D-Link®

Version 1.0 | 06/22/2012

User Manual

Pocket Cloud Router

DIR-506L

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	May 18, 2012	• Initial release

Trademarks

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

Copyright © 2012 by D-Link Systems, Inc.

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

Table of Contents

Preface i
Manual Revisions i
Trademarks i
Replace icons 1
Package Contents 1
System Requirements 2
Introduction 3
Features 4
Hardware Overview 5
Front/Top 5
Side/Left 6
Back 7
Router Setup Diagram 8
Wireless Installation Considerations 9
Setting Up Your DIR-506L 10
Initial Setup Wizard 11
SharePort Mobile App (iOS, Android) 13
Web-based Configuration 16
Setup 17
Internet Settings 17
Internet Connection Setup Wizard 18
Manual Internet Setup 22
Wireless Settings 30
Wireless Network Setup Wizard 31
Manual Wireless Network Configuration 33
Manual Wireless - Router Mode 34
Manual Wireless - Access Point Mode 37
Manual Wireless - Repeater Mode 38
Network Settings 39
Media Server 40
Storage 41
Advanced 42
Virtual Server 42
Application Rules 43
MAC Address Filter 44
URL Filters 45
Outbound Filters 46
Inbound Filters 47
SNMP 48
Routing 49
Guest Zone 50
Advanced Wireless 51
Advanced Network 52
Tools 53
Administrator Settings 53
Time and Date 54
SysLog 55
Email Settings 56
System Settings 57
Firmware Upgrade 58

Dynamic DNS 59
System Check 60
Schedules 61
Status 62
Device Info 62
Logs 63
Statistics 64
Wireless Client List 65
Help 66

Connecting a Wireless Client 67
WPS Button 67
Windows® 7 68
WPA/WPA2 68
WPS 71
Windows Vista® 75
WPA/WPA2 76
WPS/WCN 2.0 78
Windows® XP 79
WPA/WPA2 80

Troubleshooting 82

Wireless Basics 86
What is Wireless? 87
Tips 89

Networking Basics 90
Assign a Static IP address 91

Technical Specifications 92

GPL Code Statement 93

Safety Statements 108

Package Contents

DIR-506L Pocket Cloud Router

Ethernet cable

USB cable

Rechargeable battery

Quick Install Guide

If any of the above items are missing from your package, please contact your reseller.

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n or 802.11g wireless clients • 10/100 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 8 or higher • Firefox 8.0 or higher • Safari 4.0 or higher • Google Chrome (16.0.9.12.75) **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

Introduction

TOTAL PERFORMANCE
Combines award winning router features and Wireless N 150 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 Pocket Cloud Router (DIR-506L) lets you create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the DIR-506L 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.

TOTAL NETWORK SECURITY
The DIR-506L 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 802.11n and 802.11g 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 provides an up to 150 Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Compatible with 802.11g Devices** - The is still fully compatible with the IEEE 802.11g standards, so it can connect with existing 802.11g devices.

- **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 and website address.

    - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.

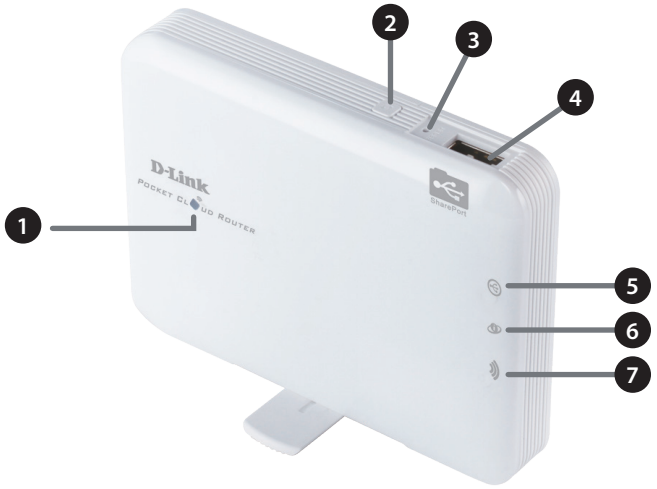
    - **Secure Multiple/Concurrent Sessions** - The can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the 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 802.11n and 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Hardware Overview

Front/Top



1	Device Status LED Indicator	If Device Status LED is *flashing green when the device is on*, power is being provided by the battery. If Device Status LED is *solid green when the device is on*, battery is fully charged and power adapter attached. If Device Status LED is *solid amber when the device is on*, the device is charging the battery. If Device Status LED is *solid amber when the device is off with the battery inside*, the battery is charging. If Device Status LED is *solid red when the device is on*, the battery is low. If Device Status LED is *flashing red when the device is on*, the battery temperature is high. If Device Status LED is *off and the power adapter is plugged in*, and battery has finished charging. If Device Status LED is *off*, no power adapter is plugged in and no battery is inside.
2	WPS Button	Pressing the WPS button allows additional devices to connect securely and automatically.
3	Reset Button	Pressing the Reset button restores the DIR-506L to its original factory default settings.
4	USB Port	Connect a USB flash drive to configure the wireless settings using SharePort™ Mobile and SharePort™ Web File Access. Both allow you to share a USB or a storage device with your local network.
5	USB LED Indicator	If the USB LED is *solid green*, a USB storage device is attached. If the USB LED is *flashing green*, the DIR-506L is accessing files in the USB storage device.
6	Ethernet LED Indicator	If the Ethernet LED is *solid green*, an Ethernet connection is established If the Ethernet LED is *flashing green*, data packets are being transferred via Ethernet
7	Wi-Fi LED Indicator	If the Wi-Fi LED is *flashing green*, a data packet transferred. If the Wi-Fi LED is *flashing green every second for two minutes*, it is showing the WPS status.

Hardware Overview

Side/Left

1	Ethernet LAN/WAN Port	The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.
2	Power Switch	Turns the DIR-506L on and off.
3	Mini USB Port	This port provides power to the router and charges the battery.

Hardware Overview

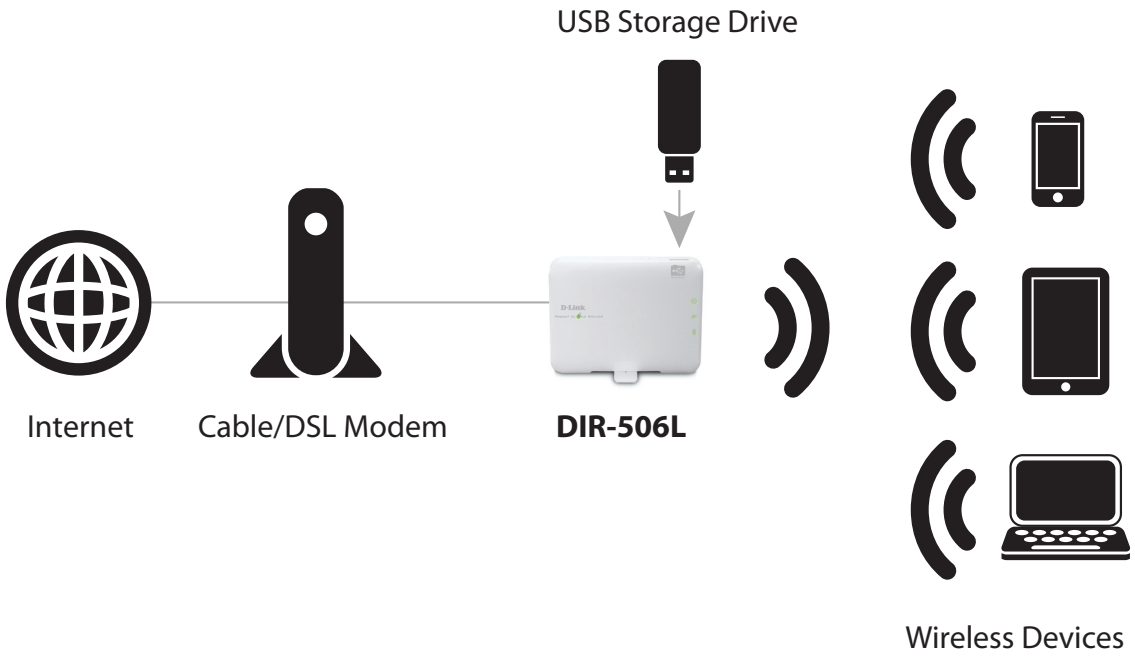
Back

1	Battery cover	Slide the battery cover to remove it and access the battery compartment.
2	Battery compartment	Insert the rechargeable battery into the compartment, making sure the contact points on the battery are properly aligned with the contact points of the device. After proper insertion, replace the battery cover.

Note: Using a rechargeable battery other than the one that came with your package may cause damage to your device and will void its warranty.

Router Setup Diagram

The DIR-506L connects to your cable modem, DSL modem, or other Internet source and shares your Internet connection with your devices wirelessly, providing Internet access for an entire home or office. You can also share files with other computers or devices on your wireless network by using the SharePort Mobile feature.



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.

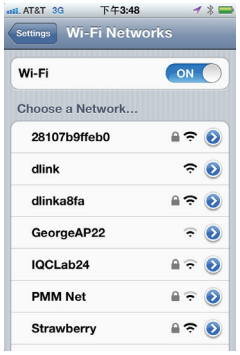
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

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 in not in use.

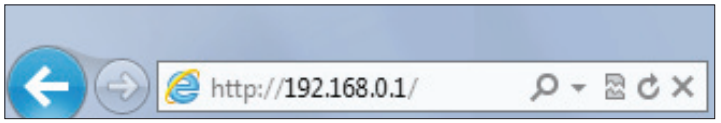
Setting Up Your DIR-506L

1. Plug in your DIR-506L mini-USB to a powered USB port on a computer to begin use. This will also charge the battery if you have one installed. Verify that the device status LED is on before continuing.

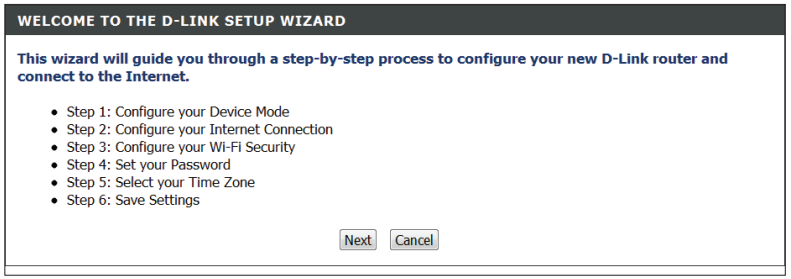
2. From your laptop or mobile device, go to your Wireless Utility to display the available wireless networks and select the Wi-Fi name that is printed on the Wi-Fi Configuration Note included in your package (ex: **dlink-a8fa).** Then, enter the Wi-Fi password also printed on the Wi-Fi Configuration Note **(akbdj1936).**



3. Open your web browser, and type **http://192.168.0.1** in the address bar to begin the Setup Wizard.



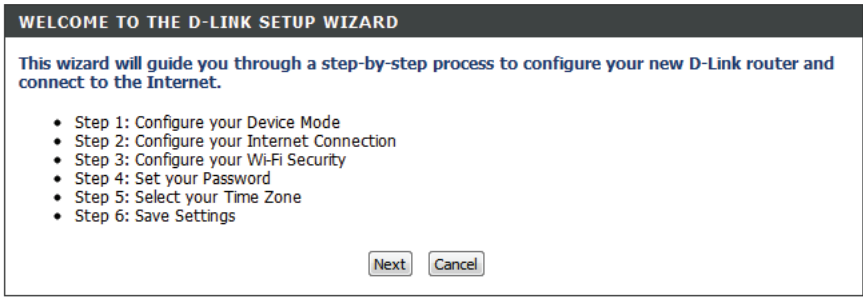
Please follow the on-screen instructions to complete setup.



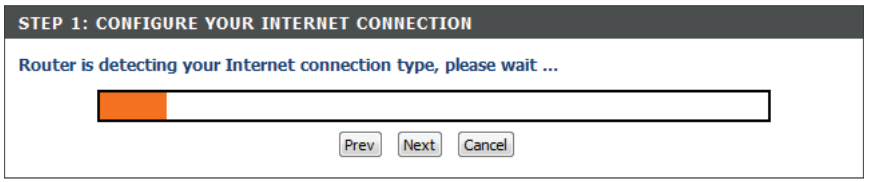
Initial Setup Wizard

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.

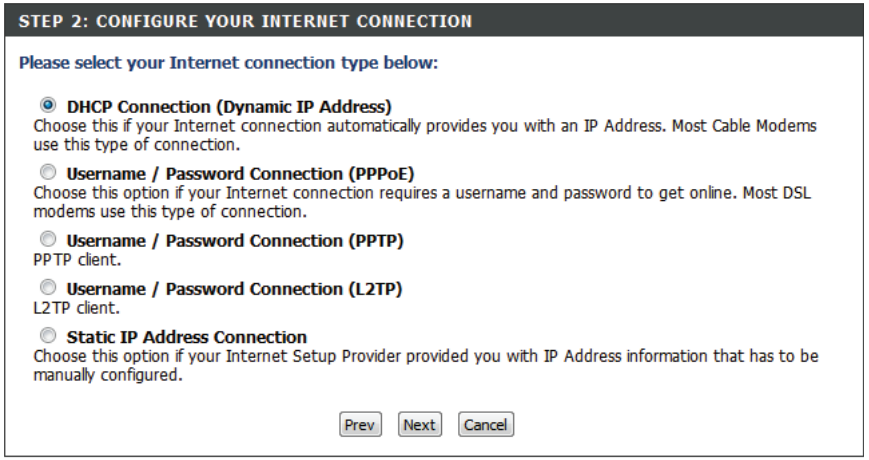


If you chose Router mode, the DIR-506L will try to detect what type of Internet connection you have and will ask you for the related settings. Enter the settings for your connection and click **Next**.



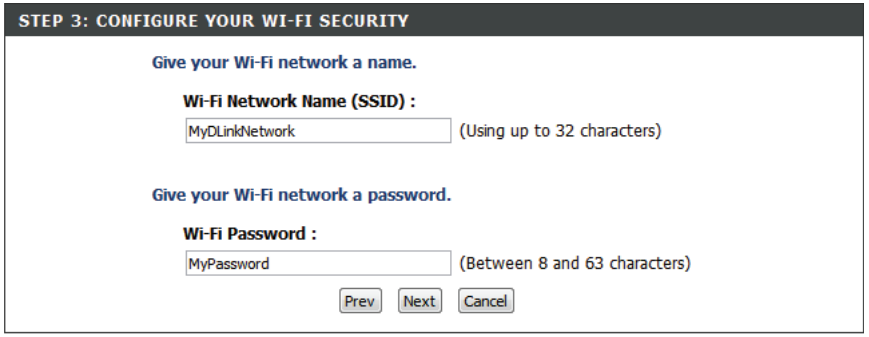
If your Internet connection cannot be detected(or if you click the **Prev** button after the previous step), you will need to select which type of Internet connection you have. Select your Internet connection type, then click the **Next** button and enter the related settings.

Note: Most cable modem connections use DHCP, and most DSL modem connections use **PPPoE**. If you are not sure which connection type you use or what settings to enter, contact your Internet service provider.

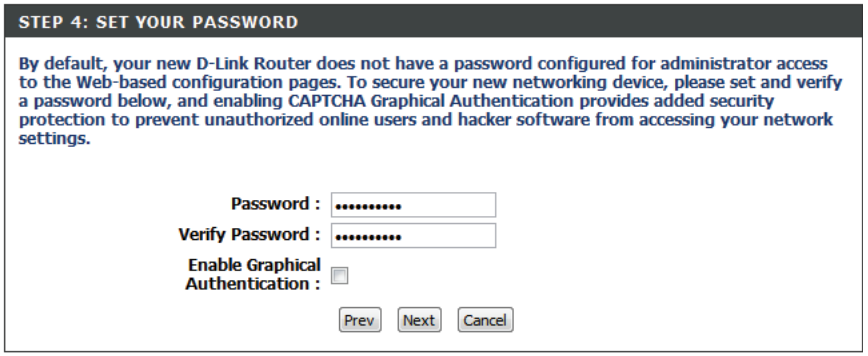


Create a wireless security passphrase or key (between 8-63 characters). Your wireless clients will need to have this passphrase or key entered to be able to connect to your wireless network.

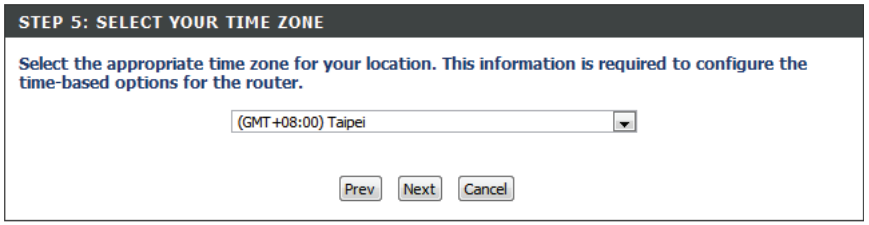
Click **Next** to continue.



Enter a password to secure configuration access to your router. Please note that this password will be used to log in to the configuration interface, but is not the same as the password used for your wireless network. Check the **Enable Graphical Authentication** box to enable CAPTCHA authentication for added security. Click **Next** to continue.



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



Setup is complete, and your wireless network name and password will be displayed. It is recommended that you write this information down for future reference. Click **Save** to save your settings and reboot the router.

SharePort Mobile App (iOS, Android)

The SharePort Mobile app allows you to remotely access files stored on a USB flash drive or USB external hard drive connected to the DIR-506L. For more information on using this feature, please refer to "Storage" on page 41.

Note: The SharePort Web/SharePort Mobile feature of the DIR-506L can only be used when the device is configured for **Router** mode in the wireless settings.

1. Plug your USB flash drive into the USB port on top of the DIR-506L.

2. Use your iOS or Android mobile device to scan the QR code to the right to download the **SharePort Mobile** app.

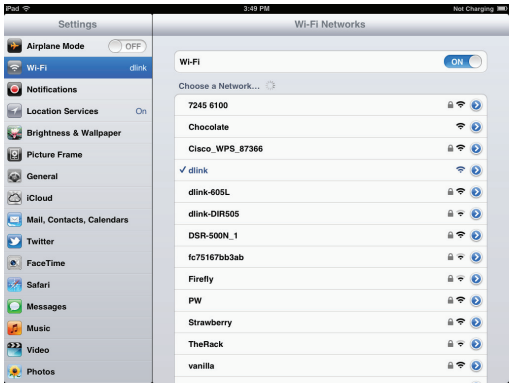
   You can also search for the **SharePort Mobile** app directly in the iOS App Store or the Android Market/Google Play.

iOS

Android

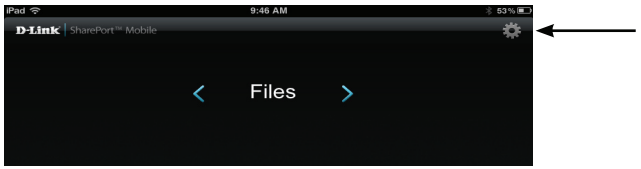
4. From your iOS mobile device, tap **Settings.**

5. Click **Wi-Fi** and select the network (SSID) that you assigned during initial setup. Then, enter your Wi-Fi password.



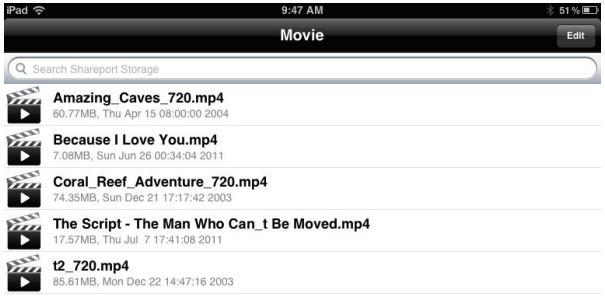
6. Once connected, tap the **SharePort** icon, and the SharePort app will load.

7. Tap on the **Settings** gear icon located on the right top corner of the screen. Then, click **Edit** to enter your User Name and Password. Once you finish, click **Done** to continue.



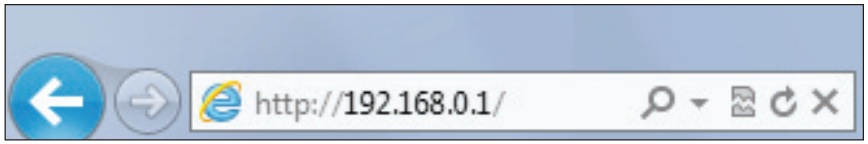
8. You can now use the SharePort Mobile app to access the files on your USB storage drive.

Note: If you connect a USB storage drive with many files or with a large capacity, it may take a while for the DIR-506L to scan and catalog your files.



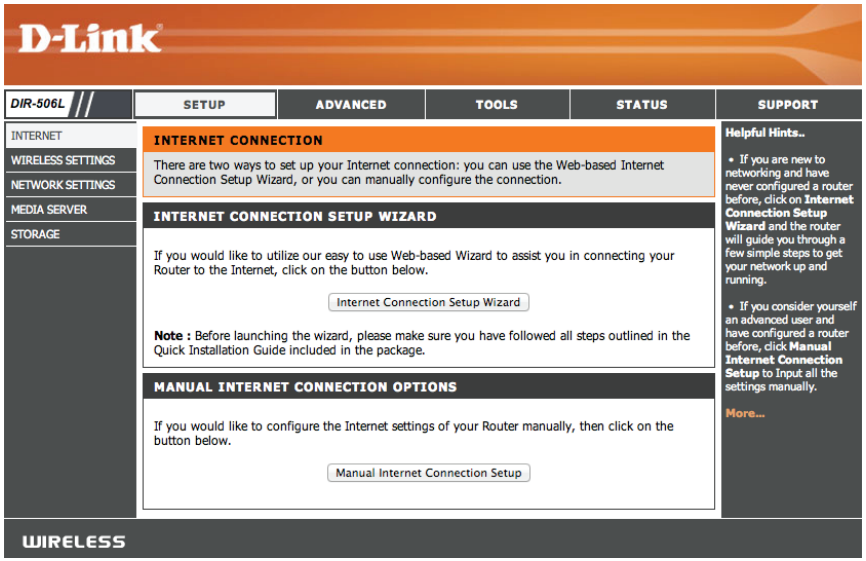
Web-based Configuration

To access the configuration utility in any of the modes of the DIR-506L, open a web-browser and enter **http://dlinkrouter** in the address bar.



Select **Admin** from the drop-down menu and then enter your password. By default, the password is blank.

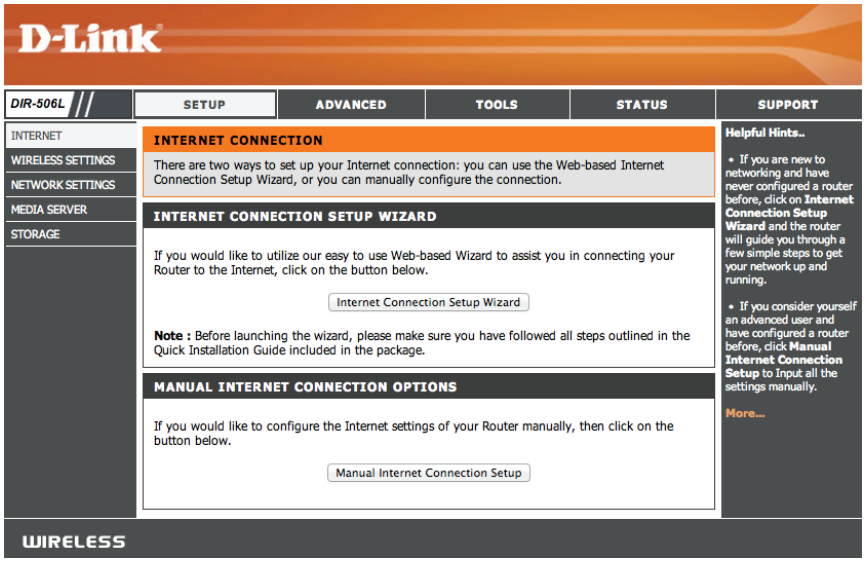
The configuration interface will open, and you can configure the different settings of the DIR-506L.



Setup
Internet Settings

If you want to configure your router to connect to the Internet using a setup wizard, click **Internet Connection Setup Wizard**, and continue to the next page.

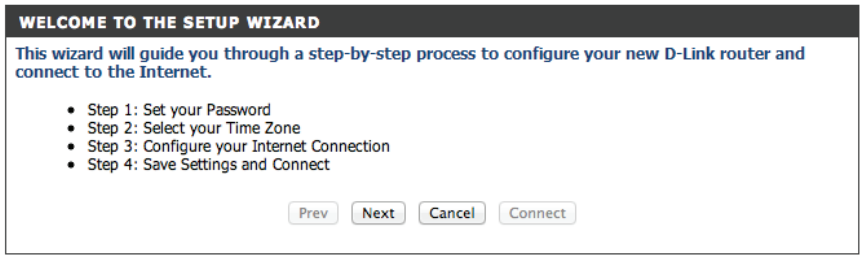
To configure your Internet settings manually, click the **Manual Internet Connection Setup** button and go to "Manual Internet Setup" on page 22.



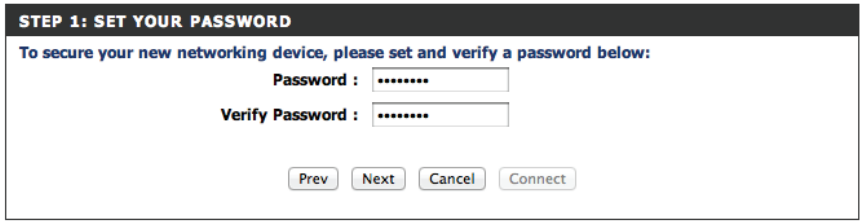
Internet Connection Setup Wizard

The Internet Connection Setup Wizard is designed to guide you through a step-by-step process to configure your DIR-506L and connect to the Internet.

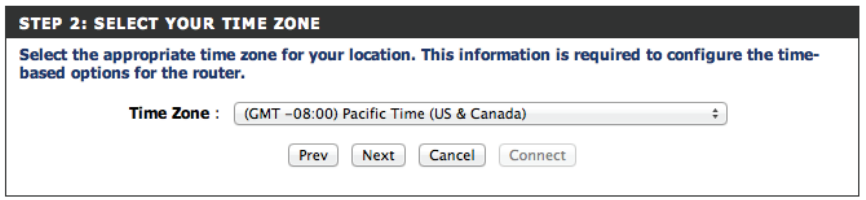
Click **Next** to continue.



In order to secure your router, please enter a new password. Click **Next** to continue.

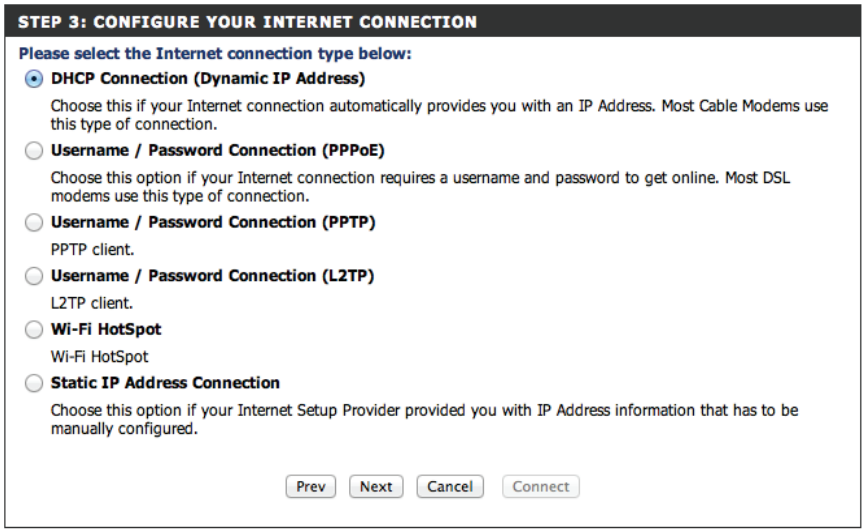


Select your time zone from the drop-down menu and click **Next** to continue.



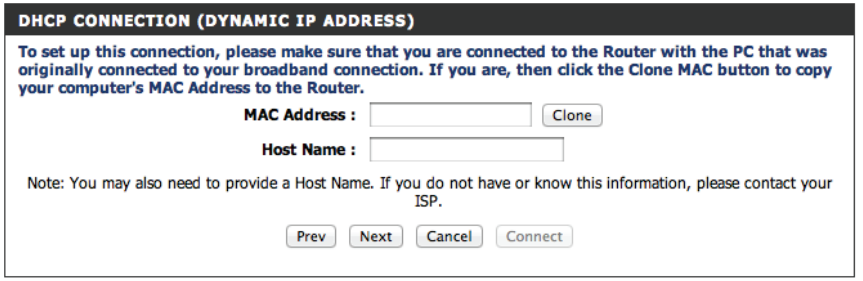
Select which type of Internet connection you have. Select your Internet connection type, then click the **Next** button and enter the related settings.

Note: Most cable modem connections use DHCP, and most DSL modem connections use **PPPoE**. If you are not sure which connection type you use or what settings to enter, contact your Internet service provider.

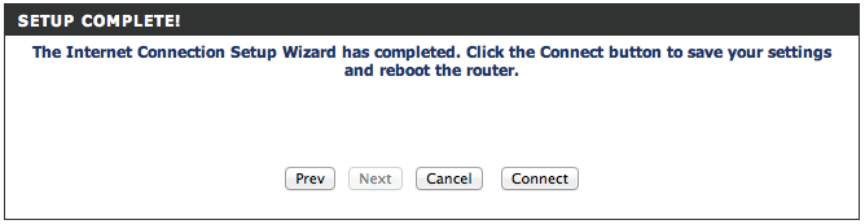


If you selected **DHCP Connection**, you will see the following screen. If your ISP requires you to enter a MAC address and Host Name, fill them in here. You can click the **Clone MAC button** to enter your current computer's MAC address.

Click **Next** to continue.

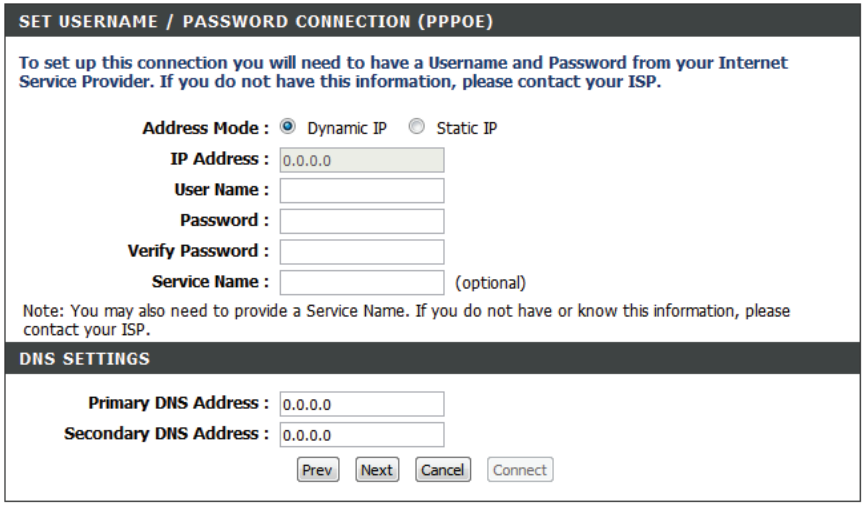


Setup is complete, and your wireless network name and password will be displayed. It is recommended that you write this information down for future reference. Click **Save** to save your settings and reboot the router.

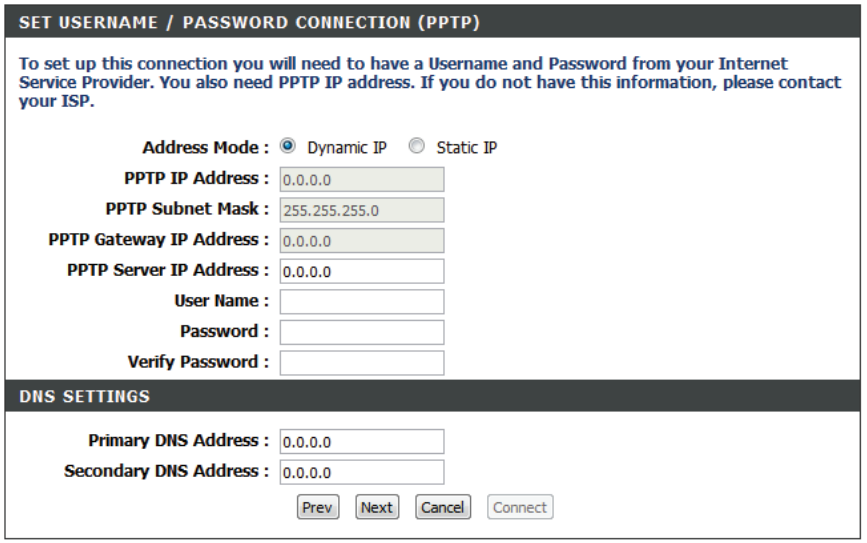


If you selected **PPPoE Connection**, you will see the following screen. Enter your PPPoE username, password and verify password, then click **Next** to continue.

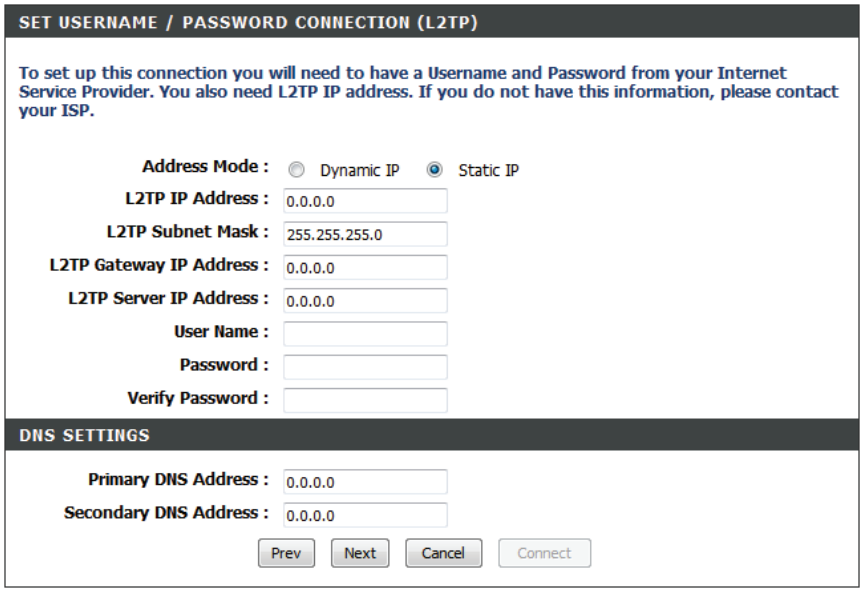
Note: Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.



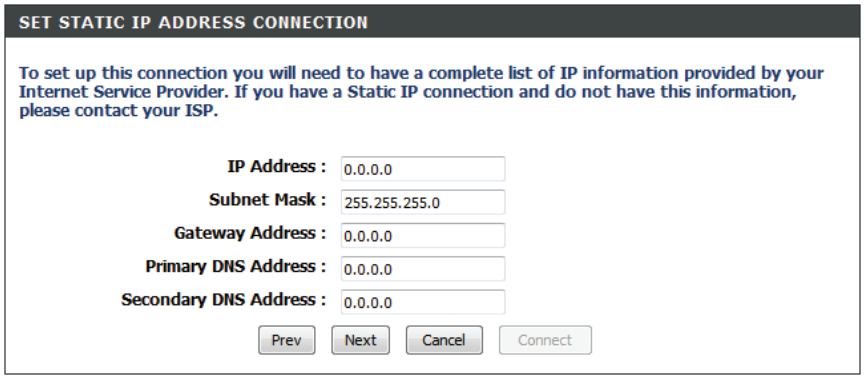
If you selected **PPTP Connection**, you will see the following screen. Enter your PPTP username, password, and other information supplied by your ISP. Click **Next** to continue.



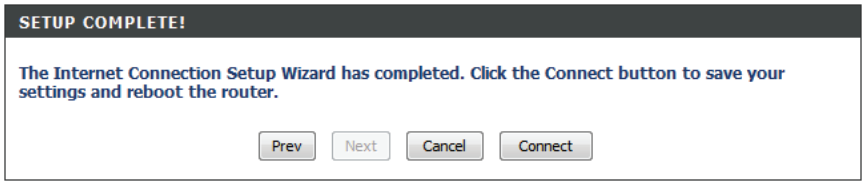
If you selected **L2TP Connection**, you will see the following screen. Enter your L2TP username, password, and other information supplied by your ISP. Click **Next** to continue.



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



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

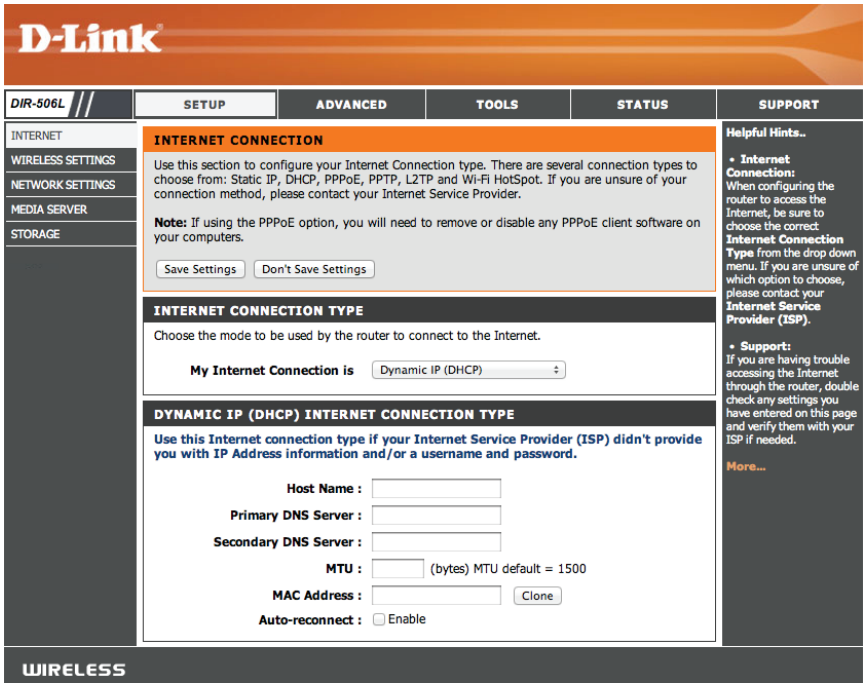


Manual Internet Setup

If you clicked **Manual Internet Connection Setup** on the **Internet Settings** page, you will see this screen. Here, you can configure the Internet connection for your DIR-506L. After making your changes, click the **Save Settings** button.

My Internet Connection is: Select the connection mode to use: **Dynamic IP (DHCP)**, **PPPoE**, **PPTP**, or **L2TP**. The remaining settings will change depending on which connection mode you use.

Note: Most cable modem connections use DHCP, and most DSL connections use PPPoE. If you are not sure which connection mode to use, contact your Internet service provider.



If you selected **Dynamic IP (DHCP)**, you will see the following settings.

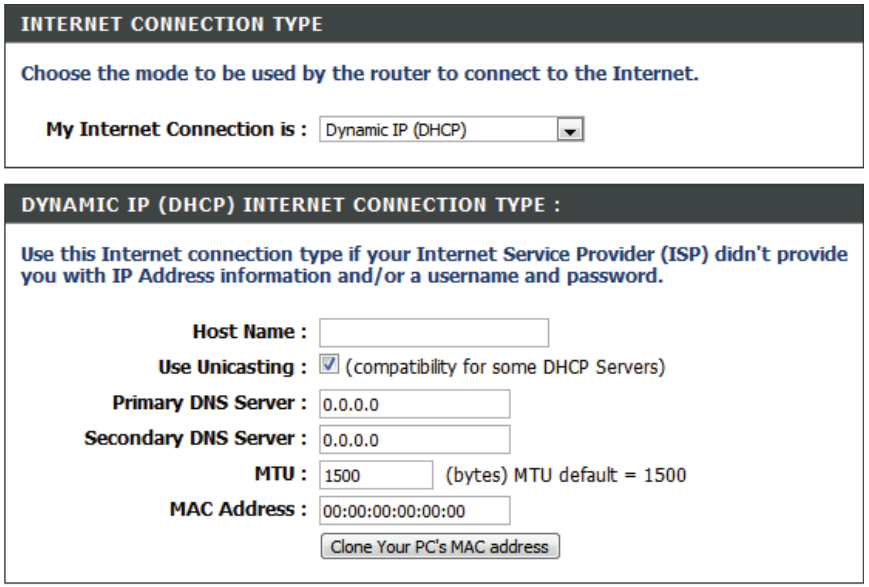
Host Name: Entering a host name is optional but may be required by some ISPs. Leave this blank if you are not sure.

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 this setting at 0.0.0.0 if you did not specifically receive these from your ISP.

MTU: If you experience connection issues, you may need to change the MTU setting for optimal performance with your specific ISP. 1492 is the default MTU.

MAC Address: If your ISP requires you to enter a MAC address, fill it in here. You can click the **Clone MAC button** to enter your current computer's MAC address.



If you selected **PPPoE**, you will see the following settings. 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.

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

IP Address: Enter the IP address (for 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).

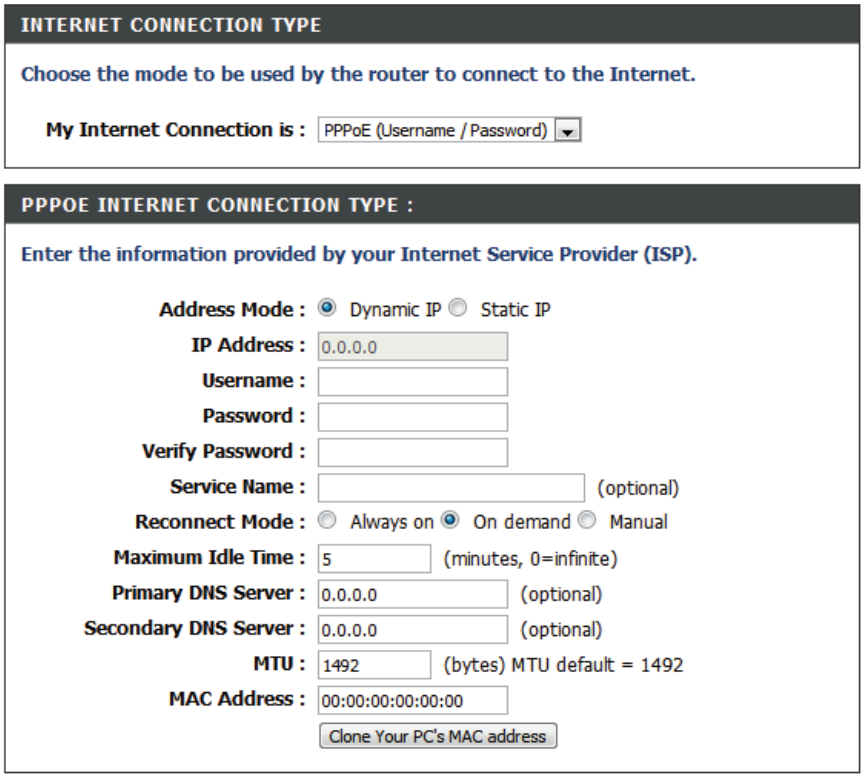
Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, set the **Reconnect Mode** to **Always on**.

Primary/ Secondary DNS Server: Enter the primary and secondary DNS server addresses (Static PPPoE only).

MTU: If you experience connection issues, you may need to change the MTU setting for optimal performance with your specific ISP. 1492 is the default MTU.

MAC Address: If your ISP requires you to enter a MAC address, fill it in here. You can click the **Clone MAC button** to enter your current computer's MAC address.



If you selected **PPTP**, you will see the following settings. Your ISP will provide you with a username and password. This option is typically used for DSL services.

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

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

PPTP Subnet Mask: Enter the primary and secondary DNS server addresses (for static PPTP only).

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

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

Username: Enter your PPTP username.

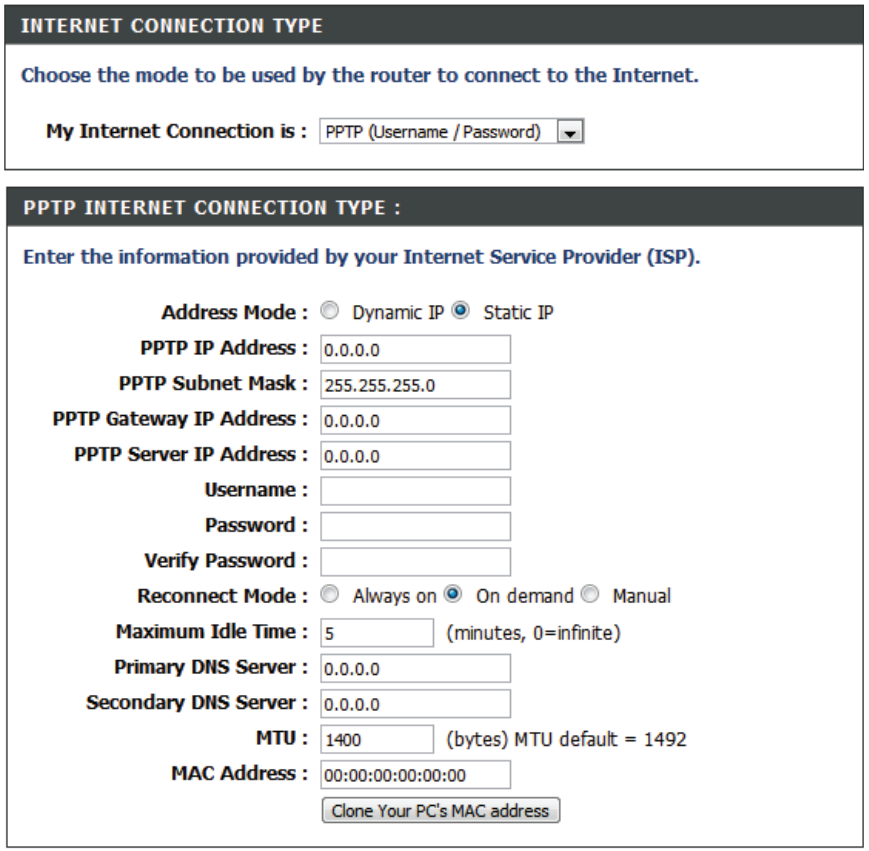
Password: Enter your PPTP password and then retype the password in the next box.

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

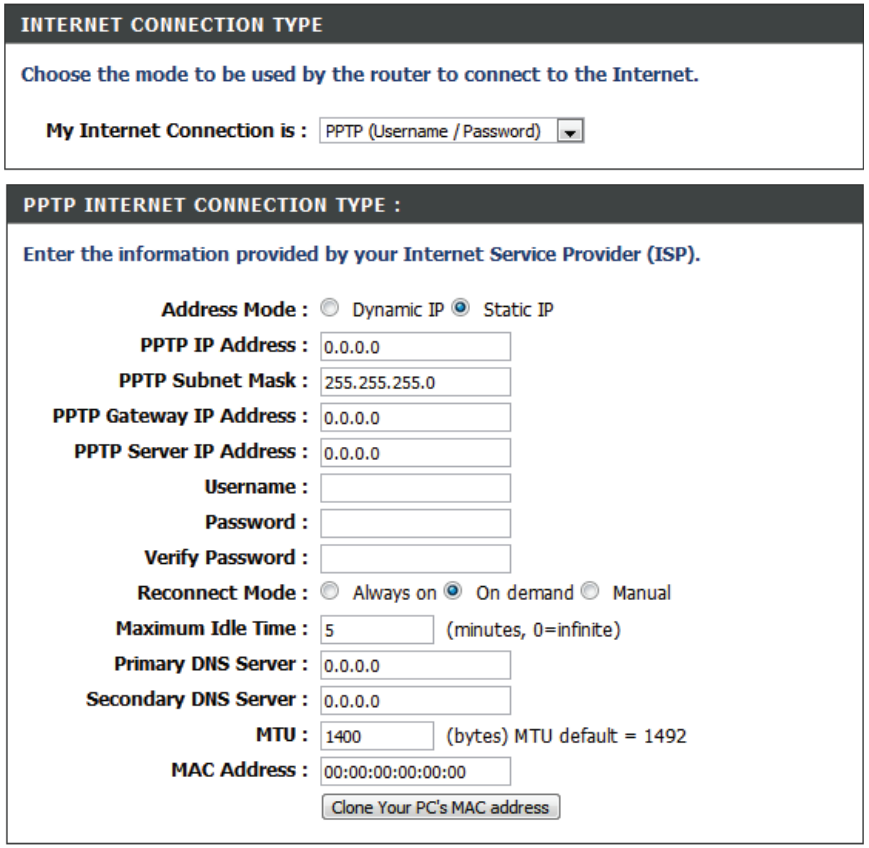
Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, set the **Reconnect Mode** to **Always on**.

Primary/ Secondary DNS Server: The DNS server information will be supplied by your ISP (Internet Service Provider.)

MTU: If you experience connection issues, you may need to change the MTU setting for optimal performance with your specific ISP. 1492 is the default MTU.



MAC Address: If your ISP requires you to enter a MAC address, fill it in here. You can click the **Clone MAC button** to enter your current computer's MAC address.



If you selected **L2TP**, you will see the following settings. Your ISP will provide you with a username and password. This option is typically used for DSL services.

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

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

L2TP IP Address: Enter the L2TP IP address supplied by your ISP (for static IP only).

L2TP Subnet Mask: Enter the subnet mask supplied by your ISP (for static IP only).

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

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

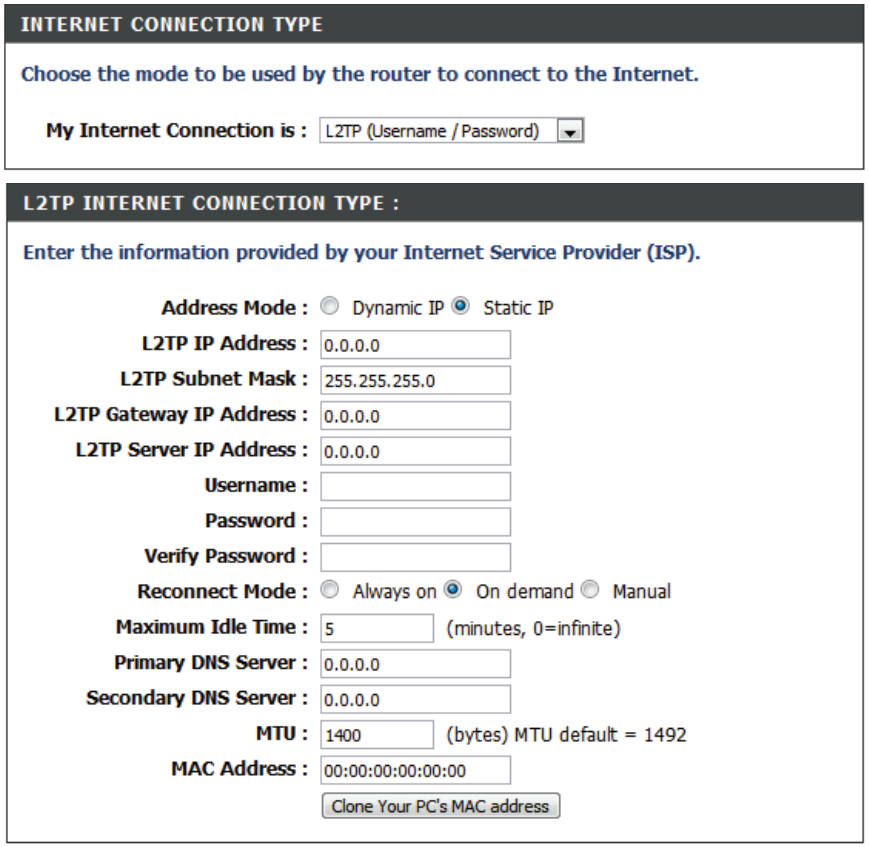
Username: Enter your L2TP username.

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

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

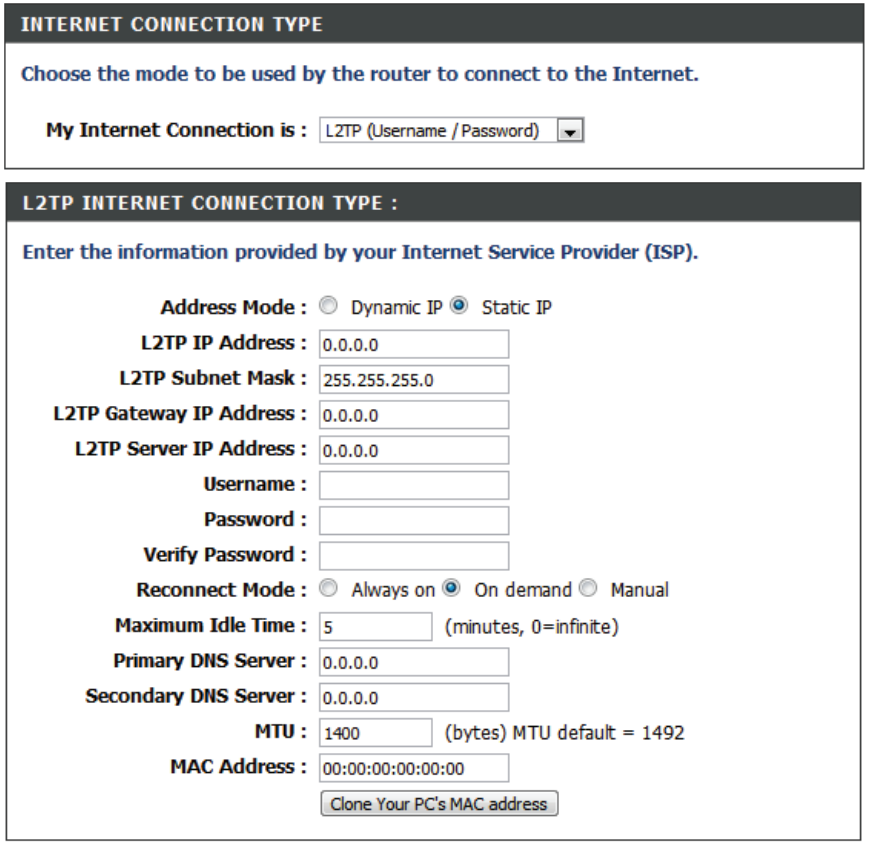
Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, set the **Reconnect Mode** to **Always on**.

Primary/ Secondary DNS Server: Enter the primary and secondary DNS server addresses (for static L2TP only).



MTU: If you experience connection issues, you may need to change the MTU setting for optimal performance with your specific ISP. 1492 is the default MTU.

MAC Address: If your ISP requires you to enter a MAC address, fill it in here. You can click the **Clone MAC button** to enter your current computer's MAC address.



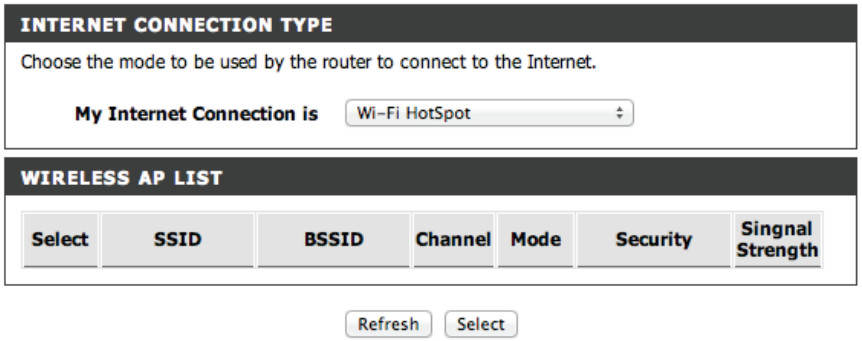
If you selected **Wi-Fi Hotspot**, the DIR-506L will scan for an available Wi-Fi hotspot to connect to. If one or more is found, they will appear in a list along with details of the signal.

My Internet Connection: Select **Wi-Fi Hotspot** from the drop-down menu.

Wireless AP List: The router will automatically scan for potential hotspot connections and add them to the **Wireless AP List**.

Refresh: The router will rescan for available hotspots.

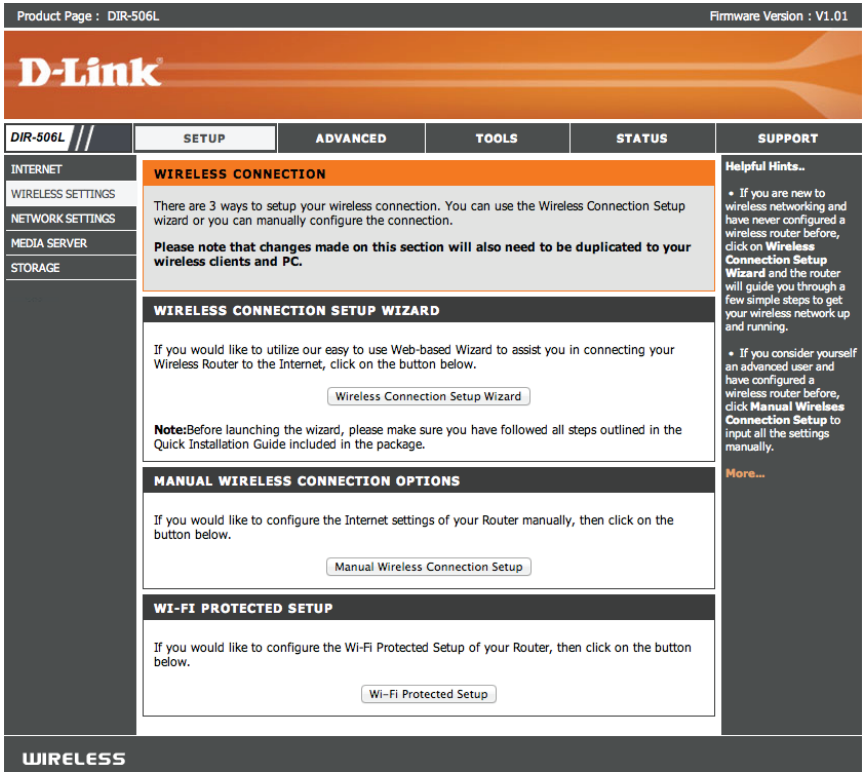
Select: When you have chosen a hotspot from the list, press **Select** to enter your credentials and connect.



Wireless Settings

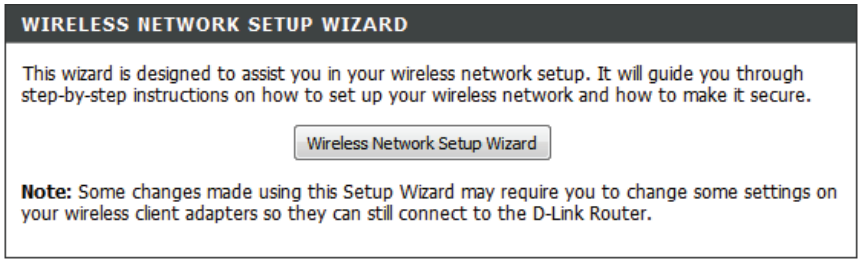
If you want to configure the wireless settings on your router using the wizard, click **Wireless Security Setup Wizard** and refer to the next page**.**

If you want to manually configure the wireless settings on your router click **Manual Wireless Network Setup** and refer to "Manual Wireless - Router Mode" on page 34.

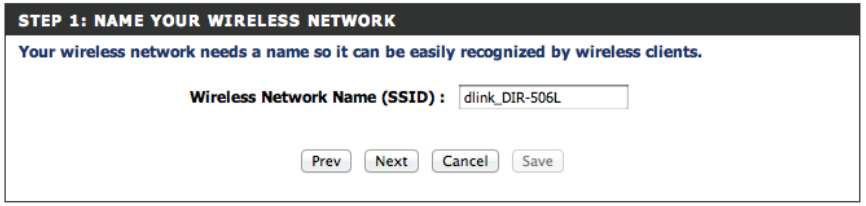


Wireless Network Setup Wizard

The Internet Connection Setup Wizard is designed to guide you through a step-by-step process to configure your wireless network.



Type your desired wireless network name (SSID) and click **Next**.



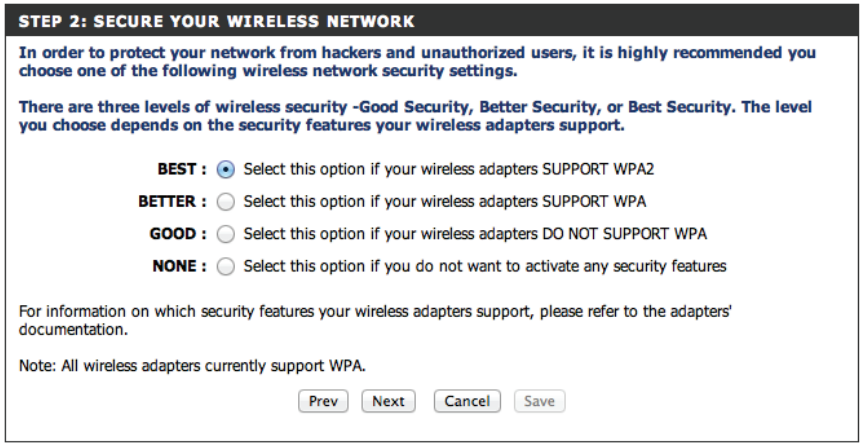
Choose your wireless security level from the following options:

BEST (Recommended): Select this option to create a network key using either AES or TKIP, and click **Next**.

BETTER: Select this option to create a network key using TKIP, and click **Next**.

GOOD: Select this option to create a network key using either ASCII or HEX, and click **Next**.

NONE (Not Recommended): Select this option if you do not with to use a network key, and click **Next**. If you select this option, wireless setup will be completed. Click **Save** to save your settings and complete the setup process.



If you selected **BEST** for your wireless security option, you will need to choose either **AES** or **TKIP** and manually enter a password for your wireless network. When you are finished, click **Next**.

If you selected **BETTER** for your wireless security option, you will need to manually enter a password for your wireless network using TKIP. When you are finished, click **Next**.

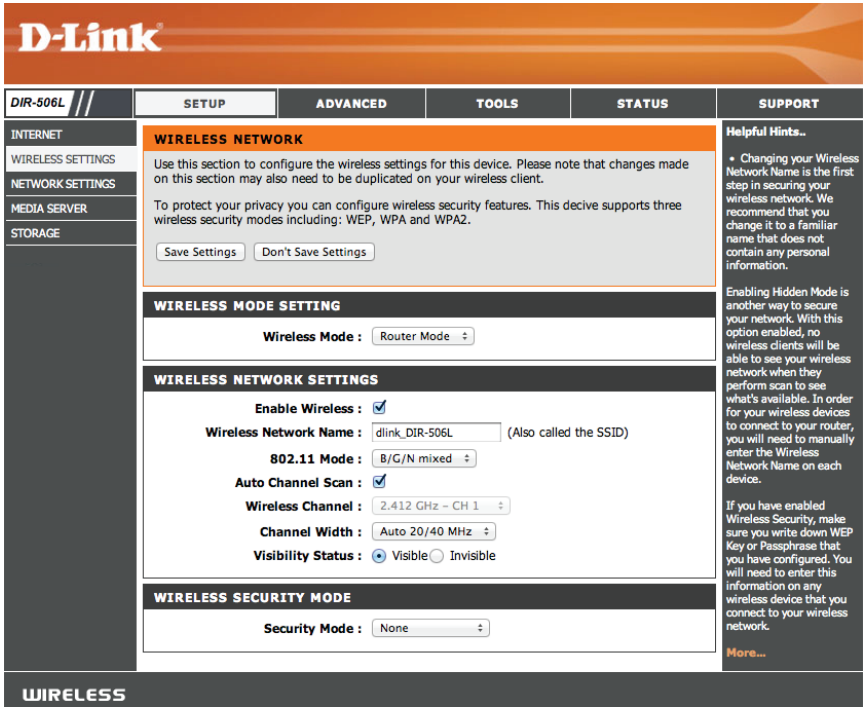
If you selected **GOOD** for your wireless security option, you will need to choose either **ACSII** or **HEX** and manually enter a password for your wireless network. When you are finished, click **Next**.

Wireless setup is now complete. Click **Save** to save your settings and complete the setup process.

Manual Wireless Network Configuration

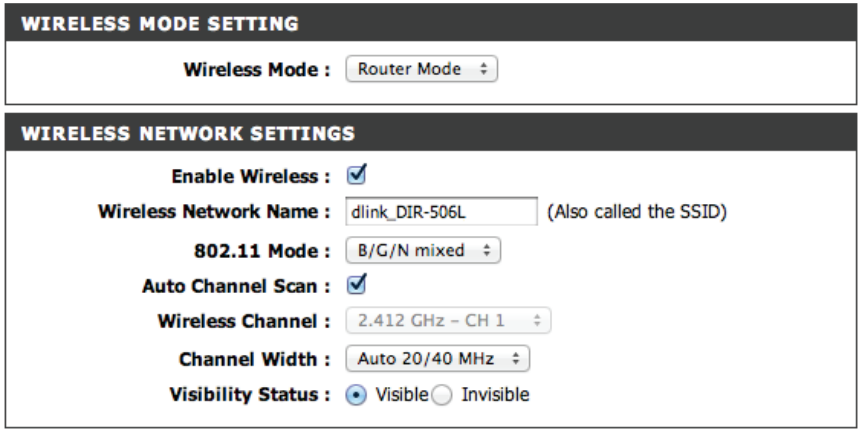
If you clicked **Manual Wireless Network Setup** you can choose what mode the DIR-506L will operate in and configure the wireless network settings. After making your changes, click the **Save Settings** button.

Wireless Mode: Choose from either **Router Mode**, **AP (Access Point) Mode**, or **Repeater Mode** from the drop down menu.



Manual Wireless - Router Mode

If you chose **Router** mode you can configure the DIR-506L as a router. After making changes to the wireless network settings, click the **Save Settings** button.



Enable Wireless: Check **Enable Wireless** to enable the wireless function. If you want to disable wireless functions, uncheck the box.

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 based on your needs:

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

Enable Auto Channel Scan: Select **Auto Channel Scan** to automatically choose the channel with the least amount of interference.

Wireless Channel: If Auto Channel Scan is unchecked, choose the channel you want to use for wireless communication.

Channel Width: Use the drop down menu to choose the width of the wireless channel you want to use.

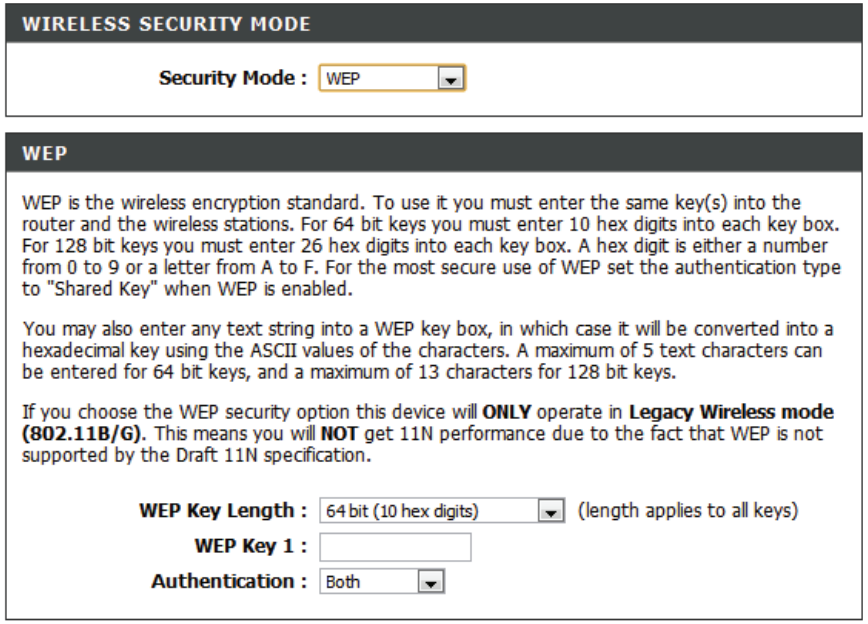
Visibility Status: If you want to broadcast the name of your wireless network choose **Visible**. Choose **Invisible** to hide it.

If you select **WEP** as your Security Mode:

WEP Key Length: Select an encryption level and key length to use. This will also set the type and length of the key you will need to enter.

WEP Key: Enter the password(key) for your wireless network. It will need to match the requirements for the WEP Key Length selected above.

Authentication: Choose what Authentication type to use.

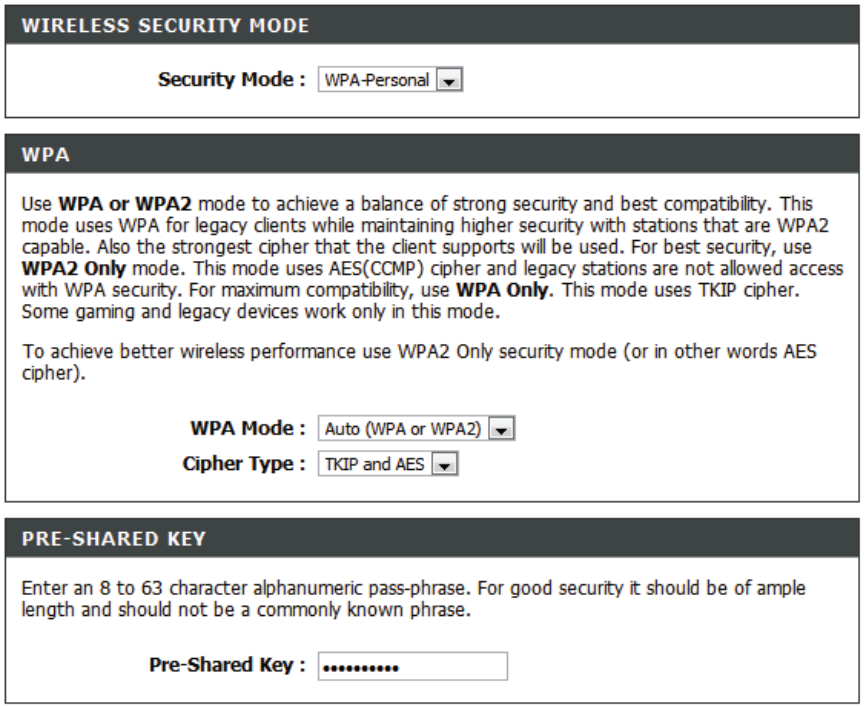


If you select **WPA-Personal** as your Security Mode:

WPA Mode: Select whether to use **WPA**, **WPA2**, or both **WPA and WPA2** for your wireless network..

Cipher Type: Choose whether to use **TKIP**, **AES**, or both **TKIP and AES** ciphers for your wireless network.

Pre-Shared Key: Enter the password(key) for your wireless network.



If you select **WPA-Enterprise** as your Security Mode:

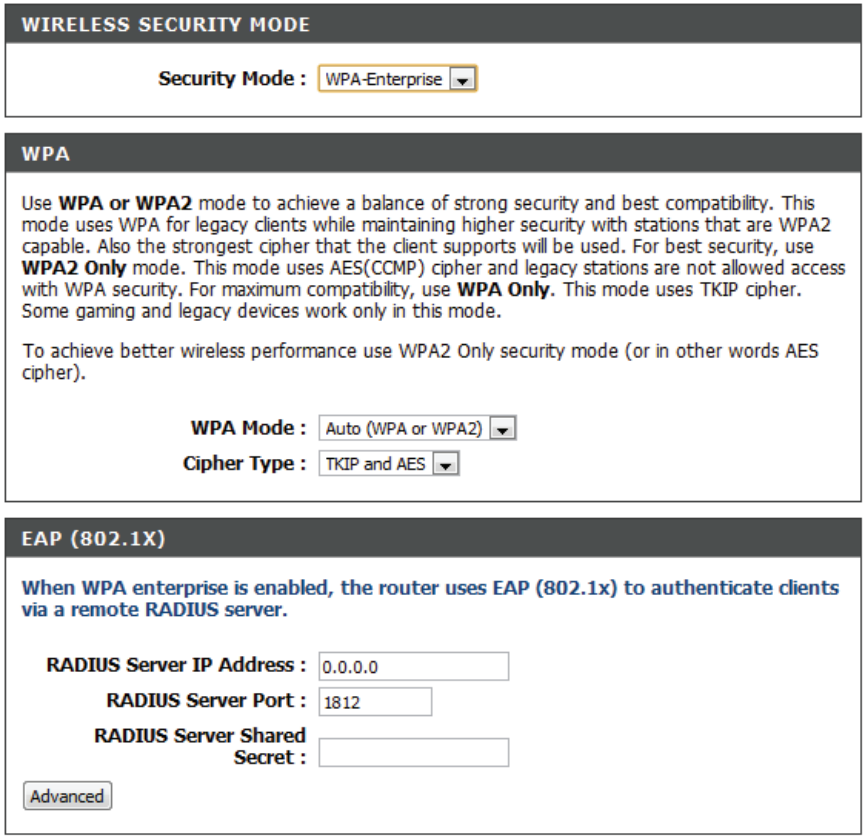
WPA Mode: Select whether to use **WPA**, **WPA2**, or both **WPA and WPA2** for your wireless network..

Cipher Type: Choose whether to use **TKIP**, **AES**, or both **TKIP and AES** ciphers for your wireless network.

RADIUS Server IP Address: Enter your RADIUS server IP address.

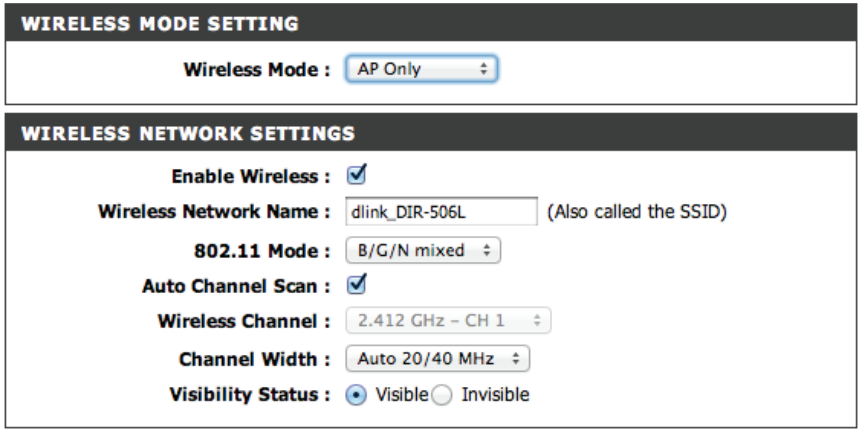
RADIUS Server Port: Enter your RADIOS server port.

RADIUS Server Shared Secret: Enter your RADIUS server shared secret.



Manual Wireless - Access Point Mode

If you chose **AP Only** mode you can configure the DIR-506L as an access point within an existing network. After making changes to the wireless network settings, click the **Save Settings** button.



Enable Wireless: Check **Enable Wireless** to enable the wireless function. If you want to disable wireless functions, uncheck the box.

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 based on your needs:

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

Enable Auto Channel Scan: Select **Auto Channel Scan** to automatically choose the channel with the least amount of interference.

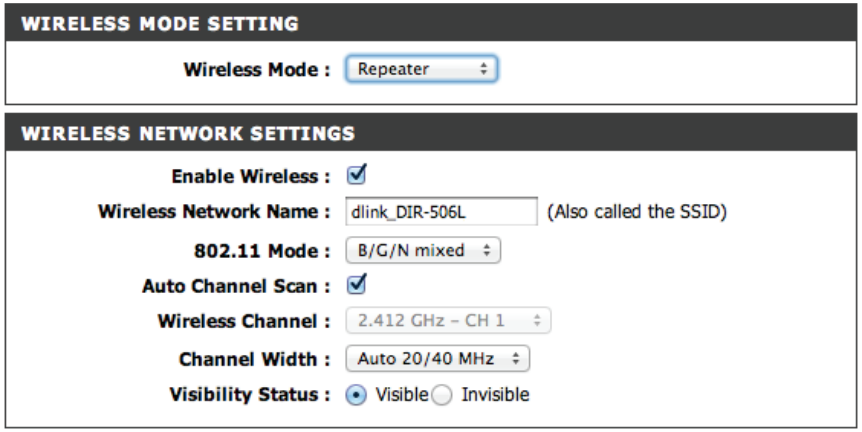
Wireless Channel: If Auto Channel Scan is unchecked, choose the channel you want to use for wireless communication.

Channel Width: Use the drop down menu to choose the width of the wireless channel you want to use.

Visibility Status: If you want to broadcast the name of your wireless network choose **Visible**. Choose **Invisible** to hide it.

Manual Wireless - Repeater Mode

If you chose **Repeater** mode you can configure the DIR-506L as a repeater for another routing device. After making changes to the wireless network settings, click the **Save Settings** button.



Enable Wireless: Check **Enable Wireless** to enable the wireless function. If you want to disable wireless functions, uncheck the box.

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 based on your needs:

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

Enable Auto Channel Scan: Select **Auto Channel Scan** to automatically choose the channel with the least amount of interference.

Wireless Channel: If Auto Channel Scan is unchecked, choose the channel you want to use for wireless communication.

Channel Width: Use the drop down menu to choose the width of the wireless channel you want to use.

Visibility Status: If you want to broadcast the name of your wireless network choose **Visible**. Choose **Invisible** to hide it.

Network Settings

This section will allow you to change the local network settings of the router and to configure the DHCP settings. After making your changes, click the **Save Settings** button.

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.

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

Local Domain Name: Enter a name for the DIR-506L.

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

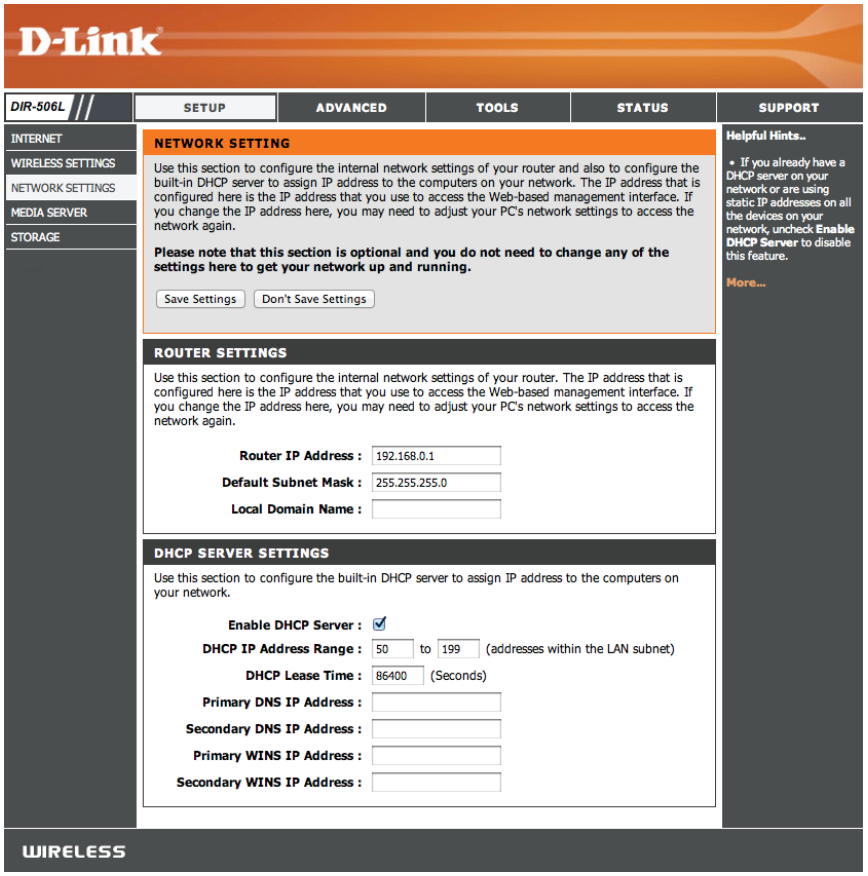
DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

Primary DNS IP Address Configure the IP address of the preferred DNS server.

Secondary DNS IP Address Configure the IP address of the backup DNS server, if any.

Primary WINS IP Address Configure the IP address of the preferred WINS server.

Secondary WINS IP Address Configure the IP address of the backup WINS server, if any.

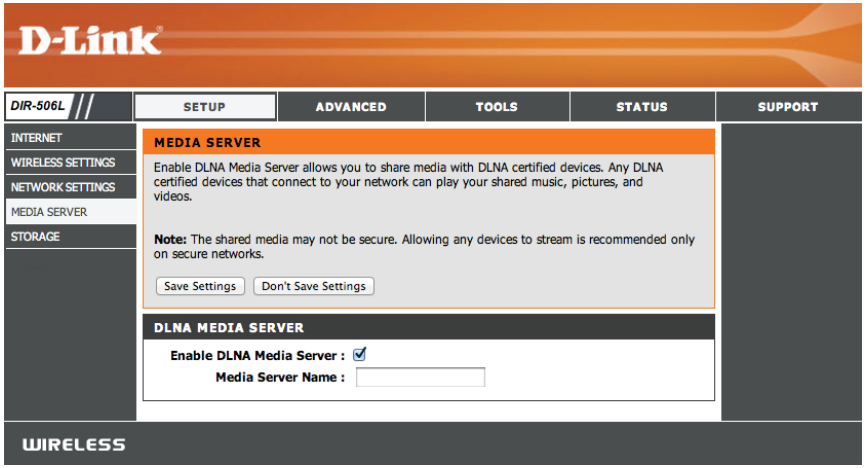


Media Server

This feature allows you to share music, pictures and videos with any devices connected to your network. After making your changes, click the **Save Settings** button.

Enable DLNA Media Server: Check this box to enable the media server feature.

Media Server Name: Enter your media server's name.



Storage

This page will allow you to access files from a USB external hard drive or flash drive that is plugged into the DIR-506L from your local network or the Internet using either a web browser or the SharePort Mobile app on a smartphone or tablet. You can create users to customize access rights to the files stored on the USB drive. After making changes, click the **Save Settings** button.

Enable Shareport Web Access: Tick this checkbox to enable sharing files stored on a USB storage drive connected to the DIR-506L.

HTTP Access Port: Enter a port to use for HTTP web access to your files (8181 is the default). You will have to add this port to the IP address of the DIR-506L when connecting. For example: http://192.168.0.1:8181

Allow Remote Access: Check to enable remote access to your router's storage.

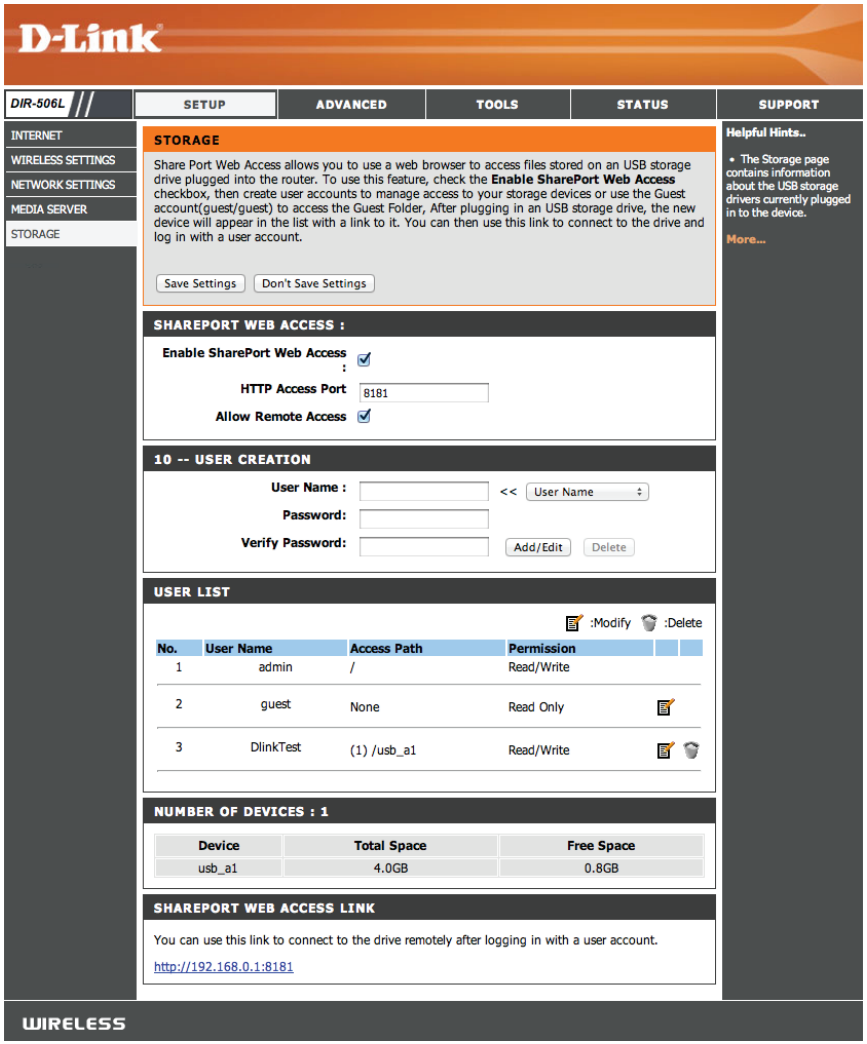
User Name: To create a new user, enter a user name. To edit an existing user, use the dropdown box to the right.

Password/Verify Password: Enter a password you want to use for the account, re-enter the password in the **Verify Password** text box, then click **Add/Edit** to save your changes.

User List: This section shows existing user accounts. There are **admin** and **guest** accounts by default.

Number of Devices: This section shows you information about the USB storage device plugged into the router.

SharePort Web Access Link This will give you a direct link to the web access interface that you can click on or copy and paste.



Advanced
Virtual Server

This will allow you to open a single port. If you would like to open a range of ports, refer to "Application Rules" on page 43. After making your changes, click the **Save Settings** button.

Name: Enter a name for the rule or select an application from the drop-down menu and click << to automatically fill in the rule with the default settings for that application.

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 the **<<** button to automatically fill in the IP address.

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.

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

Application Rules

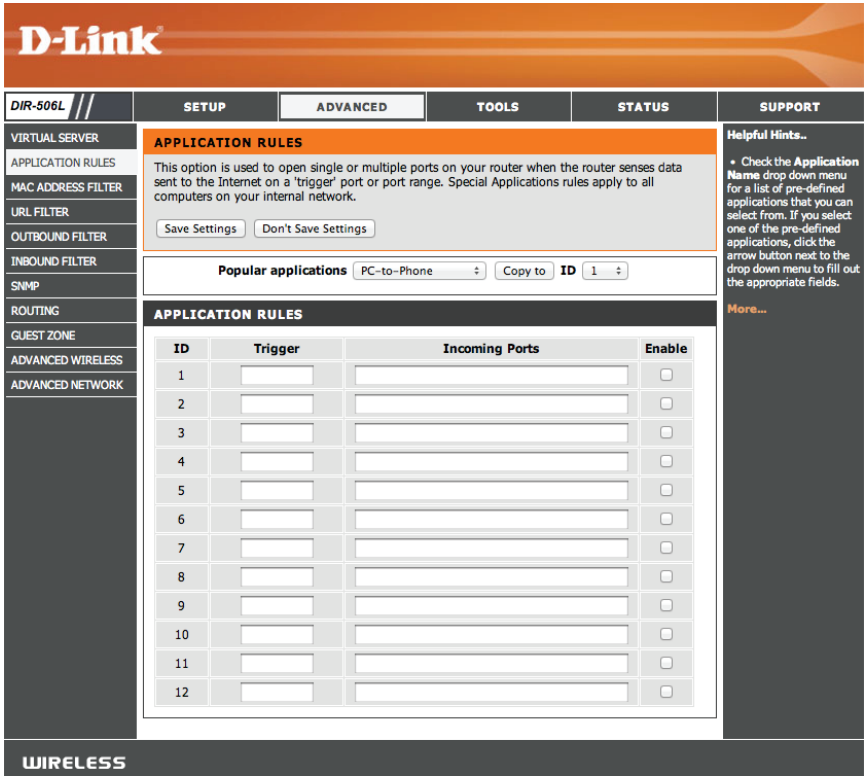
Some applications may require multiple connections, such as Internet gaming, video conferencing, and VoIP calls over the Internet. These applications may have difficulty working through NAT (Network Address Translation). Application Rules allow some of these applications work with the DIR-506L. If you need to run applications that require multiple connections, specify the port normally associated with the application in the **Trigger Port** setting and the ports associated with the trigger port to open them for inbound traffic. After making your changes, click the **Save Settings** button.

Popular applications: Enter a name for the rule or select an application from the drop-down menu and click << to automatically fill in the rule with the default settings for that application.

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

Incoming Ports: Enter the ports you want to allow incoming traffic when the trigger port is activated.

Enable: Check to enable this rule or leave unchecked to ignore it.



MAC Address Filter

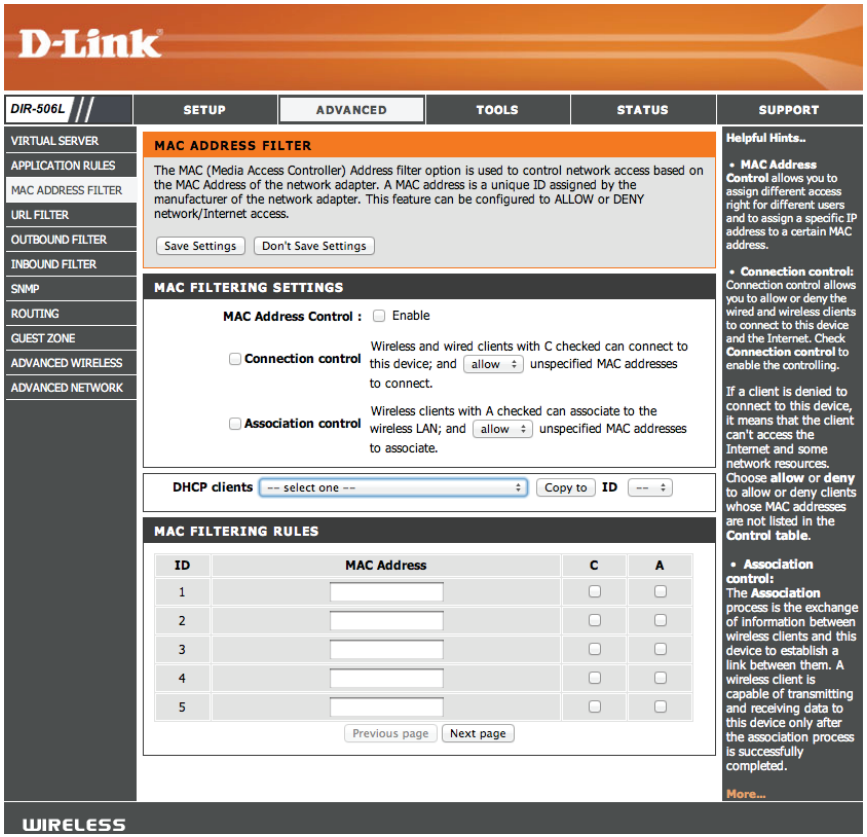
Use MAC (Media Access Control) Filters to control access to your network based on the MAC addresses of connected clients. You can set MAC address filtering to only allow the listed MAC addresses to connect, or block access to all listed MAC addresses. After making your changes, click the **Save Settings** button.

MAC Address Control: Click **Enable** to allow MAC filtering.

Connection Control: When this option is selected, only PCs and devices with MAC addresses listed below with the 'C' option checked can connect to the router. The drop-down menu will allow you to choose whether all other MAC addresses that are not in the list will be blocked or allowed to connect.

Association Control: When this option is selected, only PCs and devices with MAC addresses listed below with the 'A' option checked can associate themselves with the wireless LAN. The drop-down menu will allow you to choose whether all other MAC addresses that are not in the list will be blocked or allowed to associate.

MAC Address: Enter the MAC addresses you would like to filter and then select whether you want them group with the 'C' (Connection Control) group, the 'A' (Association Control) group, or both. If the control groups are not enabled, these designations will be ignored.

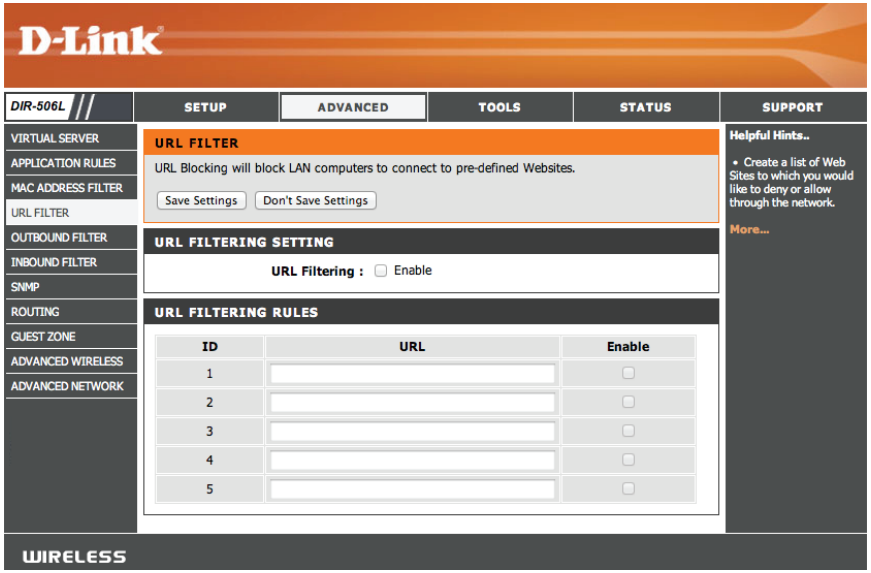


URL Filters

Website Filters are used to allow you to set up a list of websites to either allow or block access to. After making your changes, click the **Save Settings** button.

URL Filtering: Check the **Enable** box to allow website filter rules.

URL Filtering Rules: Enter the websites you want to block or allow in the text boxes. Any website address that contains the text entered will be blocked once you click **Enable** and then save your settings..



Outbound Filters

The Outbound Filter option is an advanced method of controlling data sent from the DIR-506L. With this feature you can configure outbound data filtering rules that control data based on an IP address range. Outbound Filters can be used on outbound packets.

Outbound Filter: Check the **Enable** box to allow outbound filtering rules.

Use schedule rule: Select from the drop-down menu how you want the rule to be scheduled and apply this schedule to existing rules.

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

Allow/Deny all to pass: Here you decide whether to use the outbound filters to allow or deny passage of addresses and ports that match the filter rules you set.

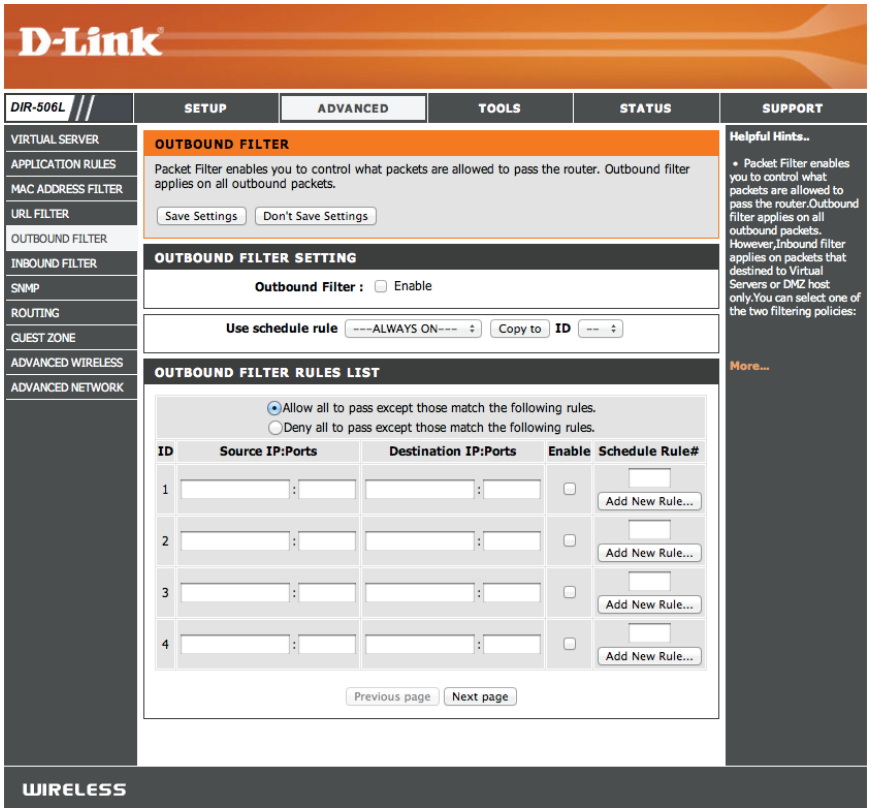
Source IP and Ports: Enter the source IP address and port. Enter 0.0.0.0 if you do not want to specify an IP range.

Destination IP and Ports: Enter the destination IP address and port. Enter 0.0.0.0 if you do not want to specify an IP range.

Enable: Check this box to enable the rule you are creating.

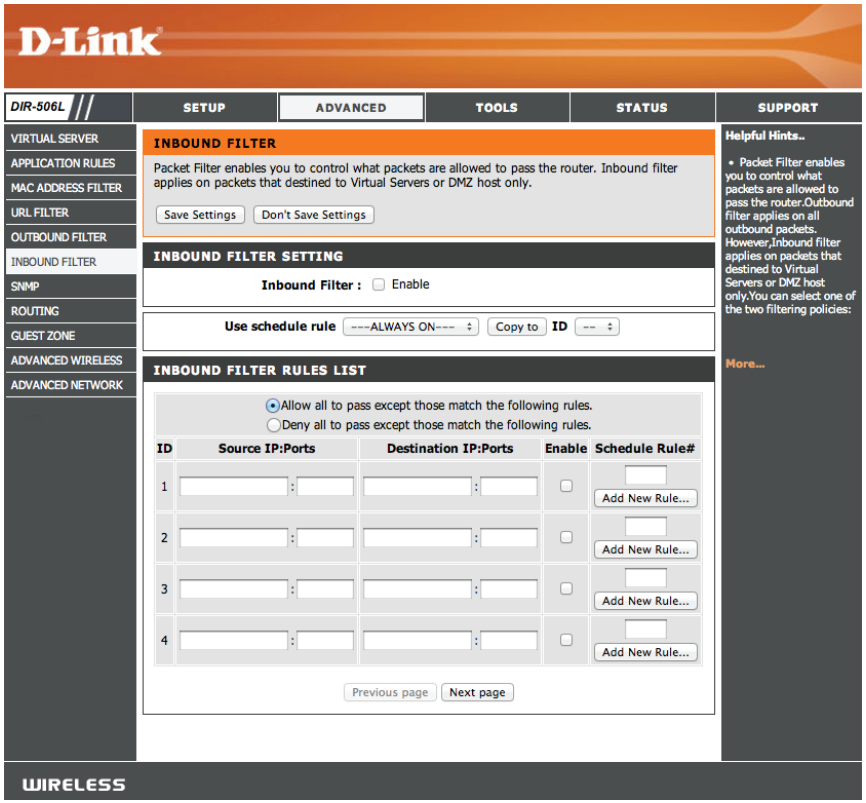
Schedule Rule #: Provide an identification number for the rule.

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



Inbound Filters

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



Inbound Filter: Check the **Enable** box to allow inbound filtering rules.

Use schedule rule: Select from the drop-down menu how you want the rule to be scheduled and apply this schedule to existing rules.

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

Allow/Deny all to pass: Here you decide whether to use the inbound filters to allow or deny passage of addresses and ports that match the filter rules you set.

Source IP and Ports: Enter the source IP address and port. Enter 0.0.0.0 if you do not want to specify an IP range.

Destination IP and Ports: Enter the destination IP address and port. Enter 0.0.0.0 if you do not want to specify an IP range.

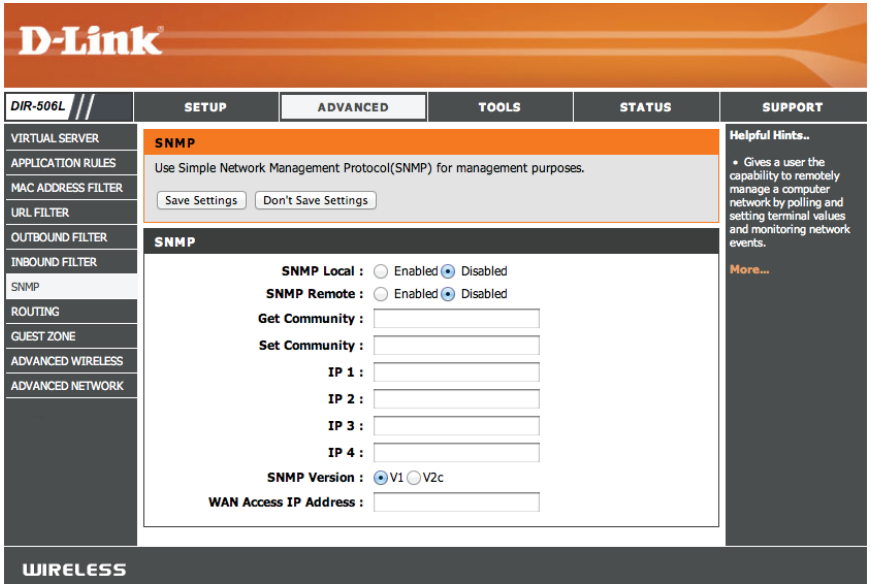
Enable: Check this box to enable the rule you are creating.

Schedule Rule #: Provide an identification number for the rule.

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

SNMP

The Simple Network Management Protocol is an application layer protocol to remotely manage network devices so you can find and solve network problems with ease. After making your changes, click the **Save Settings** button.



SNMP Local: Enable this option to allow local SNMP management.

SNMP Remote: Enable this option to allow remote SNMP management.

Get Community: Enter a name for the read community of your SNMP server.

Set Community: Enter a name for the write community of your SNMP server.

IP 1: Set the first IP address to be managed here.

IP 2: Set a second IP address to be managed here.

IP 3: Set a third IP address to be managed here.

IP 4: Set a fourth IP address to be managed here.

SNMP Version: Choose the version of SNMP to be used by your server.

WAN Access IP Address: Enter the IP address used for WAN access here.

Routing

The Routing option is an advanced method of customizing specific routes of data through your network. After making your changes, click the **Save Settings** button.

RIP: Select **Enable** to turn on routing and auto-select the RIP version, or select **RIPv1** or RIPv2.

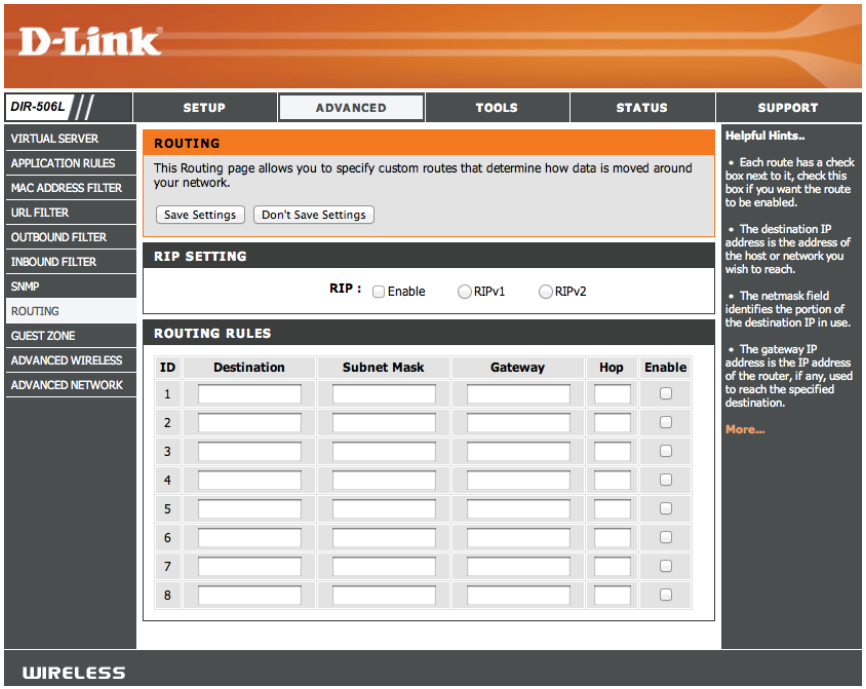
Destination IP: Enter the IP address of packets that will take this route.

Subnet Mask: Enter the netmask of the route, please note that the octets must match your destination IP address.

Gateway: Enter your next hop gateway to be taken if this route is used.

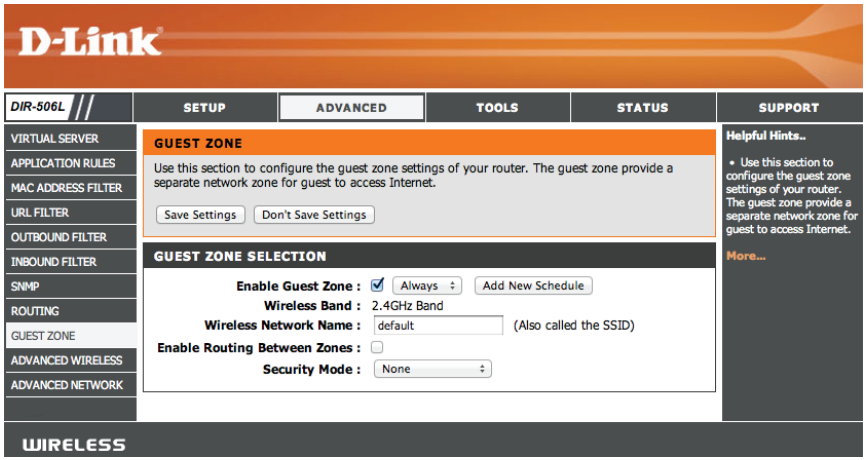
Hop: Enter a number to represent the hop value of this route.

Enable: Check to enable this route or leave unchecked to ignore it.



Guest Zone

The Guest Zone feature allows you to create a separate wireless network for guests to access the Internet without allowing them to connect to your own devices. After making your changes, click the **Save Settings** button.



Enable Guest Zone: Tick this checkbox to enable the Guest Zone feature.

Add New Schedule: Select when the Guest Zone will be active. The schedule may be set to **Always**, which will allow the Guest Zone to be on at all times. You can select a schedule you created, or you can click the **Add New Schedule** button to create a schedule.

Wireless Network Name: Enter a wireless network name (SSID) for your guest zone. It should be different than the network name of your main wireless network.

Enable Routing Between Zones: Check to allow network connectivity between the Guest Zone and your main network.

Security Mode: Here, you can select between **None**, **WEP**, **WPA-Personal**, and **WPA-Enterprise**. Refer to "Wireless Settings" on page 30 for information on how to configure the different security modes.

Advanced Wireless

This screen allows you to set various advanced wireless settings of your DIR-506L. Unless you are experiencing specific problems, it is recommended that you leave these settings at their default values. After making your changes, click the **Save Settings** button.

Beacon Interval This value determines the frequency in which packets broadcast by the router will synchronize the wireless network. Choose a value here.

Transmit Power: Use the dropdown box to set the transmit power of the antennas.

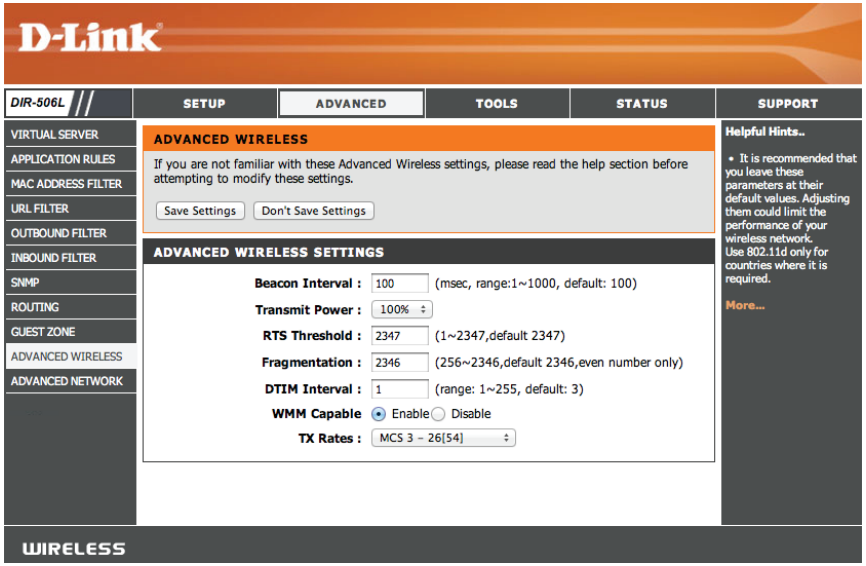
RTS Threshold: Enter the size of each Request to Send frame.

Fragmentation: Enter a value of the maximum size for a packet before the data is fragmented into multiple packets.

DTIM Interval: Set your Delivery Traffic Indication Message rate here.

WMM Capable: WMM is Quality of Service(QoS) for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

TX Rates: Select the TX data rate you would like to use from the drop-down menu.

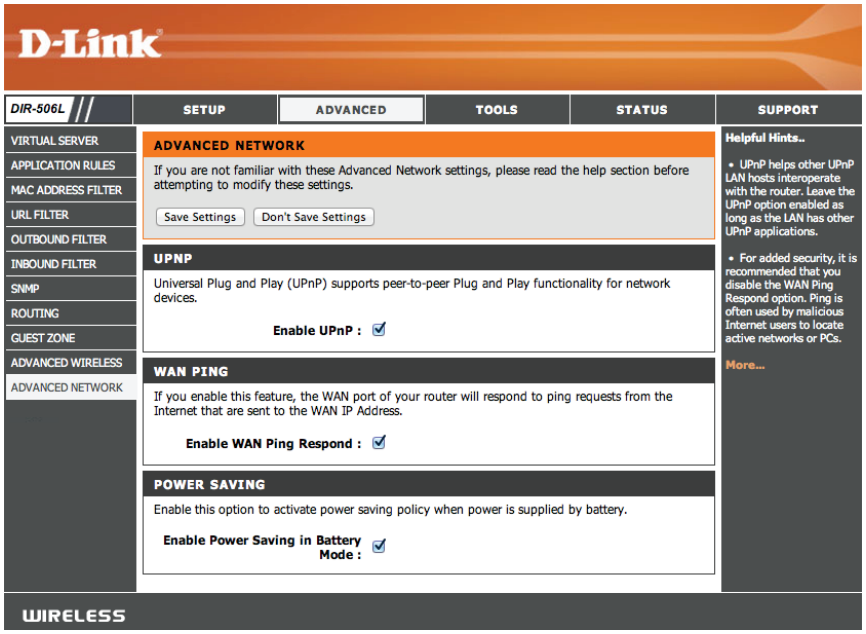


Advanced Network

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

Enable WAN Ping Respond: Checking the box will allow the DIR-506L to respond to pings. Unchecking the box may provide some extra security from hackers.

Enable Power Saving in Battery Mode: Checking this box will allow the router to minimize the power usage when disconnected from a power source and using the battery, while still providing the necessary power for normal operations.



Tools

Administrator Settings

This page will allow you to change the password for the administrator account for configuring the settings of the DIR-506L. You can also turn on remote management. After making your changes, click the **Save Settings** button.

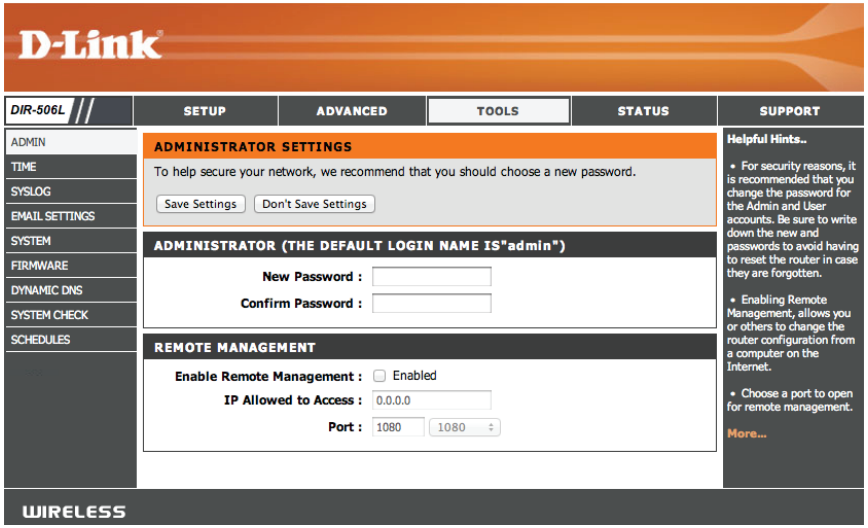
New Password: Enter a new password for the Administrator Login Name. The administrator can make changes to the settings.

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

Enable Remote Management: Remote management allows the DIR-506L to be configured over the Internet through a web browser. A username/password is still required to access the configuration interface.

IP Allowed to Access: This is the IP that will be used to access the DIR-506L configuration interface when using remote management.

Port: This is the port number to be used for remote management.



Time and Date

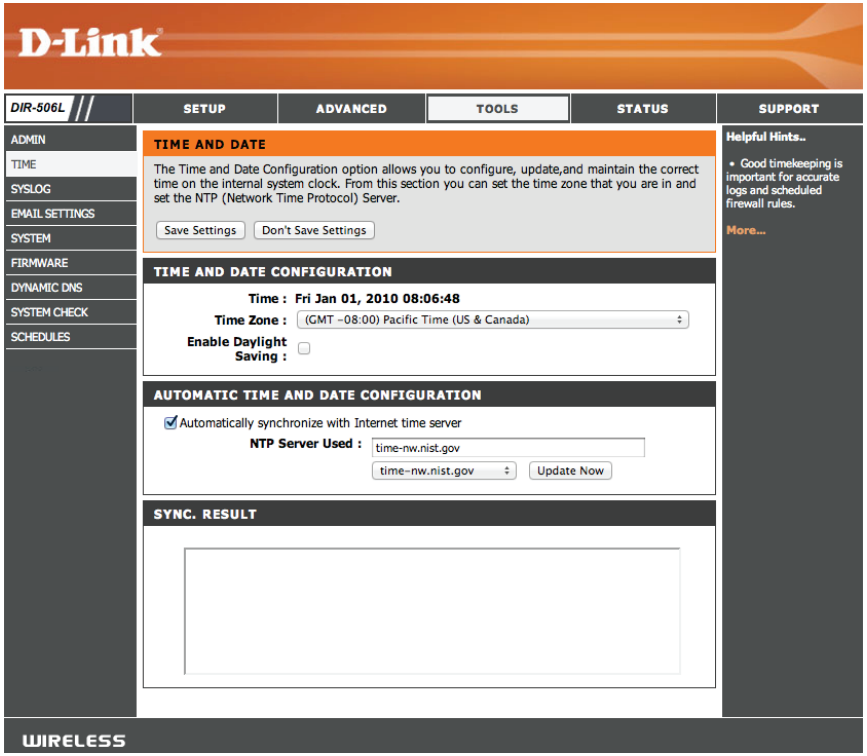
The Time page allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in. Daylight Saving can also be configured to automatically adjust the time when needed. After making your changes, click the **Save Settings** button.

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

Enable 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.

Auto Sync: 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.

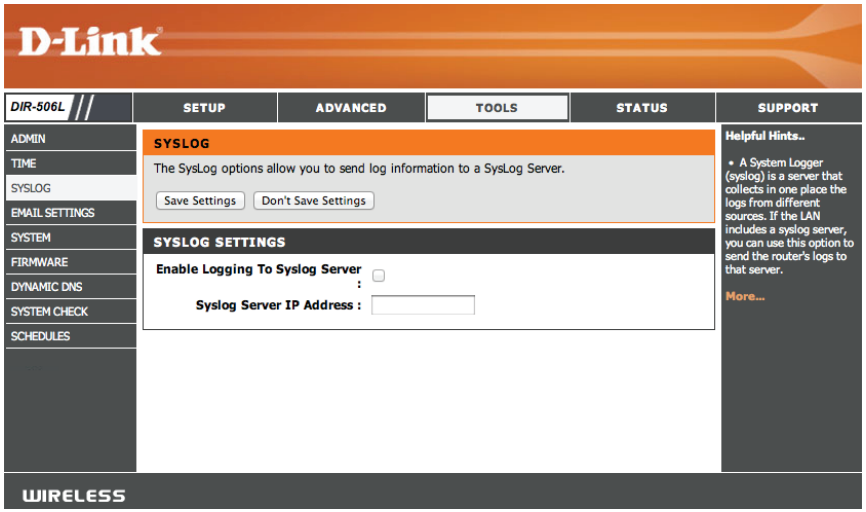


SysLog

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

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

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



Email Settings

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

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

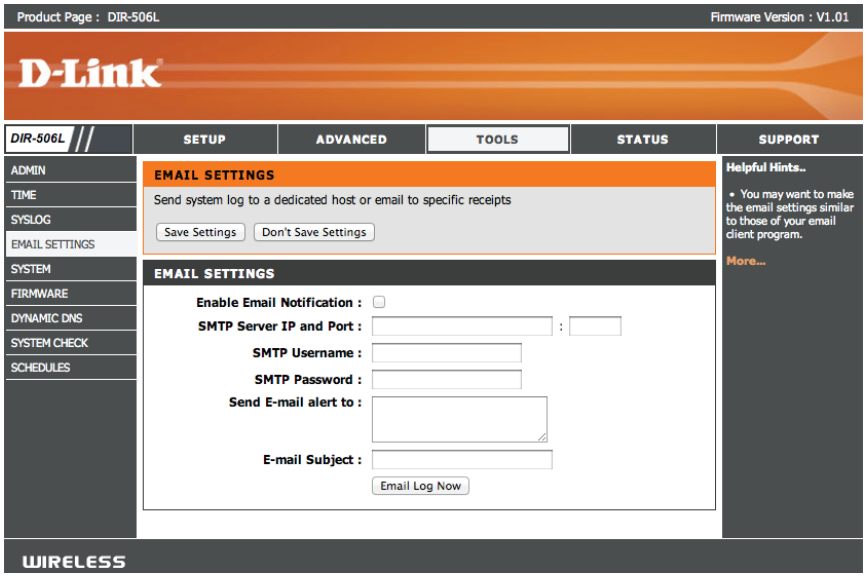
SMTP Server IP and Port: Enter the SMTP server address and SMTP port used for sending email.

SMTP Username: Enter your account username for sending email.

SMTP Password: Enter the password associated with the account.

Send E-mail alert to: Enter the email address(es) where you would like your email alerts delivered.

E-mail Subject: Enter a subject line for the alert emails.



System Settings

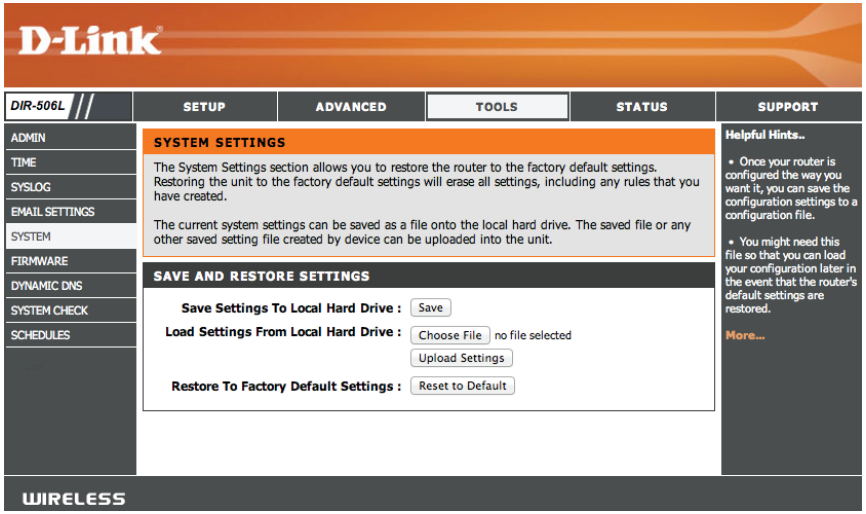
This page allows you to save and restore your configuration, reset and reboot the DIR-506L, and remove any added language packs.

Save Settings To Local Hard Drive: Clicking the **Save** button will allow you to save the current repeater configuration settings to a file on the hard disk of the computer you are using. You will then see a file dialog where you can select a location and file name for the settings.

Load Settings From Local Hard Drive: Use this option to load previously saved configuration settings. Click **Browse** to find a previously saved configuration file. Then, click the **Upload Settings** button to transfer those settings to the DIR-506L.

Restore to Factory Default Settings: This option will restore all configuration settings back to the factory default settings. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save your current configuration settings, use the **Save** button above.

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

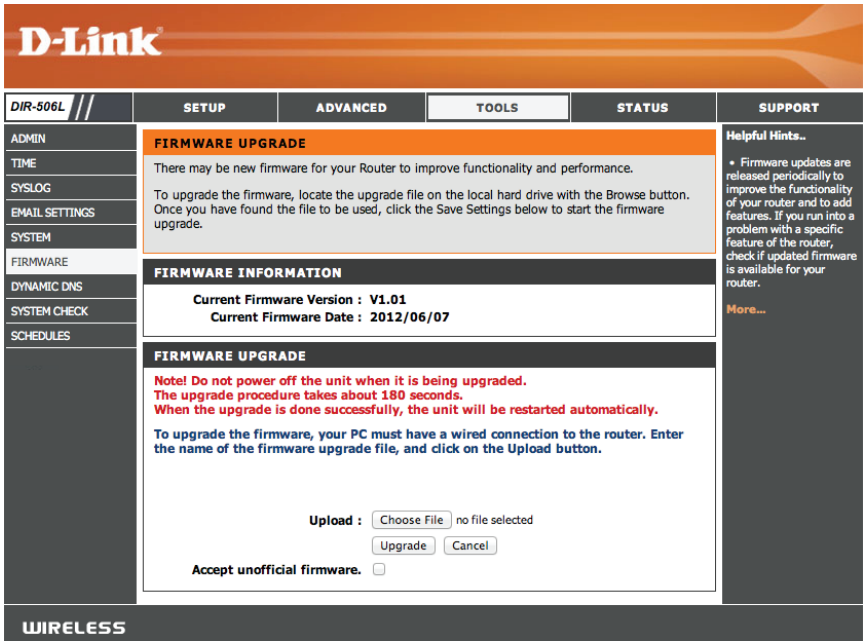


Firmware Upgrade

You can upgrade the firmware of the DIR-506L 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 upgrade. 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.

Upload: After you have downloaded the new firmware, click **Choose File** to locate the firmware update on your hard drive. Click **Upgrade** to complete the firmware upgrade. Do not disconnect from the DIR-506L or power your computer or DIR-506L off during the upgrade process.

Accept unofficial firmware: Check this box to apply a firmware file that is not an official release from D-Link. Using this option is not recommended.



Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) behind your 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. After making your changes, click the **Save Settings** button.

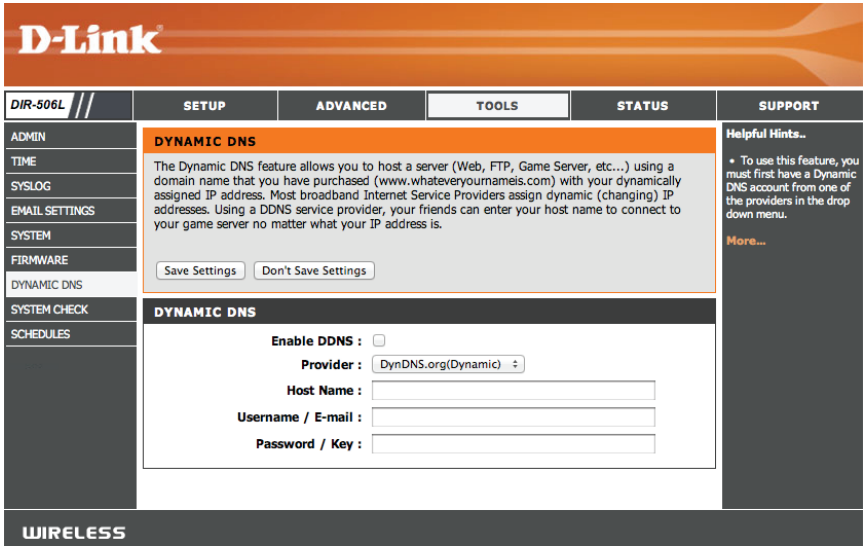
Enable Dynamic DNS: Tick the checkbox to enable DDNS.

Provider: Select your DDNS service from the drop-down menu.

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

Username or E-mail: Enter the Username or key for your DDNS account.

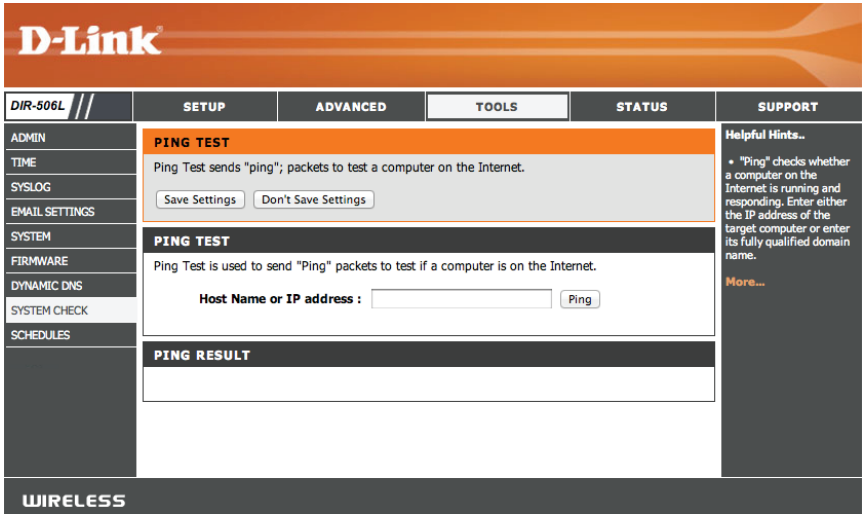
Password or Key: Enter the Password or key for your DDNS account.



System Check

This page allows you to run a ping test to check your Internet connectivity.

Host Name or IP address: The Ping Test is used to send ping packets to test if your is connected to the Internet. Enter the host name or IP address that you wish to ping and click the **Ping** button.



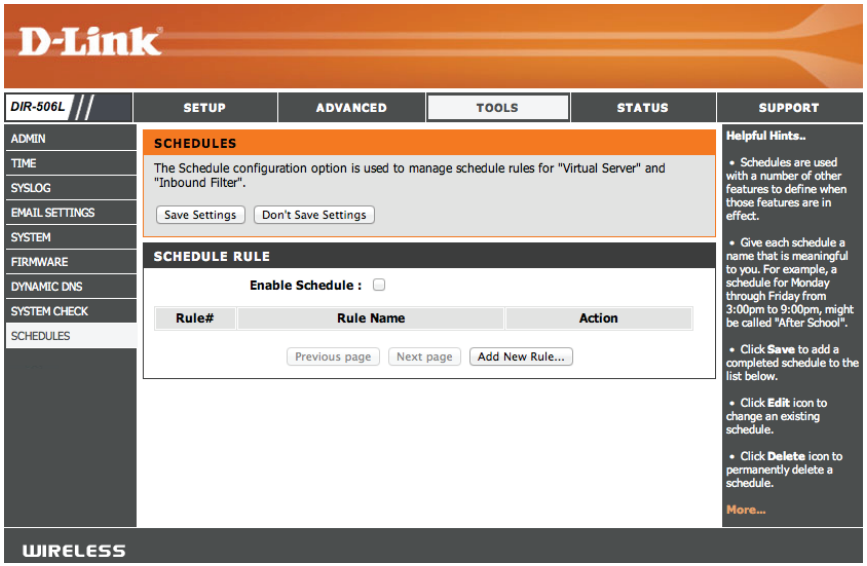
Schedules

You can create schedules for use with some of the features of the DIR-506L, which will allow those features to be active during certain times of the day or week.

Enable Schedule: Allows the DIR-506L to apply schedule rules for the filters you have configured.

After entering the details of your schedule, click the **Save** button to save your changes.

Schedule Rules List: The list of created schedules will be listed here. Click the **Add New Rule** button to create a schedule rule.



Status

Device Info

This page displays the current information for the DIR-506L. It will display the LAN and wireless LAN information.

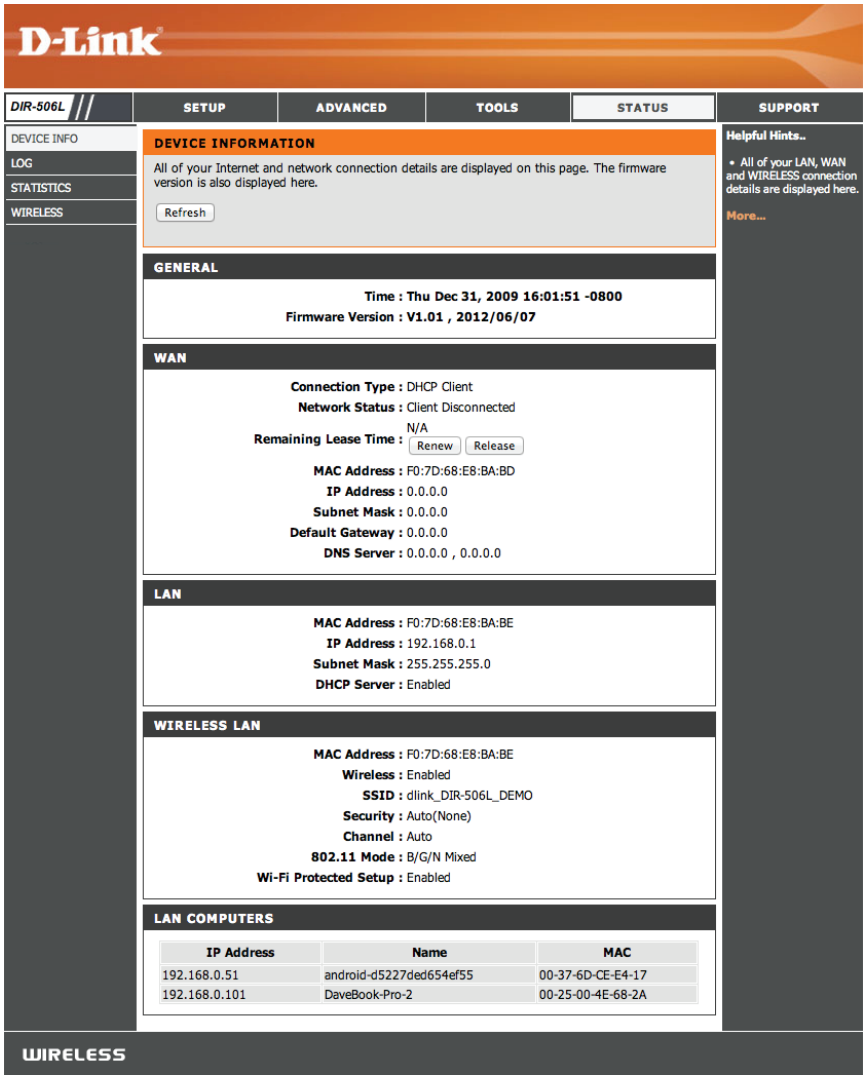
General: Displays the time and firmware version.

WAN Displays information about the connection to your modem or Internet connection.

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.

LAN Computers: Displays information about the devices on your local network.



Logs

The DIR-506L keeps a running log of events and activities occurring on the DIR-506L. If the DIR-506L is rebooted, the logs are automatically cleared.

Log Options: There are several types of logs that can be viewed: **System Activity, Debug Information, Attacks, Dropped Packets** and **Notice**.

Previous: This button directs you to the previous page of the log.

Next: This button directs you to the next page of the log.

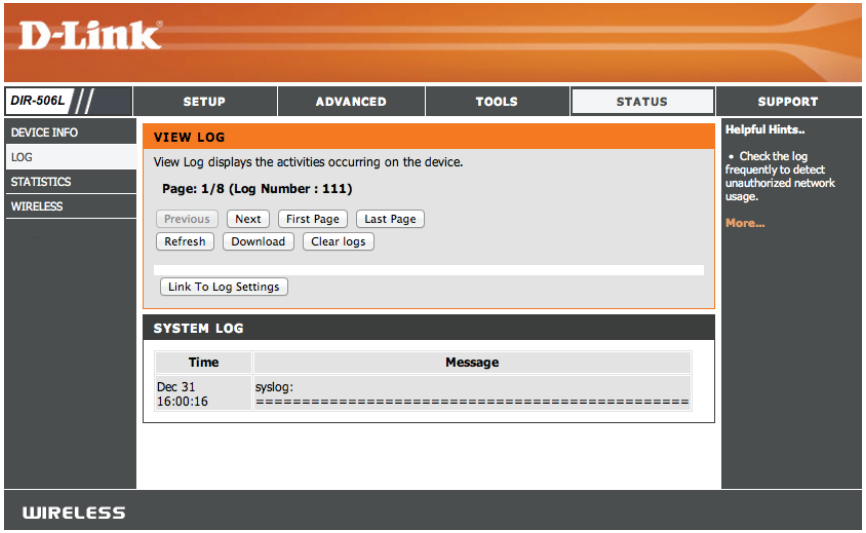
First Page: This button directs you to the first page of the log.

Last Page: This button directs you to the last page of the log.

Refresh: This button refreshes the log.

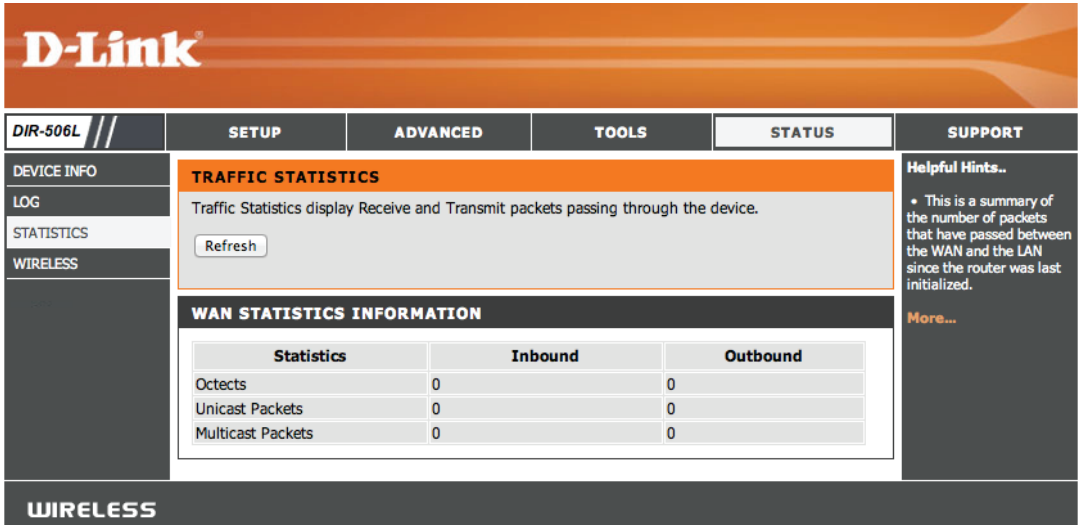
Download: This button opens dialog where you can save the current log to your hard drive.

Clear logs: This button clears all current log content.



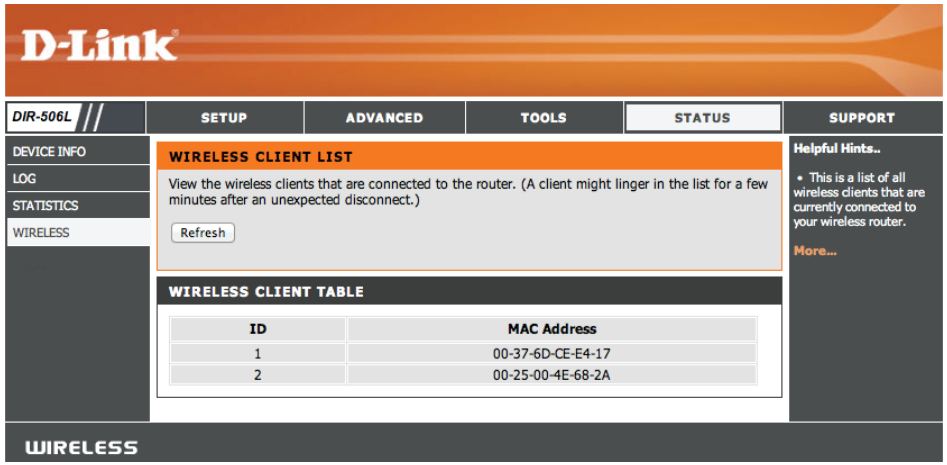
Statistics

The DIR-506L 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. Click the **Refresh Statistics** button to update the information, or click the **Clear Statistics** button to reset all statistics. The traffic counter will reset if the DIR-506L is rebooted.



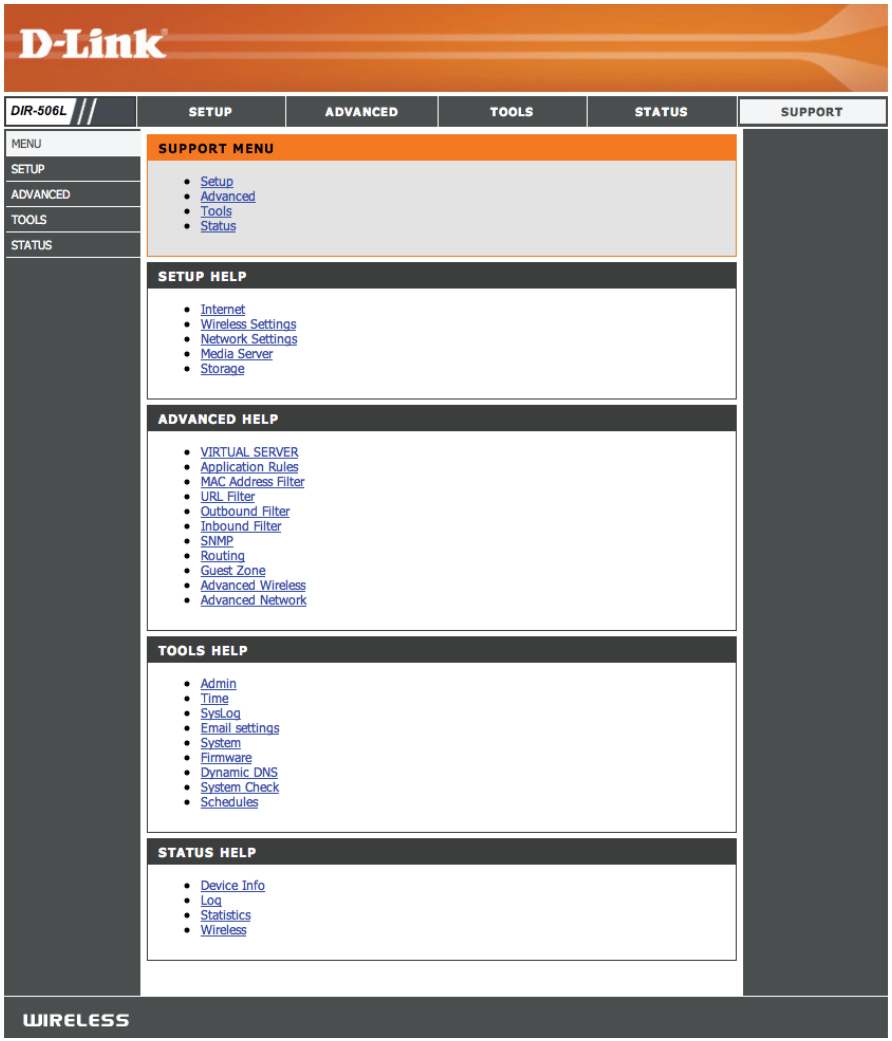
Wireless Client List

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.



Help

This screen gives you more information about the various parts of the configuration interface. Click on a link to learn more about that topic.



Connecting a Wireless Client

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-506L 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-506L 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.

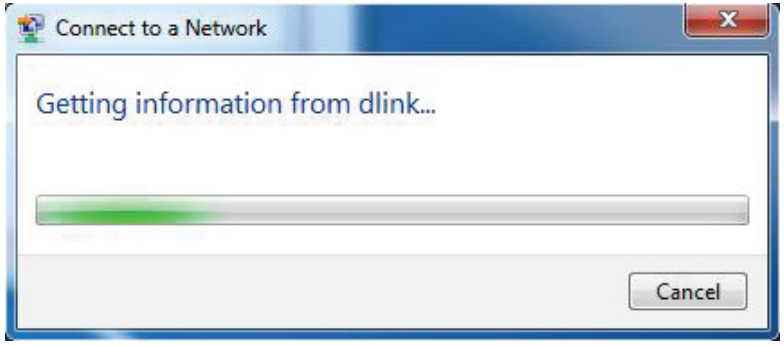
1. Click on the wireless icon in your system tray (lower-right corner).

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

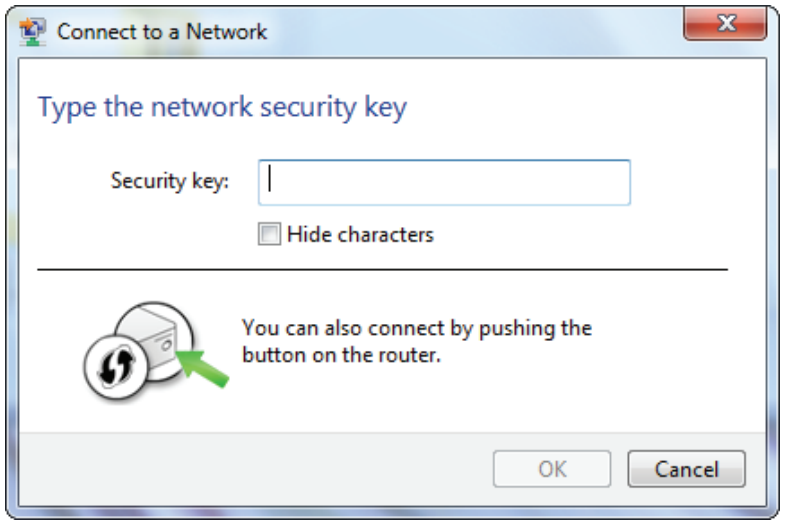
3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

   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.

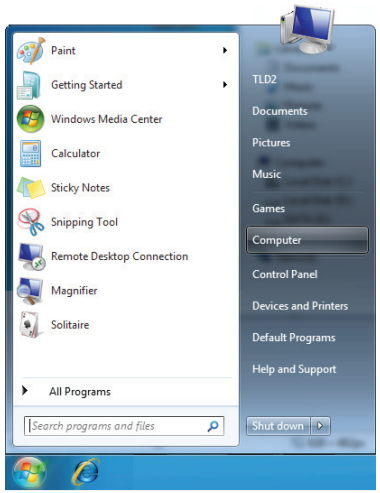


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

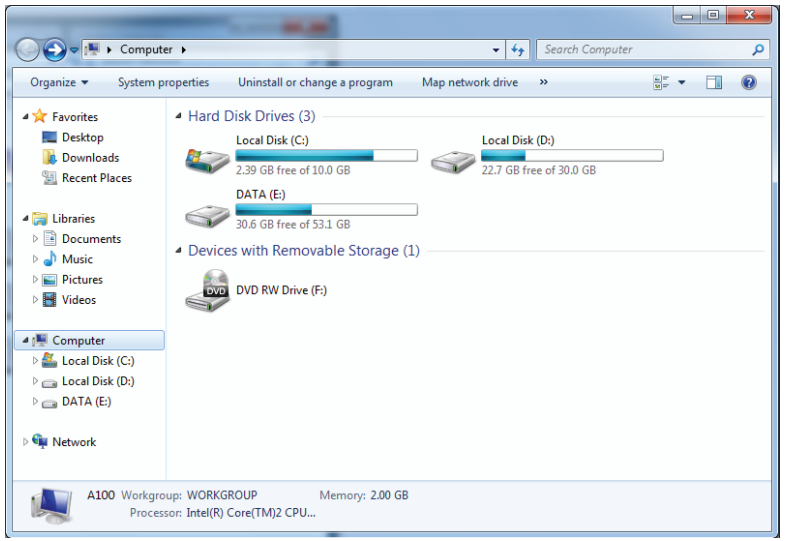
WPS

The WPS feature of the DIR-506L can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

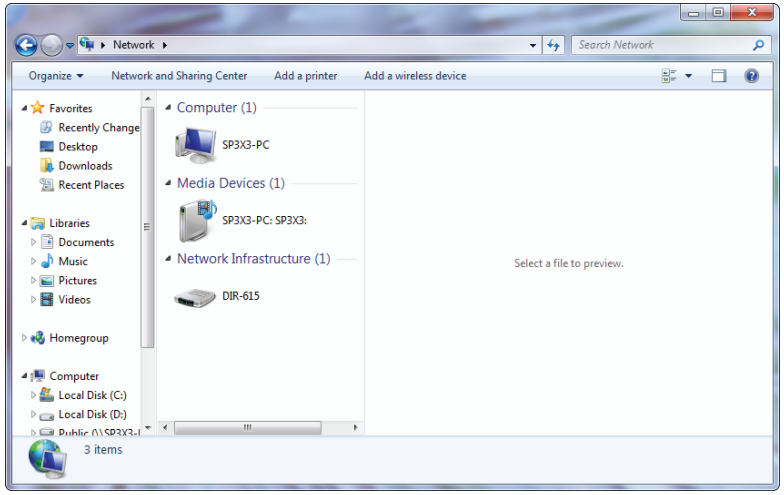
1. Click the **Start** button and select **Computer** from the Start menu.



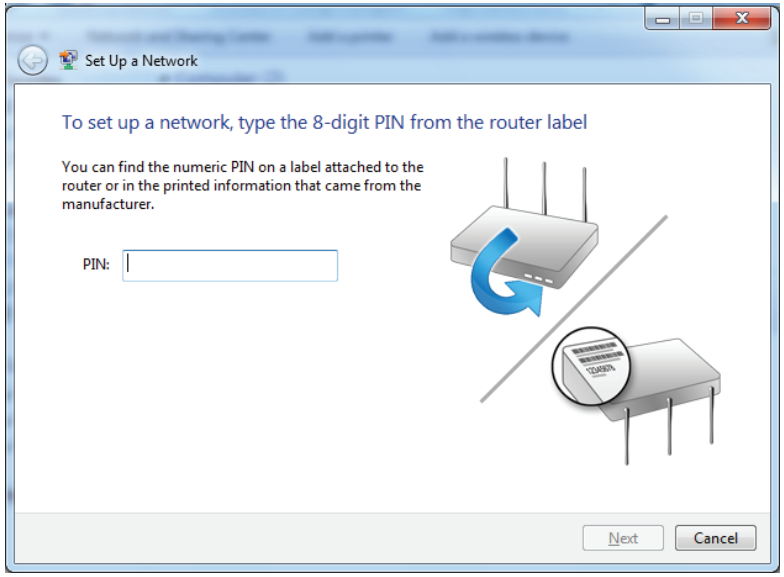
2. Click **Network** on the left side.



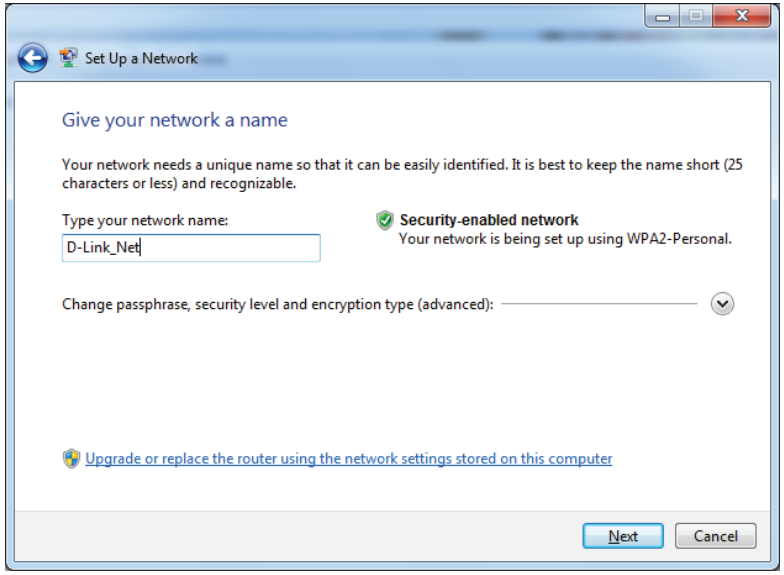
3. Double-click the DIR-506L.



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**.

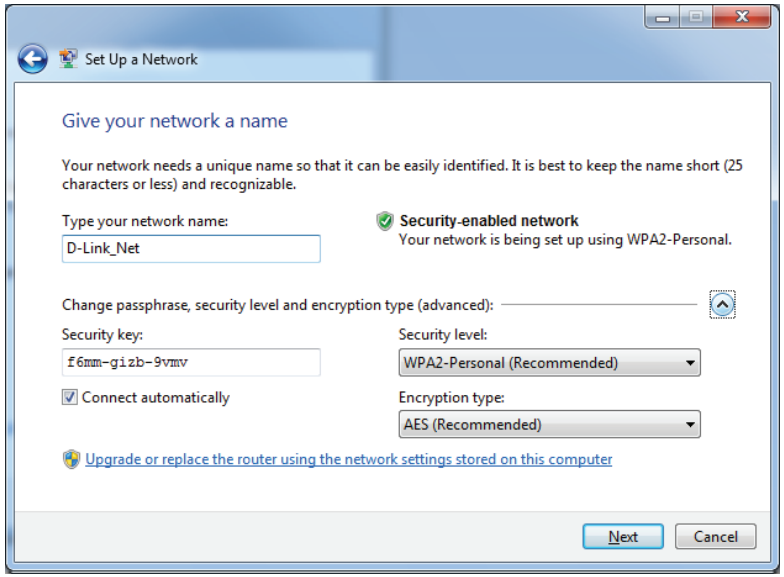


5. Type a name to identify the network.



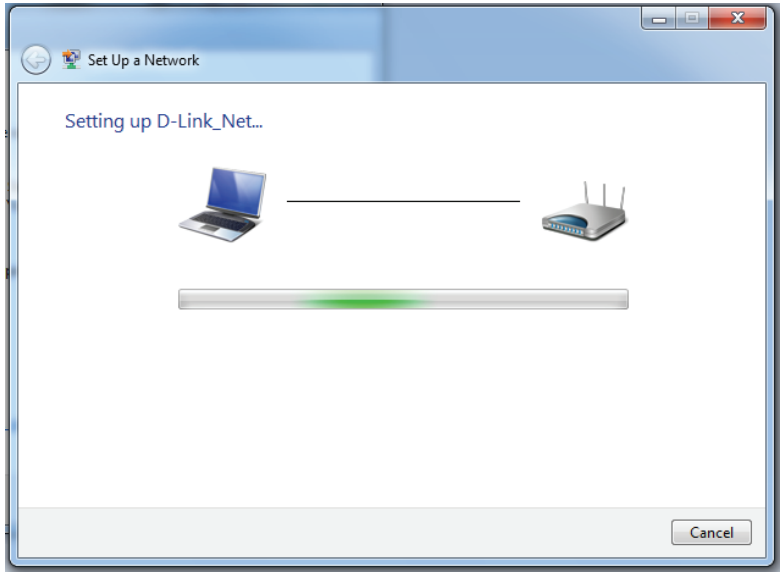
6. To configure advanced settings, click the icon.

Click **Next** to continue.



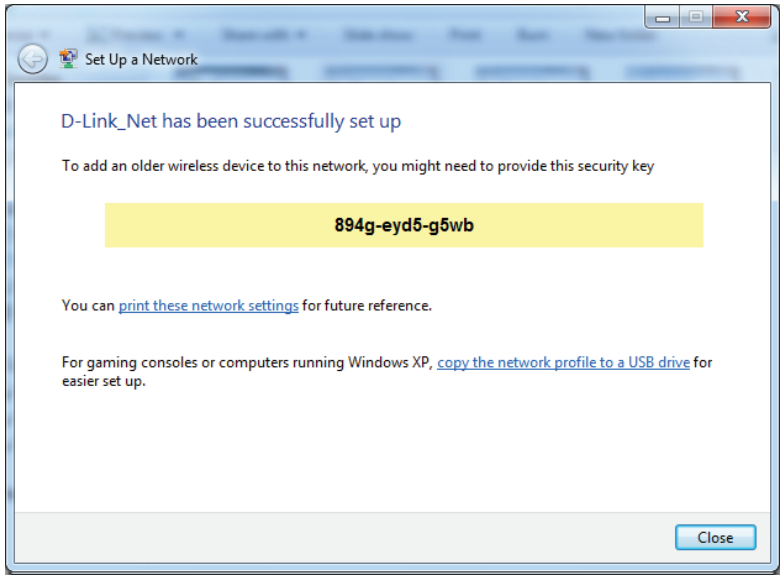
7. The following window appears while the Router is being configured.

   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.

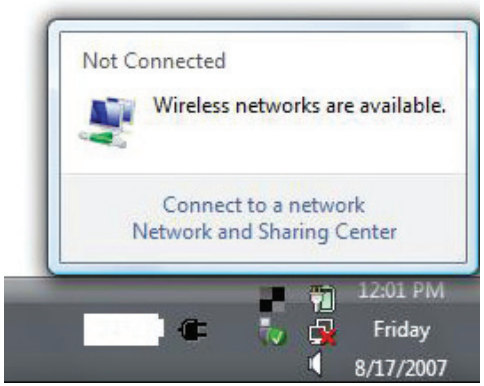
Windows Vista®

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.

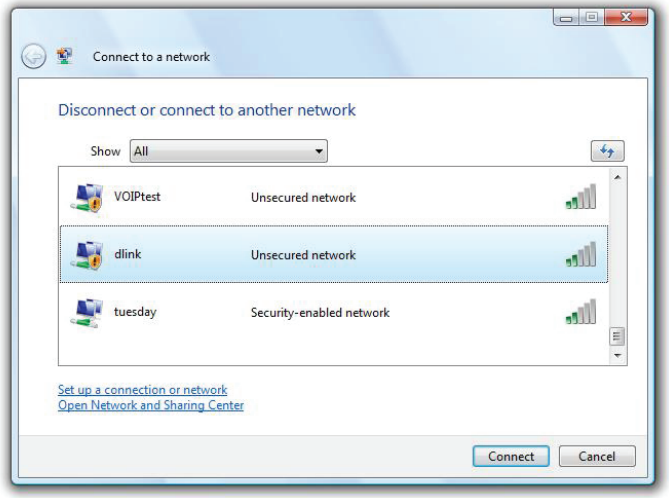
or

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.

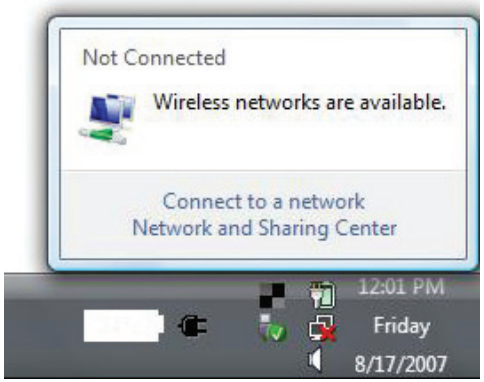
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



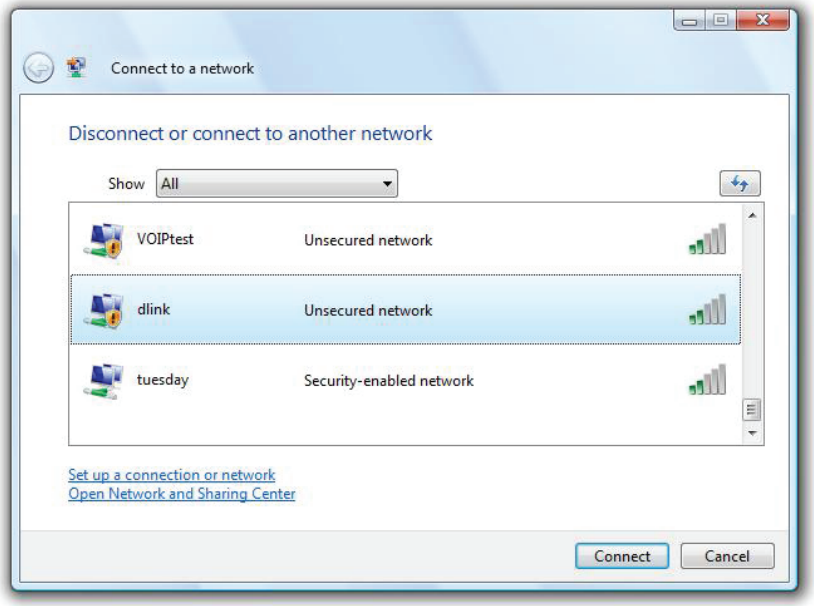
WPA/WPA2

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**.

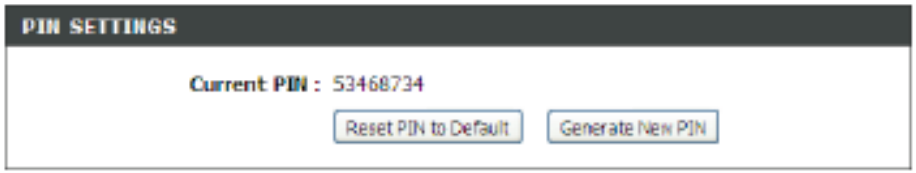
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

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.

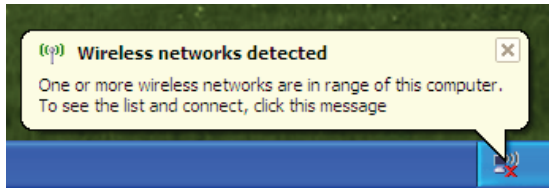


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Windows® XP

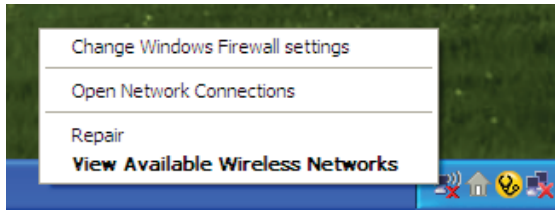
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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



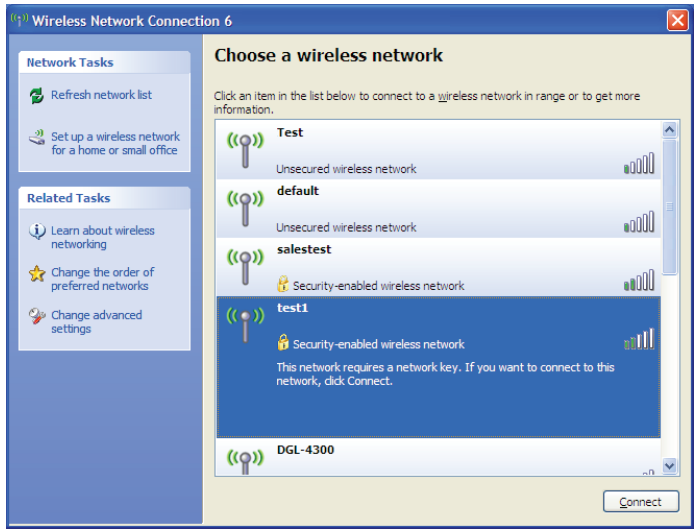
or

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.

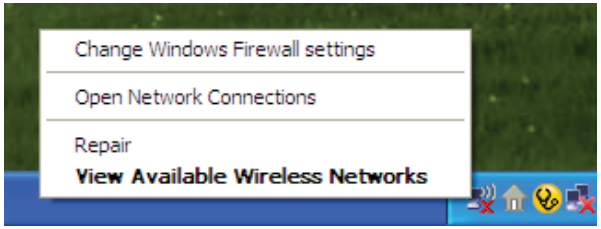
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



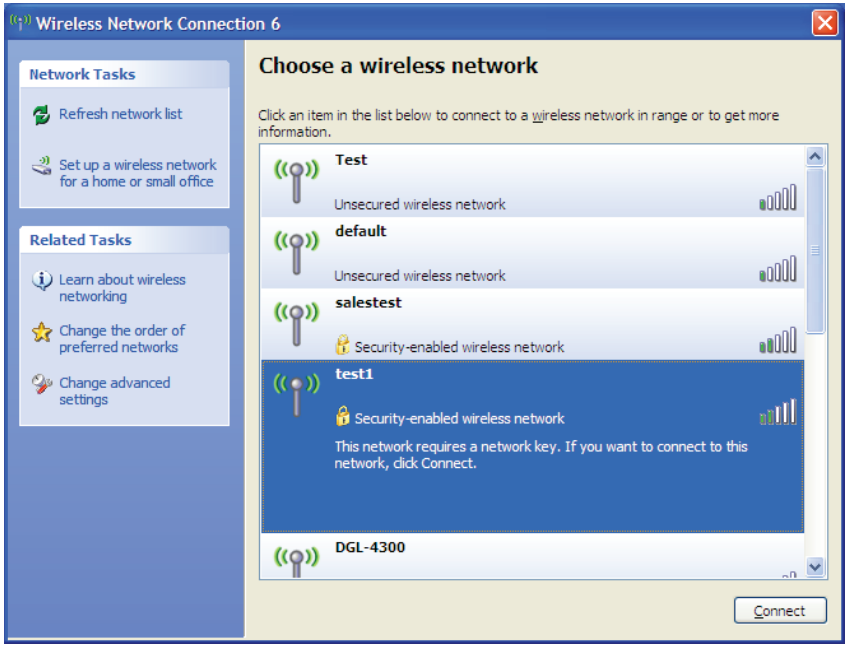
WPA/WPA2

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.

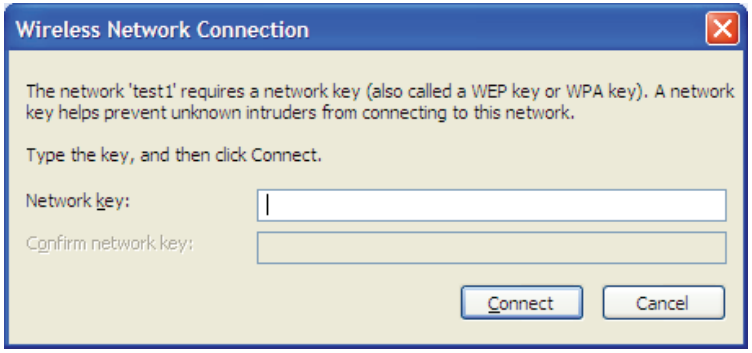
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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 . 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, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

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

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

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

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

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

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

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

Networking Basics

Check your IP address

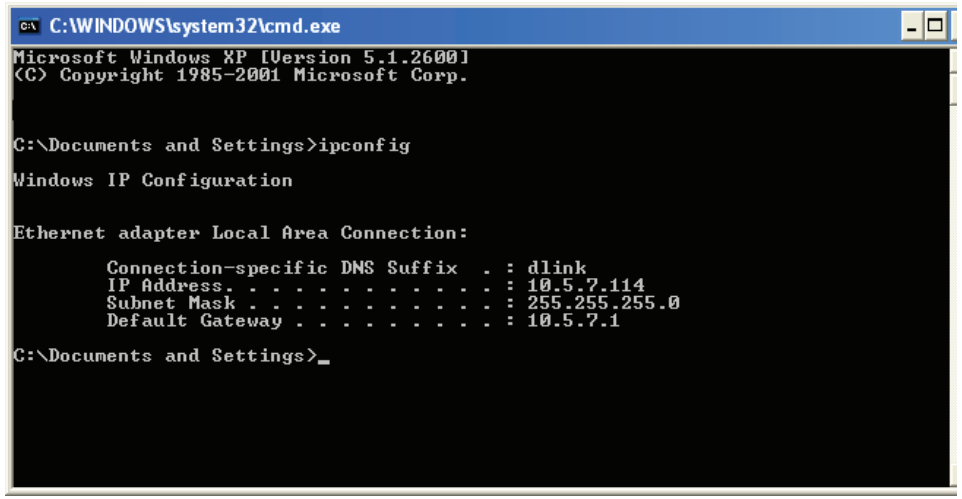
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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.



Assign a Static 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

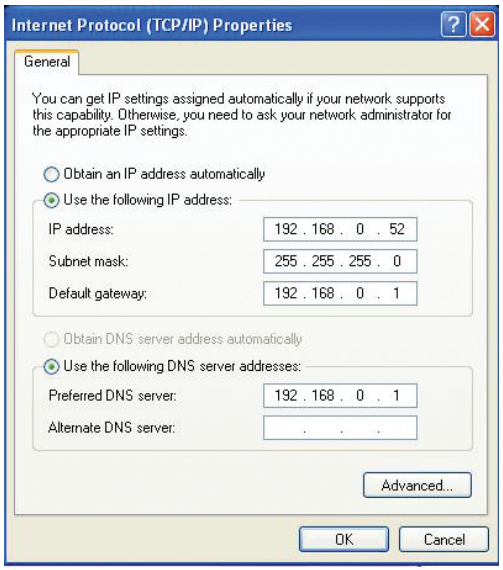
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

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 802.11g, compatible with 802.11n devices
- IEEE 802.3
- IEEE 802.3u

Wireless Modes
- Router/AP Mode
- Repeater Mode
- Wi-Fi Hot Spot Mode

Wireless Frequency Range [1]
- 2.4 GHz to 2.4835 GHz

Antennas
- Internal Antenna

Security
- Wi-Fi Protected Access (WPA/WPA2)
- WPS™ (PBC)

Advanced Features
- SharePort™ Mobile app for iOS [2]
- VPN pass-through
- Guest Zone Support
- UPnP™ Support
- Web File Access Support
- Wi-Fi WMM Quality of Service

Advanced Firewall Features
- Network Address Translation (NAT)
- Stateful Packet Inspection (SPI)
- MAC Address Filtering

Device Management
- Web UI

Diagnostic LEDs
- Power/Status

Operating Temperature
- 0 to 40 ˚C (32 to 104 ˚F)

Operating Humidity
- 0% to 90% non-condensing

Certifications
- CE
- Wi-Fi Certified
- FCC
- IC

Dimensions
- 68 x 42 x 51 mm (2.68 x 1.65 x 2 inches)

Weight
- 113.4 grams (0.25 lb)

[1] Frequency Range varies depending on local regulations

[2] SharePort Mobile app functionality only available when in Router or Wi-Fi Hotspot mode.

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 LGPLsource 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.

Safety Statements

CE Mark Warning:

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

FCC Statement:

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

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.

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.

Operations in the 5.15-5.25GHz / 5.470 ~ 5.725GHz band are restricted to indoor usage only.

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

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.

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

(i) The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems;
(ii) The maximum antenna gain (2dBi) permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

In addition, users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

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.