device to the network in the future.

9. Click **Close** to complete WPS setup.



Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows Vista® utility as seen below.

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

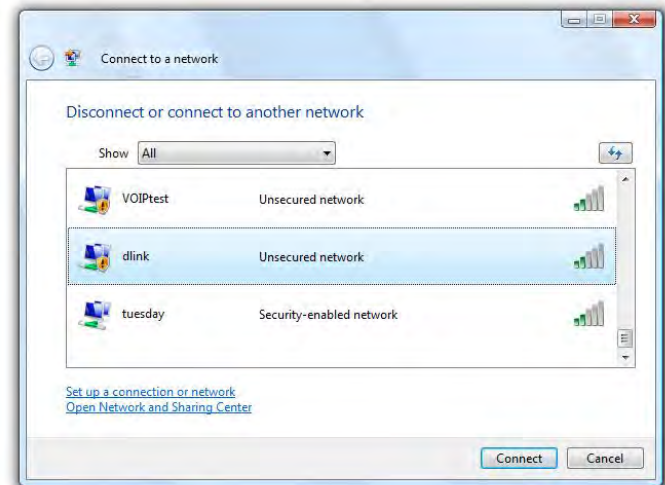
or

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



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

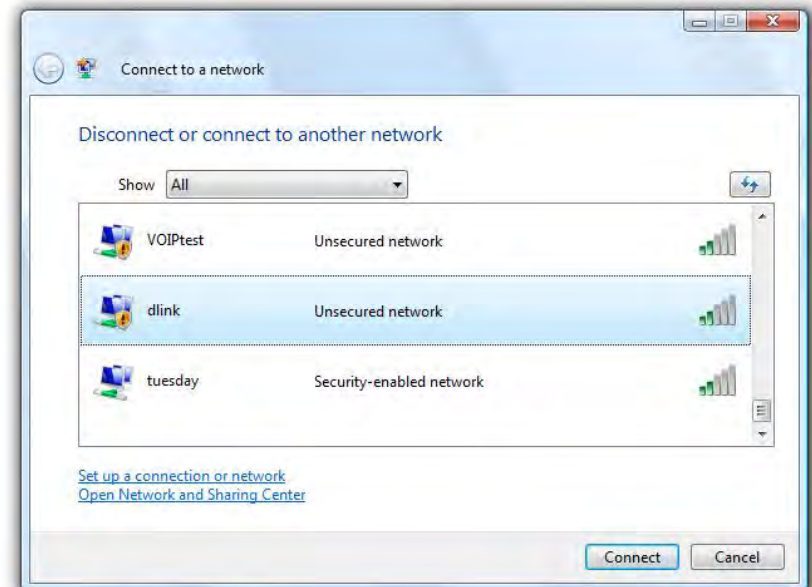
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

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

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.
2. Highlight the 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.



WPS/WCN 2.0

The router supports Wi-Fi protection, referred to as WCN 2.0 in Windows Vista®. The following instructions for setting this up depends on whether you are using Windows Vista® to configure the router or third party software.

When you first set up the router, Wi-Fi protection is disabled and unconfigured. To enjoy the benefits of Wi-Fi protection, the router must be both enabled and configured. There are three basic methods to accomplish this: use Windows Vista's built-in support for WCN 2.0, use software provided by a third party, or manually configure.

If you are running Windows Vista®, log into the router and click the **Enable** checkbox in the **Basic > Wireless** section. Use the Current PIN that is displayed on the **Advanced > Wi-Fi Protected Setup** section or choose to click the **Generate New PIN** button or **Reset PIN to Default** button.



If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Windows® XP

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

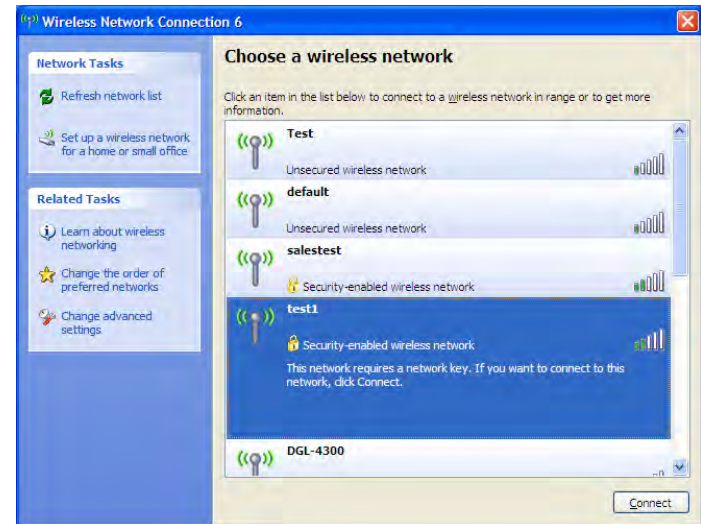
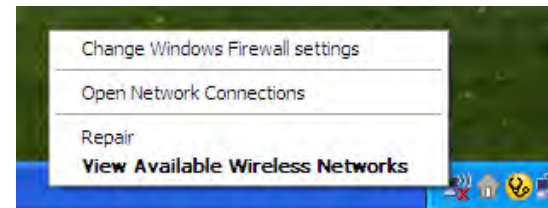
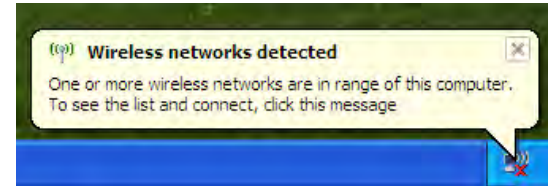
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

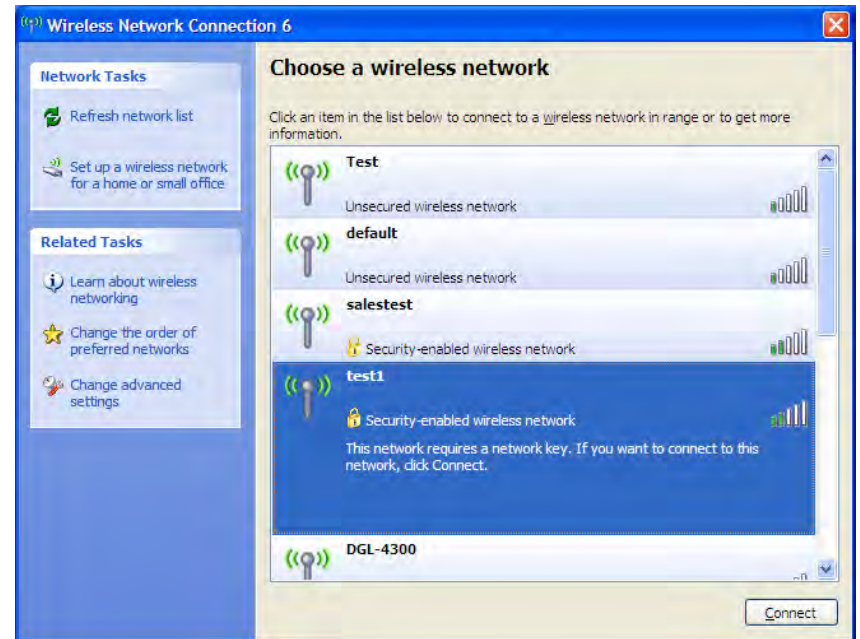
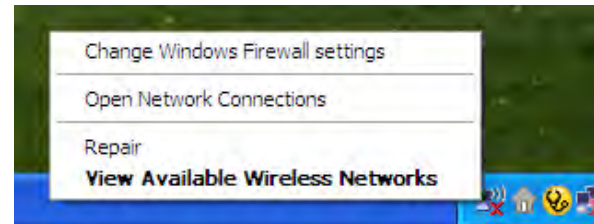
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

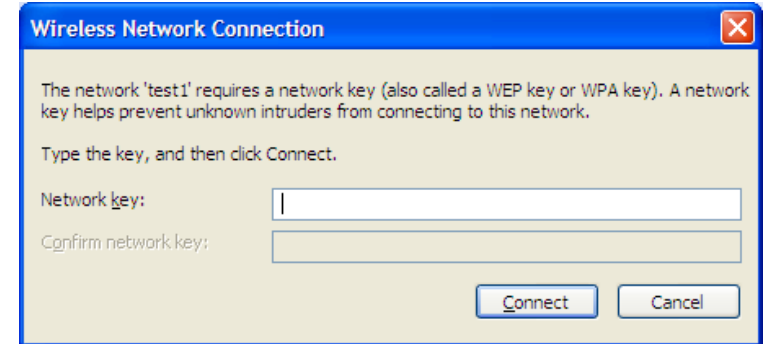
It is recommended to enable WPA on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the WPA key being used.

1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.
2. Highlight the 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-505. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Microsoft Internet Explorer® 6.0 and higher
 - Mozilla Firefox 3.0 and higher
 - Google™ Chrome 2.0 and higher
 - Apple Safari 3.0 and higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as 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 web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

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

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

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

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

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

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

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

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms
C:\>
```


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

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

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

- Open your browser, enter the IP address of your router (192.168.0.1) and click **OK**.
- Enter your username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your email. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or Wi-Fi technology is another way of connecting your computer to the network without using wires. Wi-Fi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away.

Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

Wireless technology has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

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

Where is wireless used?

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

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-505 wireless network Cardbus adapters.

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

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

Networking Basics

Check your IP address

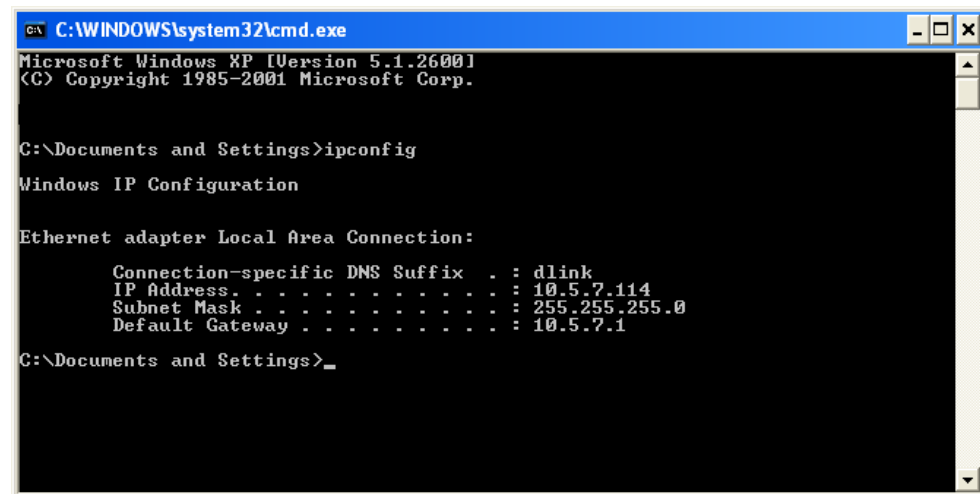
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

At the prompt, type **ipconfig** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.



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

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

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

C:\Documents and Settings>
```

Statically Assign an IP address

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

Step 1

- Windows® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.
- Windows Vista® - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections**.
- Windows® XP - Click on **Start > Control Panel > Network Connections**.
- Windows® 2000 - From the desktop, right-click **My Network Places > Properties**.

Step 2

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

Step 3

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

Step 4

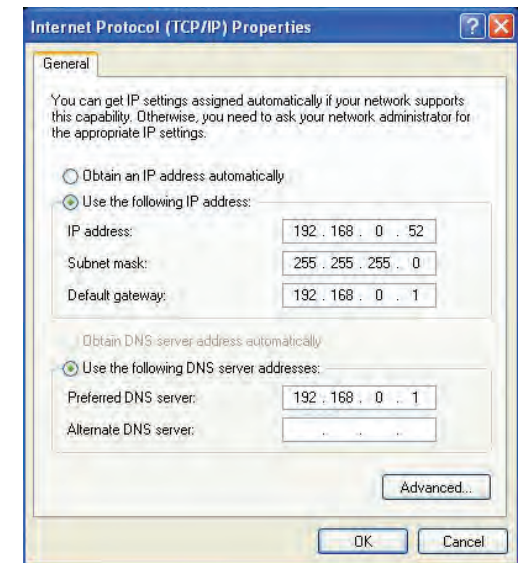
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set the Default Gateway the same as the LAN IP address of your router (I.E. 192.168.0.1).

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

Step 5

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



Technical Specifications

Standards

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

Security

- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise

Wireless Signal Rates¹

IEEE 802.11n 2.4GHz(HT20/40):

- 72.2Mbps (150)
- 57.8Mbps (120)
- 28.9Mbps (60)
- 14.4Mbps (30)
- 65Mbps (135)
- 43.3Mbps (90)
- 21.7Mbps (45)
- 7.2Mbps (15)

IEEE 802.11g:

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

Frequency Range² (North America)

- 2.412GHz to 2.462GHz (802.11g/n)

Operating Temperature

- 32°F to 104°F (0°C to 40°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- CE
- C-Tick
- UL
- IC

Dimensions

- 2.68" x 1.65" x 2"
(68 x 42 x 51mm)

Warranty

- 1 Year

AC Input

- 110~240VAC, 50/60MHz, 0.3A

¹ 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.

² Frequency Range varies depending on country's regulation.

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-505)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev C1))
- 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>

GPL Code Statement

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
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.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:

(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

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 D-Link 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 (USA):

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:

- 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 DLink 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 1-877-453-5465, 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.com/>.
- 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 either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. 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 UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, 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.

Submitting A Claim (Canada):

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 ©2012 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.

Federal Communication Commission Interference Statement:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate

radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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.

Note:

The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu,

y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and

operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

ICC Notice:

Operation is subject to the following two conditions:

- (1) This device may not cause interference and
- (2) This device must accept any interference, including interference that may cause undesired operation of the device.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

- (1) Ce périphérique ne doit pas causer d'interférence et.
- (2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

Registration

Register your product online at registration.dlink.com



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

Version 1.0
January 11, 2012