D-Link®

Version 1.0 | 01/25/2013

User Manual

DIR-505L

Preface

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

Manual Revisions

Revision	Date	Description
1.0	January 25, 2013	• Initial release for Revision A1

Trademarks

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

Table of Contents

Package Contents

DIR-505L SharePort Mobile Companion

Ethernet Cable

Wireless Configuration Card

Quick Install Guide

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

System Requirements

Network Requirements	• An Ethernet-based Internet connection (Router mode) • A wireless-based Internet connection (Hotspot mode) • A wireless router (Repeater mode) • An Ethernet router or switch (AP mode) • IEEE 802.11n or 802.11g wireless clients
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows® 8, 7, Vista®, or XP (SP 2 or higher), Mac OS® X (10.7 or higher) • An installed Ethernet or wireless adapter **Browser Requirements:** • Internet Explorer® 7 or higher • Firefox 9 or higher • Safari 5 or higher • Google Chrome 16 or higher **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 IEEE 802.11 g/n wireless technology to provide the best wireless performance.

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

TOTAL COVERAGE
The DIR-505L delivers powerful 802.11n performance and increases the range of your wireless network by extending the range of your wireless coverage of another AP or wireless router.

ULTIMATE PERFORMANCE
The DIR-505L is a 802.11n-compliant device that delivers real world performance. Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the DIR-505L 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-505L 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 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Features

- **Faster Wireless Networking** - The DIR-505L provides up to 150Mbps* 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 DIR-505L is still fully compatible with the IEEE 802.11g standards, so it can connect with existing 802.11g, USB, and Cardbus adapters.

- **Advanced Firewall Features** - The Web-based user interface displays a number of advanced network management features including:

    - **Content Filtering** - Easily applied content filtering based on MAC address, URL, and/or Domain Name.

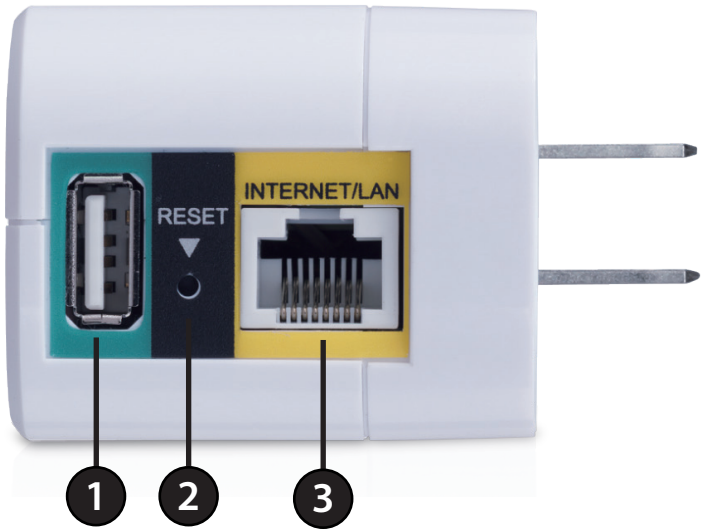
    - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.

    - **Secure Multiple/Concurrent Sessions** - The DIR-505L can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-505L can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-505L lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

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

Hardware Overview
Connections



1	**USB Port**	Connect a USB thumb drive/external hard drive using SharePort™ Mobile and SharePort™ Web File Access. Both will allow you to share files with your local network.
2	**Reset Button**	Press and hold the **Reset** button for 6 seconds to restore the DIR-505L to its original factory default settings.
3	**Ethernet Port**	The Ethernet port is used to connect to a broadband modem or to a port supplying an Internet connection (I.E. a hotel) using an Ethernet cable.

Hardware Overview

LEDs

LED Indicator	Color	Status	Description
Power/Status	**Green**	Solid Green	The device is powered ON and operating properly.
		Blinking Green	The device is processing WPS.
		Off	The device is off.
	Red	Solid Red	During boot up or system is defective.
		Off	The device is off.

Installation

The next few pages will explain the different operational modes you can use.

Operation Modes

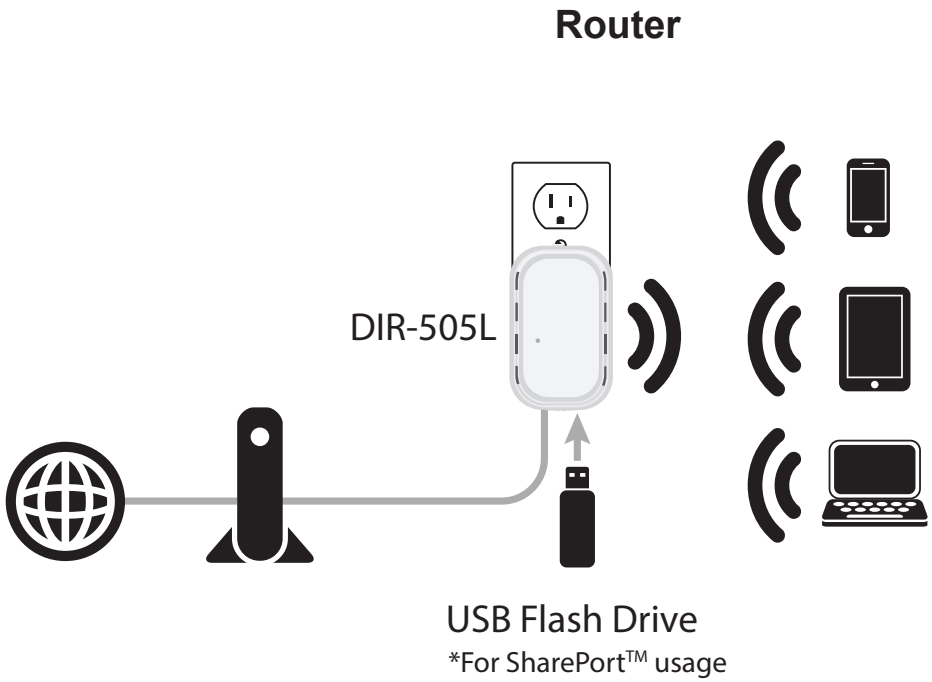
Depending on how you want to use your DIR-505L will determine which mode you use. This section will help you figure out which setting works with your setup.

- Router mode
- Access Point mode
- Repeater mode
- Wi-Fi Hotspot mode
- Charger mode

Router Mode

The DIR-505L connects to your cable modem, DSL modem or other Internet source (using Ethernet) and shares your Internet connection with your devices wirelessly. You can also share files with other computers or devices on your wireless network by using the SharePort™ feature.

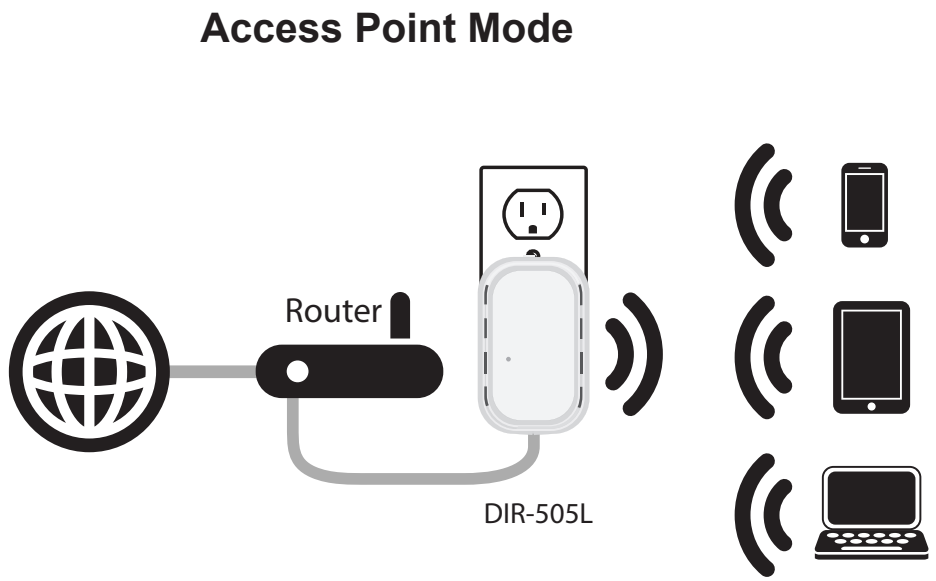
Note: *Use this mode if your Internet connection requires an Ethernet connection. If the Internet connection is wireless, like in a hotel, refer to* ***Hotspot Mode****.*



Access Point Mode

The DIR-505L can connect to an existing network and allow wireless devices to connect to the network. Plug the DIR-505L into your network (via switch or router) using an Ethernet cable. Wireless devices can now connect to the DIR-505L and access your network. Note that AP mode does not support sharing files from a USB storage drive or the SharePort Mobile app.

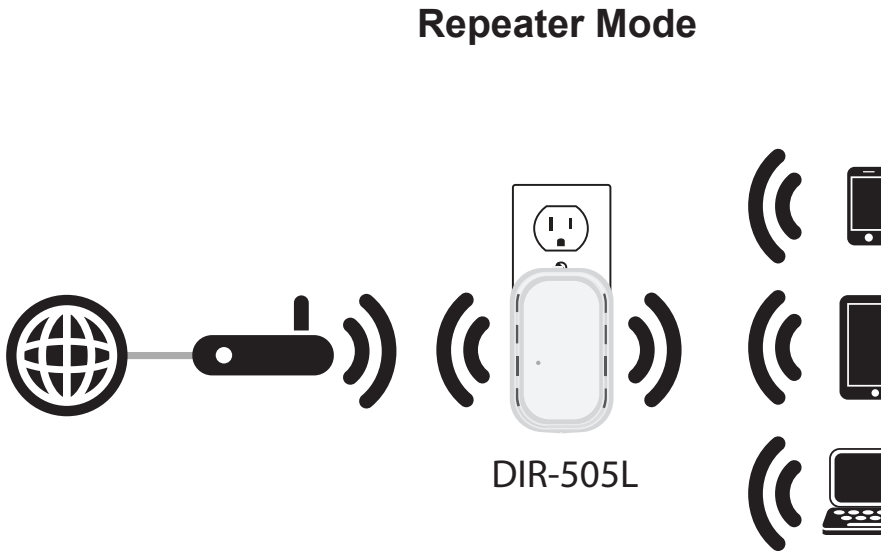
Note: *You will need a router to share an Internet connection while the DIR-505L is in Access Point mode. To share the Internet, use Router or Hotspot mode.*



Repeater Mode

In *Repeater* mode, the DIR-505L increases the range of your wireless network by extending the wireless coverage of another AP or wireless router. The APs and wireless router (if used) must be within range of each other. Make sure that all clients, APs, and the wireless router all use the same Wi-Fi Network Name (SSID) and security settings.

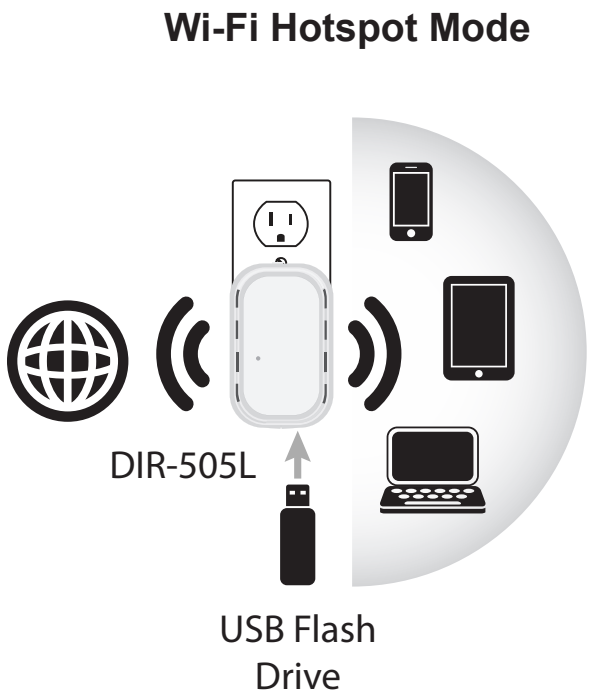
Note: *You will need a router to share an Internet connection while the DIR-505L is in Repeater mode. To share the Internet, use Router or Hotspot mode.*



Hotspot Mode

The DIR-505L can connect to an existing wireless network with an Internet connection, such as a hotspot at a hotel. This will allow you to share that single connection to multiple wireless devices. You can also share files with other computers or devices on your wireless network by using the SharePort™ Mobile app or SharePort™ web access.

Note: *Use this mode if your Internet connection is wireless. If the Internet connection requires an Ethernet cable, refer to* ***Router Mode****.*



Note: *When configuring the DIR-505L in Hotspot mode, the default IP address to access the Web UI is* ***192.168.100.1****.*

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.

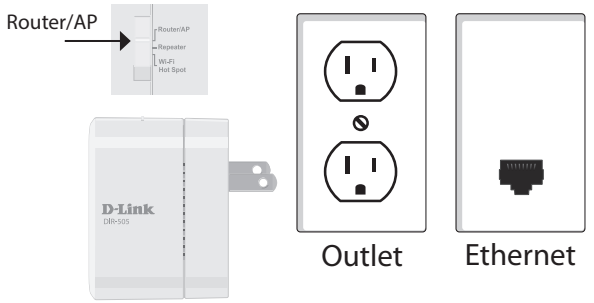
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, 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.

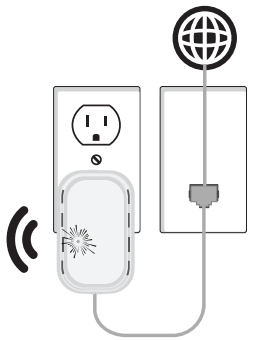
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

Manual Setup
Router/Access Point Mode

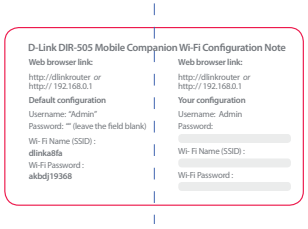
1. Find an outlet close to an Internet-enabled device. Then, move the switch to "**Router/AP Mode**" and plug the DIR-505L into a wall outlet. Verify that the power LED has turned green.



2. Connect one end of an Ethernet cable into the Ethernet port of the Internet-enabled device (such as a modem or Ethernet port in a hotel) and then plug the other end of this cable into the Ethernet port of the DIR-505L.



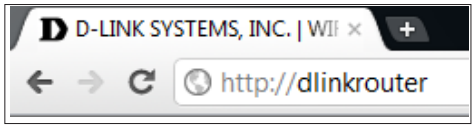
3. From your laptop or mobile device go to your Wireless Utility to display the available wireless networks and select the Wi-Fi name that is displayed on your companion card (ex: **dlink-a8fa**). Then, enter the Wi-Fi password included on your card (**akbdj1936**).

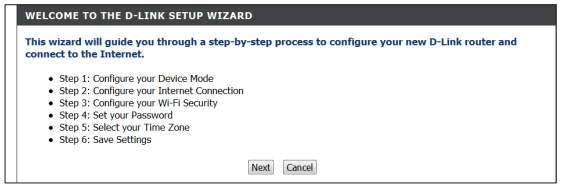


4. Open a web browser. First-time users will automatically be directed to the wizard. Please follow the on-screen instructions to complete the setup.

   Type **http://dlinkrouter** (or **http://192.168.0.1**) in the address bar if the wizard does not appear. Once the setup is complete then proceed to the next step.

   *If you are using a Mac or tablet, type **http:/dlinkrouter.local** in the address bar.

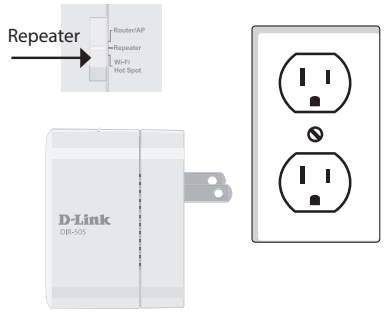




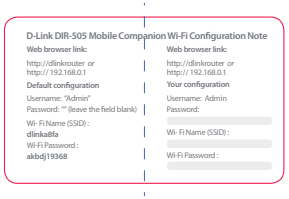
5. From your laptop or mobile device, go to your wireless utility to display the available wireless networks and select the network that you created for internet access.

Repeater Mode

1. Move the switch to "**Repeater Mode**," then plug the DIR-505L into a wall outlet and verify that the power LED has turned green.

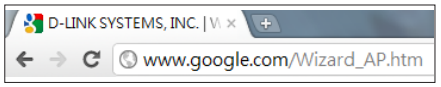


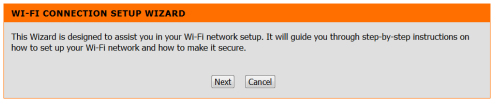
2. From your laptop or mobile device go to your Wireless Utility to display the available wireless networks and select the network found on your companion card (ex: **dlink-a8fa**). Then, enter the Wi-Fi password included in your card (**akbdj1936**).



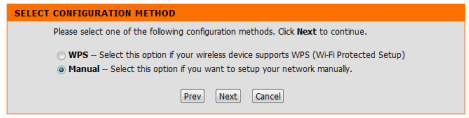
3. Open a web browser. First-time users will automatically be directed to the wizard. Please follow the on-screen instructions to complete the setup.

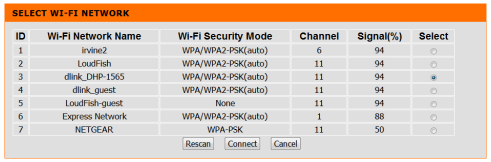
   If the wizard does not appear, type **http://dlinkrouter.local** in the address bar. Click **Launch Wireless Setup Wizard** to continue.



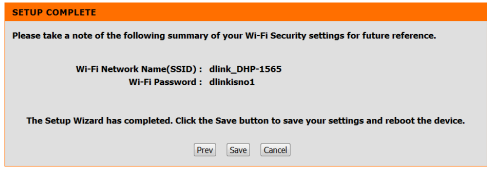


4. Select the configuration method and click **Next**.
   For *Manual Configuration*, select the Wi-Fi network you would like the DIR-505L to connect to wirelessly.





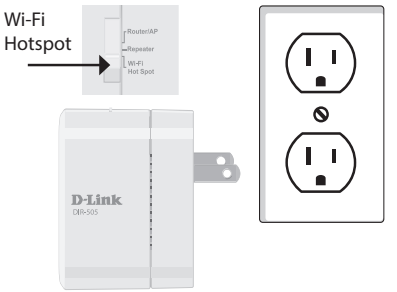
5. Enter the Wi-Fi Password and click **Next**.
   Once the second screen appears, you have successfully completed the setup. Please click **Save** and write down the SSID and password on your companion card for future reference.



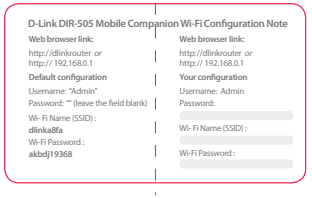
6. From your laptop or mobile device go to your wireless utility to display the available wireless networks and select the network that you previously connected to in *Step 5* for internet access.

Wi-Fi Hotspot Mode

1. Move the switch to "**Wi-Fi Hotspot**". Then, plug the DIR-505L into a wall outlet and verify that the power LED has turned green.

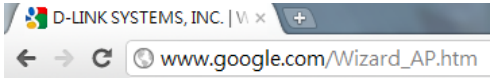


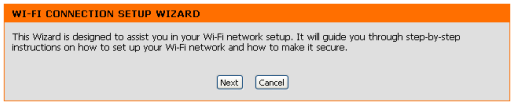
2. From your laptop or mobile device go to your Wireless Utility to display the available wireless networks and select the network that is displayed on your companion card (ex: **dlink-a8fa**). Then, enter the Wi-Fi password included in your card (**akbdj1936**).



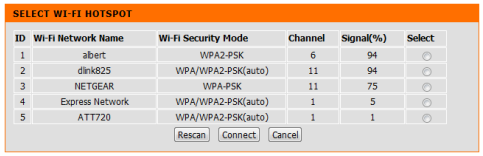
3. Open a web browser. First-time users will automatically be directed to the wizard. Please follow the on-screen instructions to complete the setup.

   If the wizard does not appear, type **http://dlinkrouter** or **192.168.100.1** in the address bar. Click **Launch Wireless Setup Wizard** to continue.

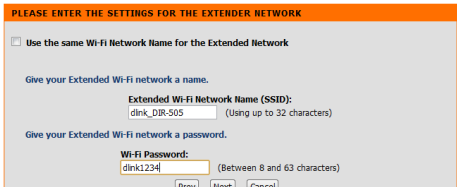


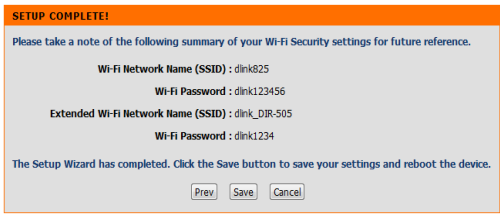


4. Select the Wi-Fi Hotspot you would like to connect to and then click **Connect** to continue. Then, enter the Wi-Fi password and click **Next** to continue.



5. If you do not wish to use the same Wi-Fi network name and would like to create your own name and password, uncheck the box. Then, enter your own Wi-Fi network name & password in the boxes. When the second screen appears, you have successfully completed the setup. Click **Save** and write down the SSID & password in your companion card for future reference.





6. From your laptop or mobile device go to your wireless utility to display the available wireless networks and select the network that you created in *Step 5*.

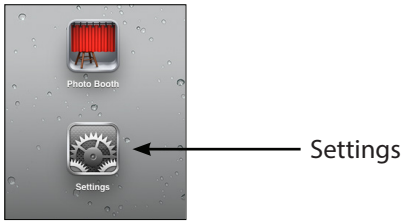
Quick Router Setup for Mobile Device

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

iOs

Android

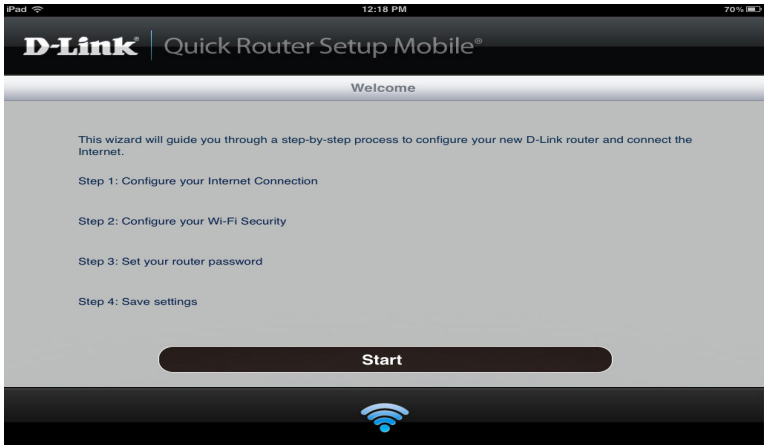
2. From your mobile device, click **Settings**. Then, click **Wi-Fi**.



3. Select the network that is displayed on your companion card (ex: **dlinka8f**). Then, enter the Wi-Fi password included in your card (ex: **akbdj1936**).

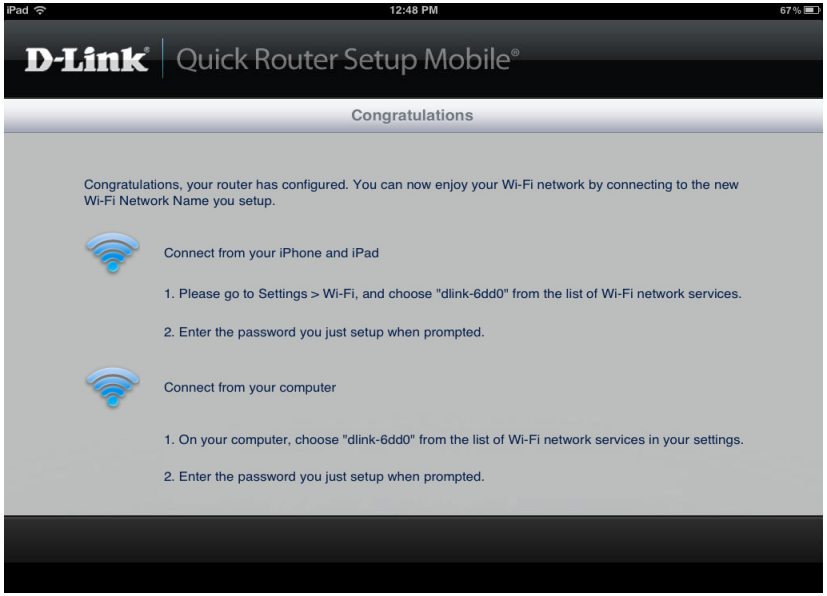
4. Once it is connected, click on the **QRS Mobile** icon.

5. Click **Start** to continue.



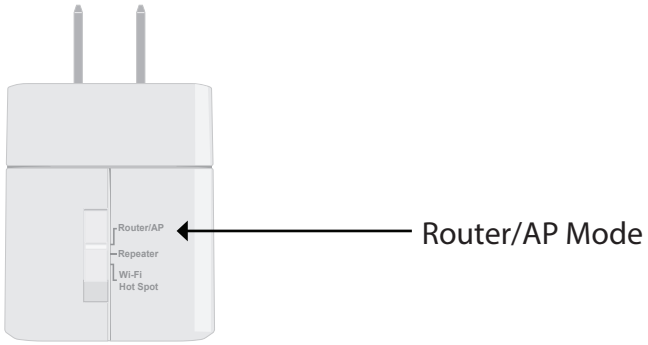
6. Follow the instructions and click **Next** to continue.

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



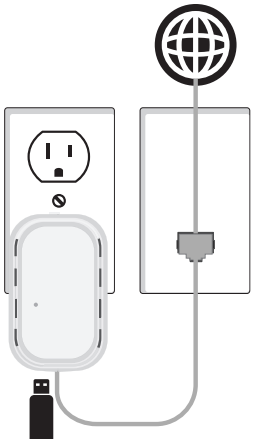
SharePort Mobile App

1. Move the switch to "**Router/AP Mode**" or "**Wi-Fi Hotspot Mode**".



2. Insert your USB thumb drive to DIR-505L first and then plug the DIR-505L into wall outlet.

Note: *Please refer to page 56 for* ***Storage*** *setup information before you proceed to the next step below.*



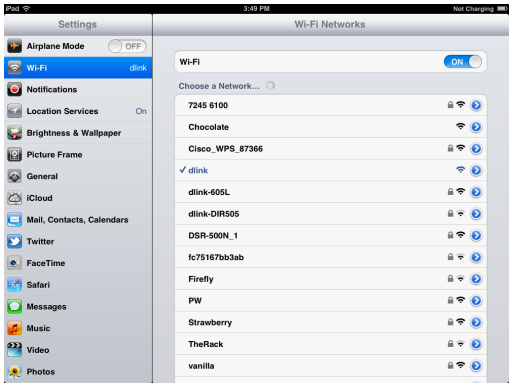
3. Scan the bar code to download the *SharePort Mobile* app from the app store to your iPhone or iPad.

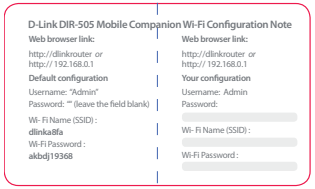
iOs

Android

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

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

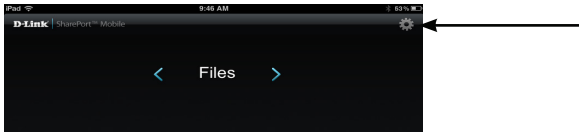




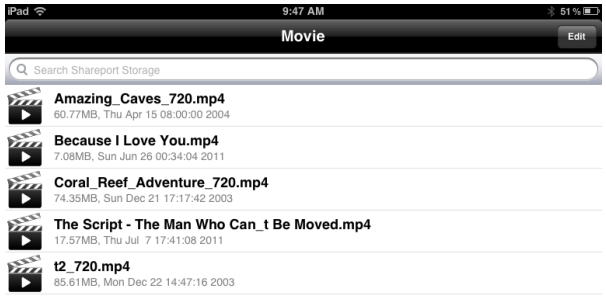
6. Once connected click on the **SharePort Mobile** icon.

7. The following screen will pop up.

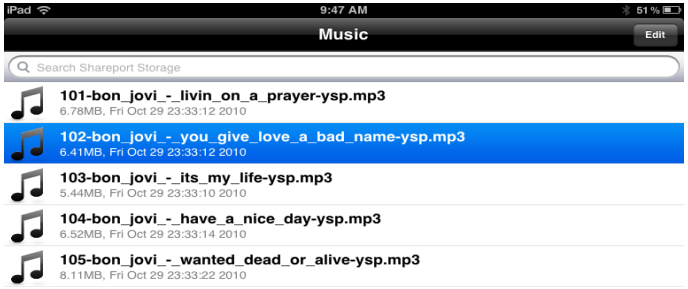
8. Click on the **Settings** icon located on the right top corner of the screen Then, click **Edit** to enter your user name and password. Once you finish, click **Done** to continue. By default, the user name is "**admin**" and the password is blank.



9. For the *Movie* section, click the **movie icon** to play your movie from your USB flash drive.



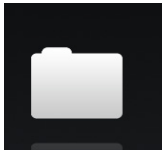
10. For the *Music* section, click the **music icon** to play your music from your USB flash drive.

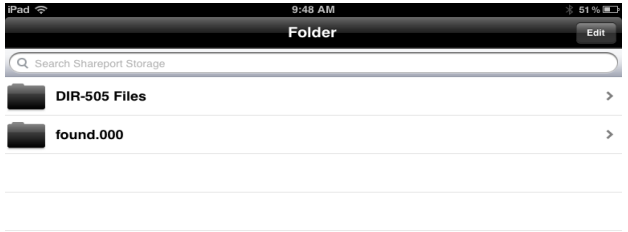


11. For the *Photo* section, click the **photo icon** to open your photo from your USB flash drive.

12. For the *Files* section, click on the **files icon** to open your file from your USB flash drive.

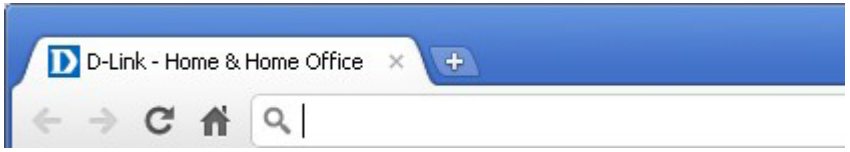
13. For the *Folder* section, click on the **folder icon** to open a file from your USB flash drive.





Router Mode
Quick Setup Wizard

If this is your first time installing the router, open your web browser. You will automatically be directed to the *Wizard Setup Screen*.

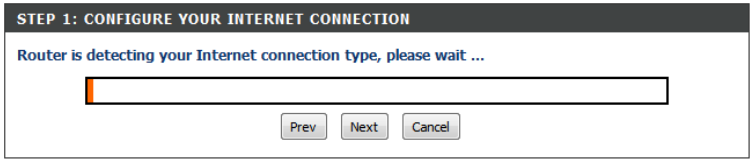


If you have already configured your settings and you would like to access the configuration utility, please refer to page 30.

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

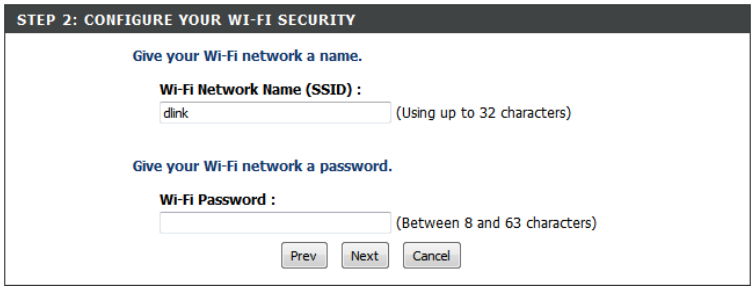
Click **Next** to continue.

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

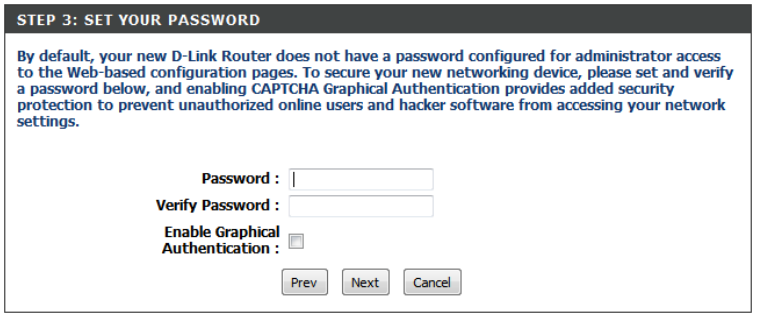


Create a wireless security passphrase or key (between 8-63 characters). Your wireless clients will need to have this passphrase or key entered to be able to connect to your wireless network.

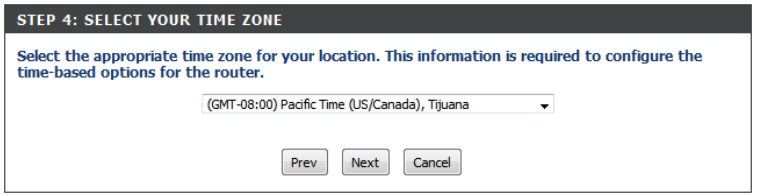
Click **Next** to continue.



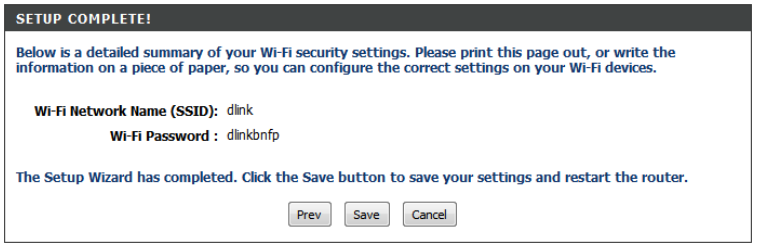
In order to secure your router, please enter a new password. Check the **Enable Graphical Authentication** box to enable CAPTCHA authentication for added security. Click **Next** to continue.



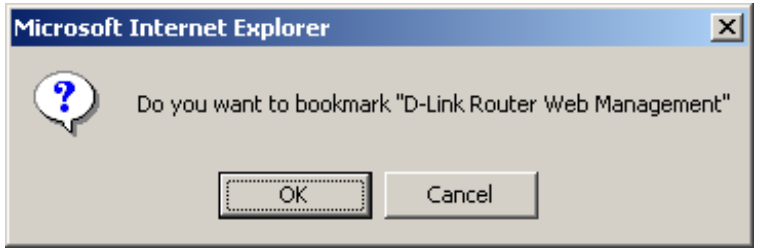
Select your time zone from the drop-down menu and click **Next** to continue.



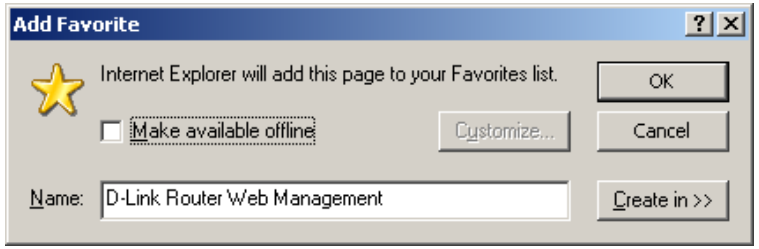
The *Setup Complete* window will display your wireless settings. Click **Save** to continue.



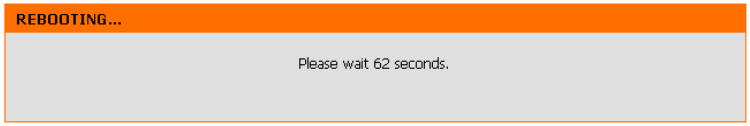
If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.



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

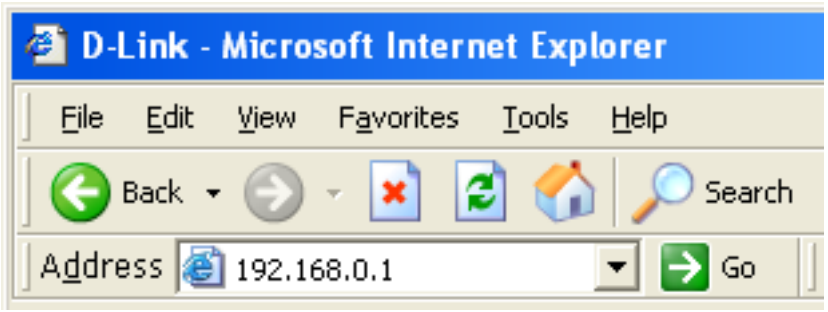


The router will now reboot. Please allow a minute or two. Click the **Continue** button once it is active.



Web-based Configuration Utility

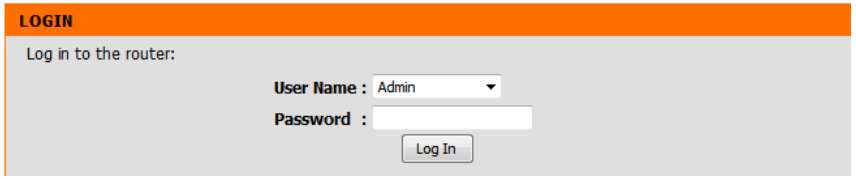
To access the configuration utility, open a web-browser, such as Internet Explorer, and enter the IP address of the router (**http://192.168.0.1**).



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

Note: *The IP address is* ***192.168.100.1*** *when the DIR-505L is in Hotspot Mode.*

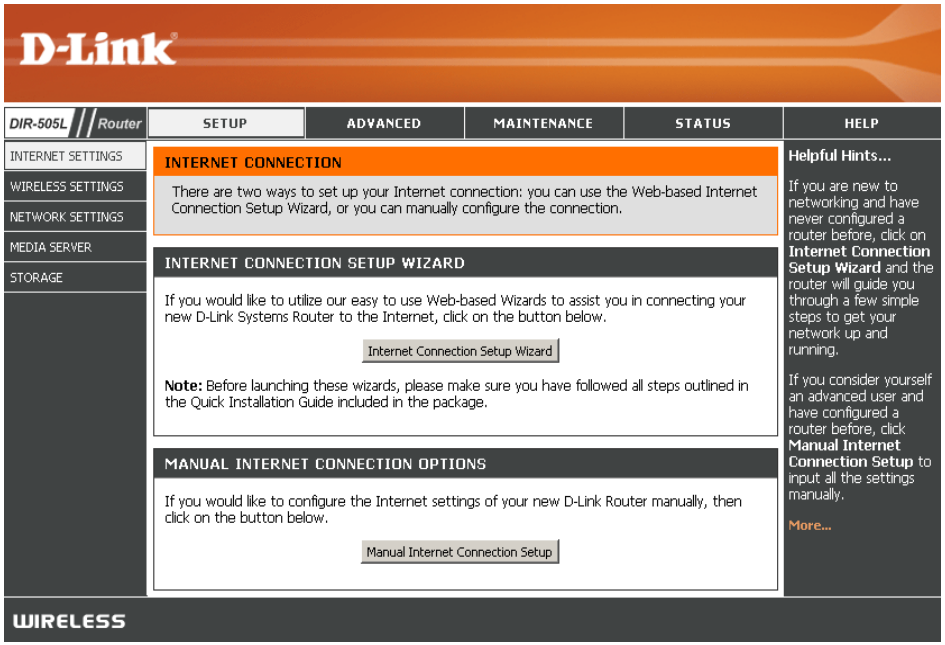
Select **Admin** from the drop-down menu. Leave the password blank by default.



Internet Connection Setup

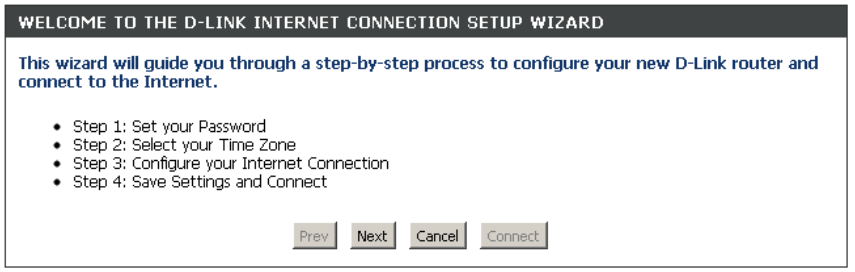
Click **Manual Internet Connection Setup** to configure your connection manually and continue to page 36.

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

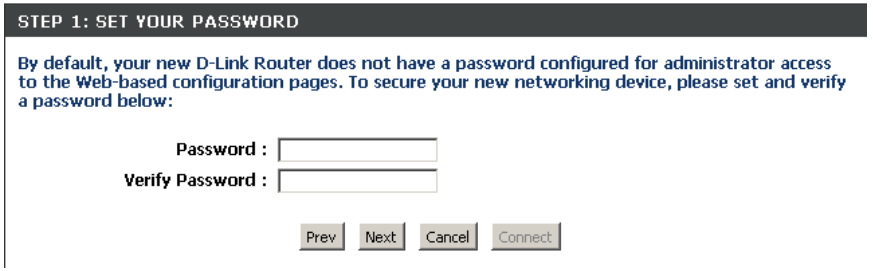


This wizard is designed to guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

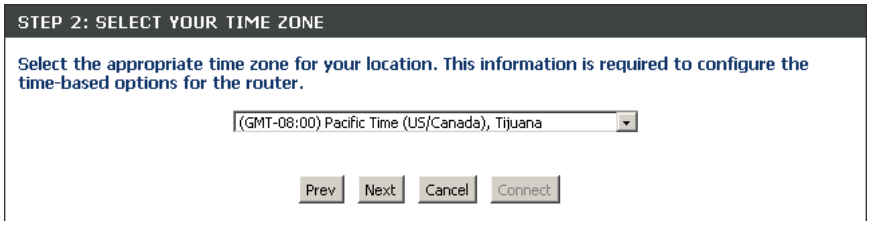
Click **Next** to continue.



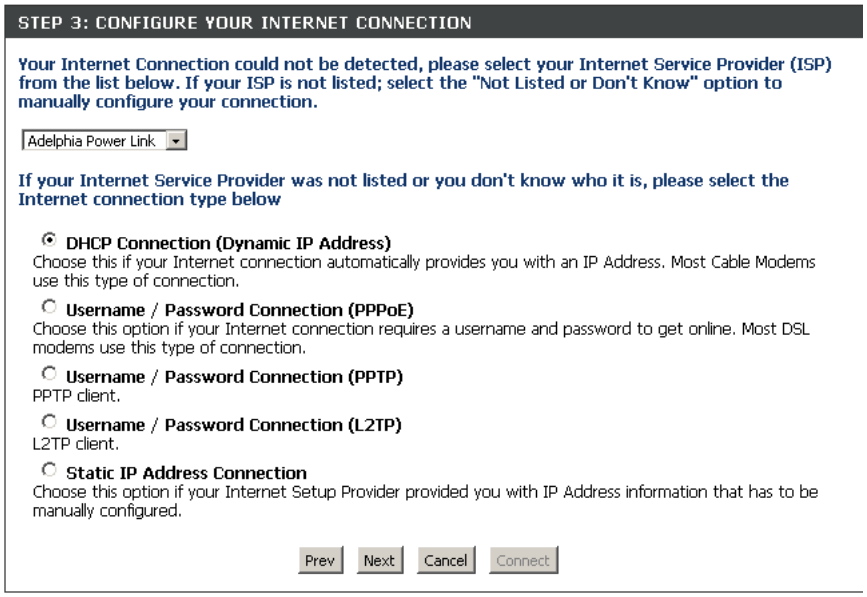
In order to secure your router, please enter a new password. Click **Next** to continue.



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

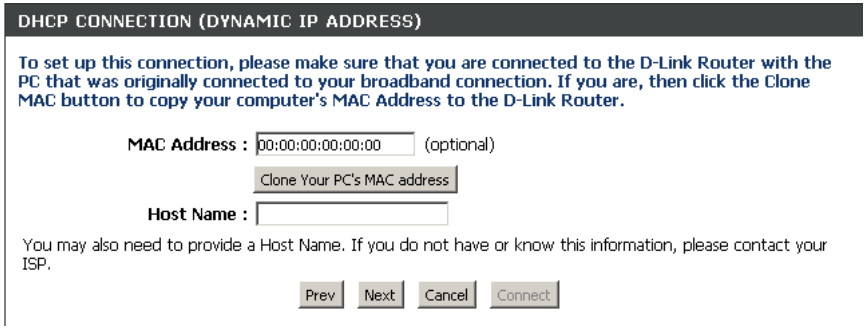


Select your Internet connection type and click **Next** to continue.

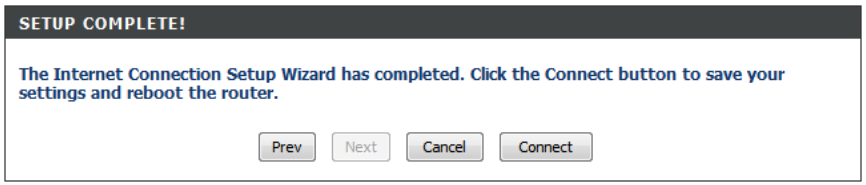


Verify that you are connected to the D-Link Router with the PC that was originally connected to your broadband connection. Then click the **Clone Your PC's MAC address** button to copy your computer's MAC (Media Access Control) address.

Click **Next** to continue.

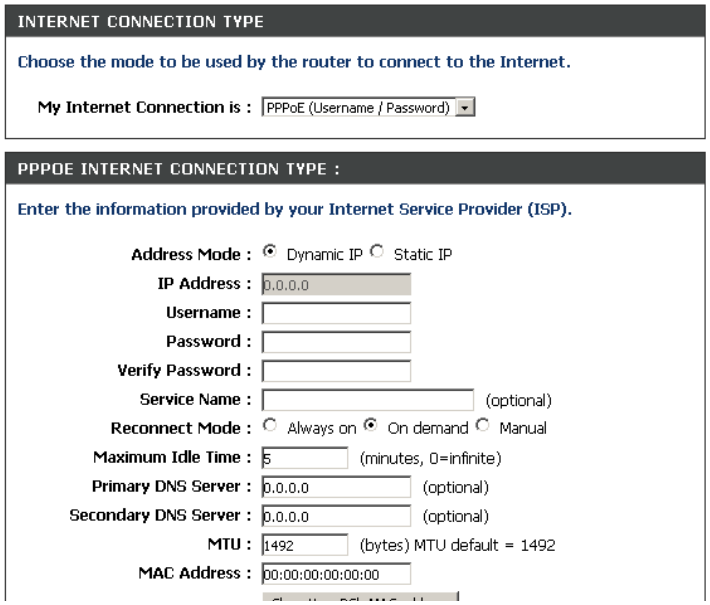


Your setup is complete. Click **Connect** to save your settings and reboot your router.

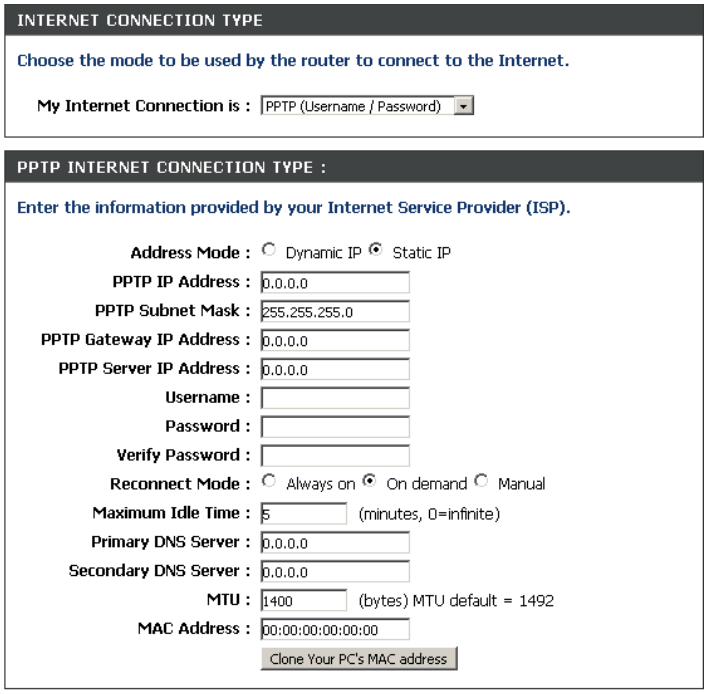


If the router detected or you selected **PPPoE**, enter your PPPoE user name, password and verify password, then click **Next** to continue.

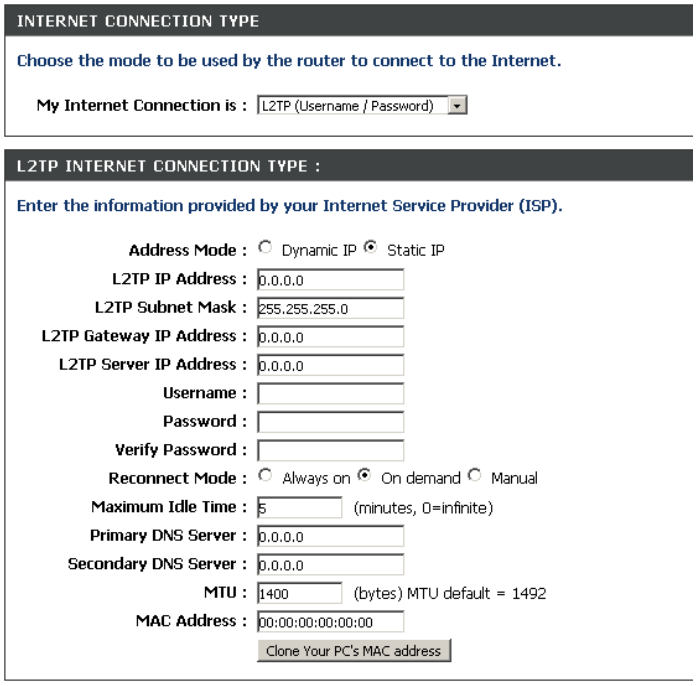
Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*



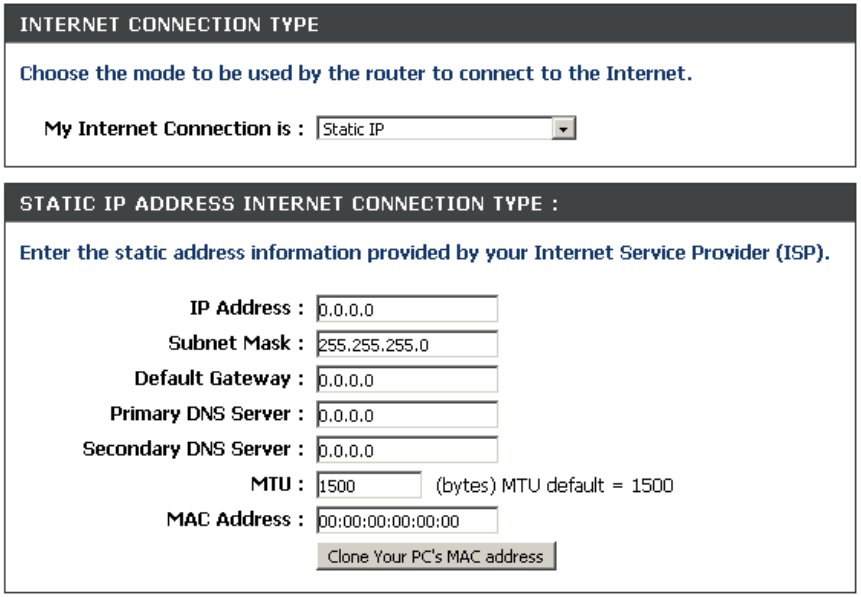
If the router detected or you selected **PPTP**, enter your PPTP user name, password, and other information supplied by your ISP. Click **Next** to continue.



If the router detected or you selected **L2TP**, enter your L2TP user name, 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.



Manual Internet Setup
Dynamic (Cable)

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

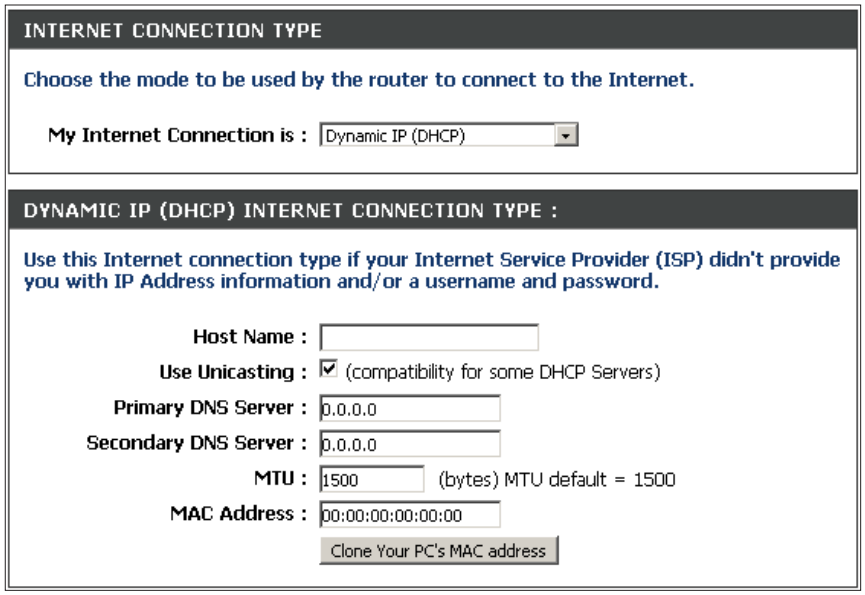
Host Name: The *Host Name* is optional but may be required by some ISPs. Leave blank if you are not sure.

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

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

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

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



Internet Setup
PPPoE

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

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

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

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

User Name: Enter your PPPoE user name.

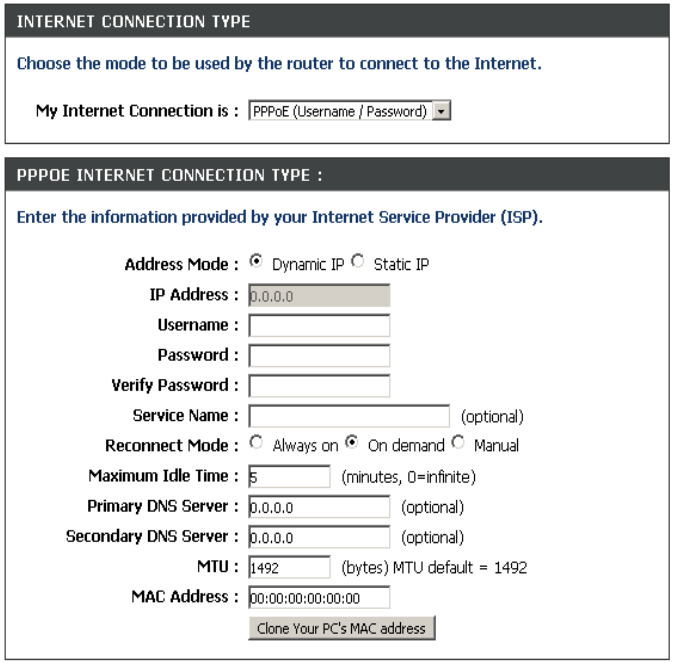
Password: Enter your PPPoE password and then retype the password in the next box.

Service Name: Enter the ISP Service Name (optional).

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

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

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



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

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

PPTP

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

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

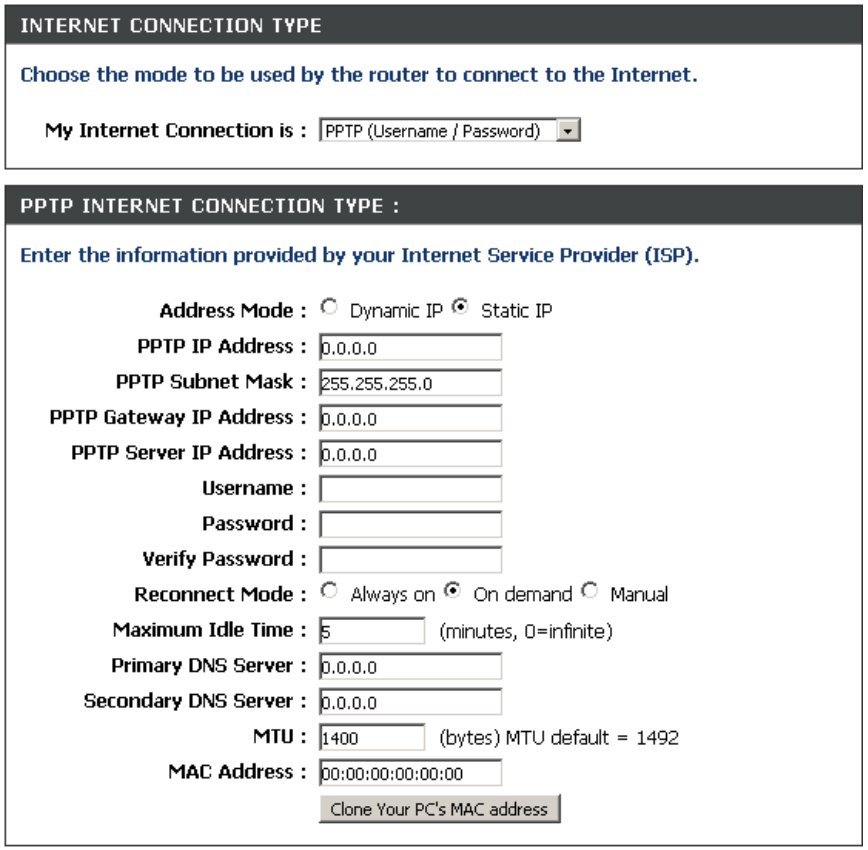
Address Mode: Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

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

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

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

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



User name: Enter your PPTP user name.

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

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

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

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

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

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

L2TP

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

My Internet Connection: Select **L2TP (User name/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 (Static only).

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

L2TP Gateway: Enter the Gateway IP address provided by your ISP.

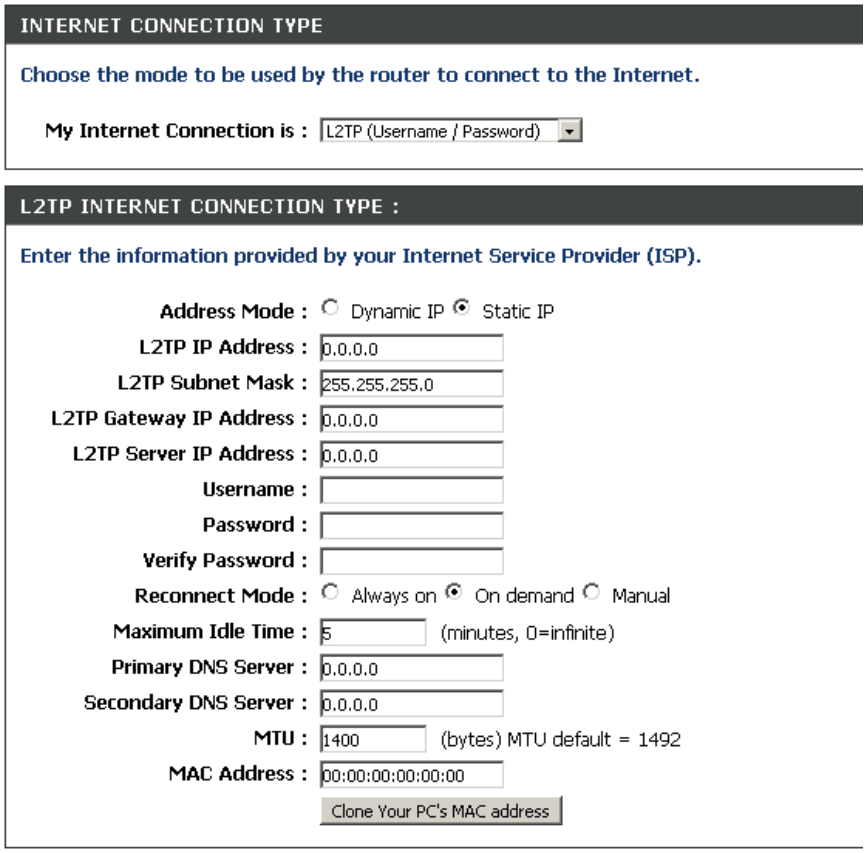
L2TP Server IP: Enter the Server IP provided by your ISP (optional).

User name: Enter your L2TP user name.

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

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

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



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

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

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

Static

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

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

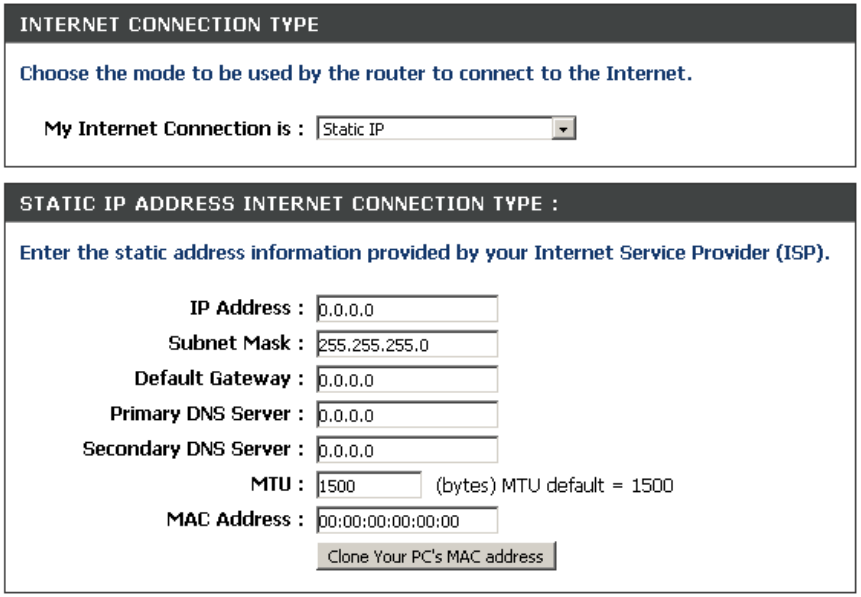
Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

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

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

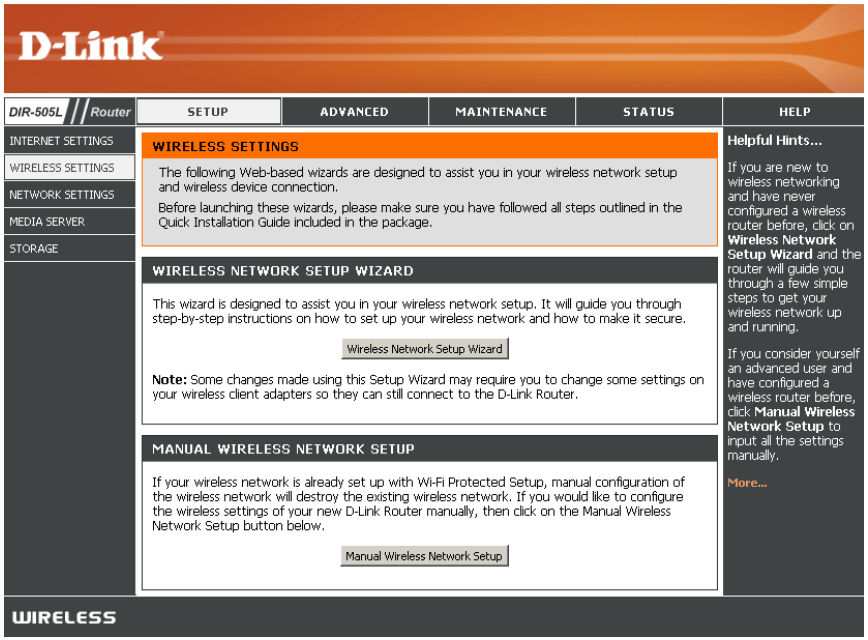
MAC Address: The default MAC address is set to the Internet port's physical interface MAC address on the broadband router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Copy Your PC's MAC Address** button to replace the Internet port's MAC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



Internet Settings

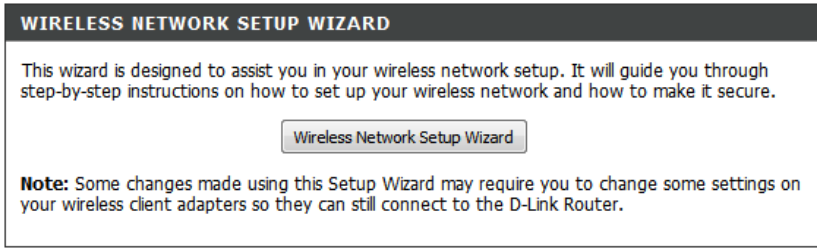
If you want to configure the wireless settings on your router using the wizard, click **Wireless Network Setup Wizard** and refer to the next page**.**

If you want to manually configure the wireless settings on your router click **Manual Wireless Network Setup** and refer to page 45.



Wireless Network Setup Wizard

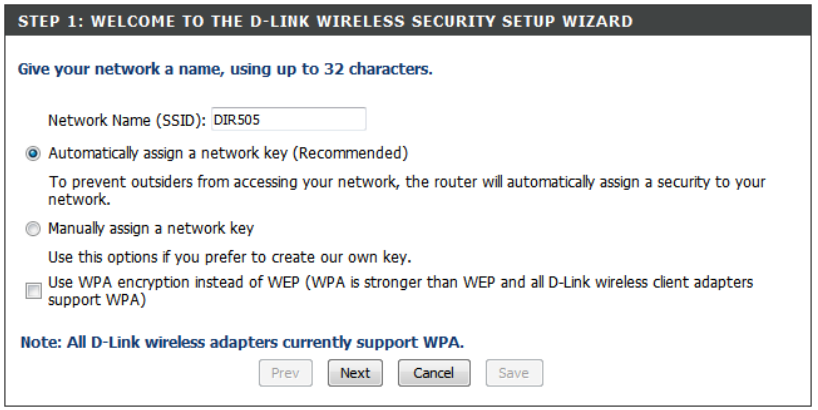
To run the security wizard, click on **Setup** at the top, then click **Wireless Settings** on the left, and then click **Wireless Network Setup Wizard**.



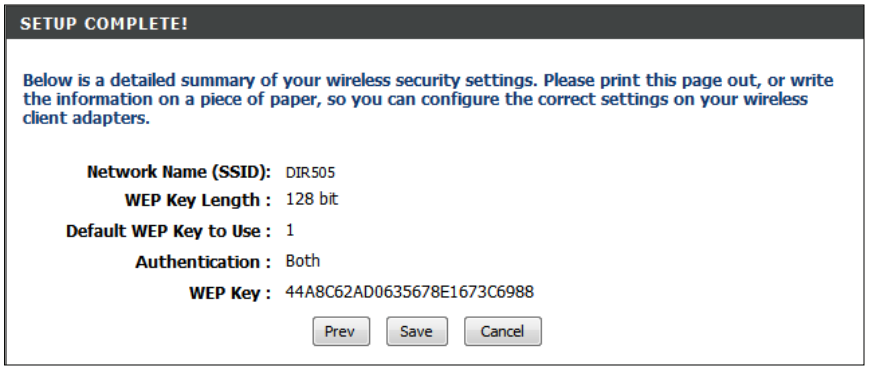
Type your desired wireless network name (SSID).

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

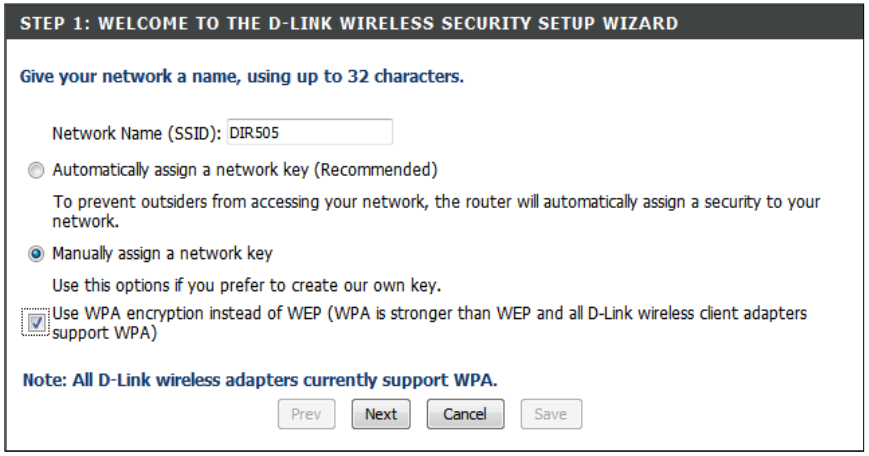
Manually: Select this option to manually enter your network key and click **Next**.



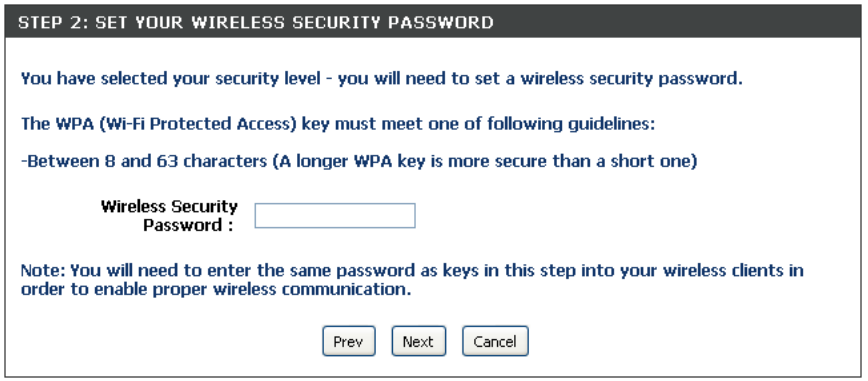
If you selected **Automatically**, the summary window will display your settings. Write down the security key and enter this on your wireless clients. Click **Save** to save your settings.



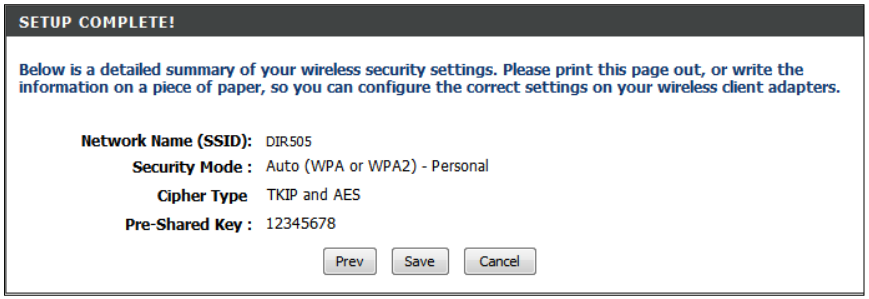
Select **Manually** to manually enter your network key and click **Next**.



Enter your Wireless Security password and click **Next** to continue.



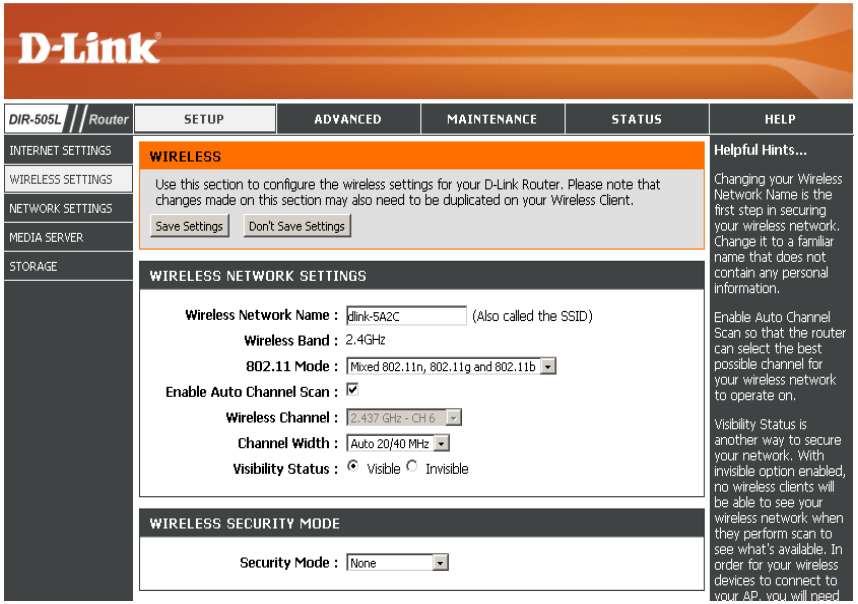
If you selected **Manually**, the following screen will appear once the setup is complete.



Manual Configuration

Wireless Settings

Router Mode



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

802.11 Mode: Select one of the following:

802.11b Only - Select if you are only using 802.11b wireless clients.

802.11g Only - Select if you are only using 802.11g wireless clients.

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

Mixed 802.11g and 802.11b - Select if you are using a mix of 802.11g and 11b wireless clients.

Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 11g wireless clients.

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

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

Wireless Channel: Indicates the channel setting for the DIR-505L. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be grayed out.

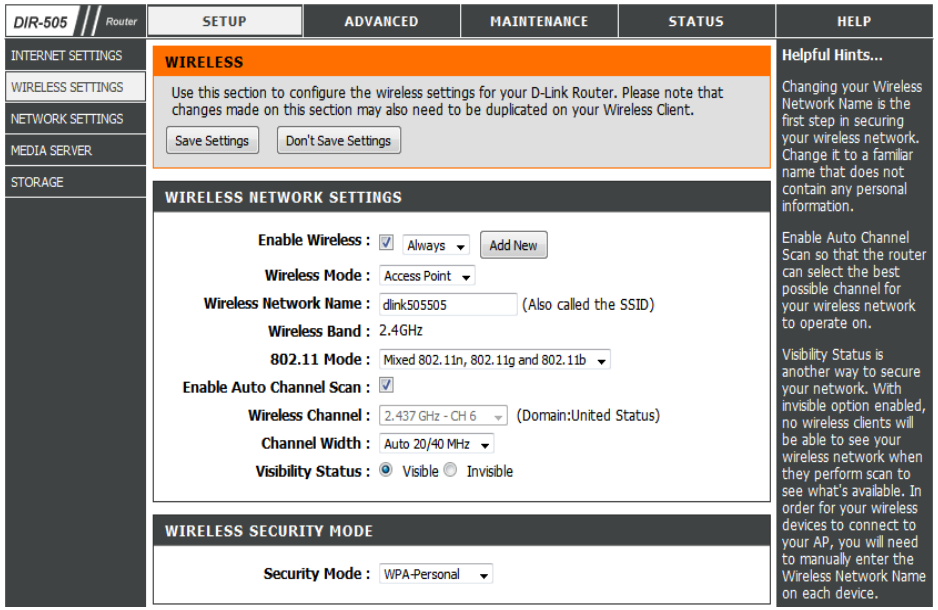
Channel Width: Select the Channel Width:
Auto 20/40 - Select if you are using both 802.11n and non-802.11n wireless devices.
20MHz - Select if you are not using any 802.11n wireless clients.

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

Security Mode: Refer to page 50 for more information regarding the wireless security.

Access Point Mode

Note: *To change between **Router Mode** and **Access Point Mode**, set the switch on the DIR-505L to the **Router/AP** setting. Then access the Web UI and click on **Setup** at the top, then click on **Internet Settings** on the left. Select **Router** or **Access Point** from the Wireless Mode drop-down list, then click **Save Settings**. The DIR-505L will then reboot in the mode you selected.*



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

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

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

Wireless Channel: Indicates the channel setting for the DIR-505L. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be grayed out.

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

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

Security Mode: Refer to page 49 for more information regarding the wireless security.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-505L offers the following types of security:

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

What is WPA

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

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

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

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

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless DIR-505L before your wireless network adapters. Please establish wireless connectivity before enabling encryption.

1. Log in to the web-based configuration by opening a web browser and entering the IP address of the router (**192.168.0.1**). Click on **Setup**, then click **Wireless Settings** on the left side, and click on **Manual Wireless Network Setup**.

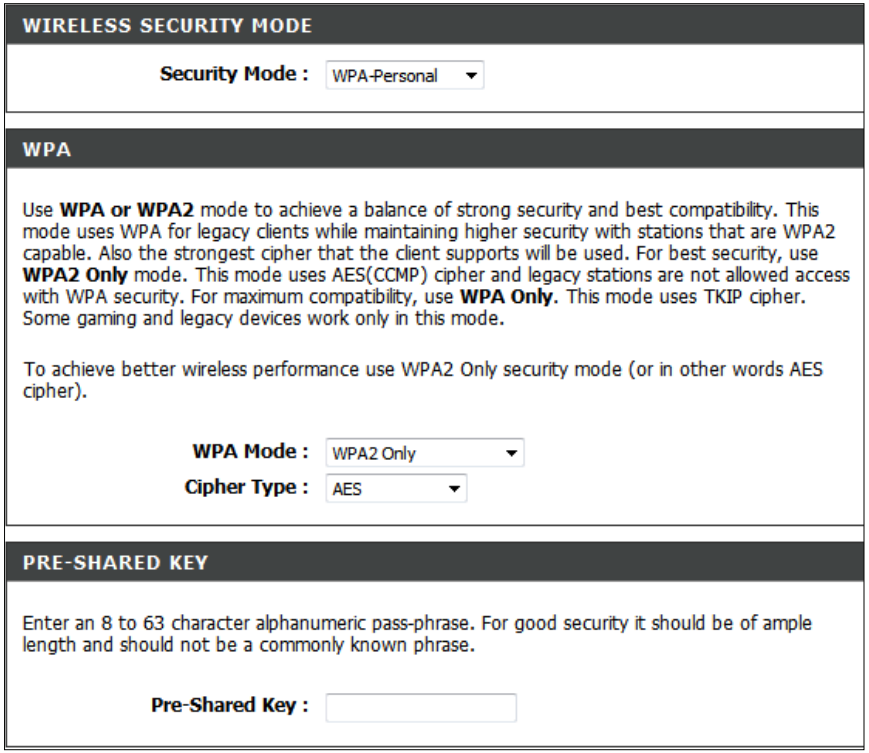
2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *WPA Mode*, select **WPA only**, **WPA2 only** or **Auto (WPA or WPA2)**.

4. Next to *Cipher Type*, select **TKIP**, **AES** or **TKIP and AES**.

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

6. Click **Save Settings** at the top of the window to save your changes. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the DIR-505L.



Configure WPA Enterprise

It is recommended to enable encryption on your wireless DIR-505L before your wireless network adapters. Please establish wireless connectivity before enabling encryption.

1. Log in to the web-based configuration by opening a web browser and entering the IP address of the router (**192.168.0.1**). Click **Setup**, then click **Wireless Settings** on the left side, and click on **Manual Wireless Network Setup**.

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

3. Next to *WPA Mode* select **Auto (WPA or WPA2).**

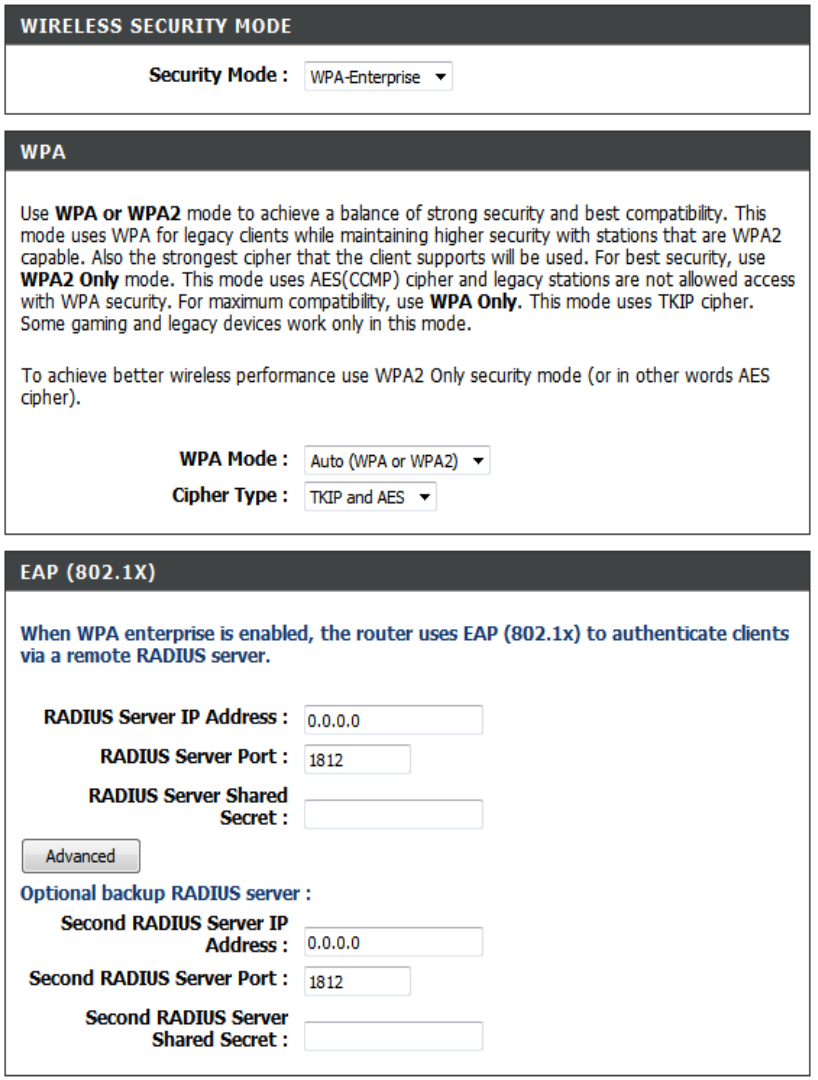
4. Next to *Cipher Mode*, select **TKIP**, **AES**, or **Auto**.

5. Next to *RADIUS Server IP Address*, enter the IP address of your RADIUS server.

6. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. **1812** is the default port.

7. Next to *Shared Secret*, enter the security key.

8. Click **Save Settings** to save your settings.



Network Settings

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

Router Settings

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

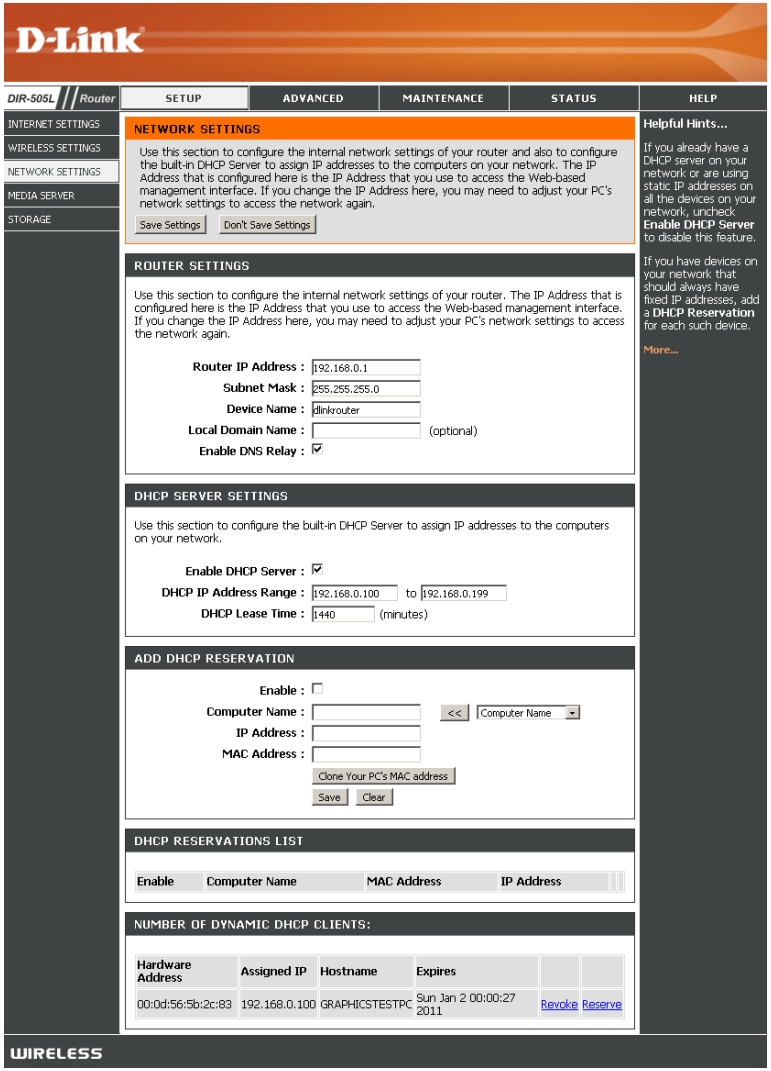
If you change the IP address, once you click **Save Settings**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

Device Name: Enter a name for the router.

Local Domain: Enter the domain name (Optional).

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



DHCP Reservation

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

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

Enable: Check this box to enable the reservation.

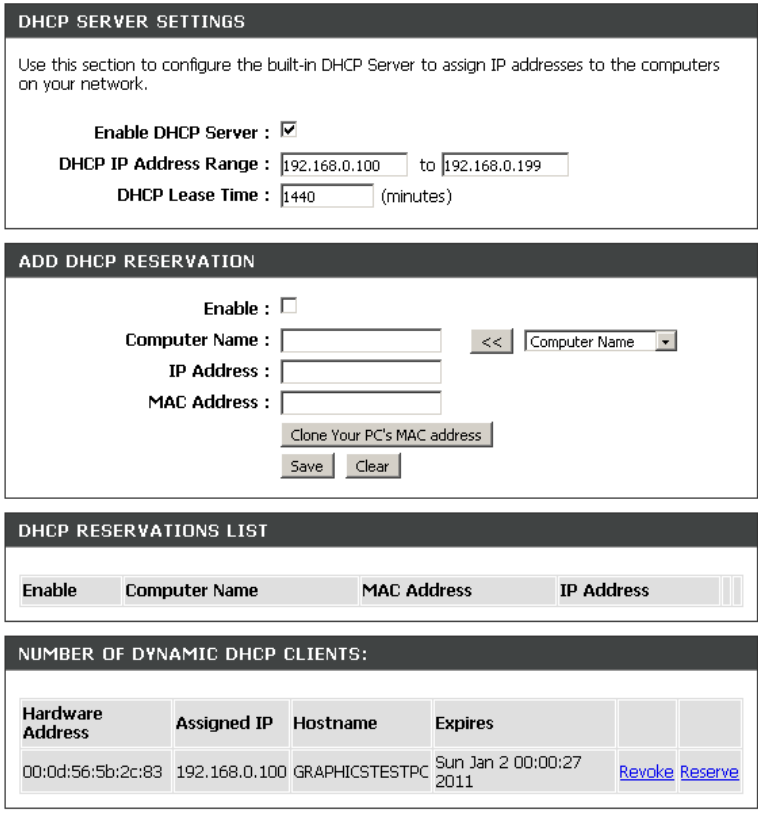
Computer Name: Enter the computer name or select from the drop-down menu and click <<.

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

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

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

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



DHCP Reservations List

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

Enable: Check to enable the reservation.

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

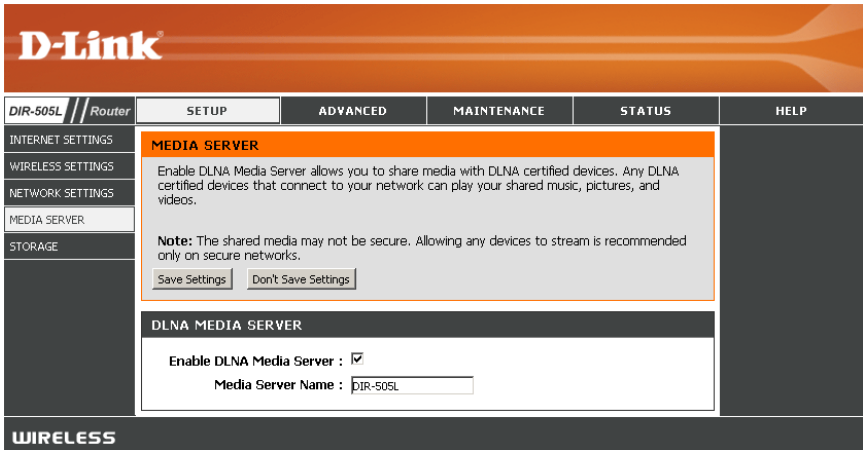
Delete: Click to remove the reservation from the list.

Media Server

This feature allows you to share music, pictures, and videos with any devices connected to your network.

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

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



Storage

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

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

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

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

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

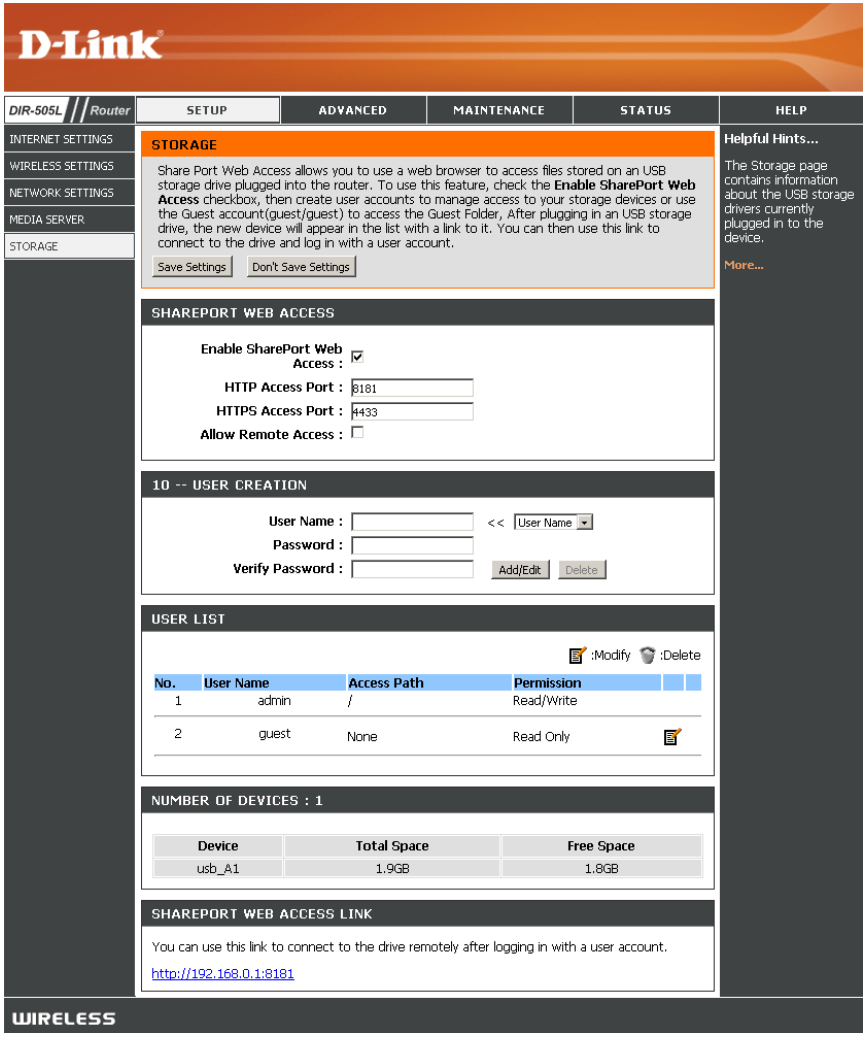
User Name: To create a new user, enter a user name.

Password: Enter a password for this account.

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

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

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



Advanced
Virtual Server

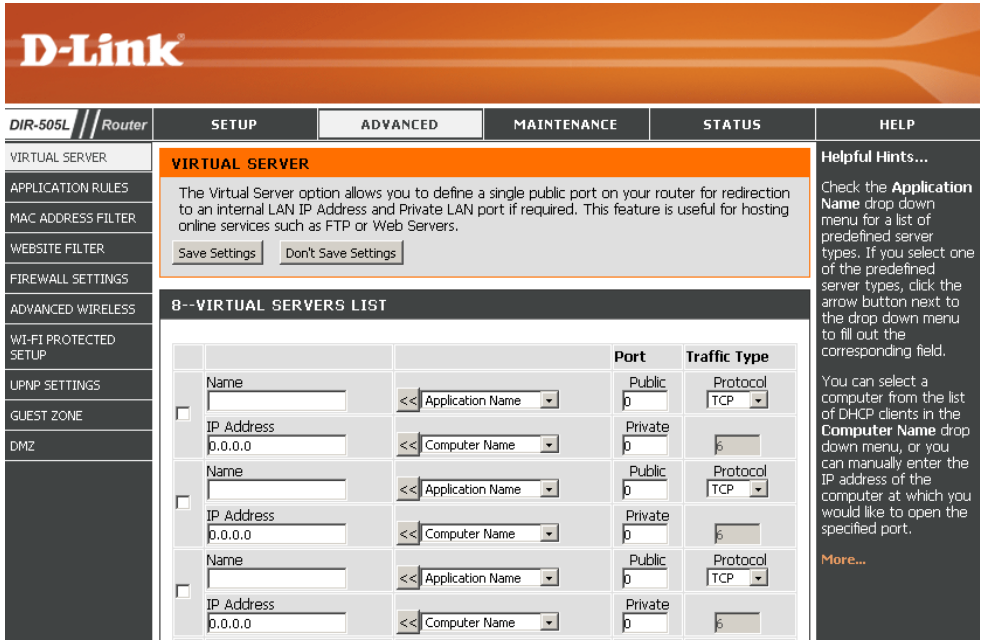
This will allow you to open a single port. If you would like to open a range of ports, refer to the next page.

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

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

Public Port/ Private 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 require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). *Special Applications* makes some of these applications work with the DIR-505L. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "*Trigger Port*" field, select the protocol type as **TCP** or **UDP**, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

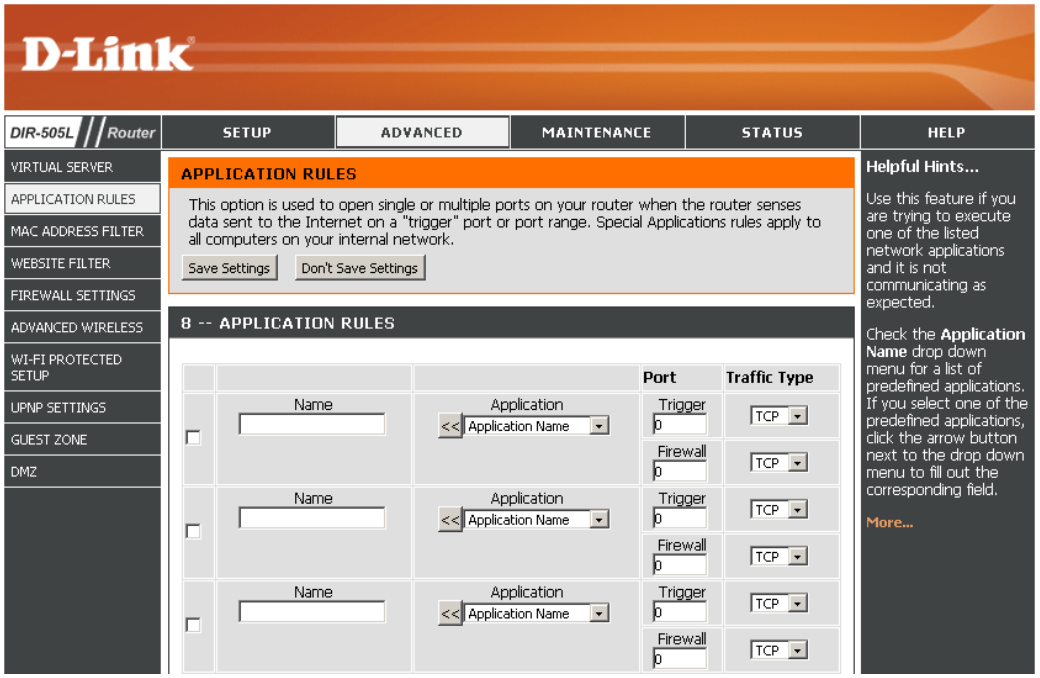
The DIR-505L provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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

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

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

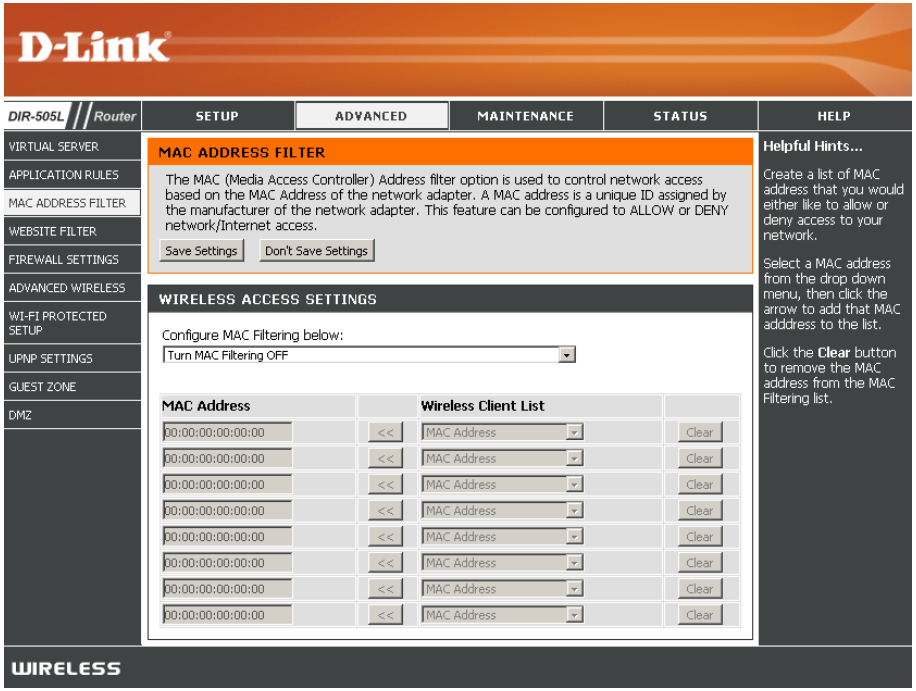
Traffic Type: Select the protocol of the trigger port (**TCP**, **UDP**, or **Both**).



MAC Address Filter

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

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

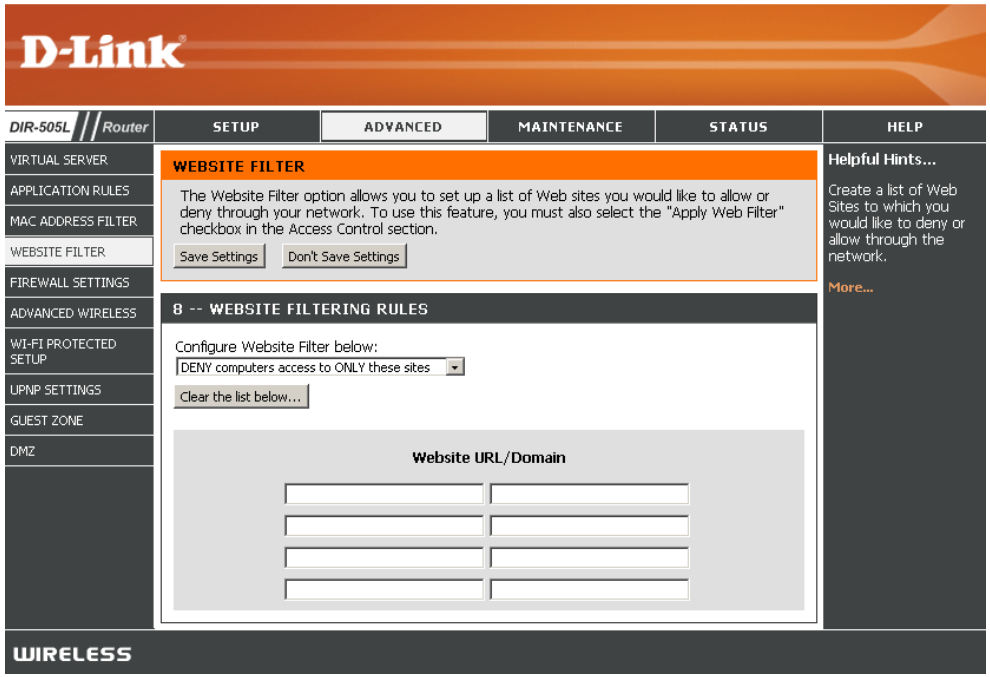


Website Filters

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

Configure Website Filter Below: Select either **DENY computers access to ONLY these sites** or **ALLOW computers access to ONLY these sites**.

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

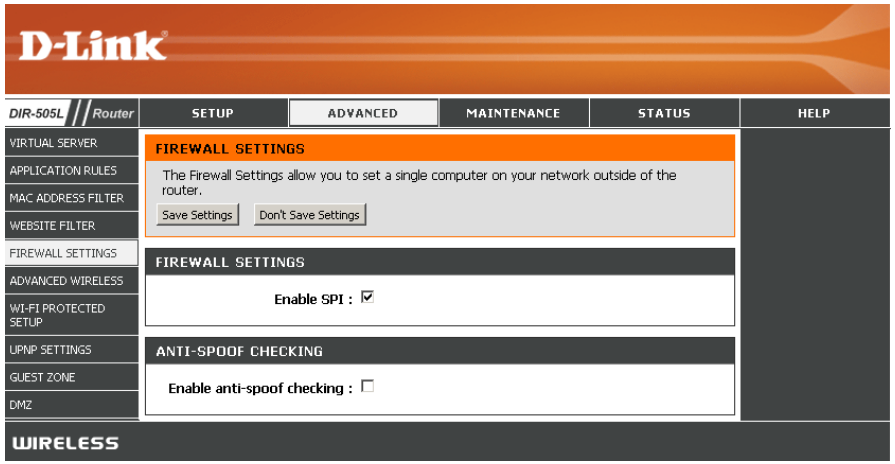


Firewall Settings

A firewall protects your network from the outside world. The DIR-505L offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications.

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

Enable Anti-Spoof Checking: Enable this feature to protect your network from certain kinds of "spoofing" attacks.



Advanced Wireless

Transmit Power: Set the transmit power of the antennas.

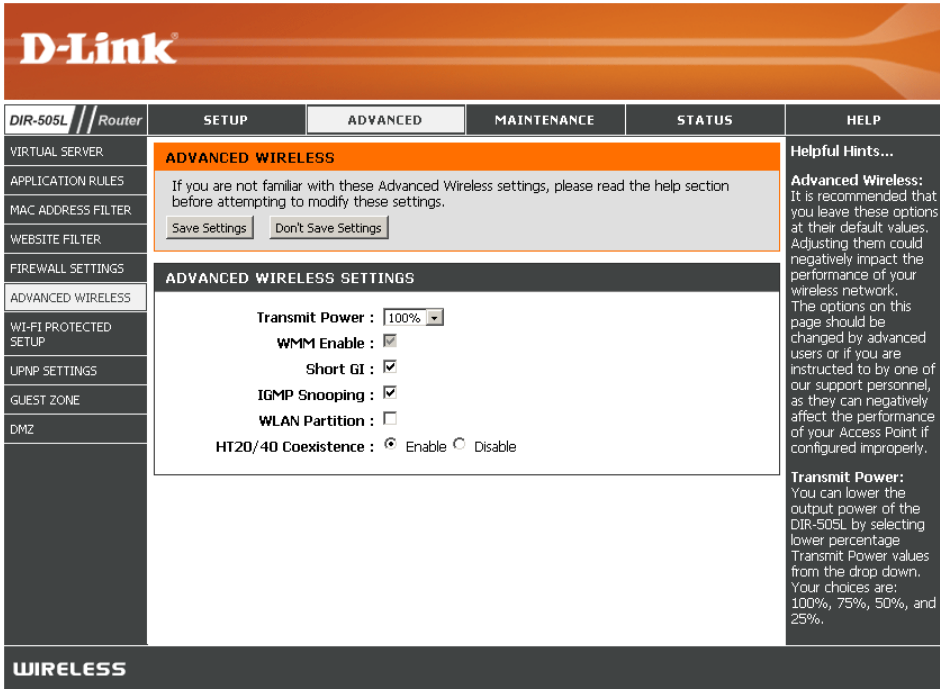
WMM Enable: WMM is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

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

IGMP Snooping: Check to enable this feature.

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

HT20/40 Coexistence: You may choose to **Enable** or **Disable** this feature. Enabling this feature allows two "channels" or paths on which data can travel to be combined to increase performance in some environments.



Wi-Fi Protected Setup (WPS)

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

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

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

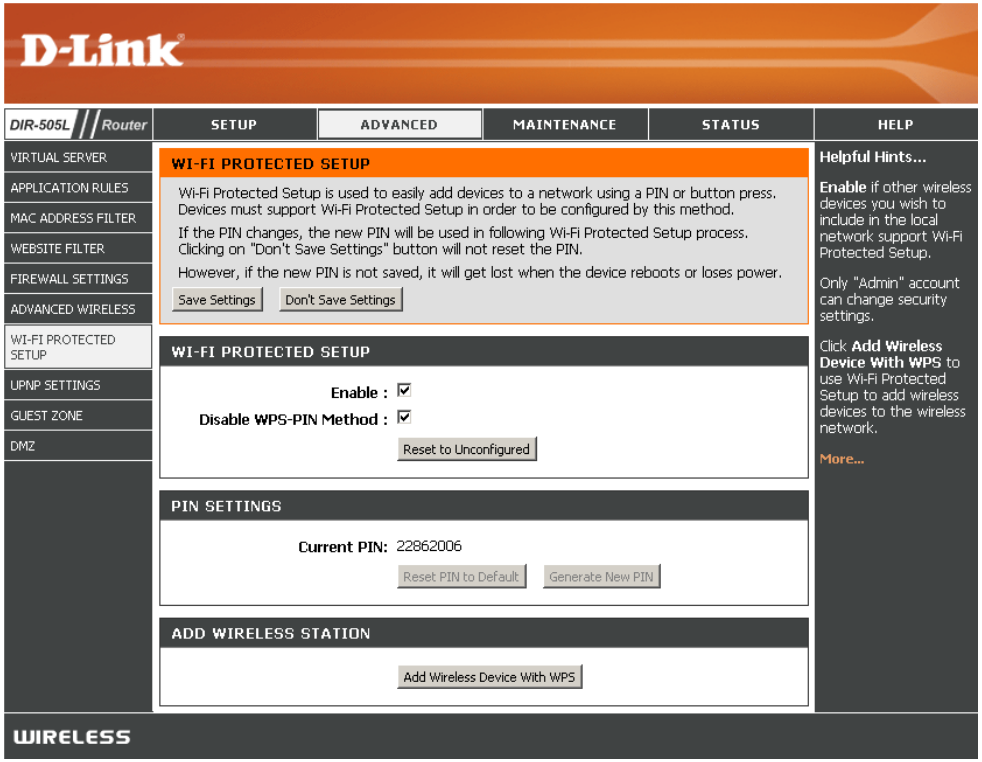
Disable WPS-PIN Method : Locking the *WPS-PIN Method* prevents the settings from being changed by any external registrar using its PIN. Devices can still be added to the wireless network using the *Wi-Fi Protected Setup Push Button Configuration* (*WPS-PBC*). It is still possible to change wireless networks settings with *Manual Wireless Network Setup* or *Wireless Network Setu Wizard*.

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

Current PIN: Shows the current PIN.

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

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



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

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

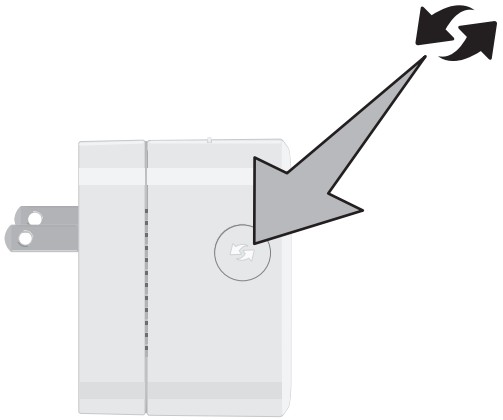
There are several ways to add a wireless device to your network. A "registrar" controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar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

Add Wireless Device with WPS: Click to start the wizard.

WPS Button

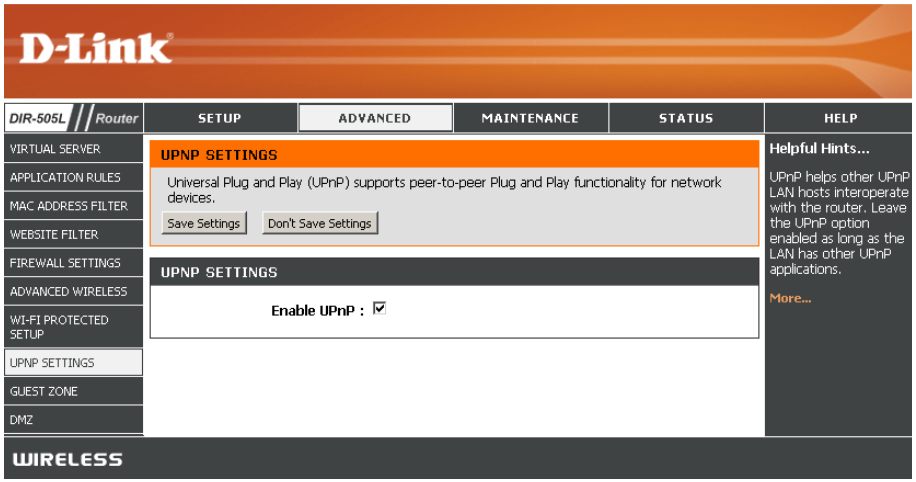
You can also simply press the **WPS** button on the side of the router, and then press the **WPS** button on your wireless client to automatically connect without logging into the router.

Refer to page 141 for more information.



UPnP Settings

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



Guest Zone

The *Guest Zone* feature will allow you to create temporary zones that can be used by guests to access the Internet. These zones will be separate from your main wireless network.

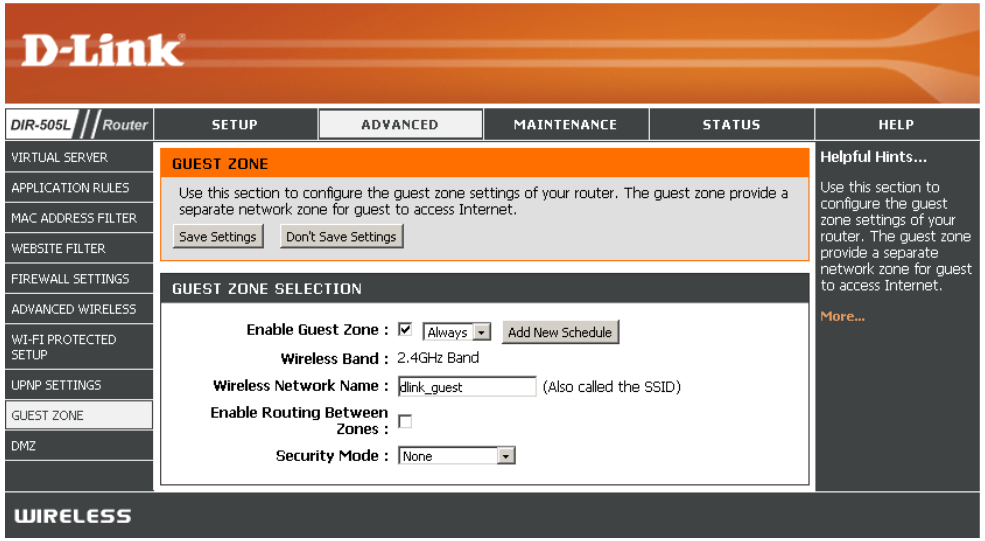
Enable Guest Zone: Check to enable the *Guest Zone* feature.

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

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

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

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

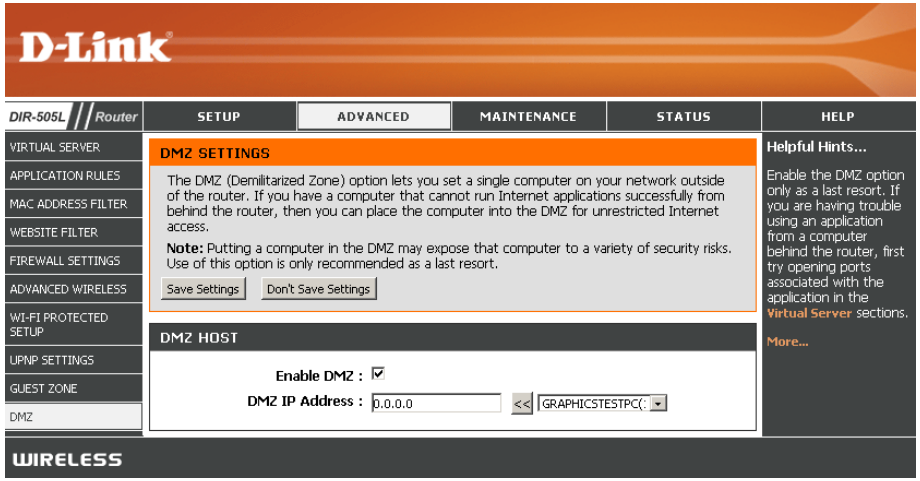


DMZ

This feature allows you to set a single computer from your network to be exposed outside of the router and get unrestricted Internet access. If you choose to expose a computer, you can enable *DMZ*. *DMZ* is short for *Demilitarized Zone*. This option will expose the chosen computer completely to the outside world.

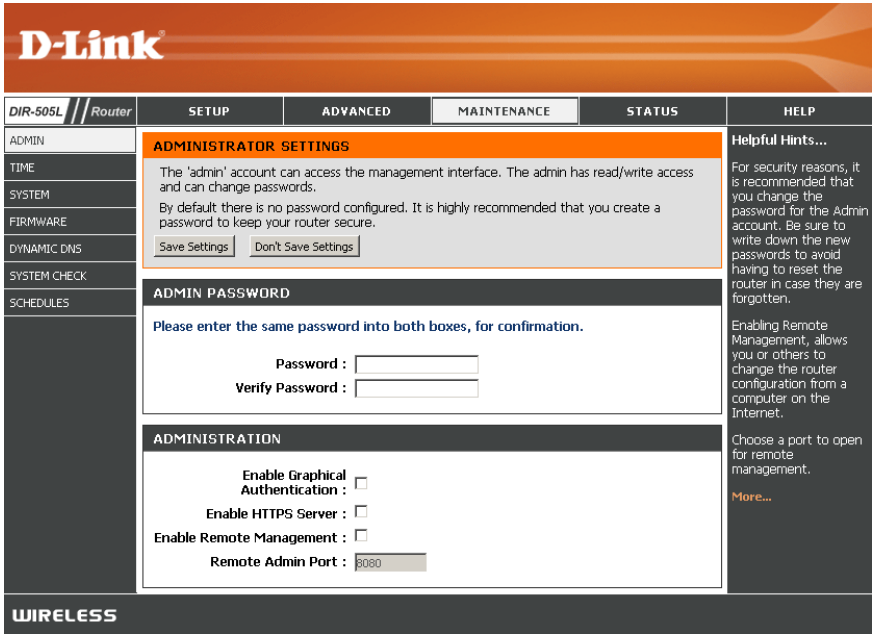
Enable DMZ: Check the box to enable *DMZ*.

DMZ IP Address: Enter the *DMZ* IP address.



Maintenance
Admin

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



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

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

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

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

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

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

Time

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

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

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

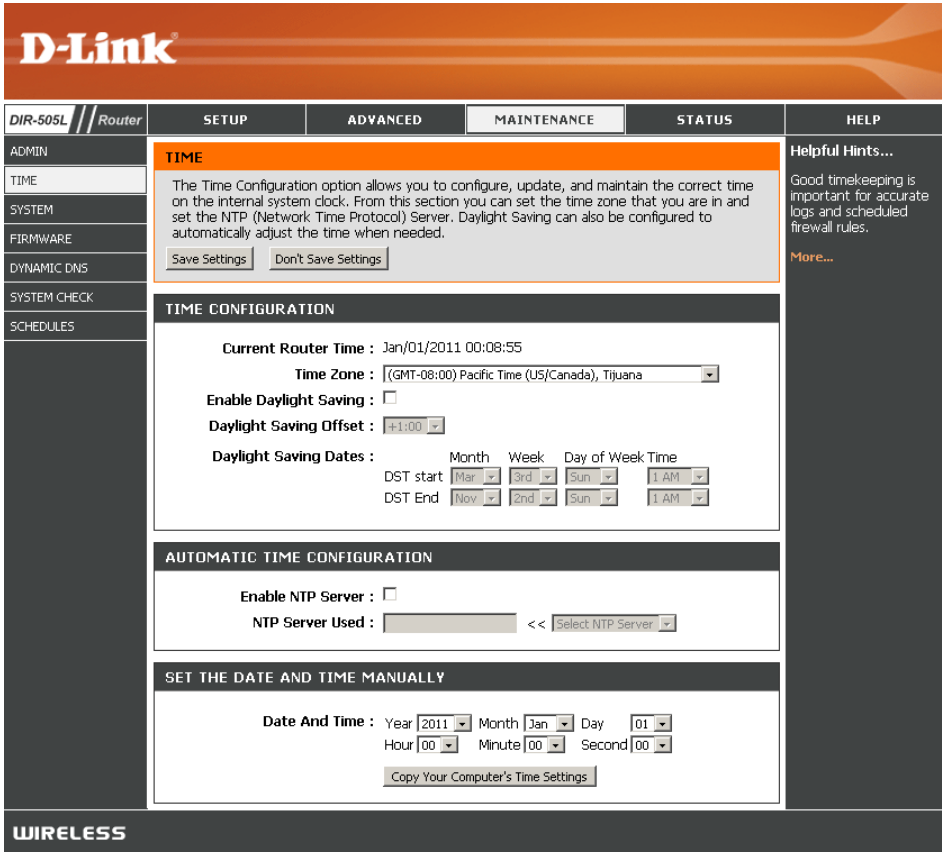
Enable Daylight-Saving: To select *Daylight-Saving Time* manually, select **enabled** or **disabled**, and enter a start date and an end date for daylight-saving time.

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

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

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

You can also click **Copy Your Computer's Time Settings** to synch the date and time with the computer you are currently on.



System

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

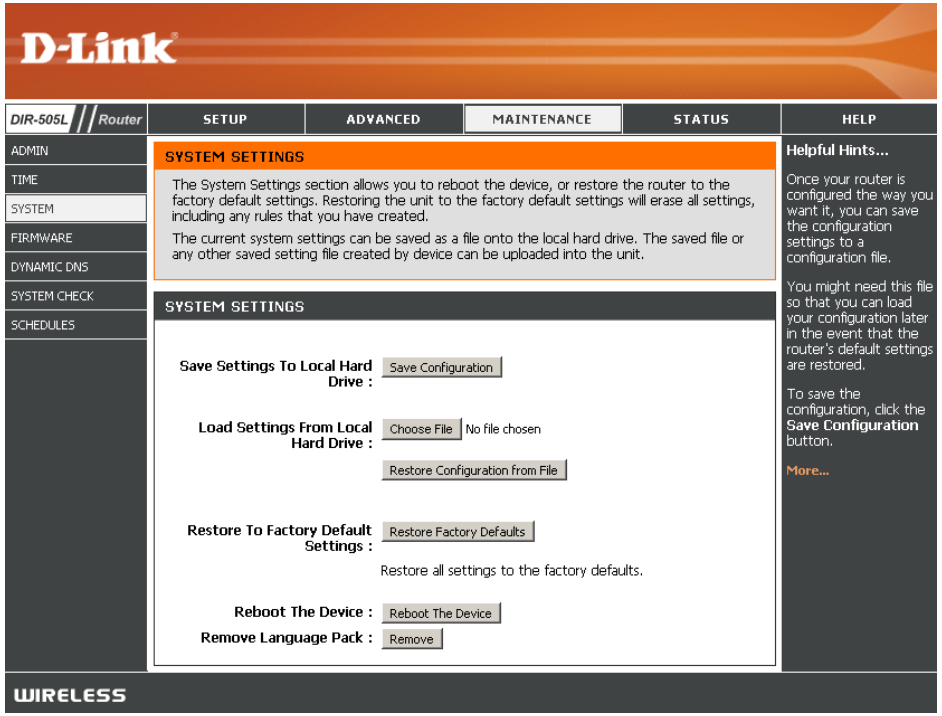
Save Settings to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. A file dialog will appear, allowing you to select a location and file name for the settings.

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

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

Reboot The Device: Click to reboot the router.

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



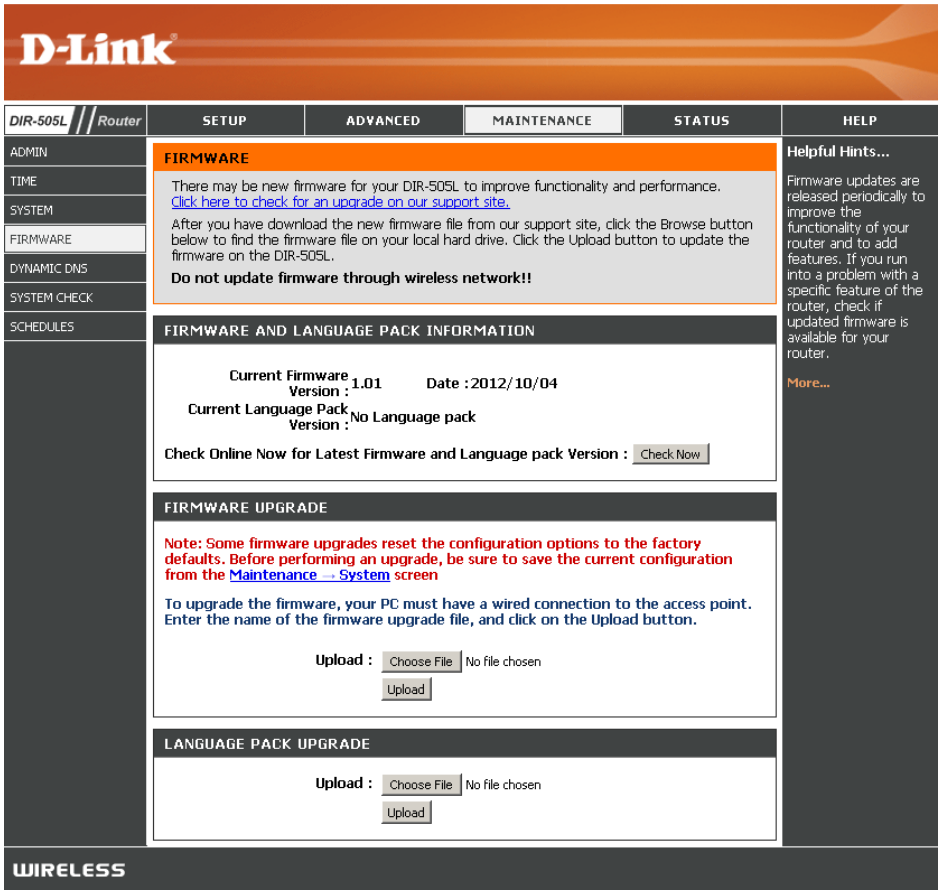
Firmware

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

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

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

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



Language Pack

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

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

Dynamic DNS

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

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

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

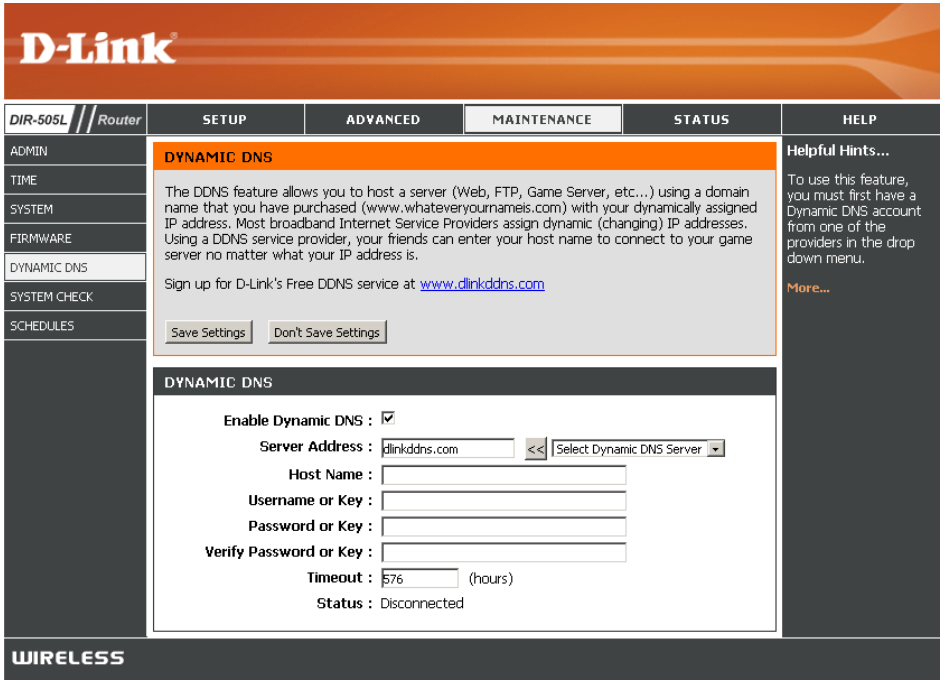
Host Name: Enter the Host Name that you registered with your DDNS service provider.

User name or Key: Enter the user name or key for your DDNS account.

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

Timeout: Enter a timeout time (in hours).

Status: Displays the current connection status.



System Settings

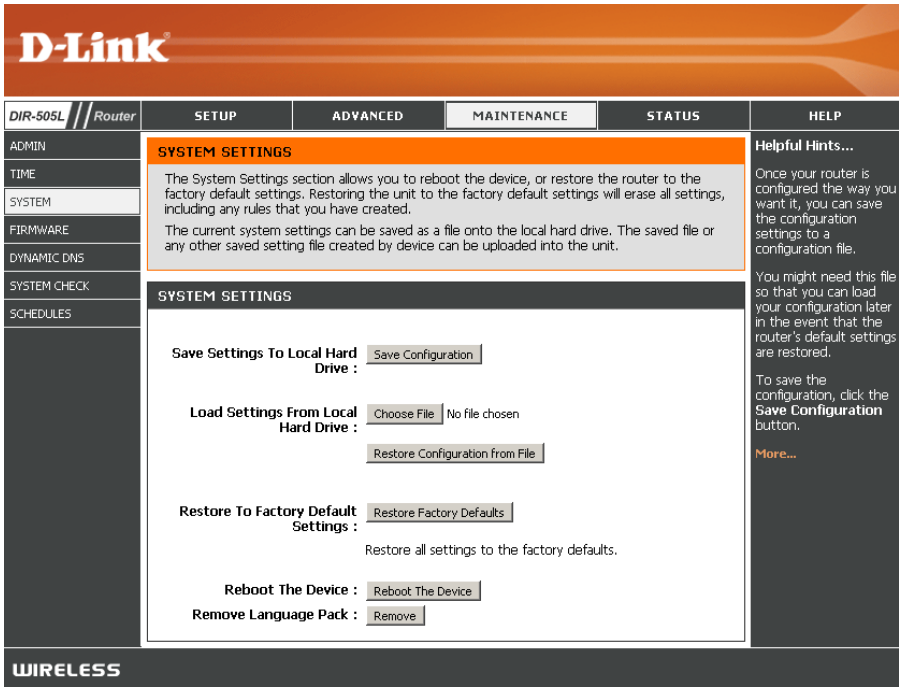
This page allows you to reboot the device or restore the router to the factory settings.

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

Load Settings from Local Hard Drive: Use this option to load previously saved router configuration settings. Use the **Choose File** to find any previously save files of configuration settings. Then, click the **Restore Configuration from File** button to transfer those settings to the Router.

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

Clear Language Pack: Click to remove all non-default language packs from the router.



Schedules

This page allows you to create a schedule to manage schedule rules for firewalls and parental control features.

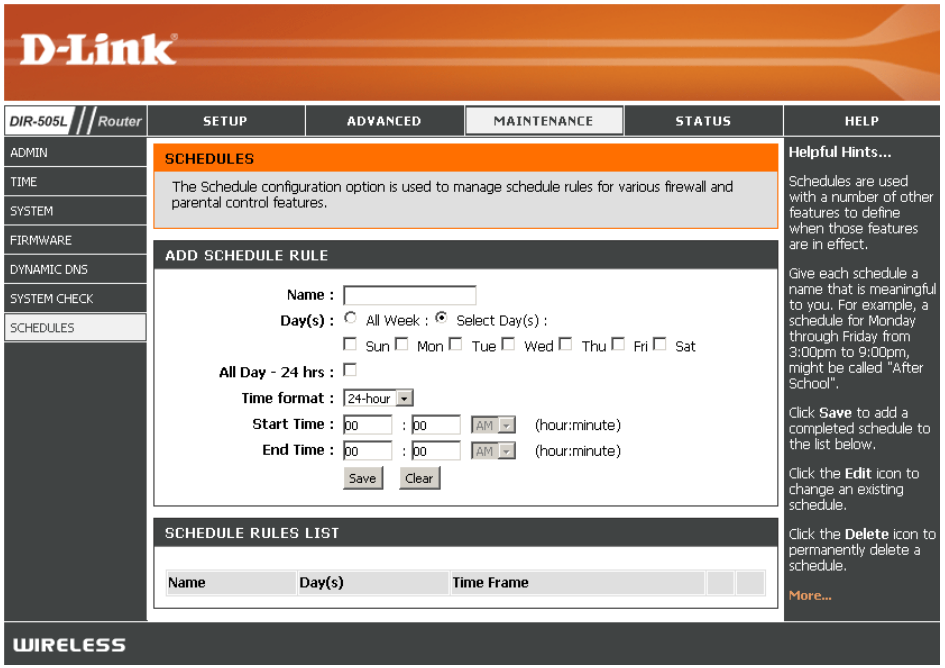
Name: Enter a name for your new schedule.

Days: Select a day, a range of days, or **All Week** to include every day.

Time format: Check **All Day - 24 hrs** or enter a start and end time for your schedule.

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

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



Status
Device Info

This page displays the current information for the DIR-505L. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a *Dynamic IP address* then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

General: Displays the router's time and firmware version.

WAN: Displays the MAC address and the public IP settings for the router.

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

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

LAN Computer: Displays the LAN client info which connects to the router.

Logs

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

Log Type: Use the radio buttons to select the types of messages that you want to display from the log. **System Activity**, **Debug Information**, **Attacks**, **Dropped Packets**, and **Notice** messages can be selected.

Log Details: Use this section to view and manage the router's log entries.

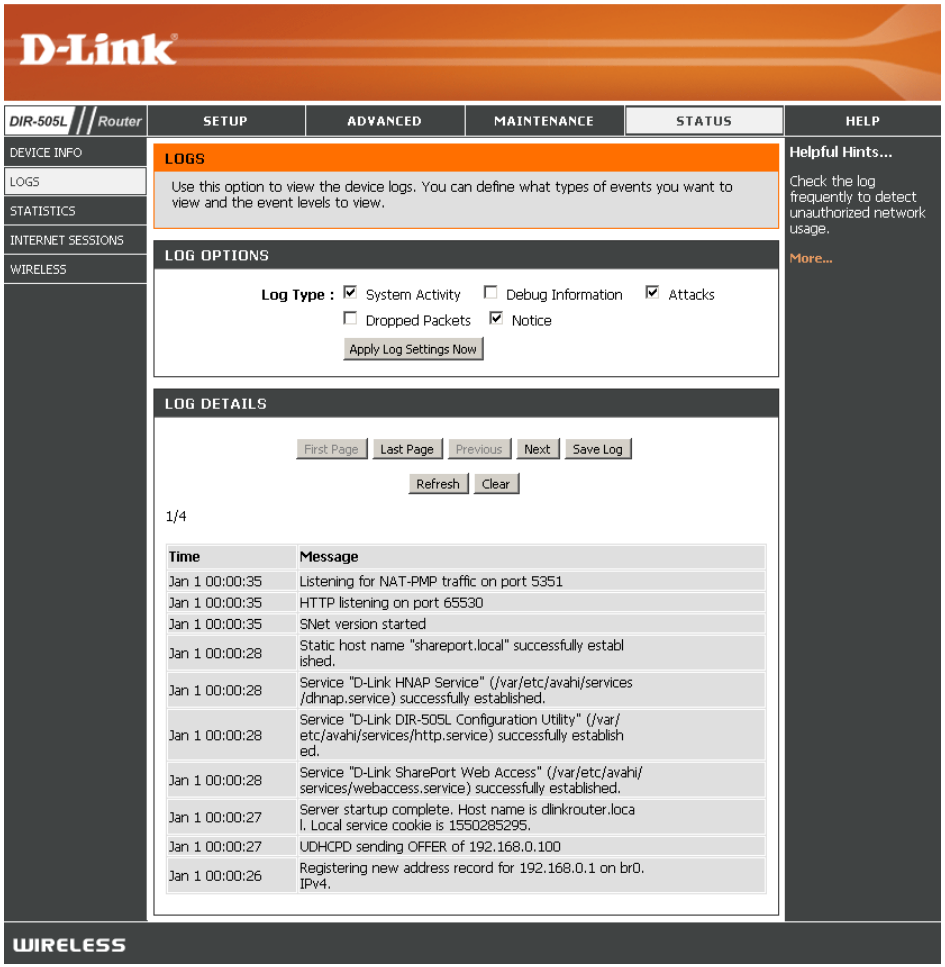
First Page: Click this button to view the first page of the router logs.

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

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

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

Clear: Clears all of the log contents.

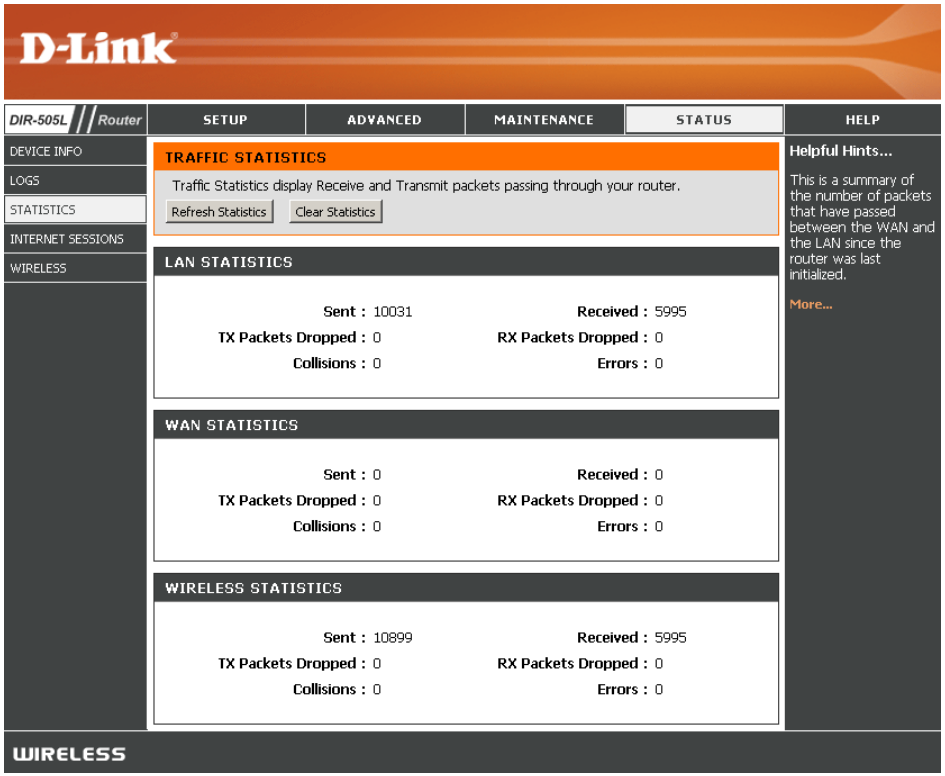


Statistics

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

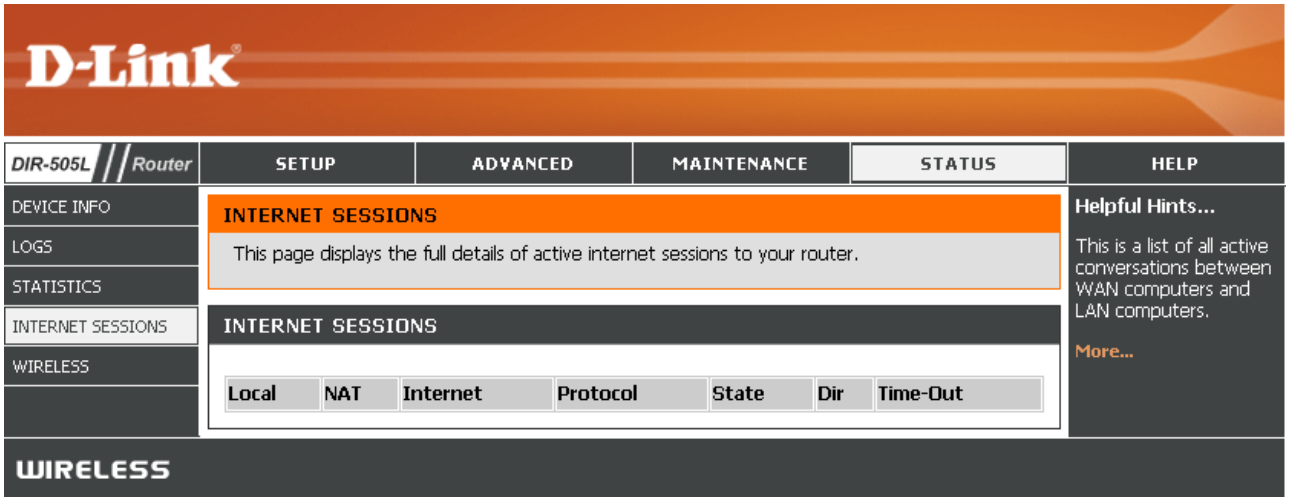
Refresh Statistics: Click the **Refresh Statistics** button to refresh the router's traffic statistics.

Clear Statistics: Click the **Clear Statistics** button to reset the router's traffic statistics.



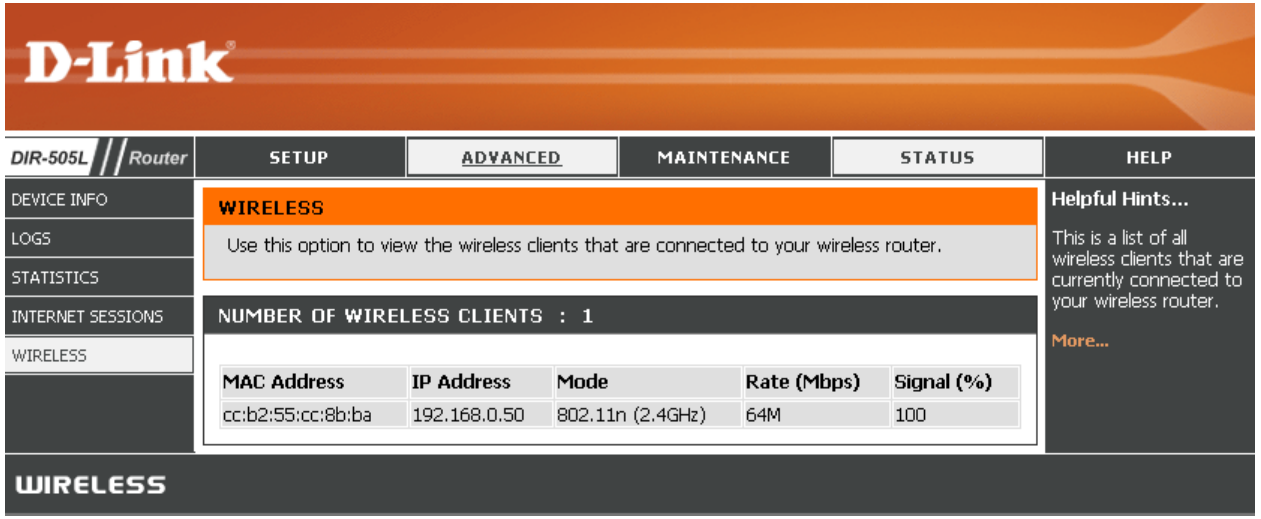
Internet Sessions

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

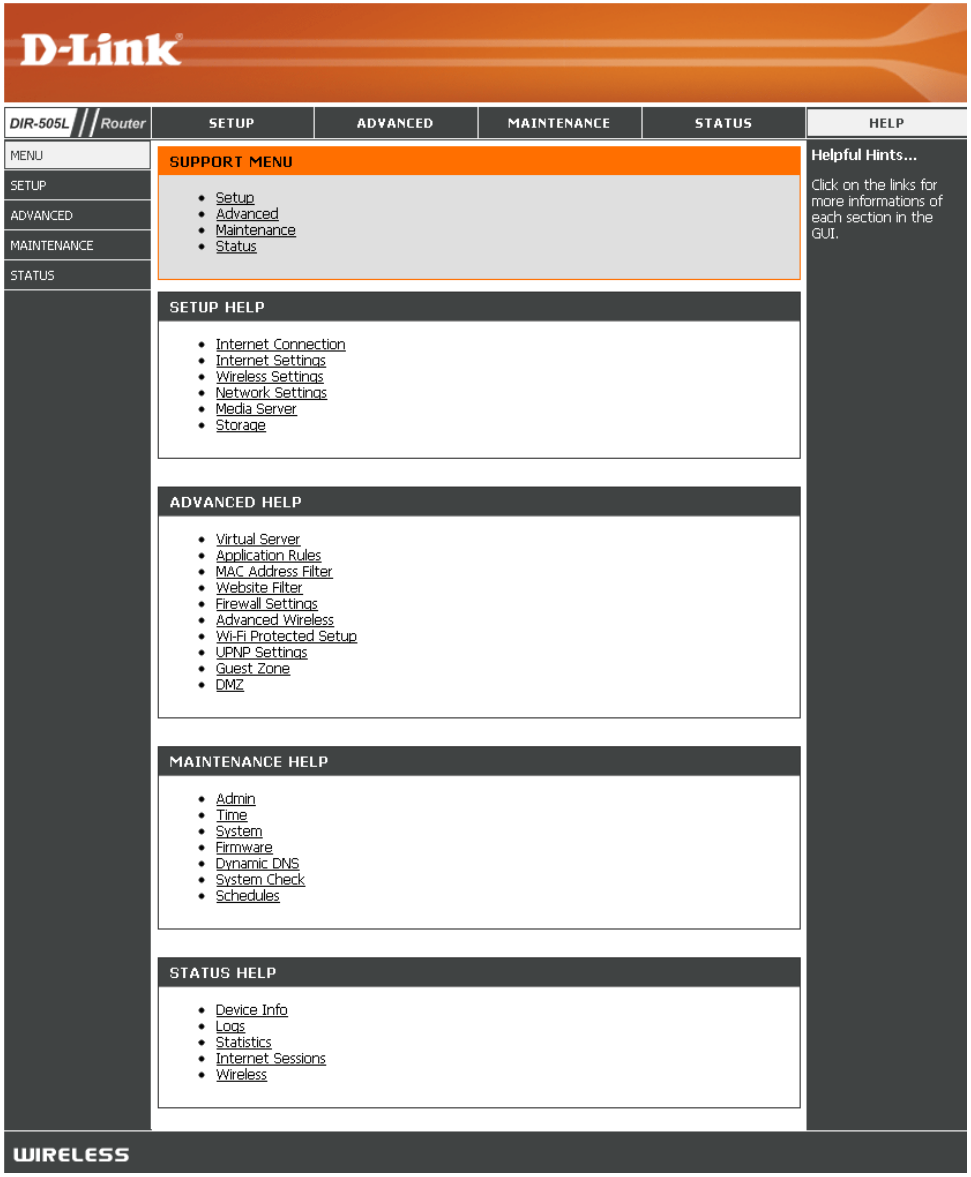


Wireless

The *Wireless Clients* table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.

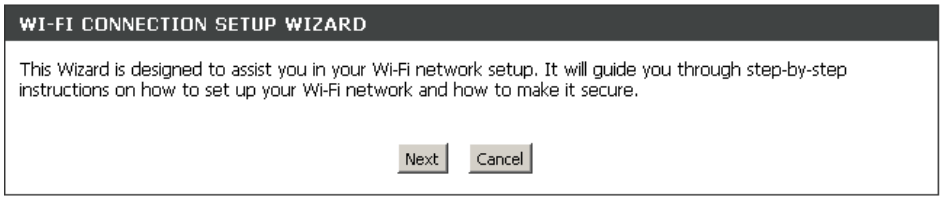


Help

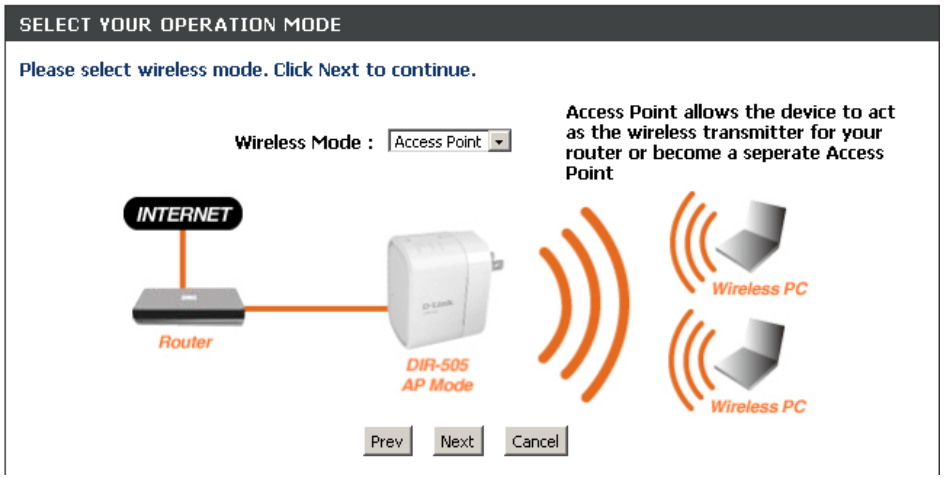

D-Link
DIR-505L Router
SETUP
ADVANCED
MAINTENANCE
STATUS
HELP
MENU
SETUP
ADVANCED
MAINTENANCE
STATUS
SUPPORT MENU
Setup
Advanced
Maintenance
Status
SETUP HELP
Internet Connection
Internet Settings
Wireless Settings
Network Settings
Media Server
Storage
ADVANCED HELP
Virtual Server
Application Rules
MAC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

Access Point Mode
Quick Setup Wizard

Click **Next** to begin the *Quick Setup Wizard*.

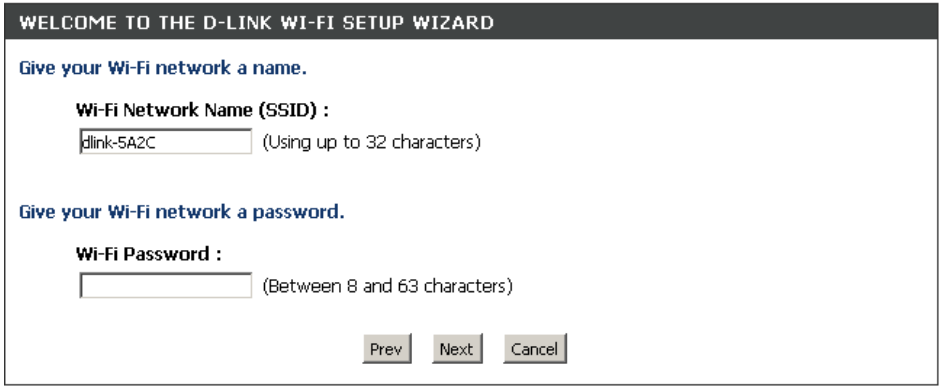


Select **Access Point** from the drop-down menu and click **Next** to continue.

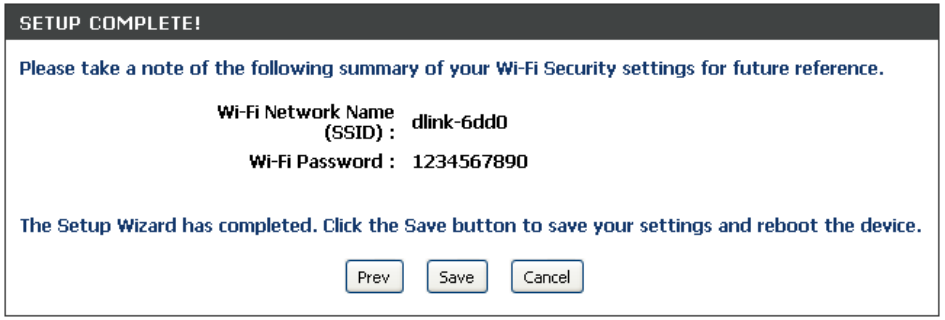


Note: *If the wizard does not open you can set the DIR-505L to* ***Access Point Mode*** *by clicking* ***Setup*** *at the top, then clicking* ***Internet Settings*** *on the left. Next, click the* ***Manual Setup*** *button. Select* ***Access Point*** *in the Wireless Mode drop-down menu. Click* ***Save Settings*** *to save your changes and reboot the DIR-505L.*

Give your Wi-Fi network a name in the box. You may use up to 32 characters. Then, enter a Wi-Fi Password and click **Next**.



When this screen appears, the setup is complete. Write down your *Wi-Fi Security Settings* information for future reference. Click the **Save** button to save your settings.



Setup

Wireless Setup

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

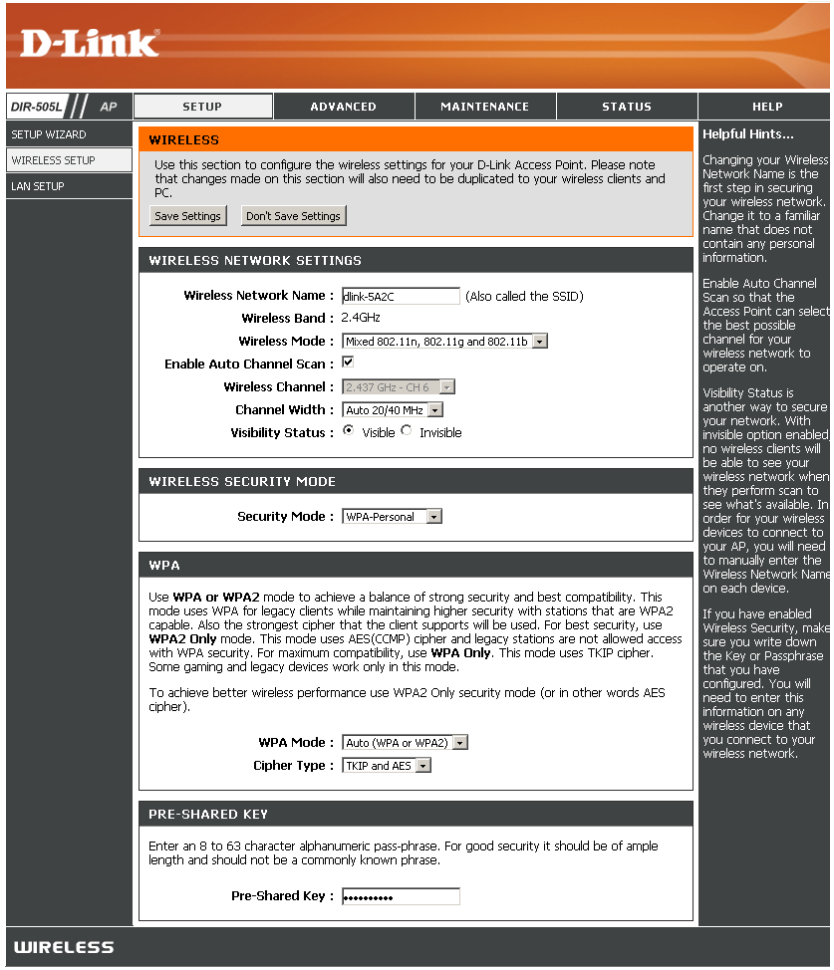
Wireless Mode: Select one of the following:
802.11g Only - Select if all of your wireless clients are 802.11g.
802.11n Only - Select only if all of your wireless clients are 802.11n.
Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 11g wireless clients.

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

Wireless Channel: Indicates the channel setting for the DIR-505L. By default the channel is set to **6**. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

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

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-505L. If **Invisible** is selected, the SSID of the DIR-505L will not be seen by *Site Survey* utilities so your wireless clients will have to know the SSID of your DIR-505L.



LAN Setup

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

Device Name: Allows you to configure the device more easily when your network is using TCP/IP protocol. Enter a name for your device.

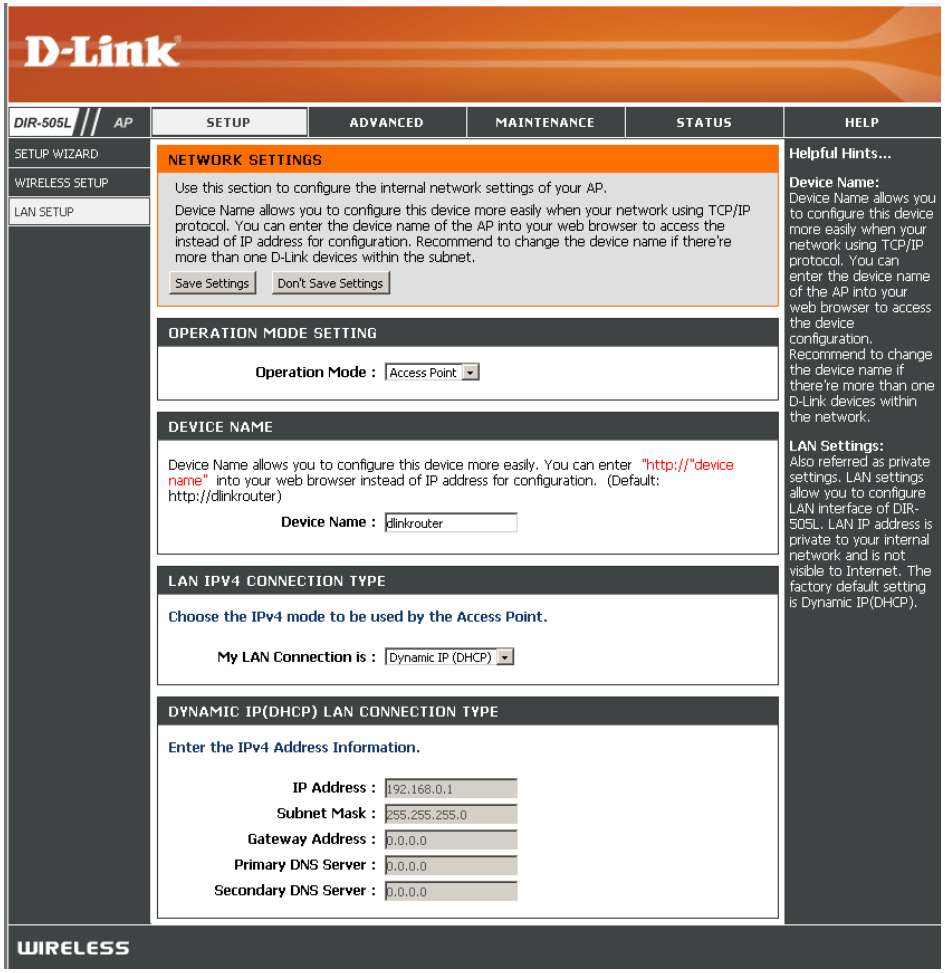
My LAN Connection is: Select from the drop-down menu the *Operation Mode* you would like to use.

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

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Gateway Address: Enter the Gateway assigned by your ISP.

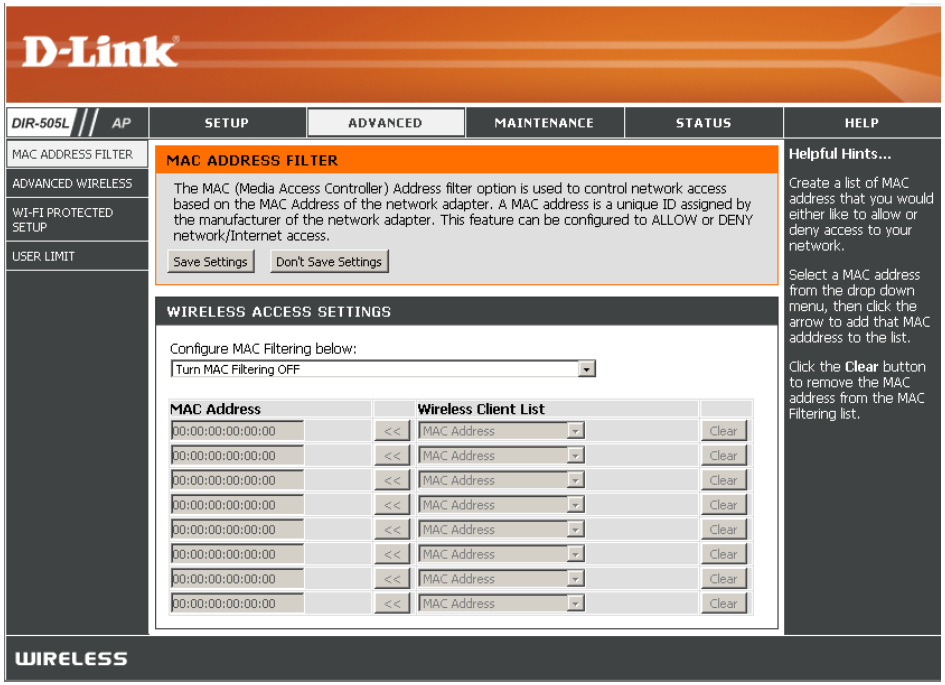
Primary/ Secondary DNS Server: Enter the Primary and Secondary DNS server IP addresses assigned by your ISP. These addresses are usually obtained automatically from your ISP. Enter the value **0.0.0.0** if you did not specifically receive these from your ISP.



Advanced
MAC Address Filter

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

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



Advanced Wireless

Transmit Power: Set the transmit power of the antennas.

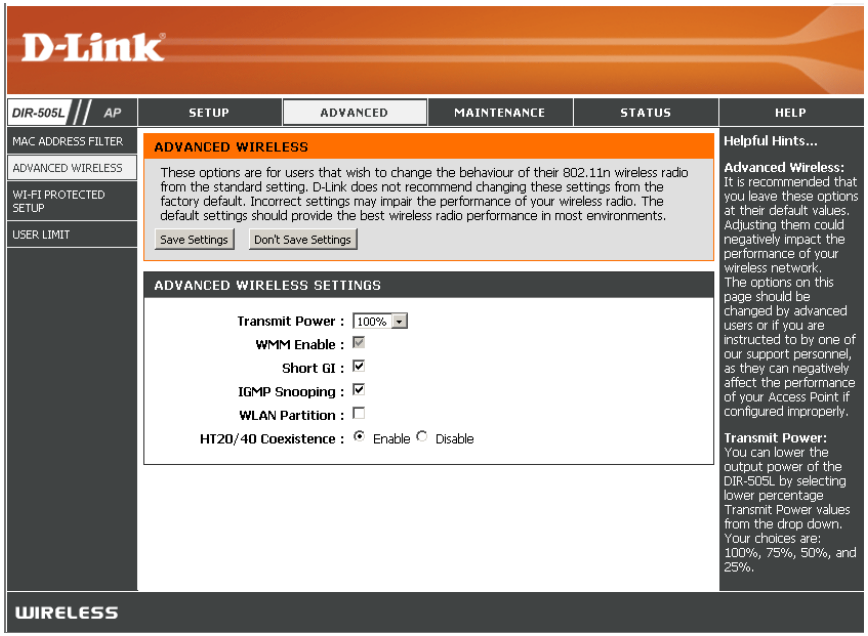
WMM Enable: *WMM* is QoS for your wireless network. This will improve the quality of video and voice applications for your wireless clients.

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

IGMP Snooping: Check to enable this feature.

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

HT20/40 Coexistence: You may choose to **Enable** or **Disable** this feature. Enabling this feature allows two "channels" or paths on which data can travel to be combined to increase performance in some environments.



Wi-Fi Protected Setup (WPS)

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

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

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

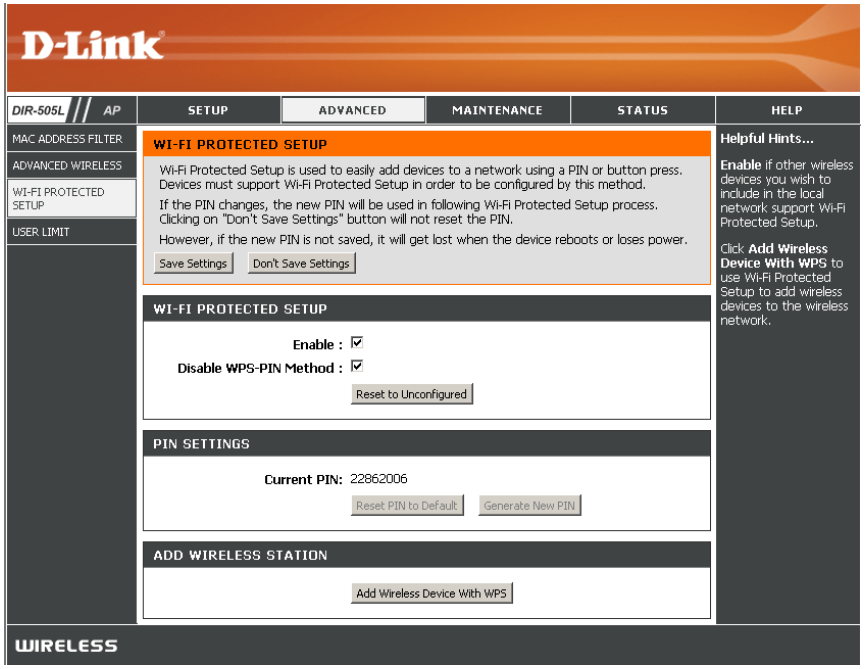
Disable WPS-PIN Method: Locking the *WPS-PIN Method* prevents the settings from being changed by any external registrar using its PIN. Devices can still be added to the wireless network using the *Wi-Fi Protected Setup Push Button Configuration* (*WPS-PBC*). It is still possible to change wireless networks settings with *Manual Wireless Network Setup* or *Wireless Network Setup Wizard*.

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

Current PIN: Shows the current PIN.

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

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



Add Wireless Devices with WPS: This wizard helps you add wireless devices to the wireless network.

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

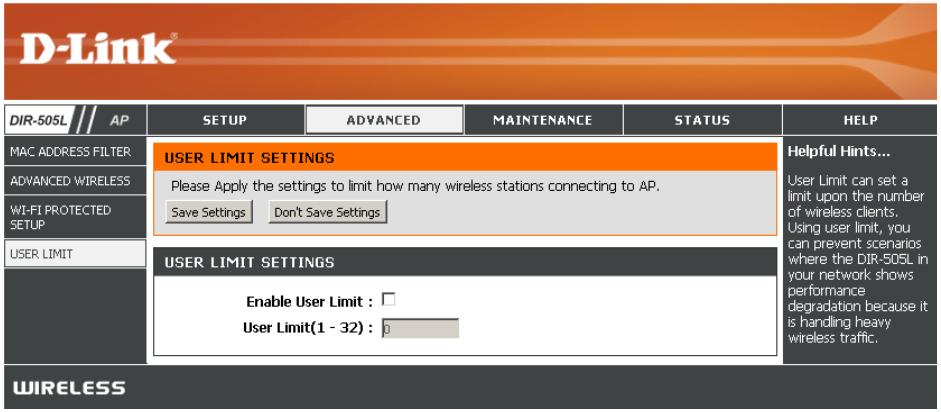
There are several ways to add a wireless device to your network. A "registrar" controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special **Wi-Fi Protected Setup** button on the device. The router acts as a registrar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

User Limit

This sections allows you to set a limit on the number of wireless clients to control wireless traffic.

Enable User Limit: Check the box to enable user limit.

User Limit (1-32): Enter a number (**1**-**32**) to regulate the user limit and wireless traffic.

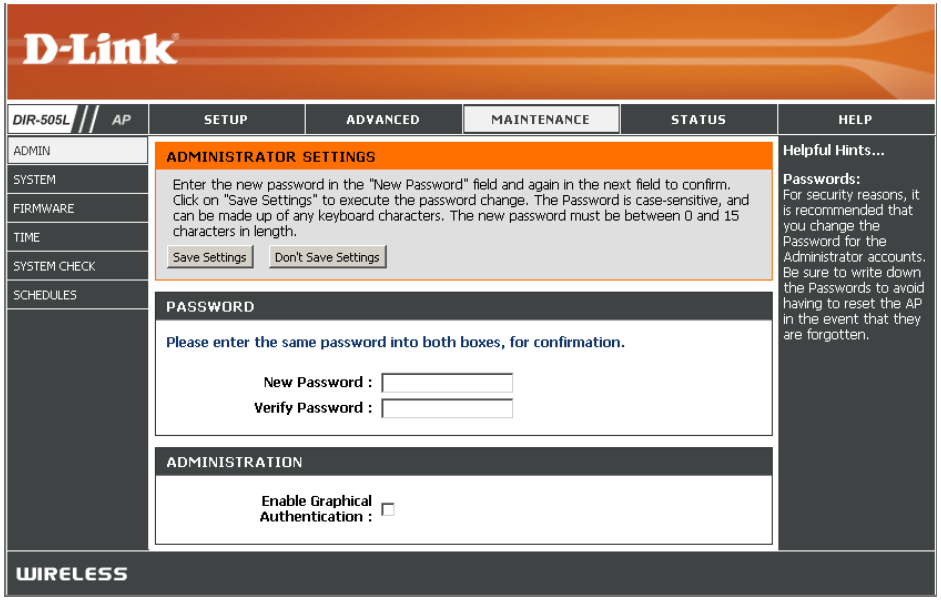


Maintenance
Admin

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

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

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



System

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

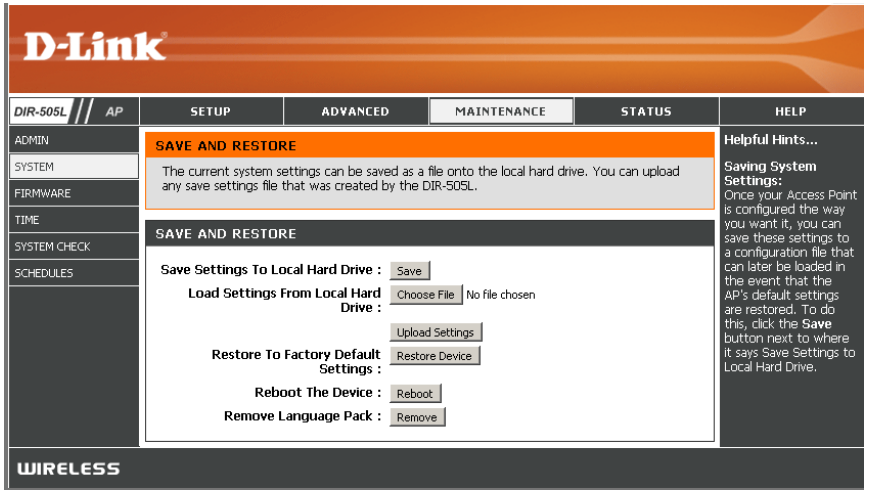
Save Settings To Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. A file dialog will appear, allowing you to select a location and file name for the settings.

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

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

Reboot The Device: Click to reboot the router.

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



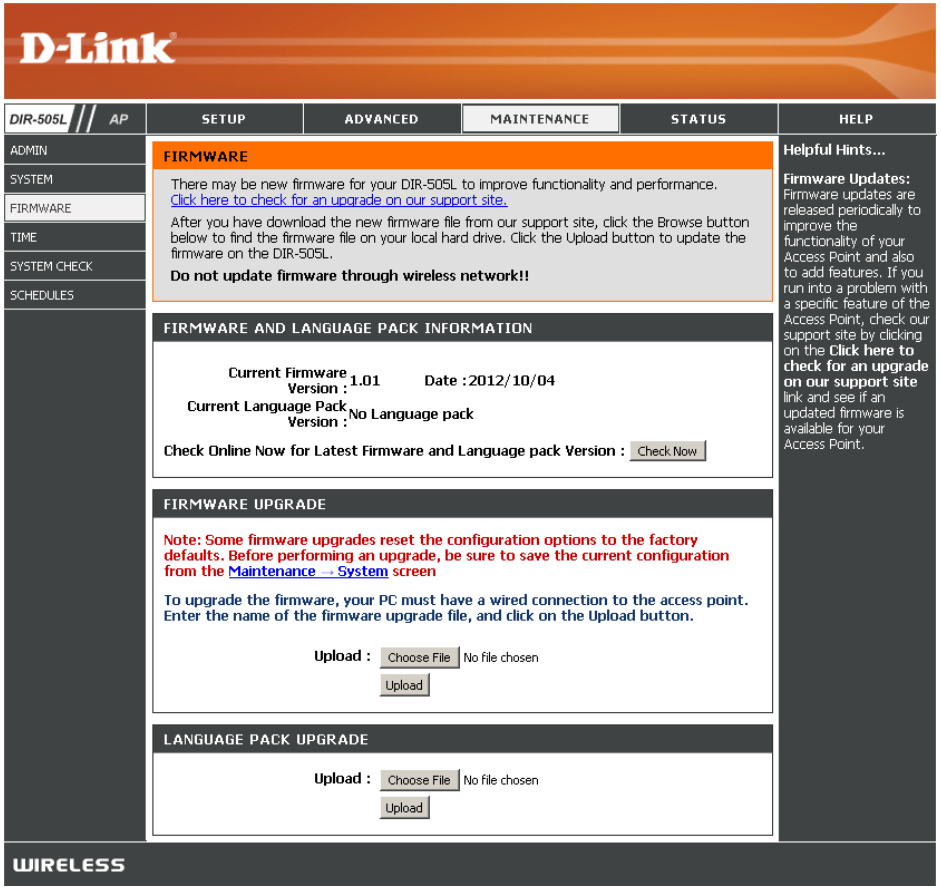
Firmware

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

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

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

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



Language Pack

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

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

Time

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

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

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

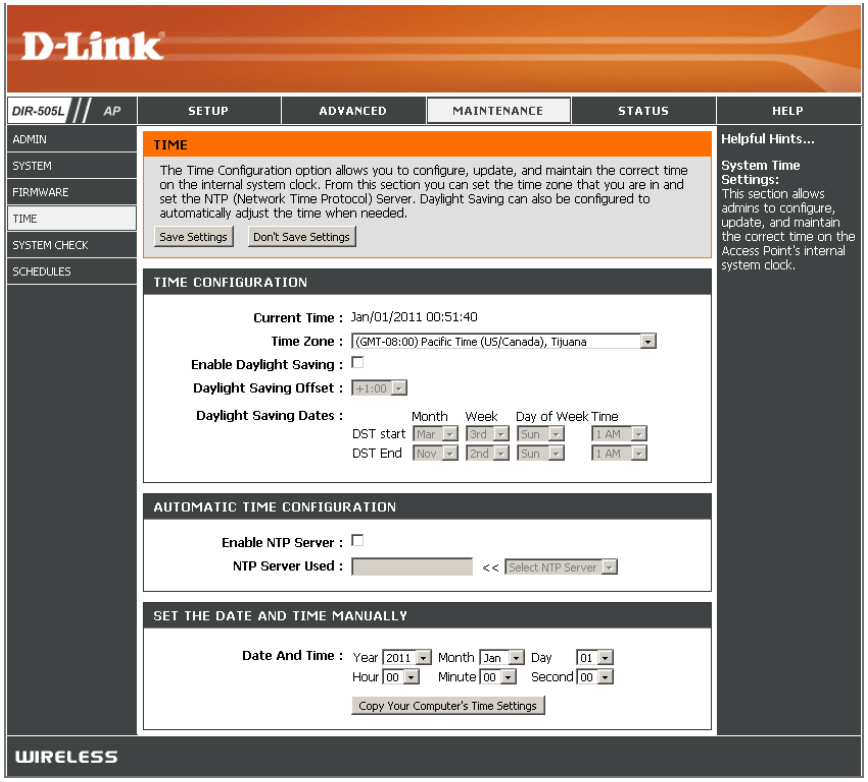
Enable Daylight-Saving: To select *Daylight-Saving* time manually, select enabled or disabled, and enter a start date and an end date for daylight-saving time.

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

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

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

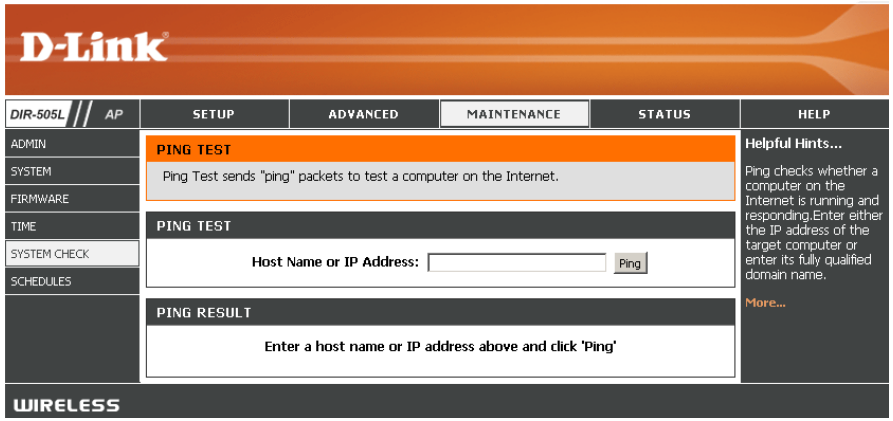
You can also click **Copy Your Computer's Time Settings** to synch the date and time with the computer you are currently on.



System Check

Ping Test: The *Ping Test* is used to send Ping packets to test if a computer is on the Internet. Enter the IP address that you wish to Ping and click **Ping**.

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



Schedules

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

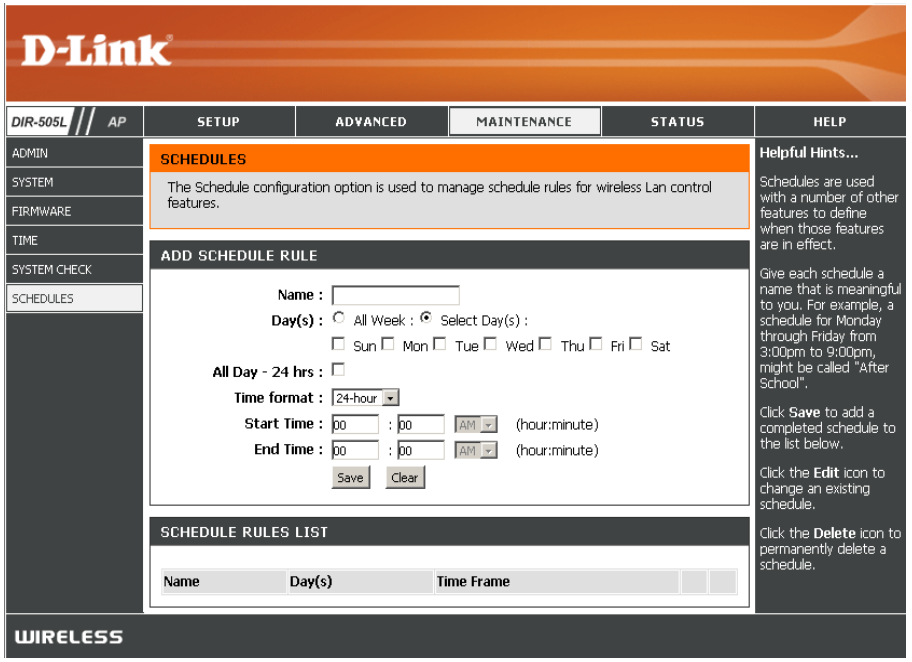
Name: Enter a name for your new schedule.

Day(s): Select a day, a range of days, or **All Week** to include every day.

Time Format: Check **All Day - 24 hrs** or enter a start and end time for your schedule.

Save: You must click **Save** for your schedules to go into effect.

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



Status
Device Info

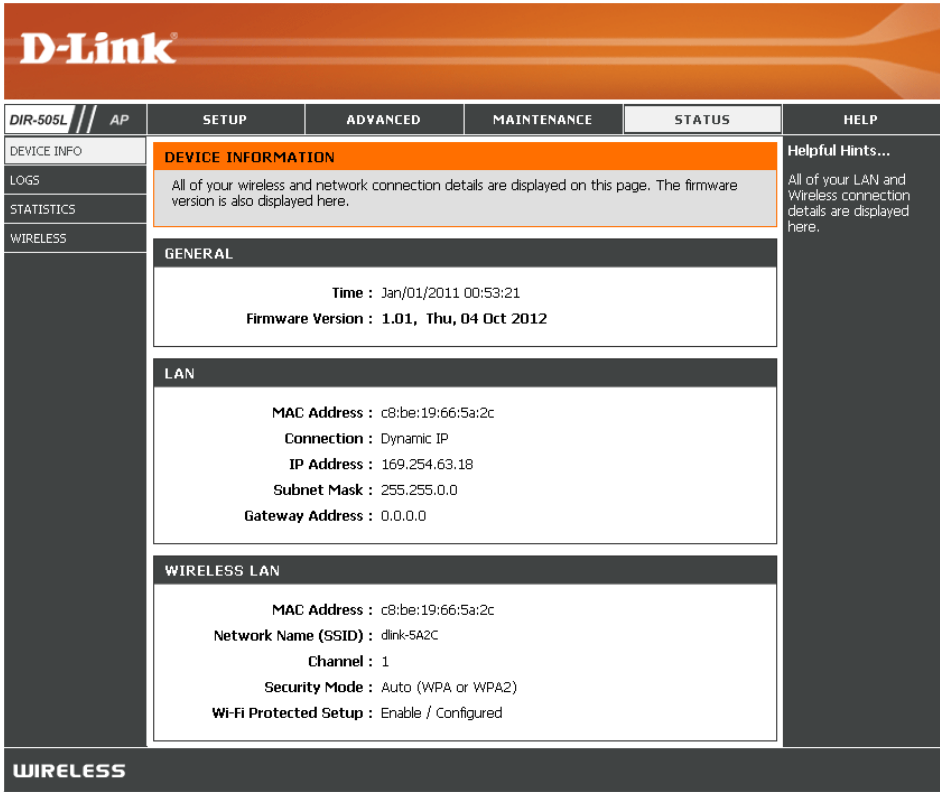
This page displays the current information for the DIR-505L. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

General: Displays the router's time and firmware version.

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

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



Logs

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

Log Type: Use the radio buttons to select the types of messages that you want to display from the log. **System Activity**, **Debug Information**, **Attacks**, **Dropped Packets**, and **Notice** messages can be selected.

Log Details: Use this section to view and manage the router's log entries.

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

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

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

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

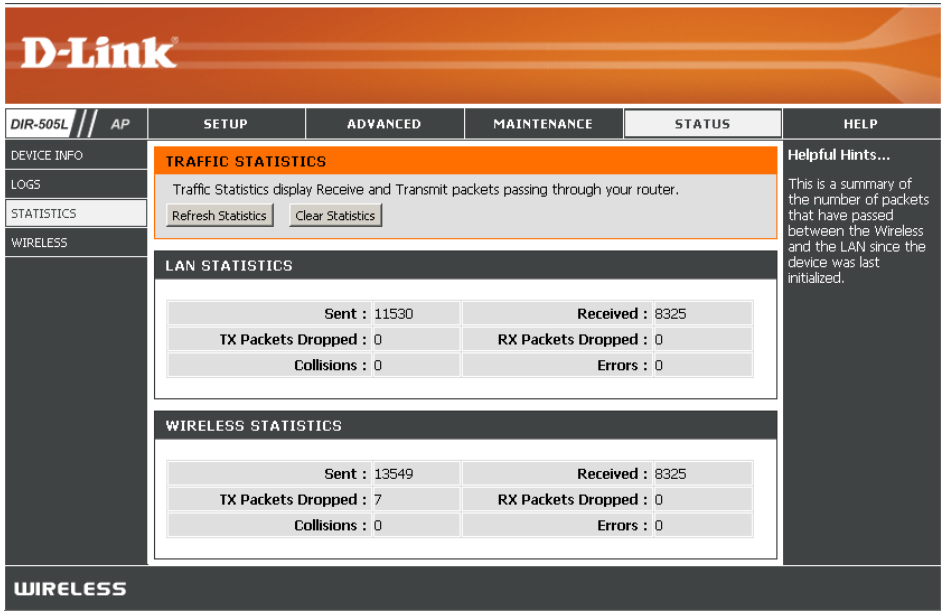
Clear: Clears all of the log contents.

Statistics

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

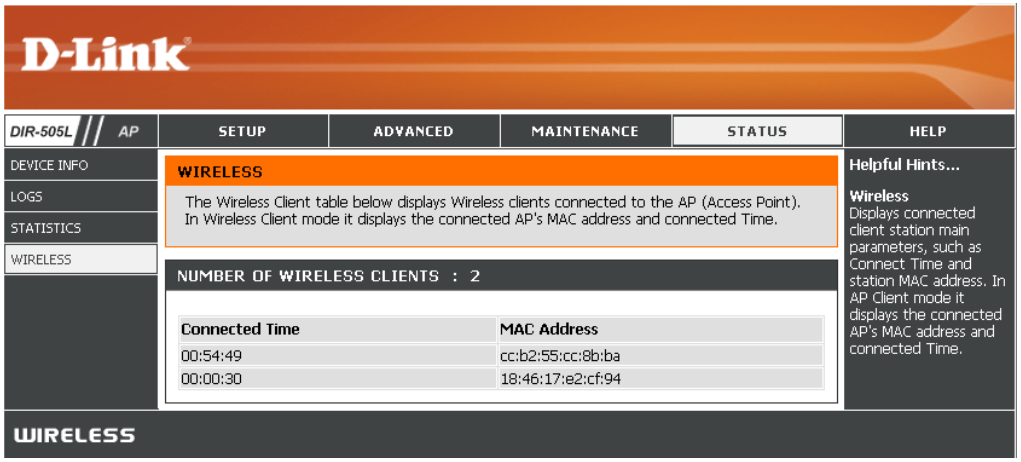
Refresh Statistics: Click the **Refresh Statistics** button to refresh the AP's traffic statistics.

Clear Statistics: Click the **Clear Statistics** button to reset the AP's traffic statistics.



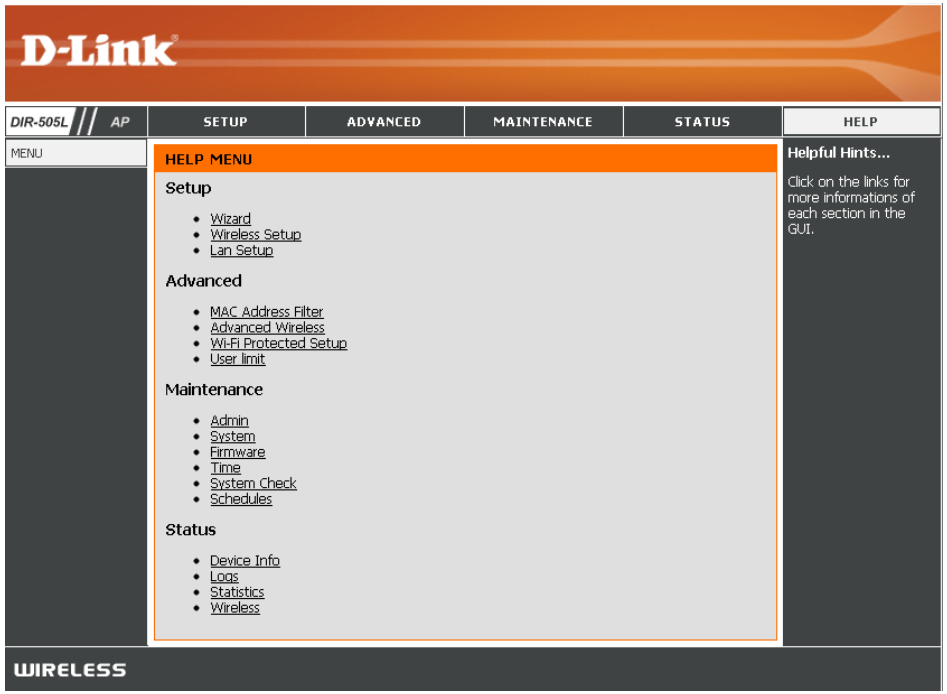
Wireless

The wireless client table displays a list of current connected wireless clients. This table also displays the connection time and MAC address of the connected wireless clients.



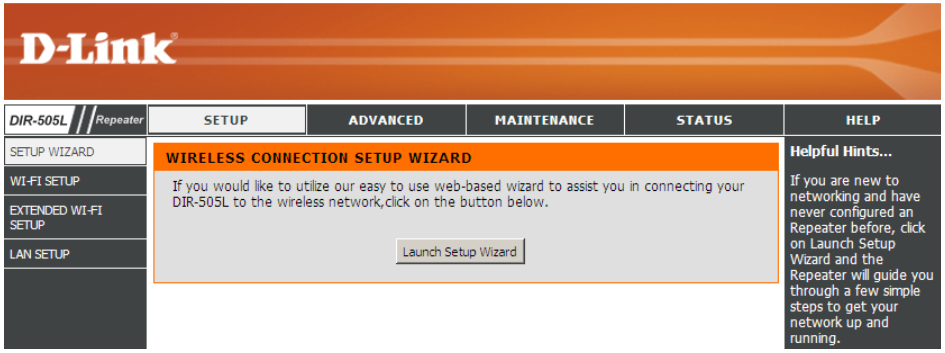
Help

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

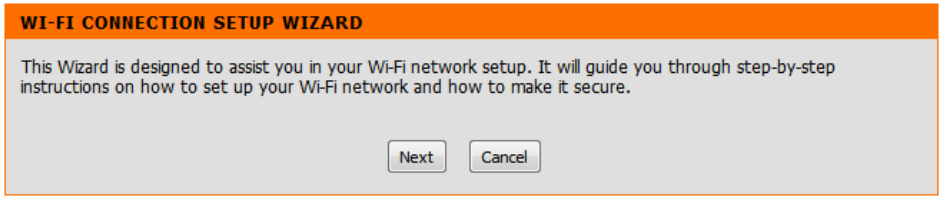


Repeater Mode
Quick Setup Wizard

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

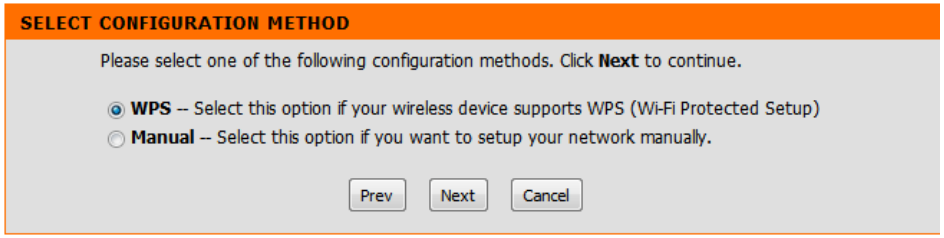


To start the *Setup Wizard* click **Next**.

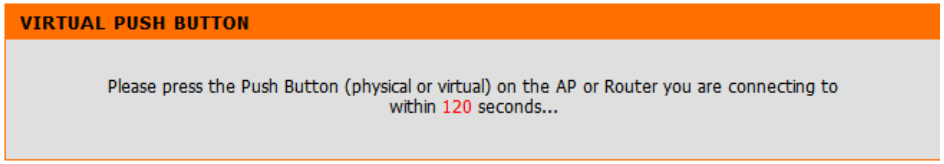


Select **WPS** as the configuration method only if your wireless device supports *Wi-Fi Protected Setup* (*WPS*).

Click **Next** to continue.

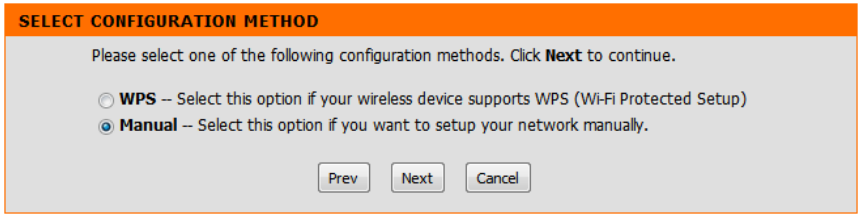


Press down the **WPS** button on the Wireless device you are adding to your wireless network.

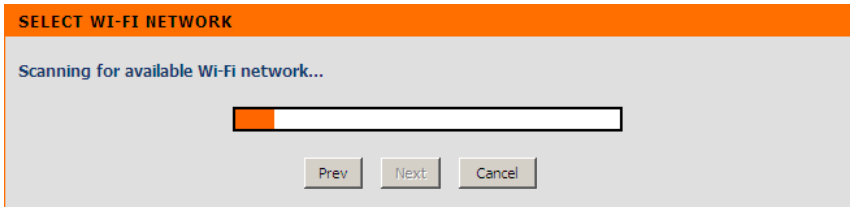


Select **Manual** as the configuration method to set up your network manually.

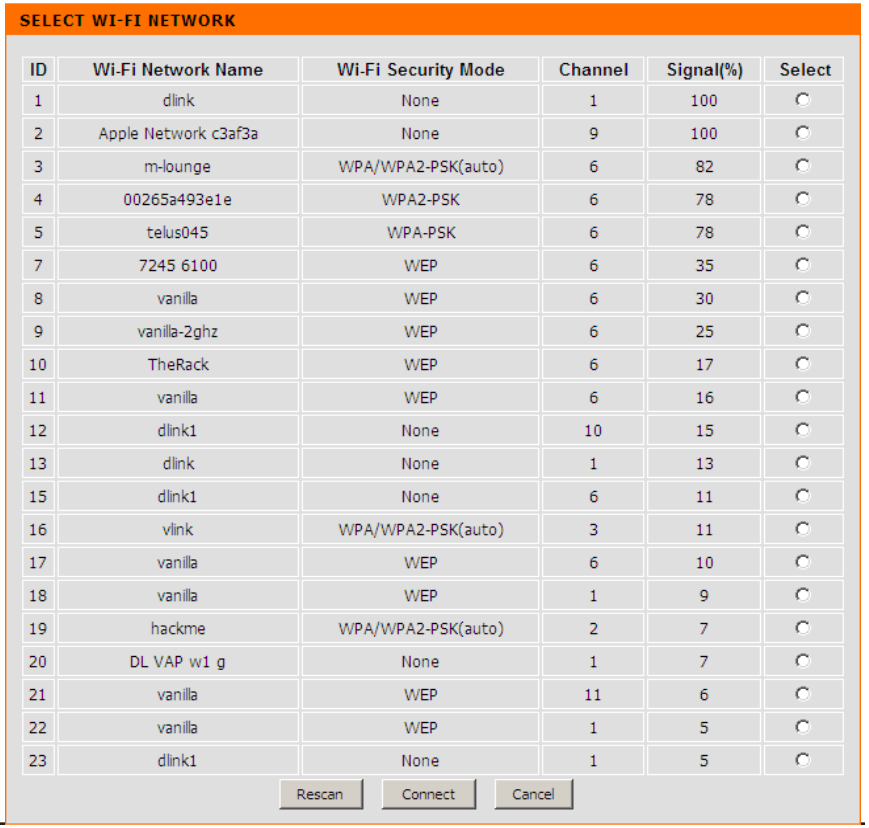
Click **Next** to continue.



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



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



Manual Configuration
Wi-Fi Setup

Use this section to manually configure the Wi-Fi settings for your D-Link Repeater.

Repeater Mode

Wireless Mode: *Repeater Mode.*

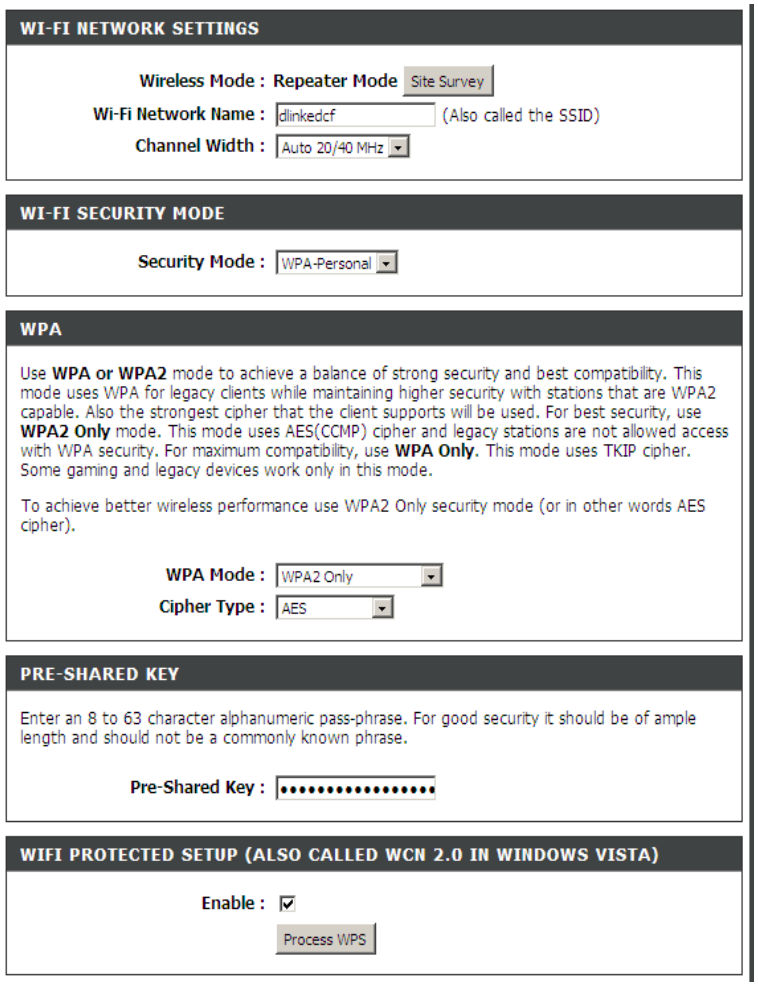
Site Surveys: Scans for available Wi-Fi networks.

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

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

Security Mode: Select **WEP** or **WPA Personal**. Refer to page 88.

Wi-Fi Protected Setup: Click **Enable** to activate the *Wi-Fi Protected Setup* (*WPS*) feature.



Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-505L offers the following types of security:

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

What is WPA?

WPA (Wi-Fi Protected Access), is a Wi-Fi standard that was designed to improve the security features of WEP (Wired Equivalent Privacy).

The 2 major improvements over WEP:

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

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

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

Configure WPA/WPA2 Personal

It is recommended to enable encryption on your wireless DIR-505L before your wireless network adapters. Please establish wireless connectivity before enabling encryption.

1. Log in to the web-based configuration by opening a web browser and entering the IP address of the repeater (**192.168.0.50**). Click on **Setup**, then click **Wireless Settings** on the left side.

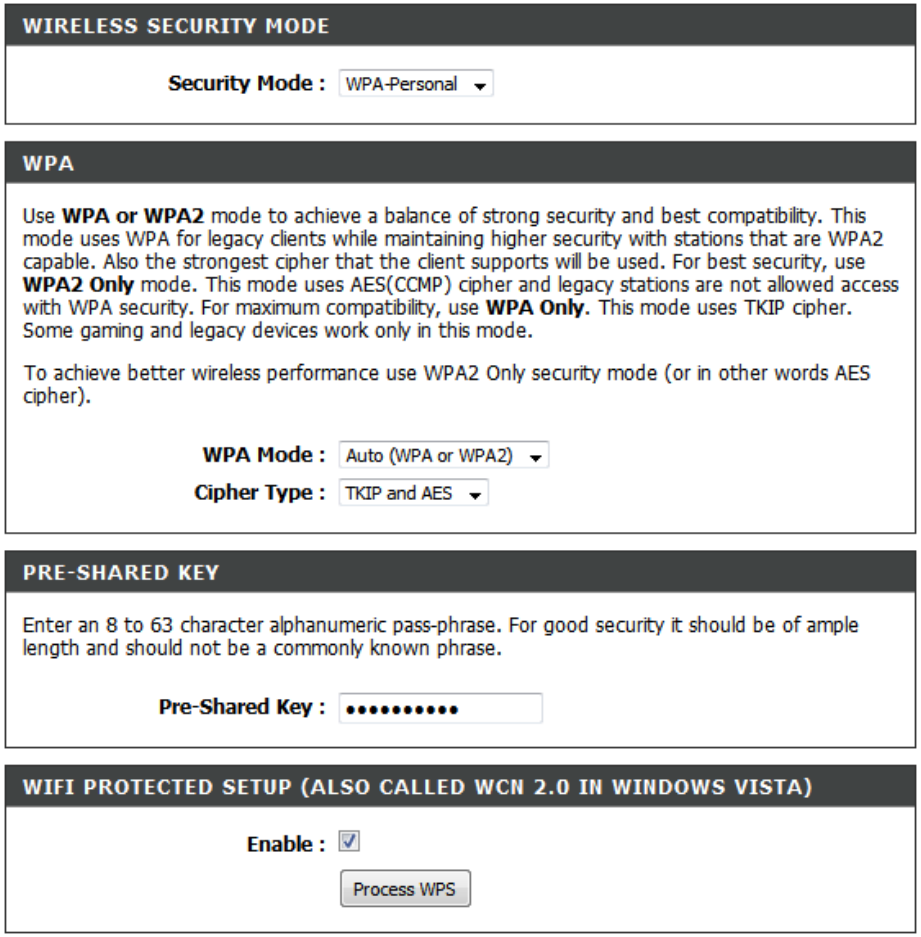
2. Next to *Security Mode*, select **WPA-Personal**.

3. Next to *WPA Mode*, select **WPA only**, **WPA2 only** or **Auto (WPA or WPA2)**.

4. Next to *Cipher Type*, select **TKIP**, **AES** or **TKIP and AES**.

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

6. Click **Save Settings** at the top of the window to save your changes. If you are configuring the repeater with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the DIR-505L.



Extended Wi-Fi Setup

This page allows you to configure the wireless LAN settings for your router by giving you the opportunity to create a new Wi-Fi Network Name for your local Wi-Fi network or use the same Network Name as the joined Wi-Fi HotSpot for your local Wi-Fi Network.

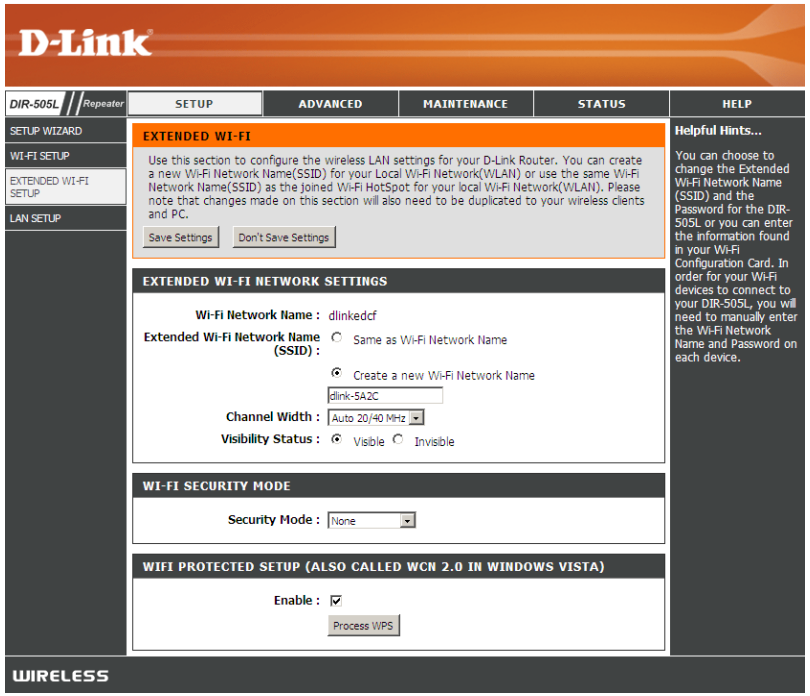
Wi-Fi Network Name: Displays the device's name.

Extended Wi-Fi Network Name (SSID): This gives you the option to select the same Wi-Fi Network Name or to Create a new Wi-Fi Network Name for your local Wi-Fi network.

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

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-505L. If **Invisible** is selected, the SSID of the DIR-505L will not be seen by *Site Survey* utilities so your wireless clients will have to know the SSID of your DIR-505L.

Wi-Fi Protected Setup: Click **Enable** to activate the Wi-Fi Protected Setup (WPS) feature.



LAN Setup

This page will allow you to configure the internal network settings of your Repeater.

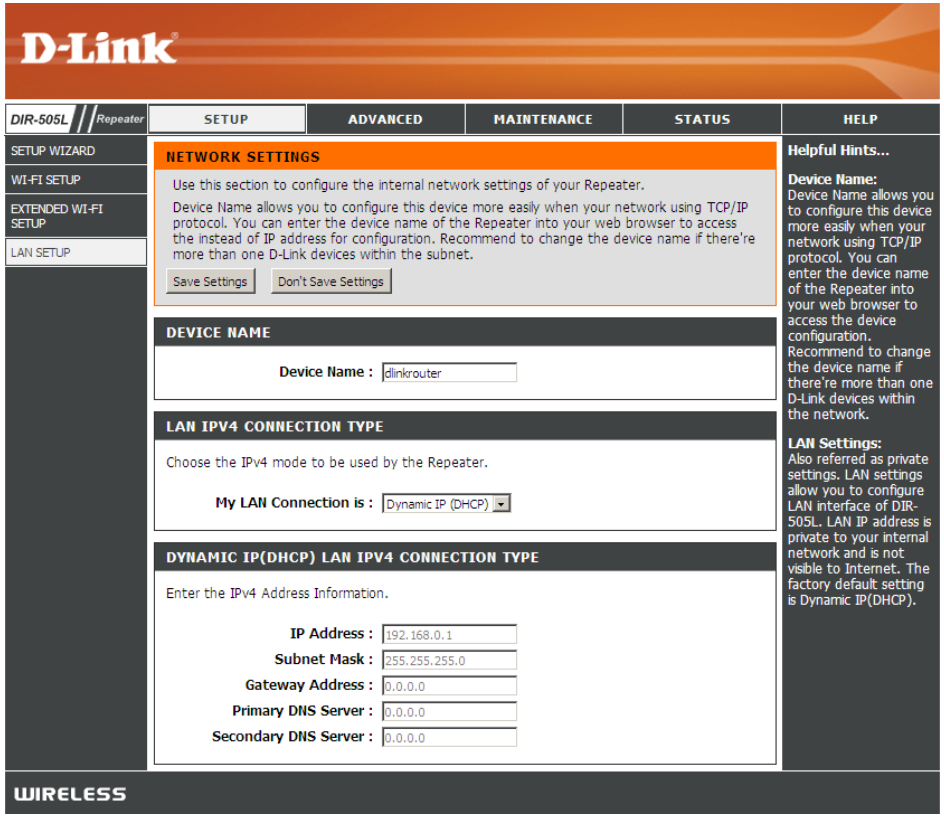
Device Name: Enter the *Device Name* of the AP. It recommended to change the *Device Name* if there is more than one D-Link device within the subnet. You can enter the device name of the AP into your web browser to access the instead of IP address for configuration. If you are using the device name to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

LAN Connection Type: Select the connector you are using from the drop-down menu.

IP Address: Enter the IP address of the access point. The default IP address is **192.168.0.50**. If you change the IP address, once you click **Apply**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

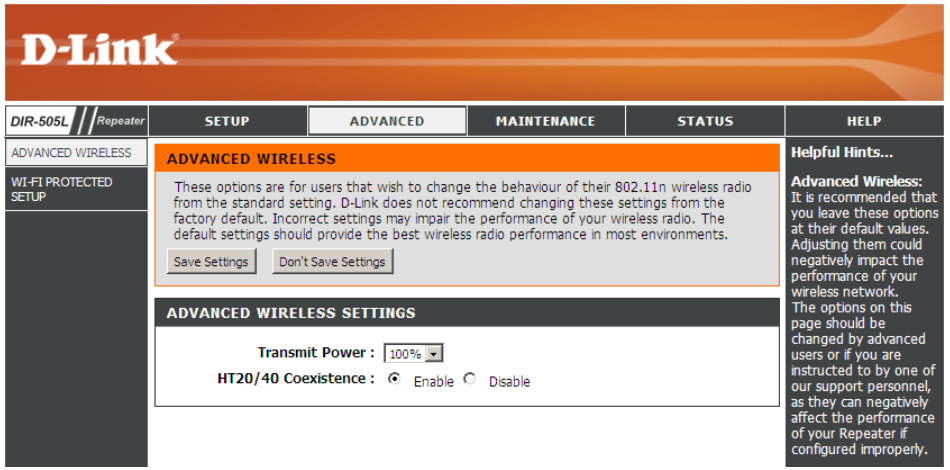
Default Gateway: Enter the *Gateway* assigned by your ISP.



Advanced
Advanced Wireless

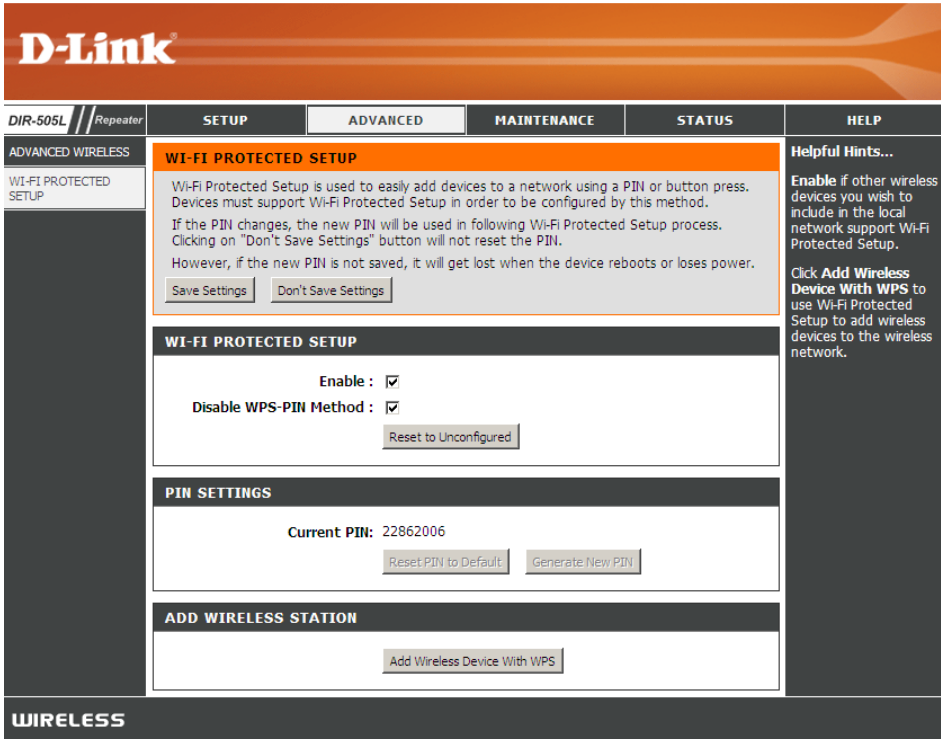
Transmit Power: Sets the transmit power of the antennas.

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



Wi-Fi Protected Setup

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



Enable: Check this box to enable the function

Disable WPS-PIN Method: Locking the *WPS-PIN Method* prevents the settings from being changed by any external registrar using its PIN. Devices can still be added to the wireless network using the *Wi-Fi Protected Setup Push Button Configuration* (*WPS-PBC*). It is still possible to change wireless networks settings with *Manual Wireless Network Setup* or *Wireless Network Setu Wizard*.

Pin Settings: This feature allows you to Reset your current PIN or to generate a new PIN.

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

Reset PIN to Default: This will allow you to restore the default PIN of your access point.

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

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

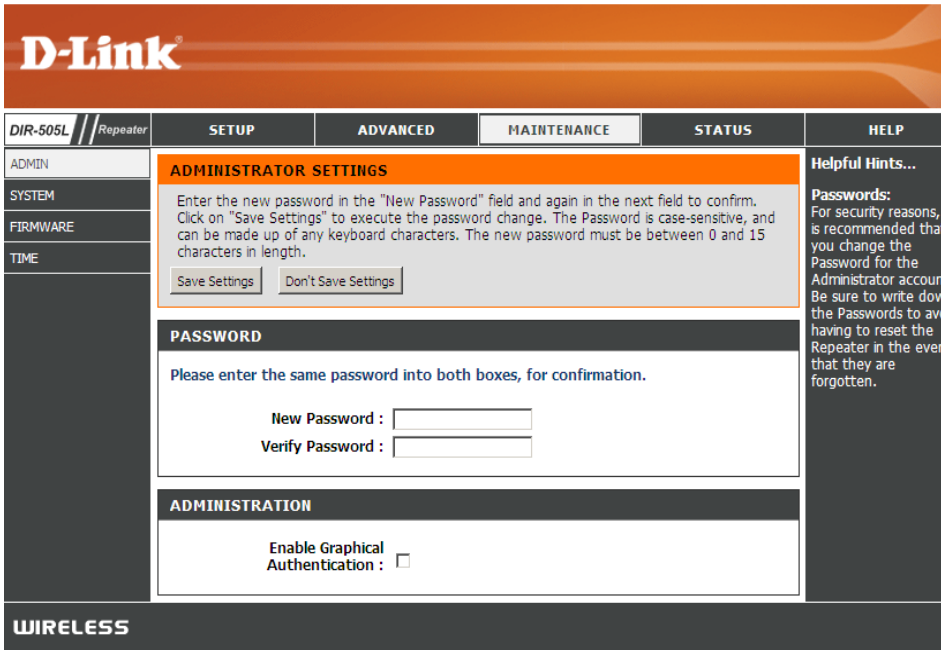
Maintenance
Admin

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

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

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

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



System

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

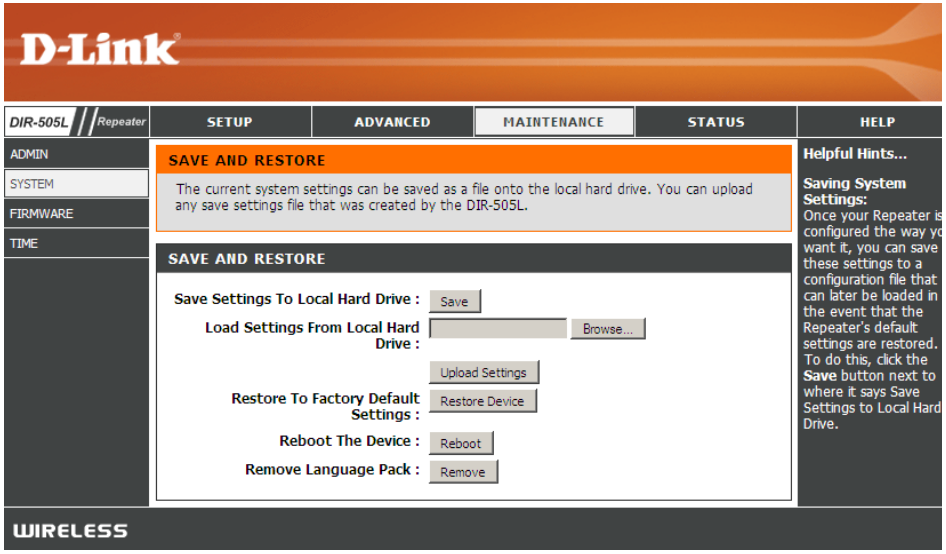
Upload from Local Hard Drive: Use this option to load previously saved access point configuration settings. Click **Browse** to find a previously saved configuration file. Then, click the **Upload Settings** button to transfer those settings to the repeater.

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

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

Reboot the Device: Click to reboot the repeater.

Remove the Language Pack: Click to remove any installed language packs.



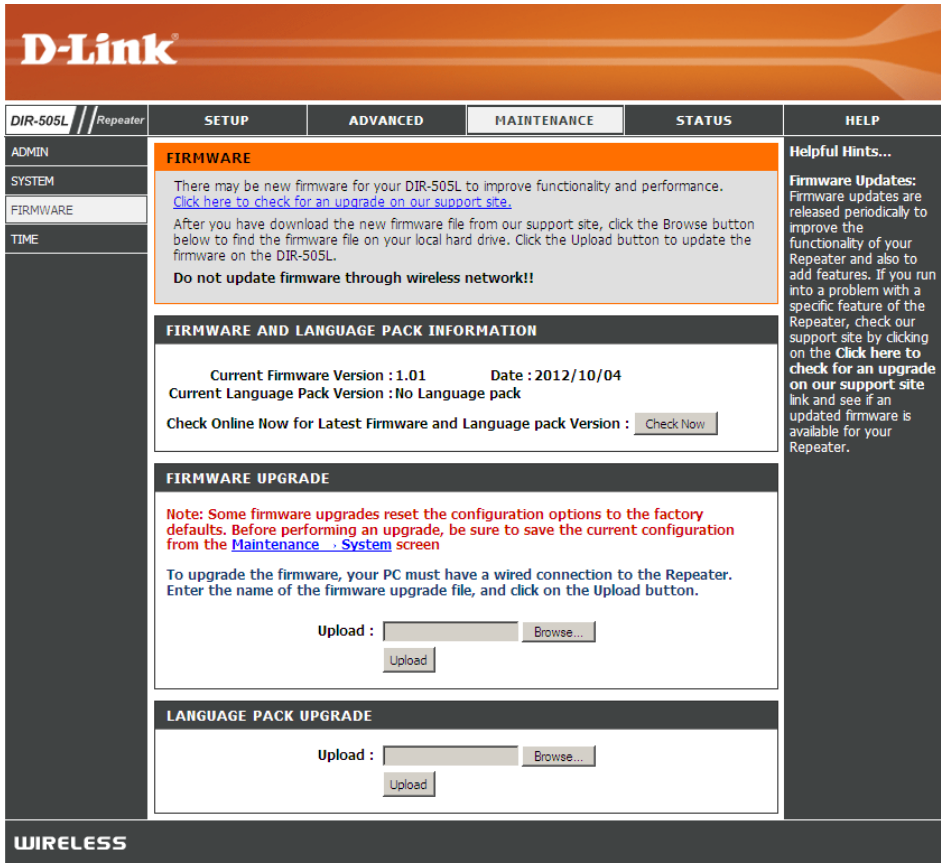
Firmware

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

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

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

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



Language Pack

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

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

Time

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

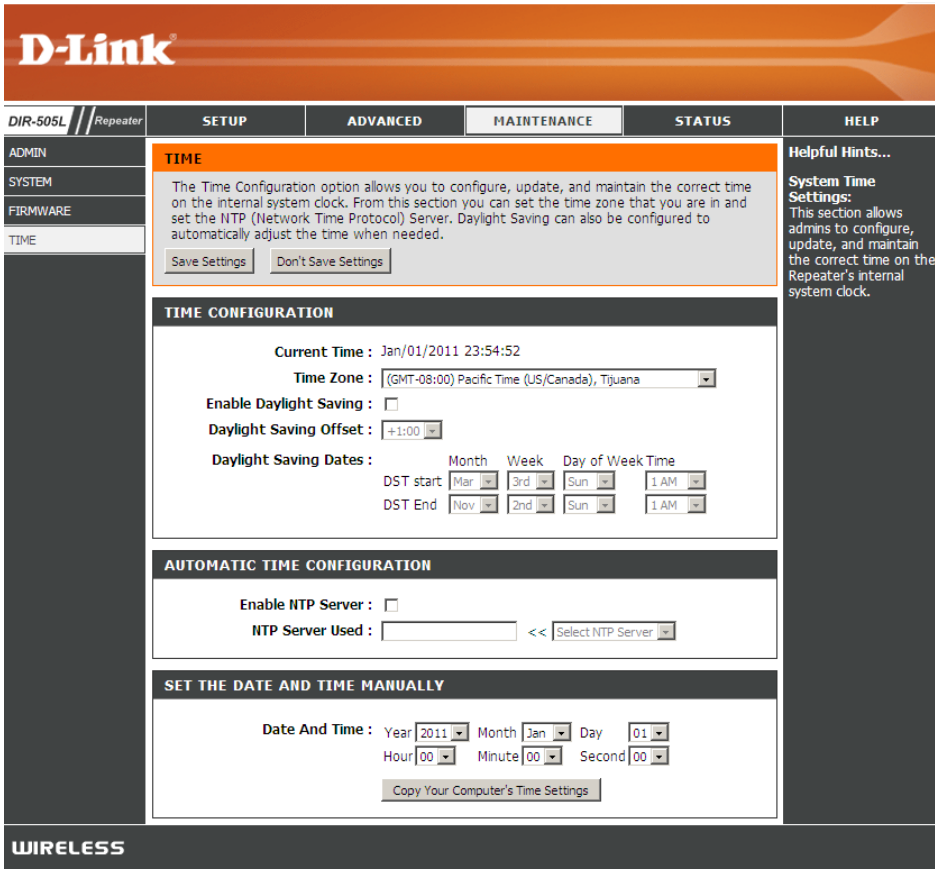
Time Zone: Select the *Time Zone* from the drop-down menu.

Daylight Saving: To select *Daylight-Saving* time manually, click the **Enable Daylight-Saving** check box. Next use the drop-down menu to select a *Daylight-Saving Offset* and then enter a start date and an end date for daylight-saving time.

Enable NTP Server: *NTP* is short for *Network Time Protocol*. *NTP* synchronizes computer clock times in a network of computers. Check this box to use a *NTP* server. This will only connect to a server on the Internet, not a local server.

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

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



Status

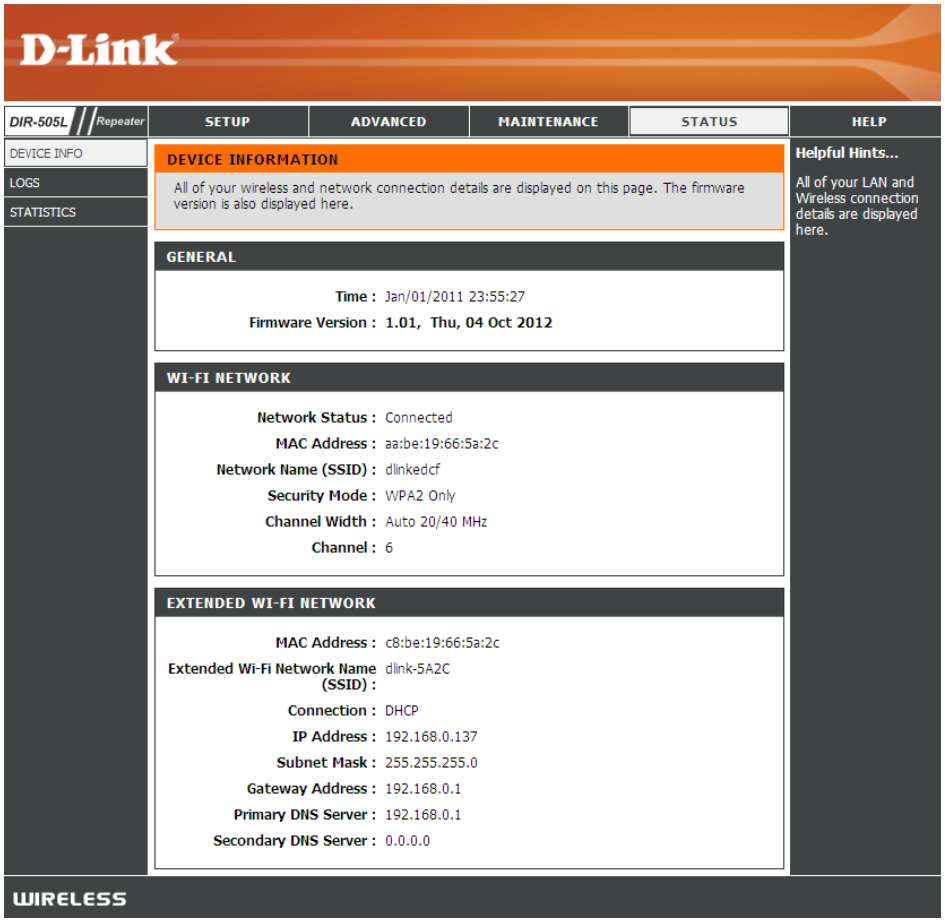
Device Info

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

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

Wi-Fi Network: Displays the MAC address, wireless setting and the private (local) IP settings for the access point.

Extended Wi-Fi Network: Displays the wireless MAC address and your wireless settings such as SSID and Channel.



Logs

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

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

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

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

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

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

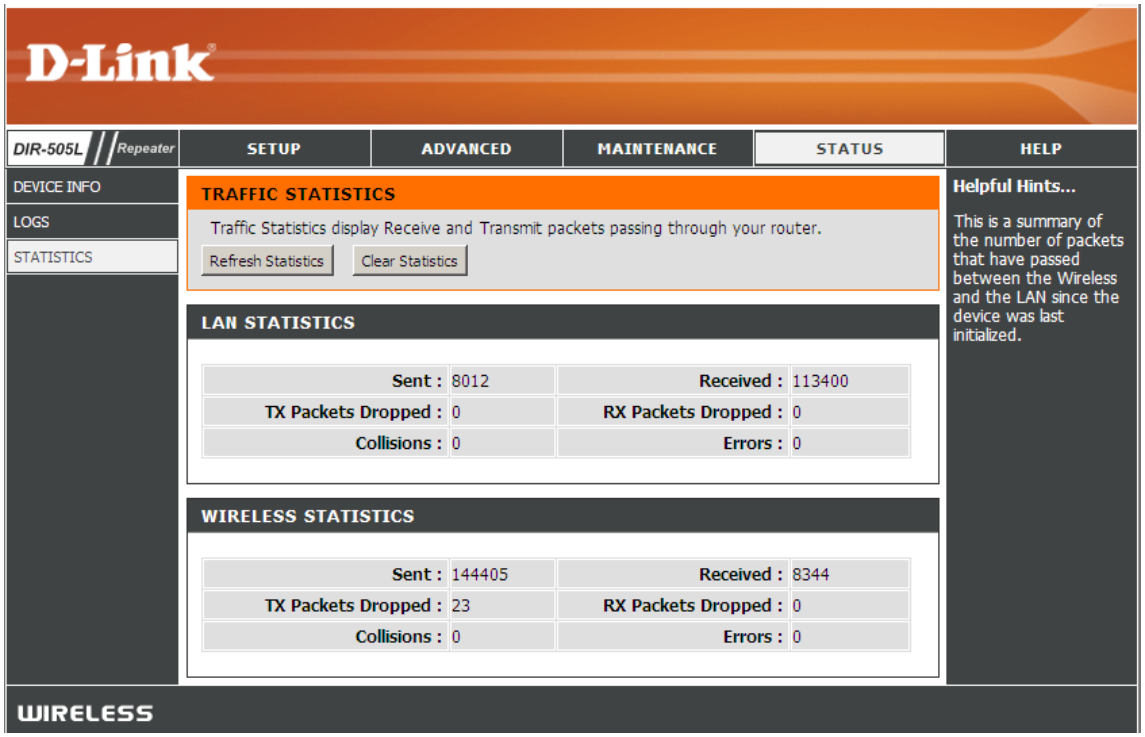
Clear Log: This button clears all current log content.

Log Settings: This button opens a new menu where you can configure the log settings.

Refresh: This button refreshes the log.

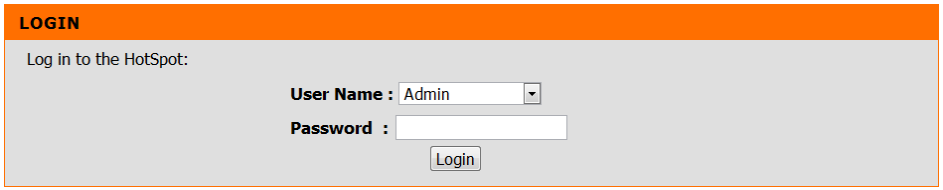
Statistics

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



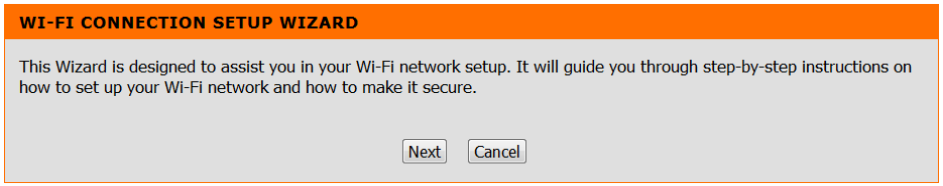
Wi-Fi Hotspot
Quick Setup Wizard

If this is your first time using this device, you will be directed to the *Setup Wizard*. If you have already completed the *Setup Wizard*, please continue to page 123.

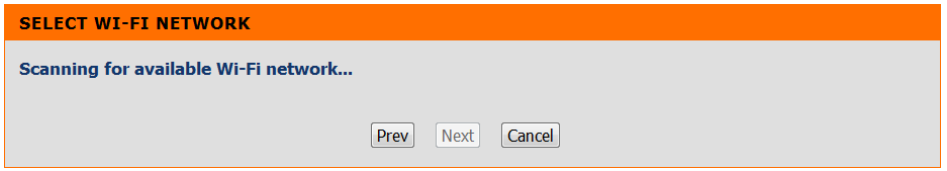


Enter **Admin** in the *User Name* field. Leave the password blank by default.

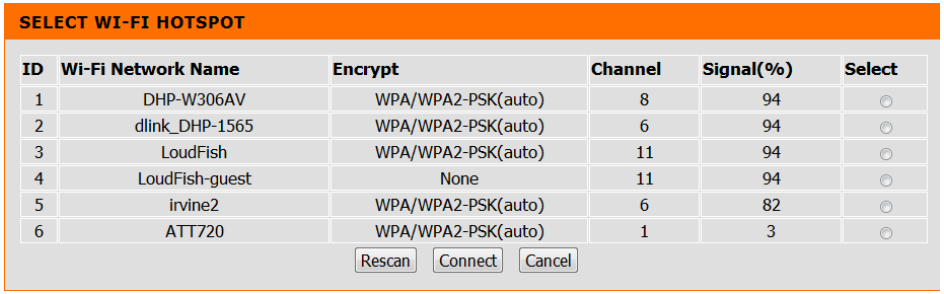
Click **Next** to continue.



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

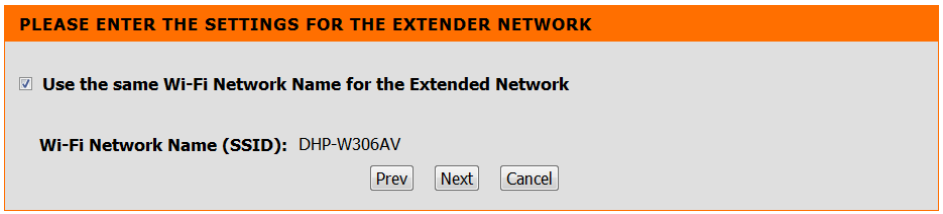


Select the Network you would like your device to connect to and click **Connect**.

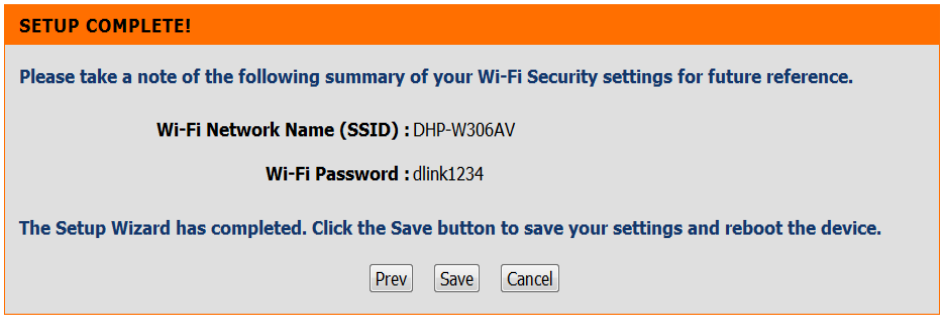


Enter the Wi-Fi password and click **Next** to continue.

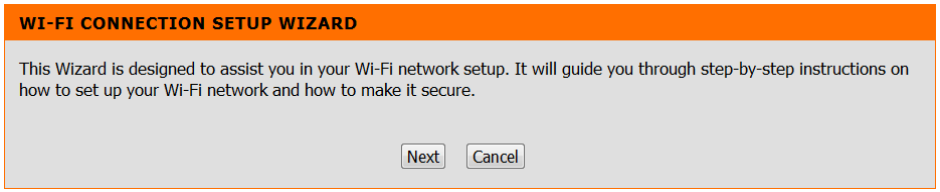
Select **Use the same Wi-Fi Network name for the extended Network** and click **Next**.



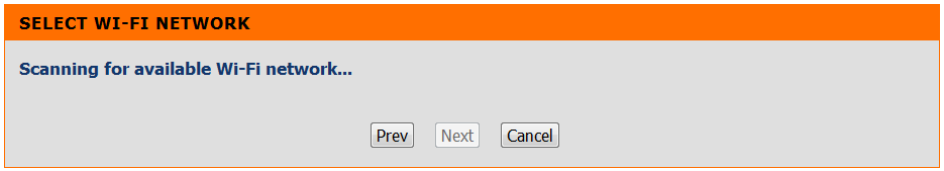
Your setup is now complete. Click **Save** to finish.



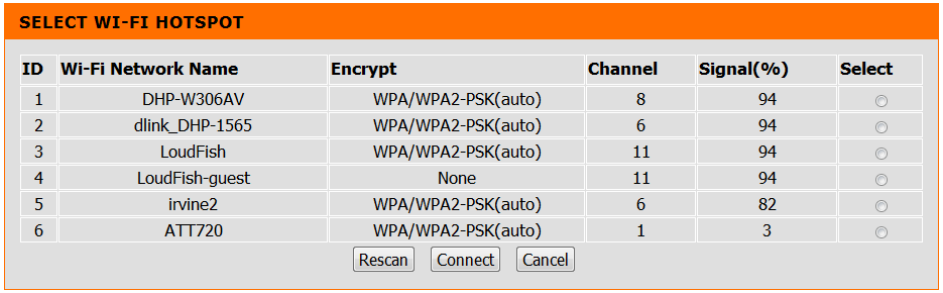
To start the wizard, click **Next** to continue.



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

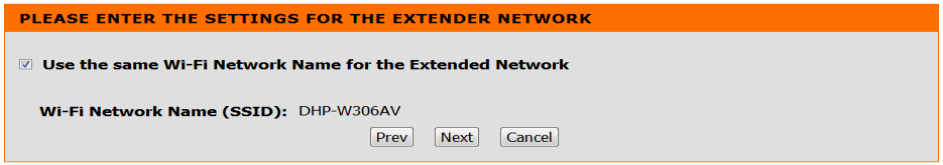


Select the Network you would like your device to connect to and click **Connect**.



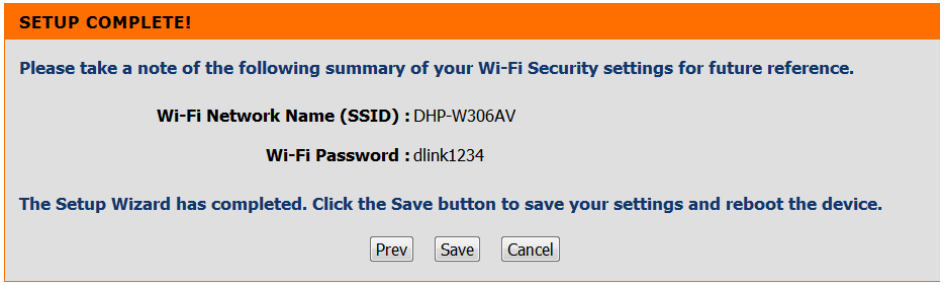
Enter the Wi-Fi password and click **Next** to continue.

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



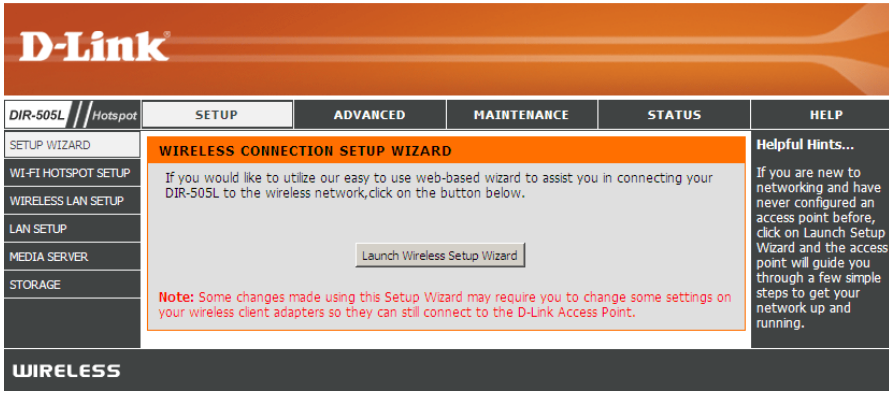
Your setup is now complete. Click **Save** to finish.

Note: To further configure your DIR-505L, go to page 124.



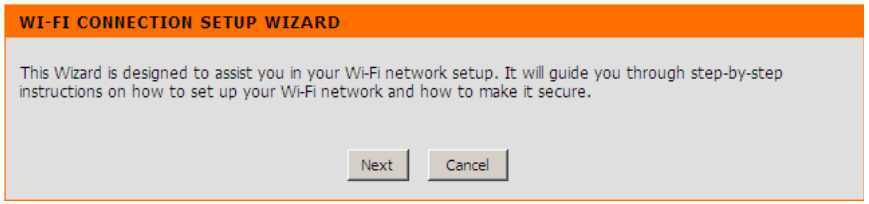
Setup Wizard

If you already configured your DIR-505L during the **Quick Setup Wizard**, skip to page 124. If you previously logged on to the router and you would like to make further configurations, follow the steps below.



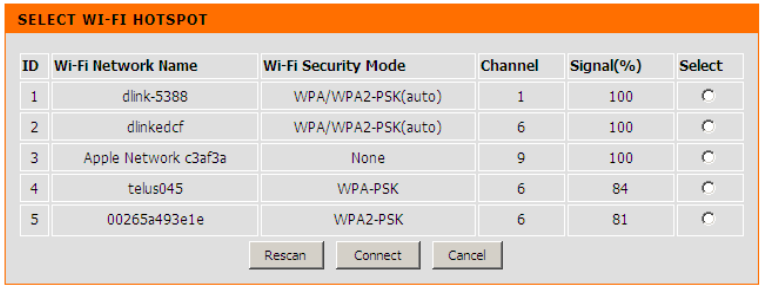
Click **Launch Wireless Setup Wizard** to begin the *Setup Wizard*.

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

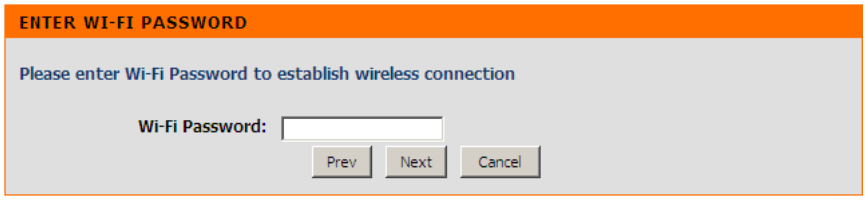


Select the Network you would like your device to connect to and click **Connect**.

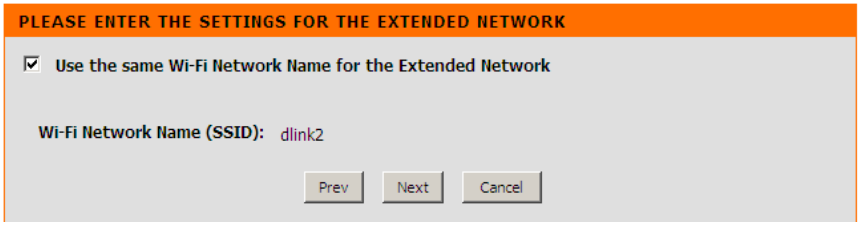
Click **Next** to continue.



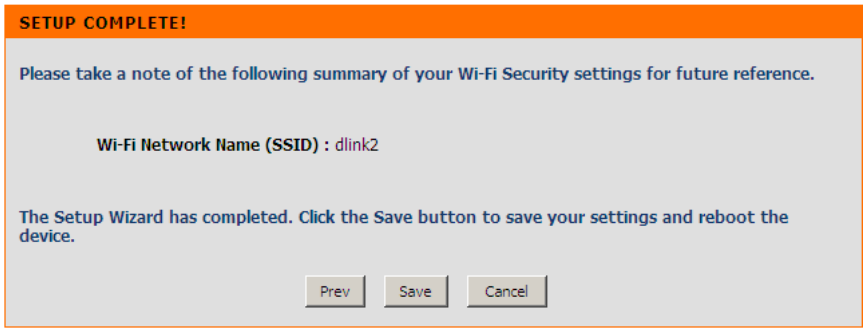
Press down the **WPS** button on the Wireless device you are adding to your wireless network.



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



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



Setup

Wi-Fi Hotspot Setup

Wireless Mode: Displays the *Wi-Fi Hotspot Mode*.

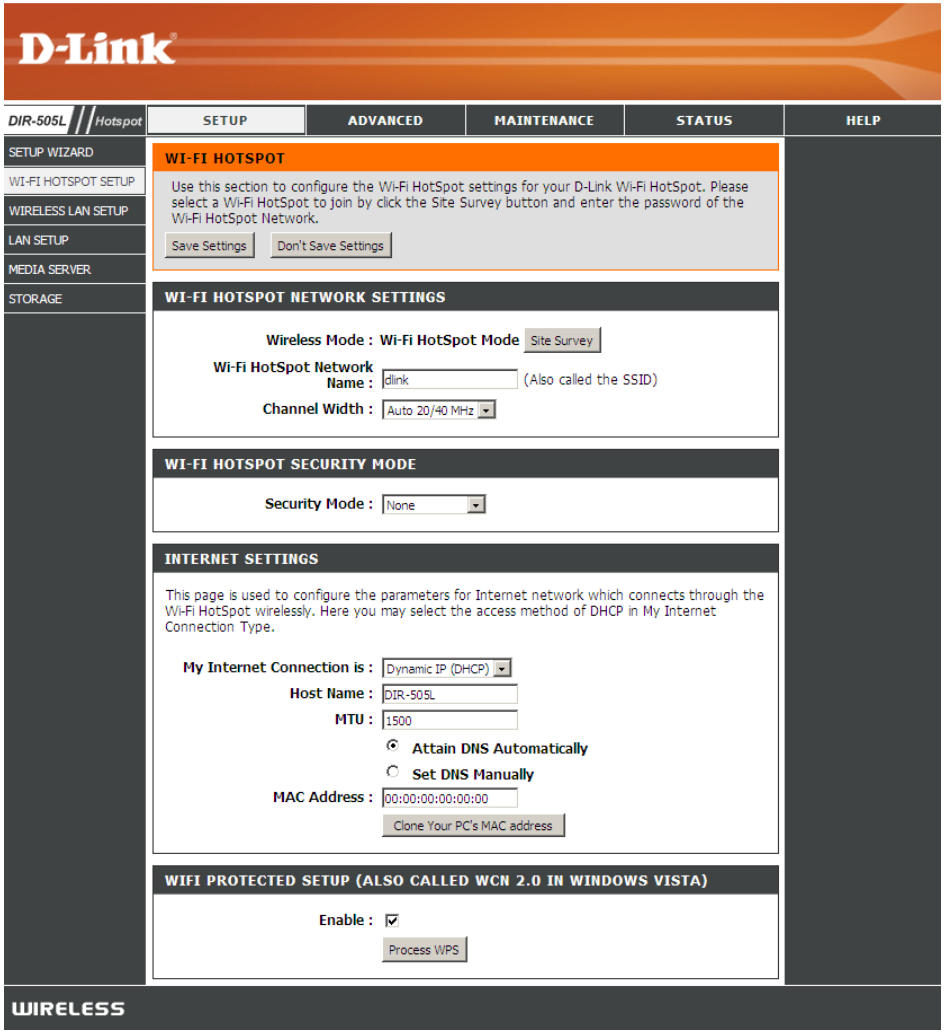
Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless *Visibility Status* is set to **Invisible**, see below). This name is also referred to as the SSID.

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

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

Wi-Fi Protected Setup: Select to enable this feature.

Process WPS: Please refer to page 141.



Internet Settings

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

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

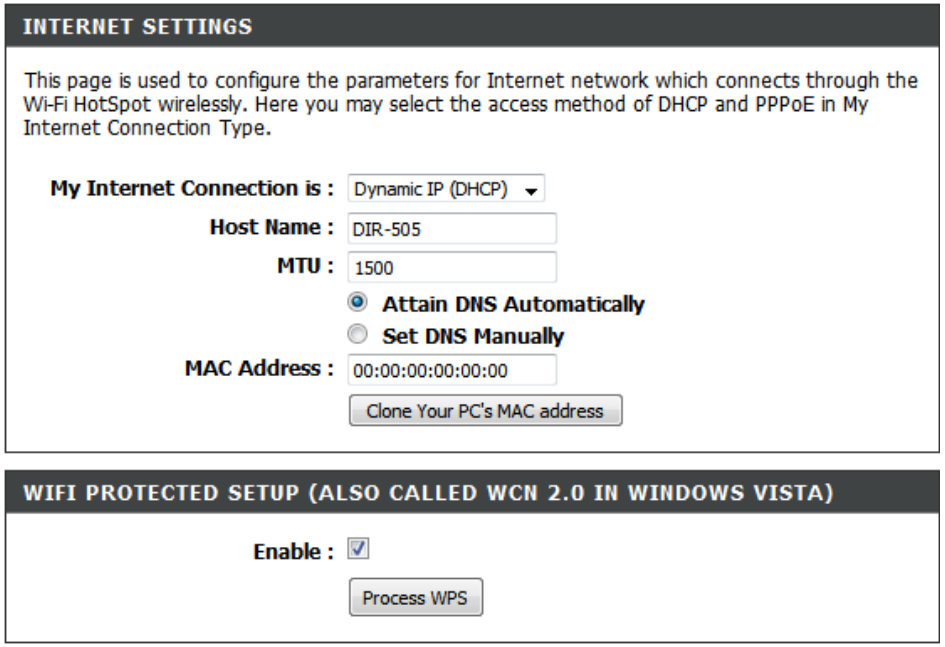
Host Name: The Host Name is optional but may be required by some ISPs. Leave blank if you are not sure.

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

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

Wi-Fi Protected Setup: Select to enable this feature.

Process WPS: Refer to page 141 for more information.



Manual Wireless Settings

Local Wi-Fi Network Name: Select **Same as Wi-Fi Hotspot Network Name** or **Create Extended SSID**.

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

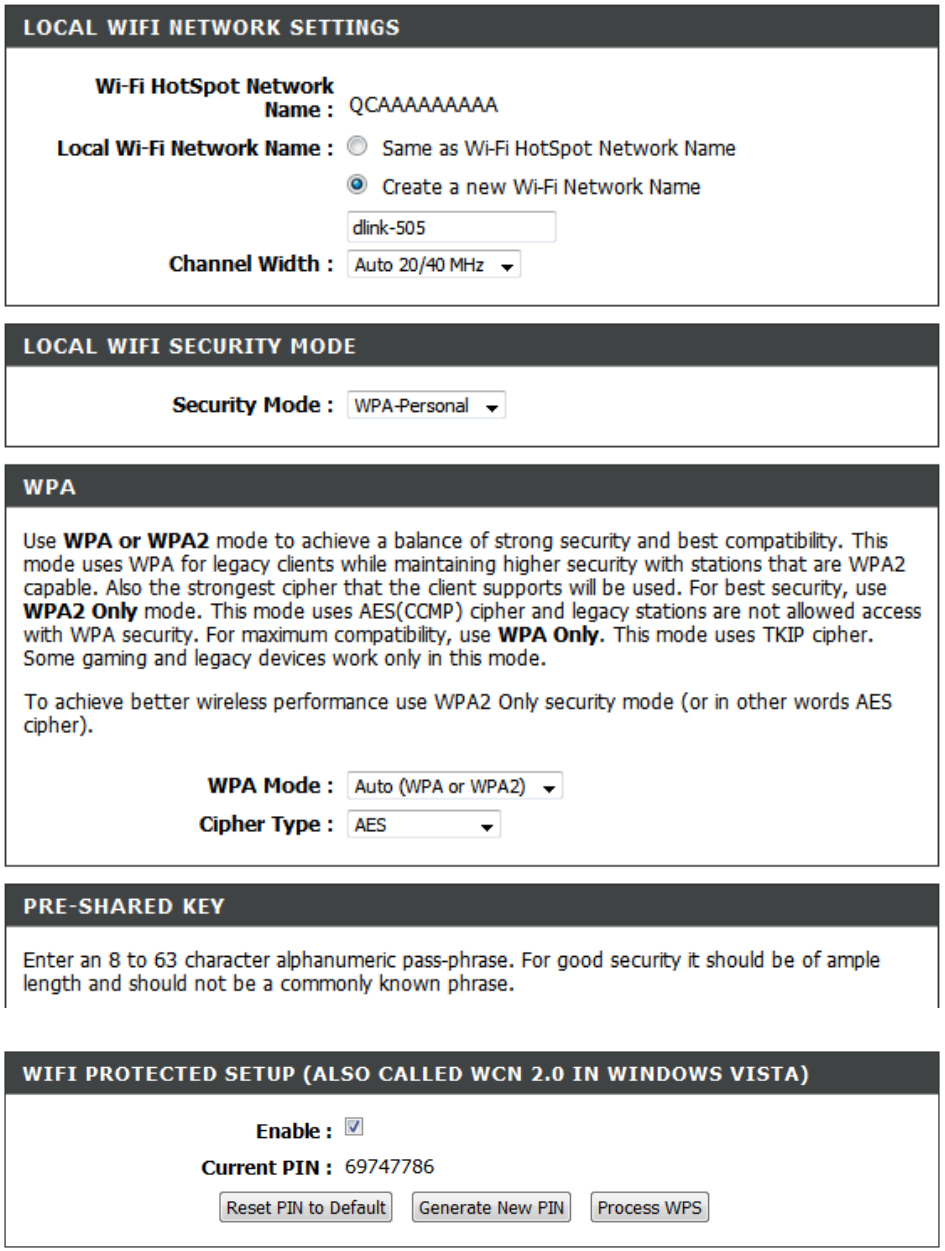
Security Mode: Select from the drop-down menu the type of security mode you would like to use.

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

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

Pre-Shared Key: Enter a key (passphrase). The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.

Wi-Fi Protected Setup: Select to enable this feature.



Setup

Wireless LAN Setup

Wi-Fi Spot Network Name: Displays the *Wi-Fi Hotspot Network Name.*

Local Wi-Fi Network Name: Select **Same as Wi-Fi HotSpot Network Name** or select **Create a new Wi-Fi Network Name**.

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

Visibility Status: This feature allows you to secure your network by giving you the option to make your network invisible to wireless clients. Select **Visible** or **Invisible.**

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

Enable Wireless: Check the box to enable the wireless function. If you do not want to use wireless, uncheck the box to disable all the wireless functions.

Process WPS: Please refer to page 141.

Manual Wireless Settings

Local Wi-Fi Network Name: Select **Same as Wi-Fi HotSpot Network Name** or **Create Extended SSID**.

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

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

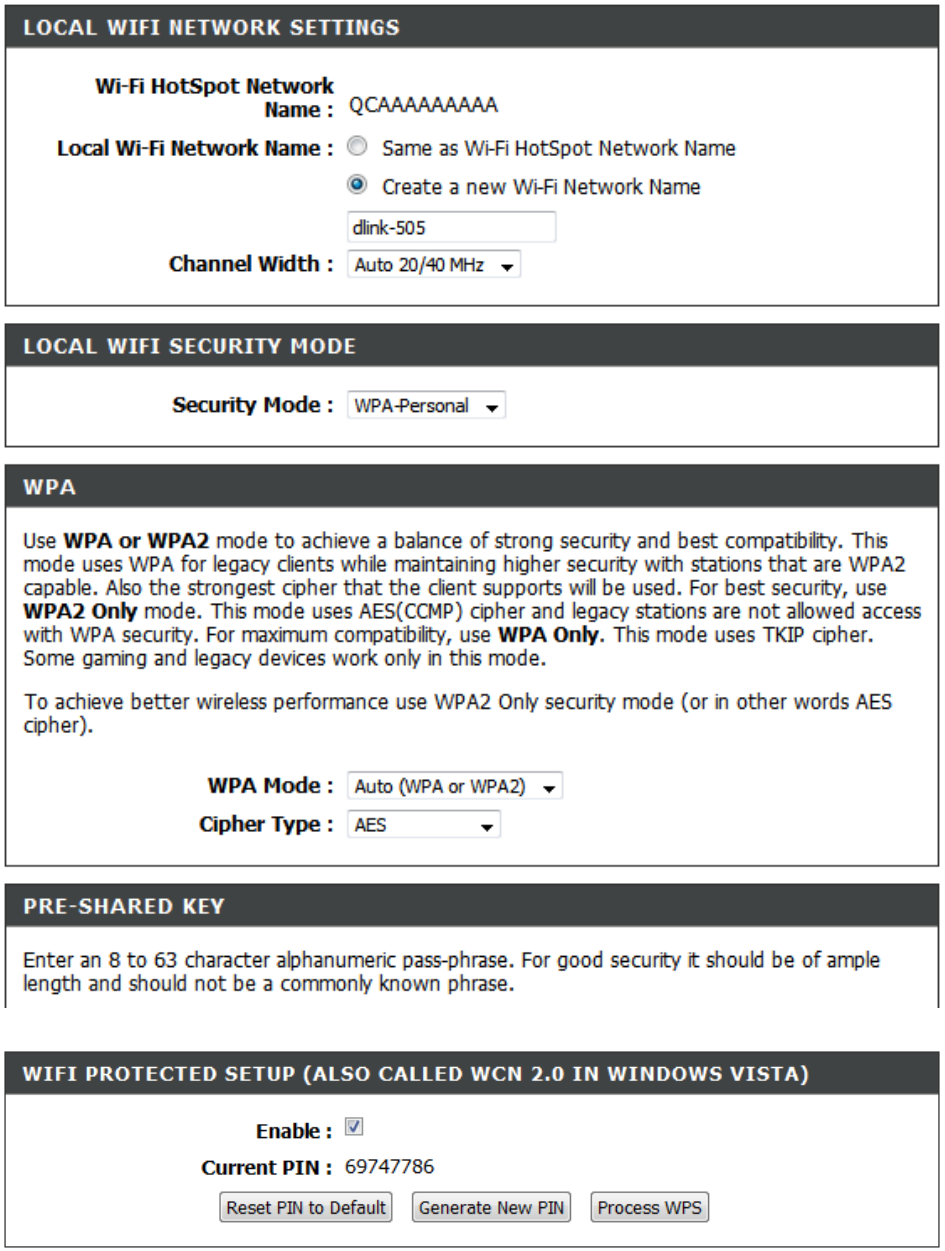
WPA Mode: Select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

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

Pre-Shared Key: Enter a key (passphrase). The key is entered as a passphrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.

Wi-Fi Protected Setup: Select to enable this feature.

Process WPS: Please refer to page 141.



LAN Setup

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

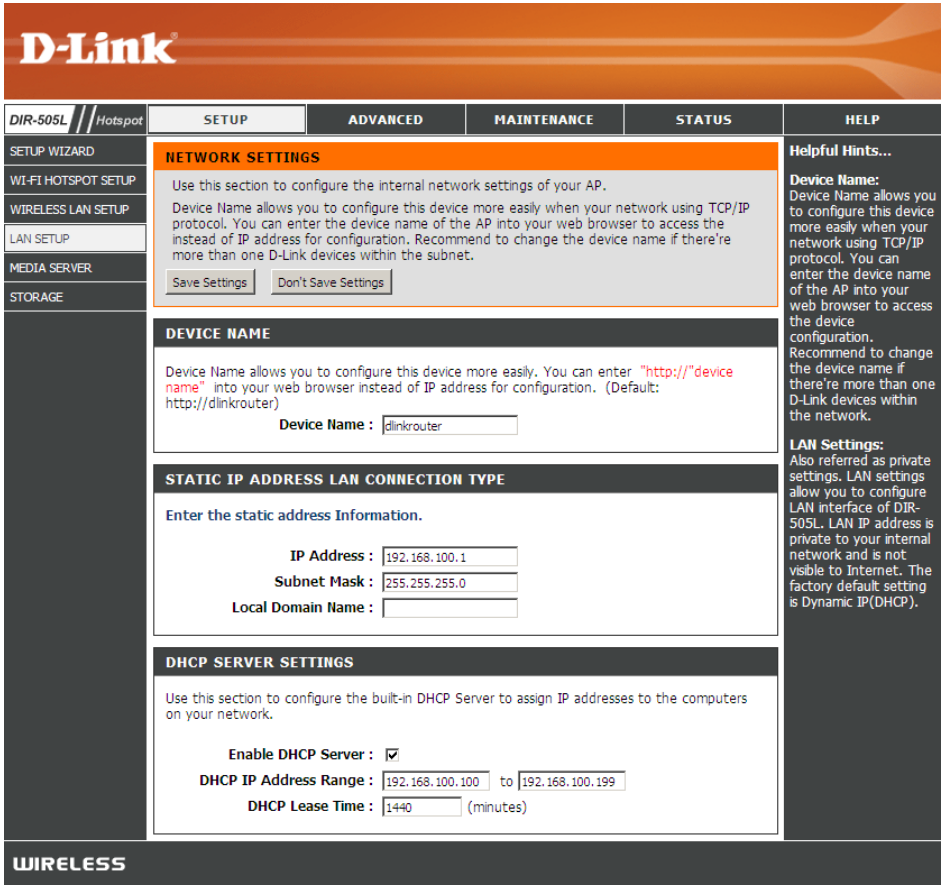
Device Name: Enter the Device Name of the AP. It is recommended to change the Device Name if there is more than one D-Link device within the subnet.

IP Address: Enter the IP address of the access point. The default IP address is **192.168.0.1**. If you change the IP address, once you click **Save**, you will need to enter the new IP address in your browser to get back into the configuration utility.

Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Local Domain Name: Enter the local domain Name.

DHCP Server Settings: Configure the built-in DHCP server to assign IP addresses to the computer on your network.

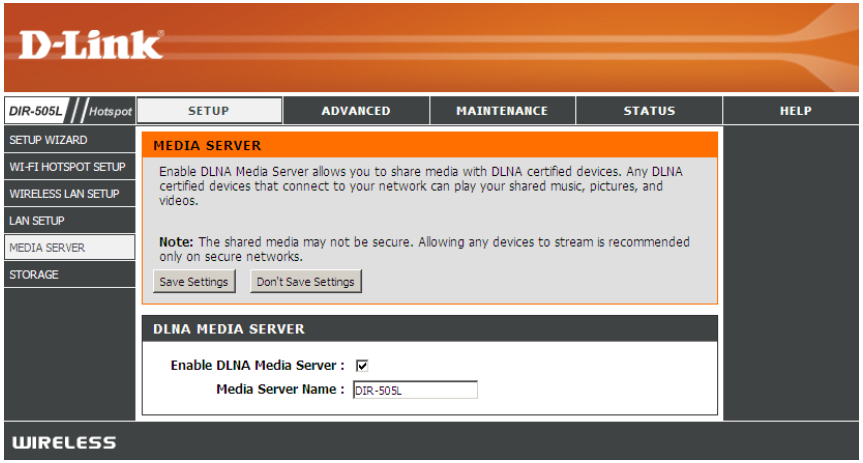


Media Server

This feature allows you to share music, pictures, and videos with any devices connected to your network.

Enable Media Server: Check this box to enable the *Media Server* feature.

Computer Name: Enter the *Media Server's* name.



Storage

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

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

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

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

Allow Remote Access: Check to enable access to your router's storage. ***Note:*** *You will have to type* ***HTTPS*** *in the URL, like in the above example.*

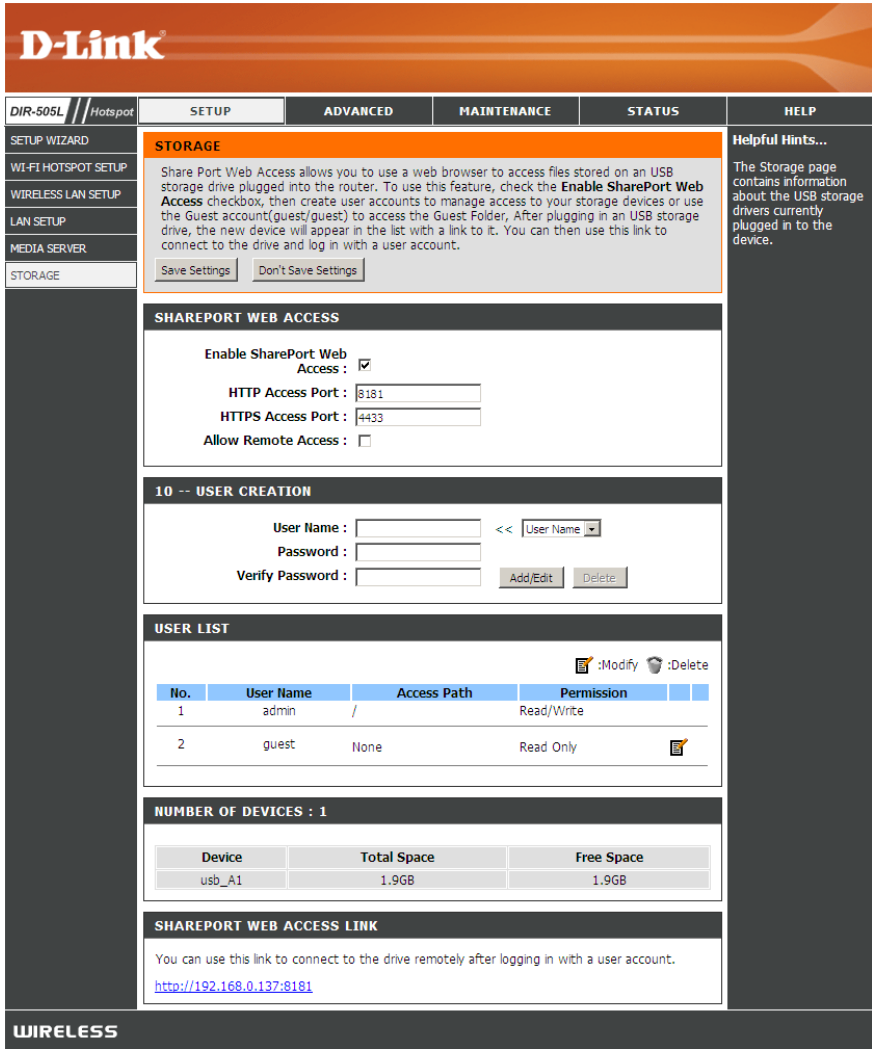
User Name: To create a new user, enter a user name.

Password: Enter a password for this account.

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

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

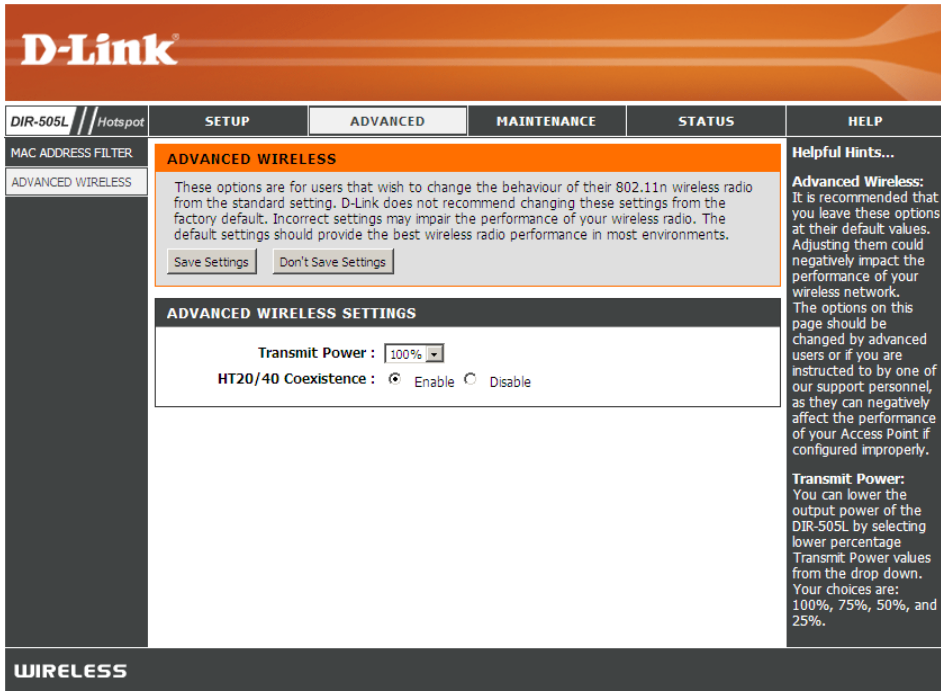
Number of Devices: Displays the USB device plugged into the router.



Advanced Wireless

Transmit Power: To set the transmit power of the antennas select from the drop-down menu.

HT 20/40 Coexistence: You may choose to **Enable** or **Disable** this feature. Enabling this feature allows two “channels” or paths on which data can travel to be combined to increase performance in some environments.



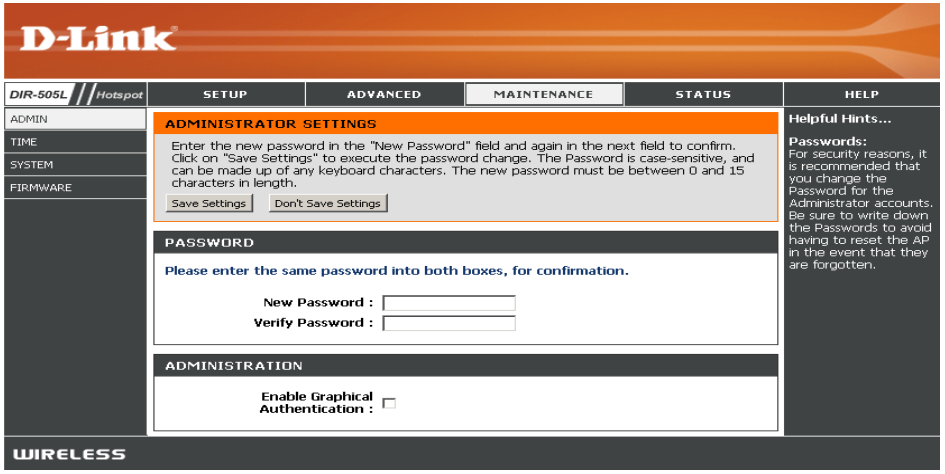
Maintenance
Admin

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

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

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

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



Time

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

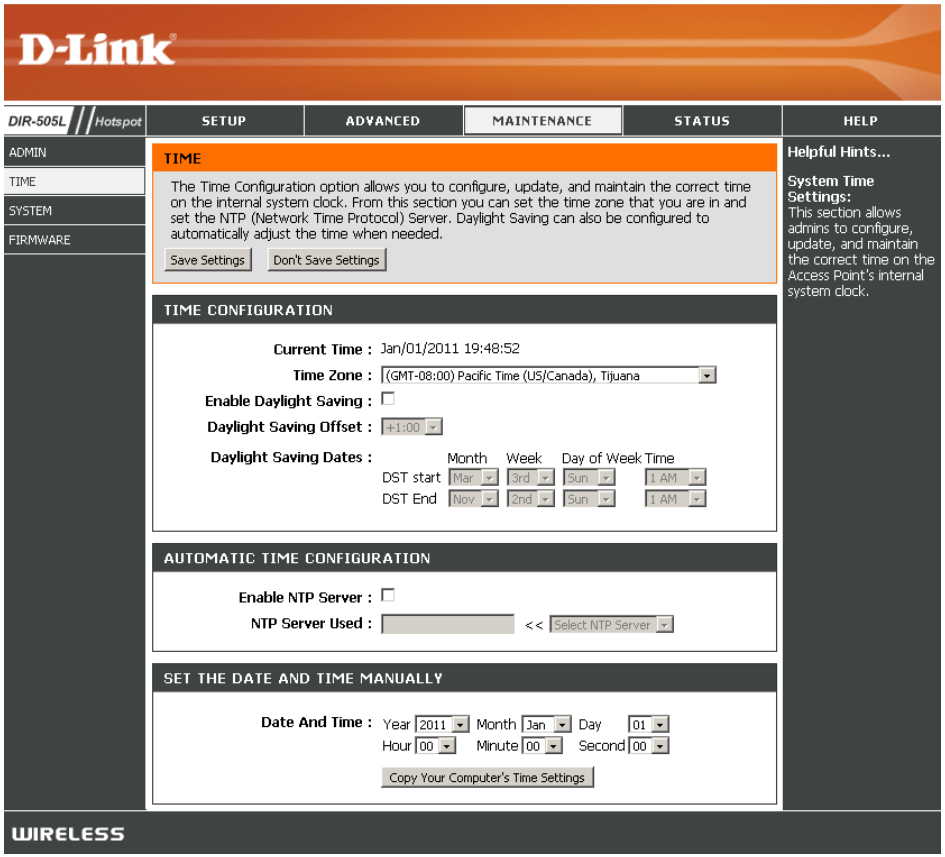
Time Zone: Select the *Time Zone* from the drop-down menu.

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.

Enable NTP Server: *NTP* is short for *Network Time Protocol*. *NTP* synchronizes computer clock times in a network of computers. Check this box to use a *NTP* server. This will only connect to a server on the Internet, not a local server.

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

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



System

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

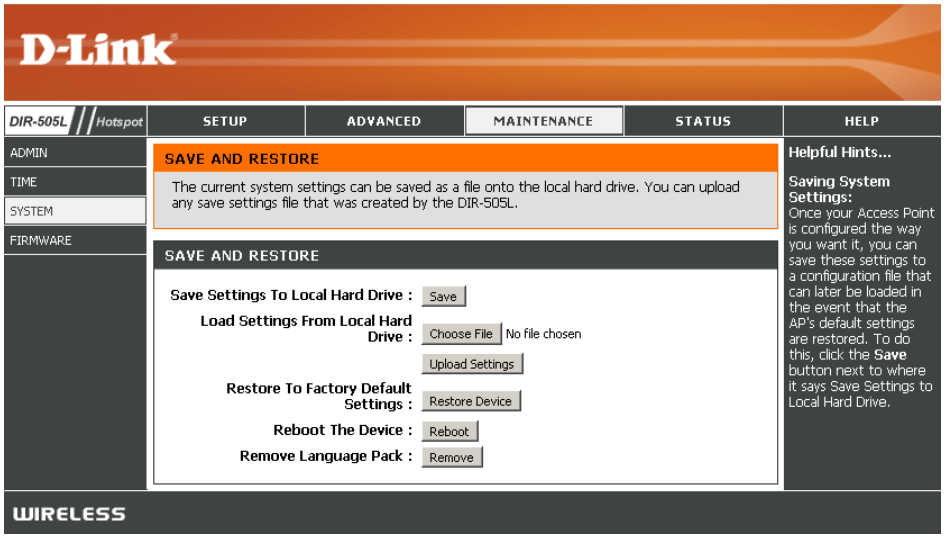
Upload from Local Hard Drive: Use this option to load previously saved access point configuration settings. Click **Browse** to find a previously saved configuration file. Then, click the **Upload Settings** button to transfer those settings to the access point.

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

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

Reboot the Device: Click to reboot the access point.

Remove Language Pack Click to remove any installed language packs.



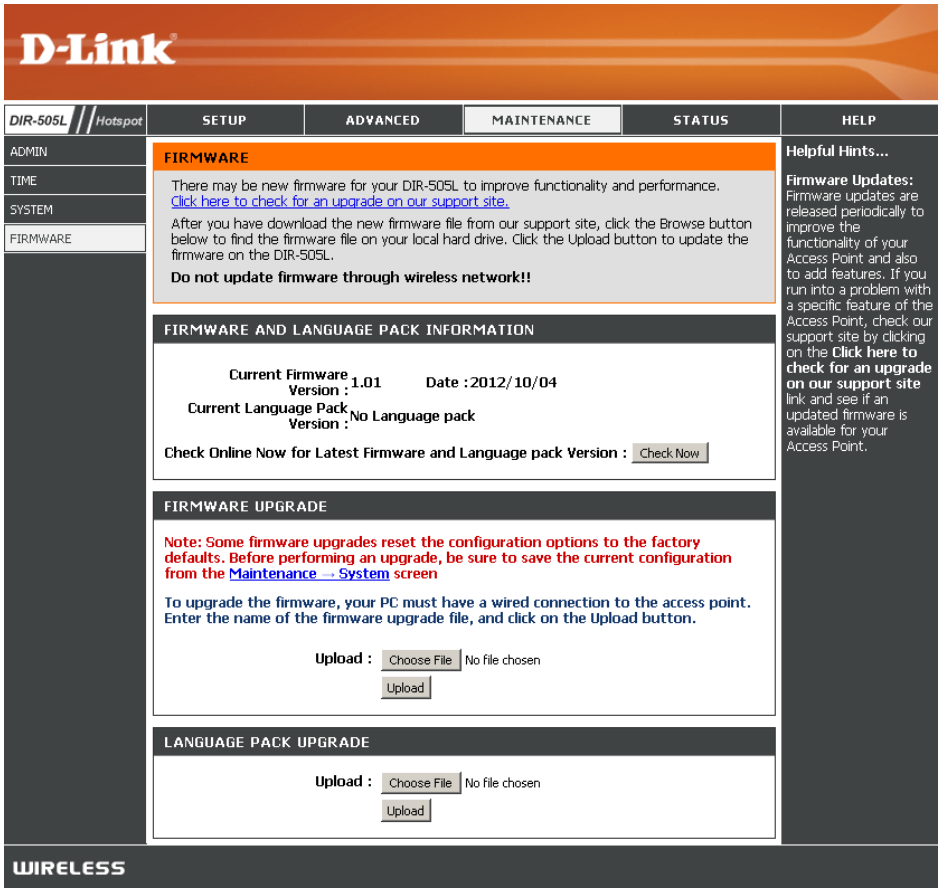
Firmware

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

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

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

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



Language Pack

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

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

Status

Device Info

This page displays the current information for the DIR-505L. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

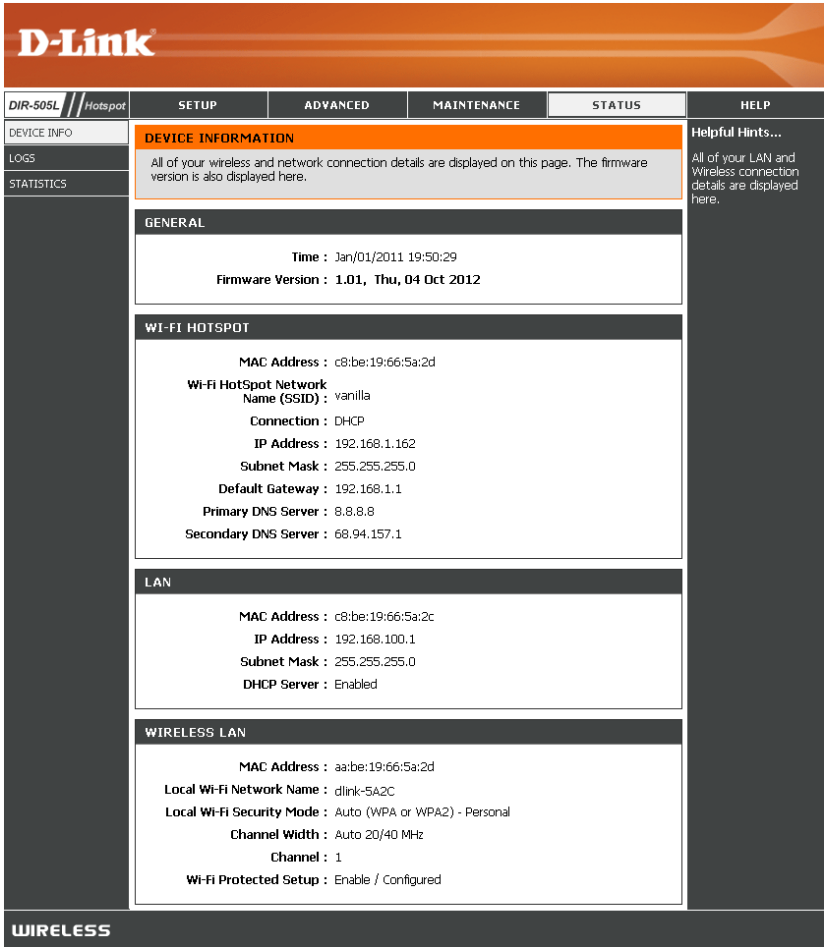
If your Internet connection is set up for PPPoE, a **Connect** button and a **Disconnect** button will be displayed. Use **Disconnect** to drop the PPPoE connection and use **Connect** to establish the PPPoE connection.

General: Displays the router's time and firmware version.

WAN: Displays the MAC address and the public IP settings for the router.

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

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



Logs

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

Log Type: Use the radio buttons to select the types of messages that you want to display from the log. **System Activity**, **Debug Information**, **Attacks**, **Dropped Packets**, and **Notice** messages can be selected.

Log Details: Use this section to view and manage the router's log entries.

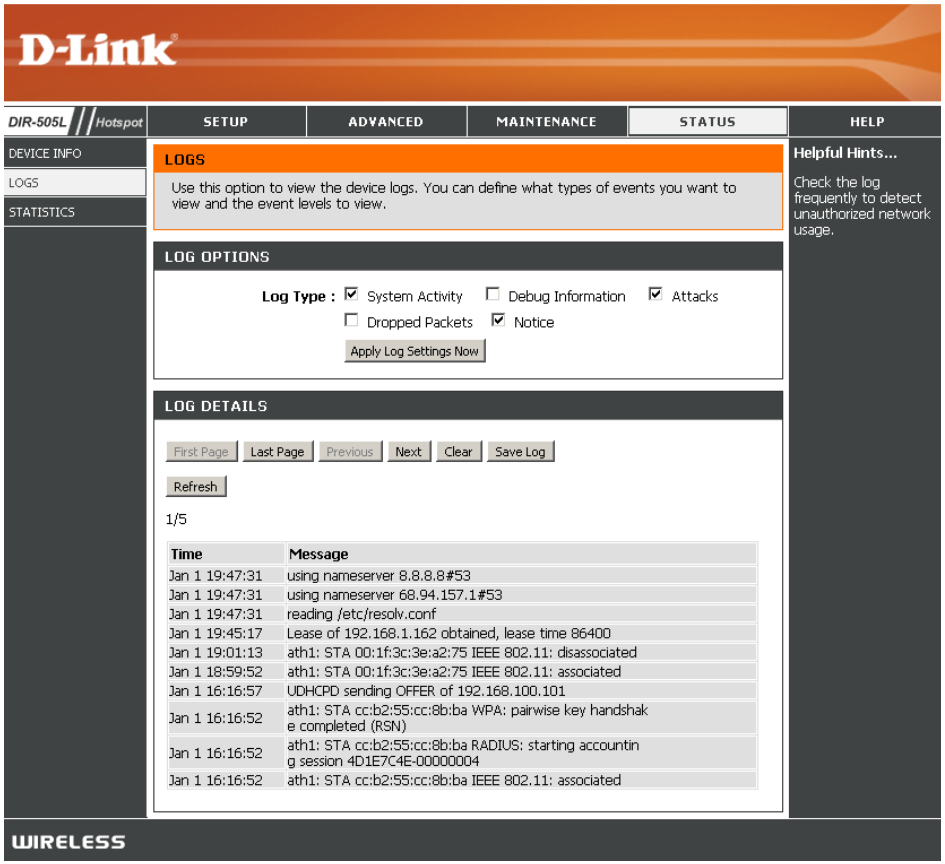
First Page: Click this button to view the first page of the router logs.

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

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

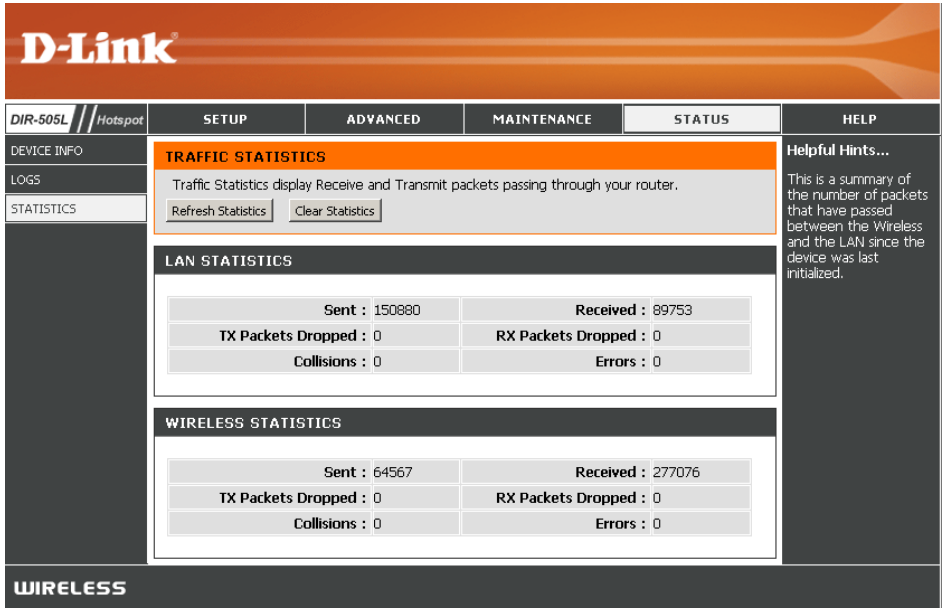
Next: Click this button to view the next page of the router logs.

Clear: Clears all of the log contents.



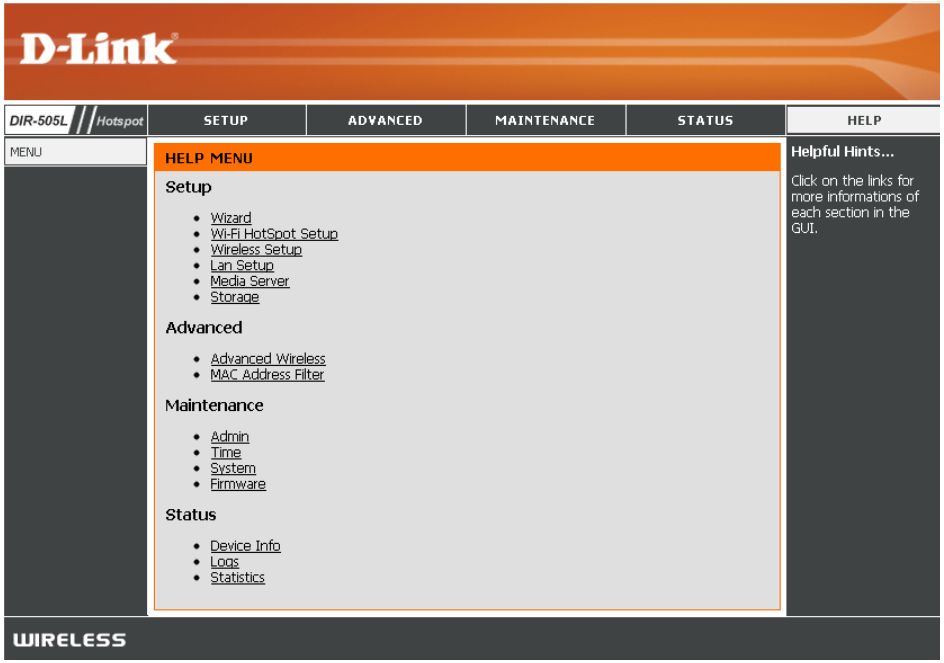
Statistics

The DIP-505L 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.



Help

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



Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is through *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-505L 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-505L for about one second. The *WPS* button will start to blink.

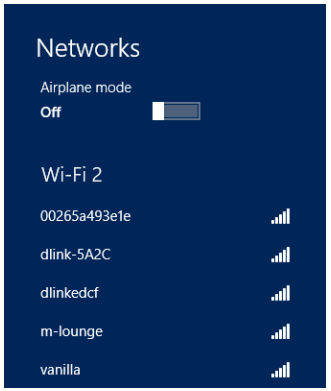
Step 2 - Within two minutes, press the **WPS** button on your wireless client (or launch the software utility and start the *WPS* process).

Step 3 - Allow up to one minute to configure. Once the *WPS* light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

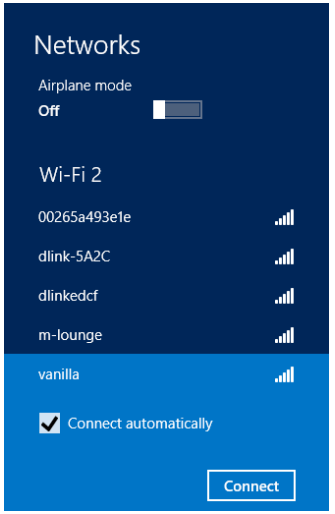
Windows® 8

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

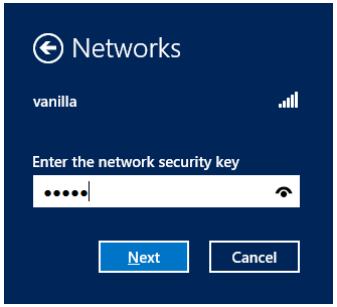
2. A list of available wireless networks will appear.



3. Click the wireless network (SSID) you want to connect to and then click **Connect**.



4. If the network is secure/encrypted, enter the Wi-Fi password (security key) and click **Next**.



5. Click either to enable or disable file sharing.

6. You will now be connected to your wireless network.

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

Windows® 7
WPA/WPA2

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

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

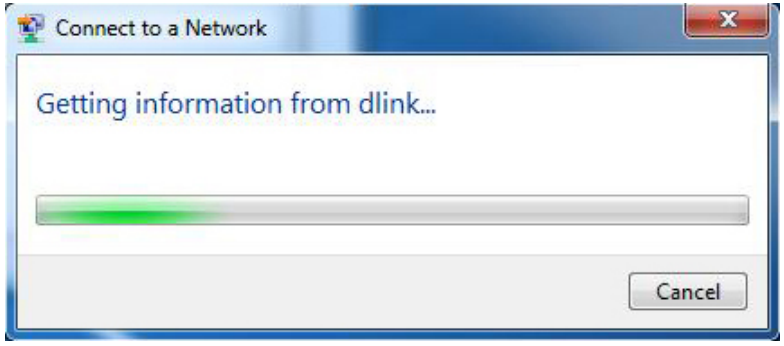
Wireless Icon

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

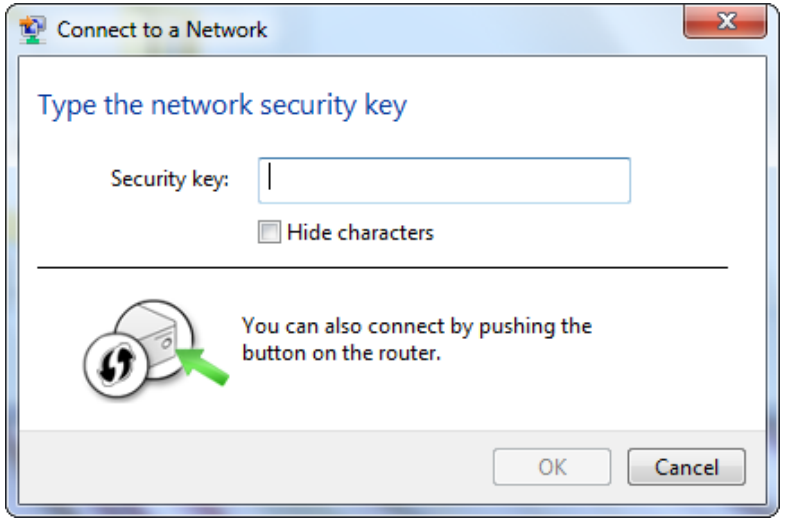
3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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

4. The following window appears while your computer tries to connect to the router.



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

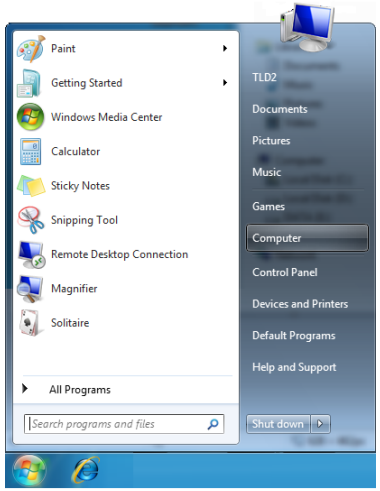


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

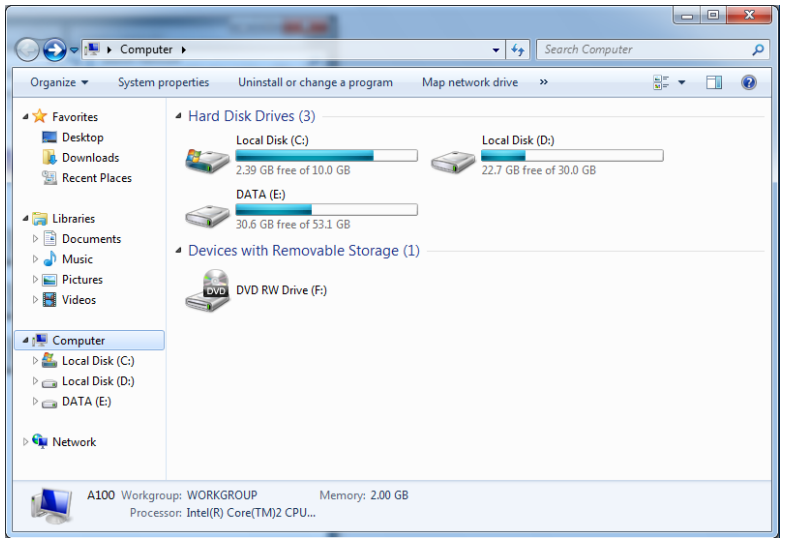
WPS

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

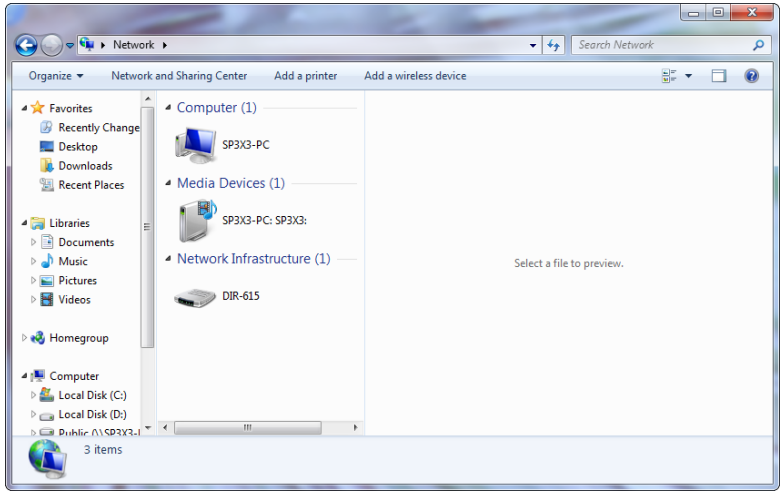
1. Click the **Start** button and select **Computer** from the Start menu.



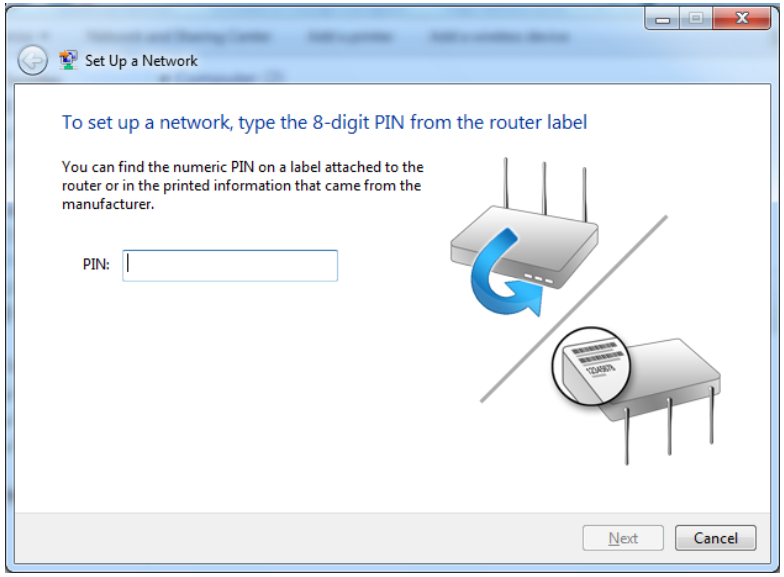
2. Click **Network** on the left side.



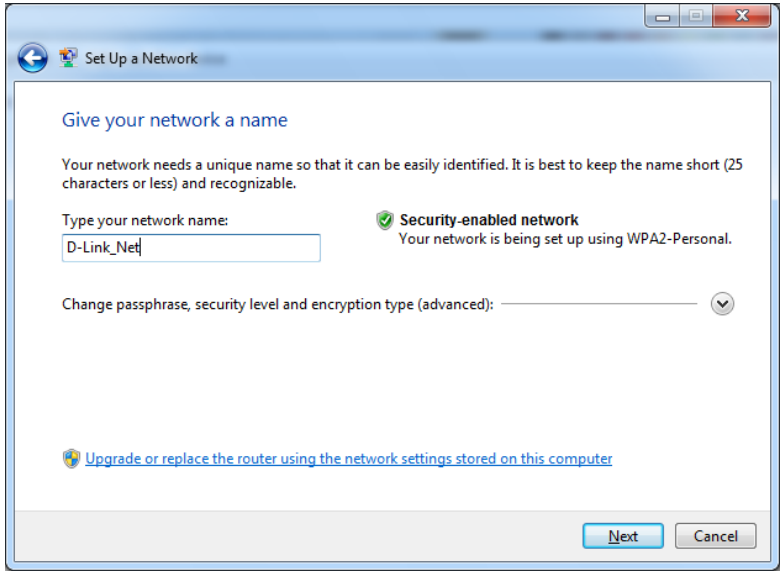
3. Double-click the **DIR-505L**.



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

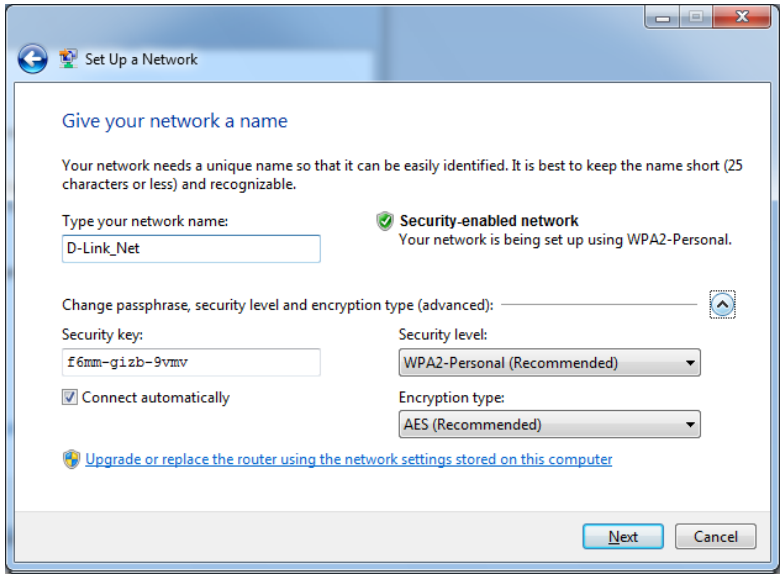


5. Type a name to identify the network.



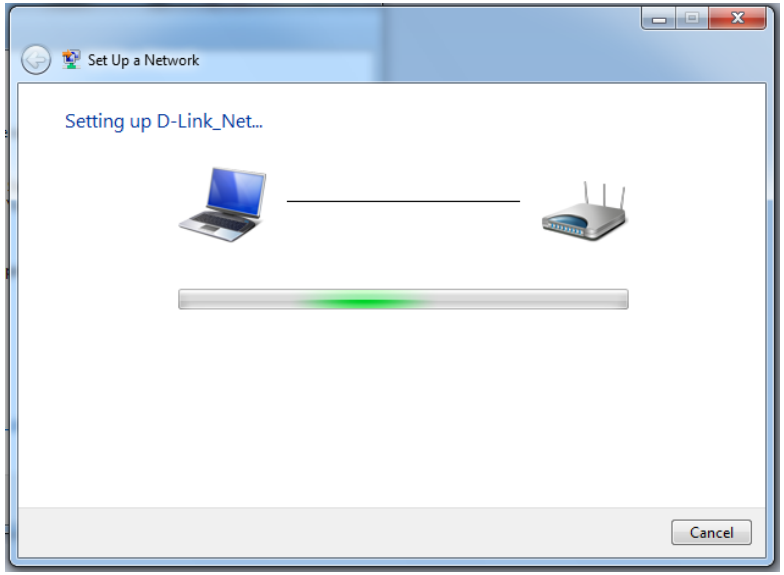
6. To configure advanced settings, click the icon.

Click **Next** to continue.



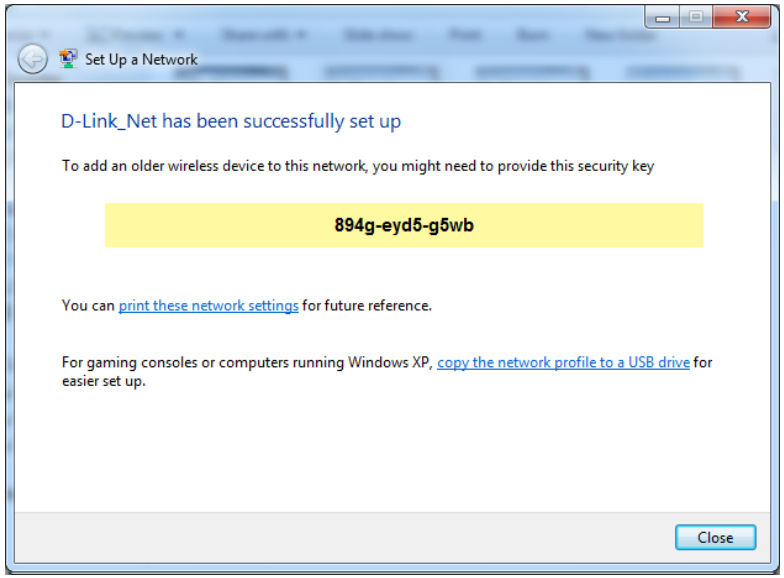
7. The following window appears while the router is being configured.

   Wait for the configuration to complete.



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

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



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

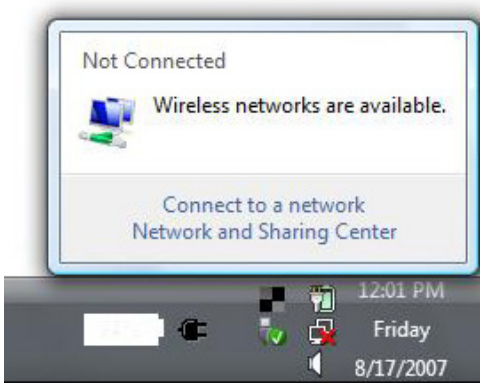
Windows Vista®

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

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

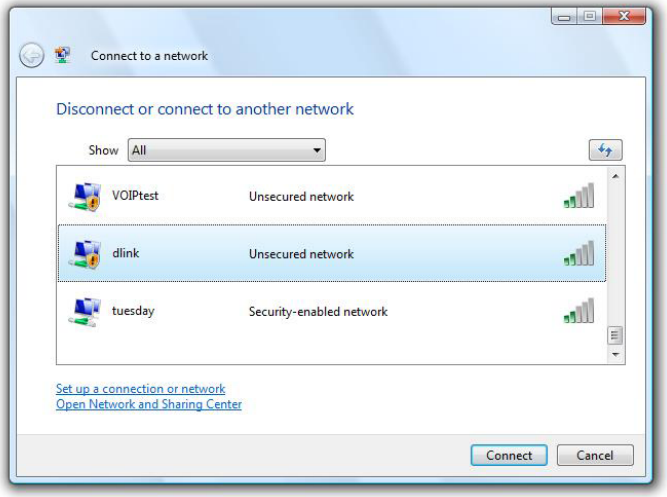
or

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



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

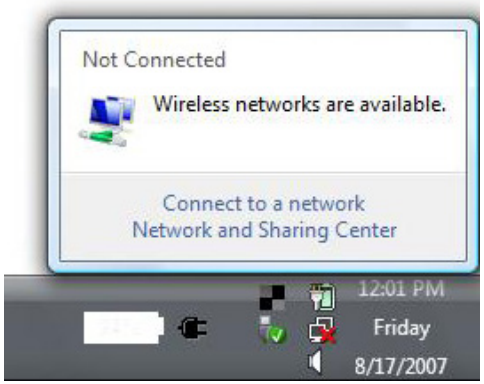
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the *Networking Basics* section in this manual for more information.



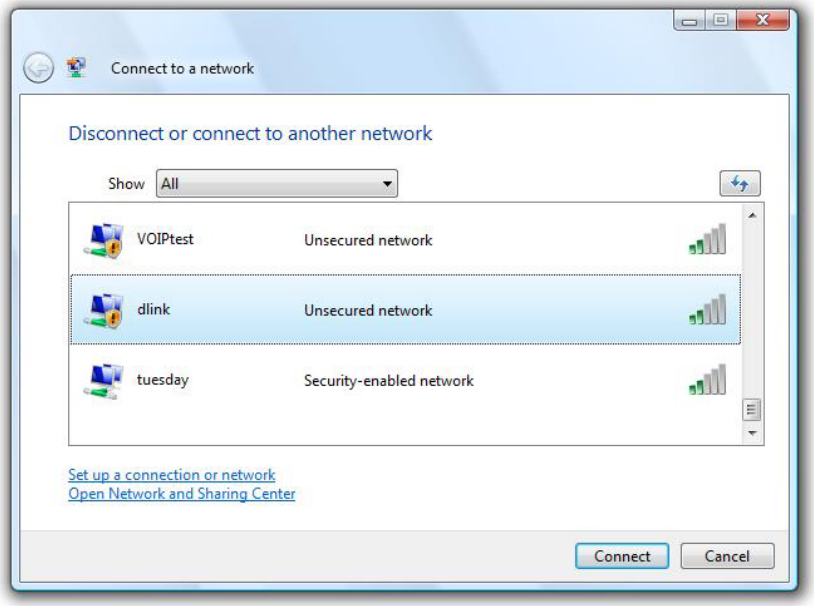
WPA/WPA2

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

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



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



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

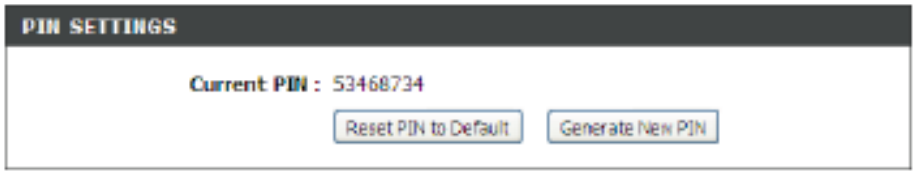
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

WPS/WCN 2.0

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

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

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

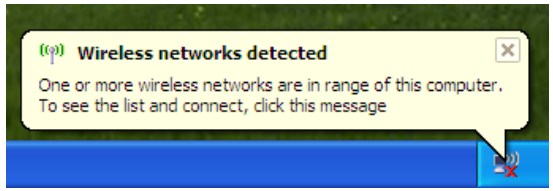


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Windows® XP

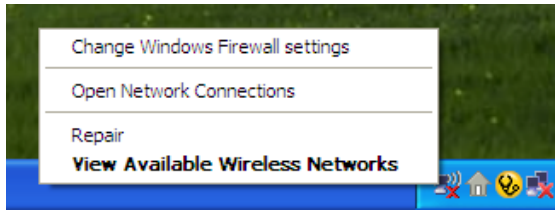
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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

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



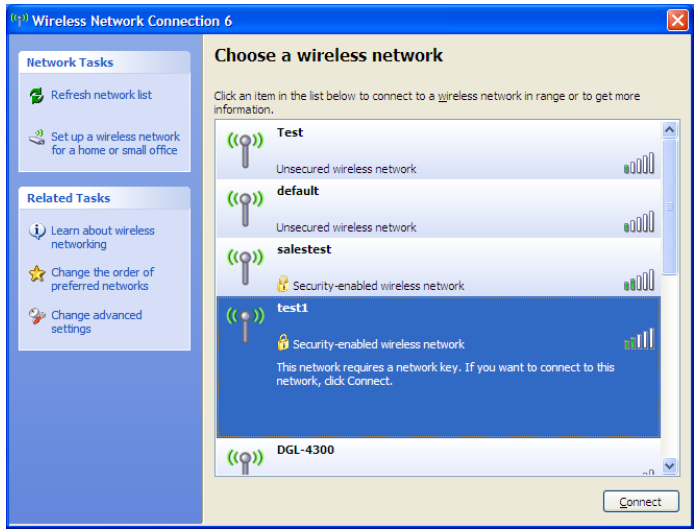
or

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



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

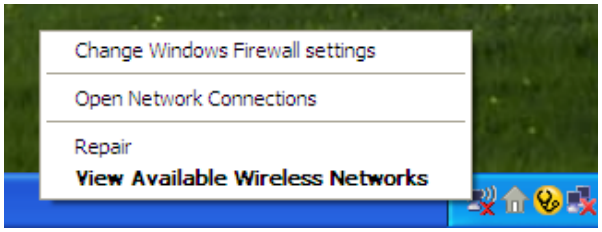
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the *Networking Basics* section in this manual for more information.



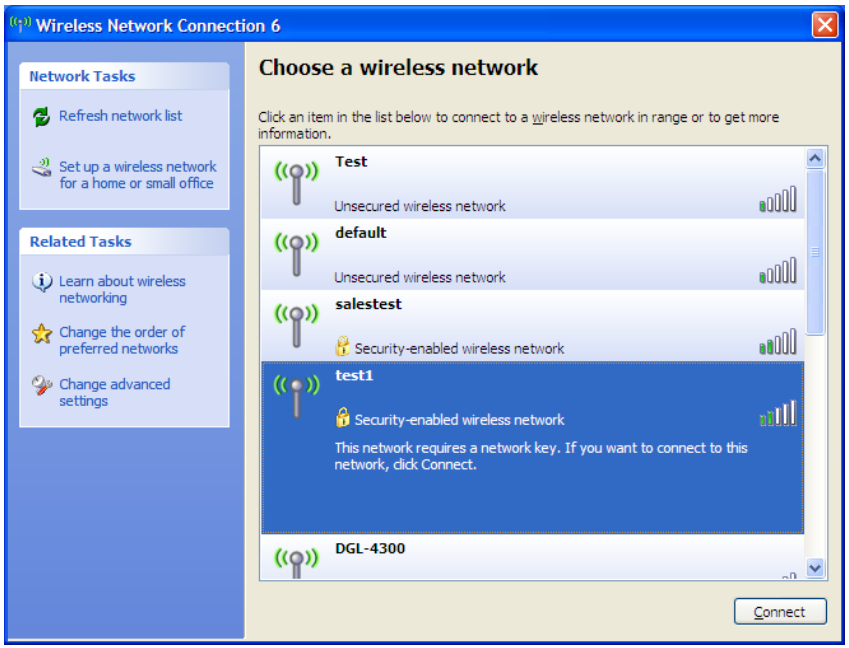
WPA/WPA2

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

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

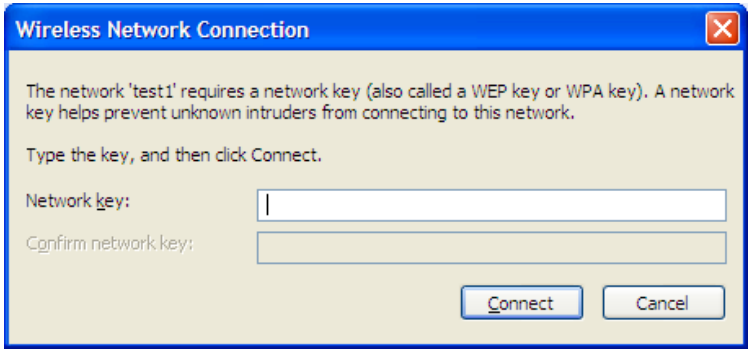


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The *Wireless Network Connection* box will appear. Enter the WPA-PSK passphrase and click **Connect**.

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-505L. 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:

    - Internet Explorer® 7 or higher
    - Firefox 9 or higher
    - Safari 5 or higher
    - Google Chrome 16 or higher

- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
    - Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** icon. From the *Security* tab, click the button to restore the settings to their defaults.
    - Click the *Connection* tab and set the dial-up option to **Never Dial a Connection**. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
    - Go to the *Advanced* tab and click the button to restore these settings to their defaults. Click **OK** three times.
    - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your 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 user name is **admin** and leave the password box empty.

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

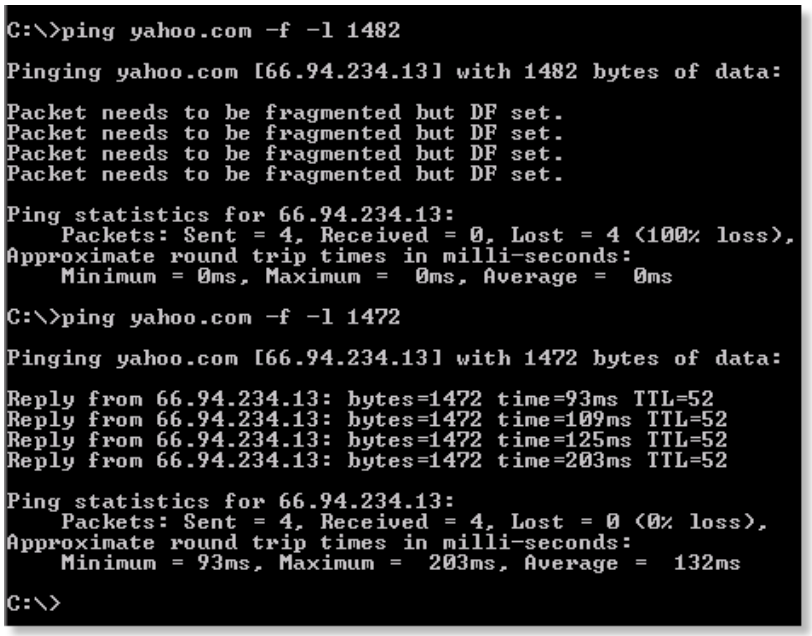
If you are having a problem sending or receiving e-mail, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

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**



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 user name (**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 e-mail. 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 e-mail, 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.

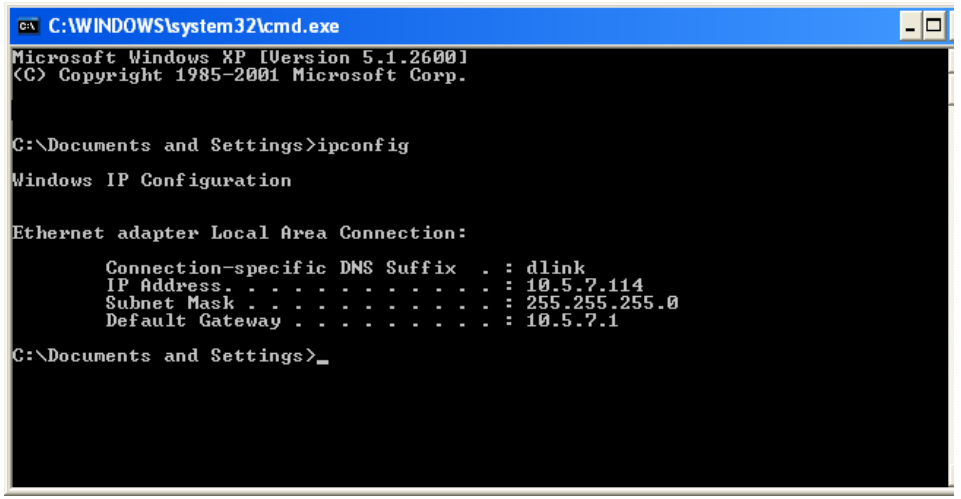
Networking Basics

Check your IP address

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

Windows® XP Users

- Click on **Start** > **Run**. In the run box type **cmd** and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and the default gateway of your adapter.



Windows® 7/Vista® Users

- Click **Start**, type **cmd** in the search box and then click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.

Windows® 8 Users

- Press the **Windows key** and **R** together. Type **cmd** in the box and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and 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.

Statically Assign an IP address

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

Step 1

Windows® 7 - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.

Windows Vista® - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections**.

Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.

Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2

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

Step 3

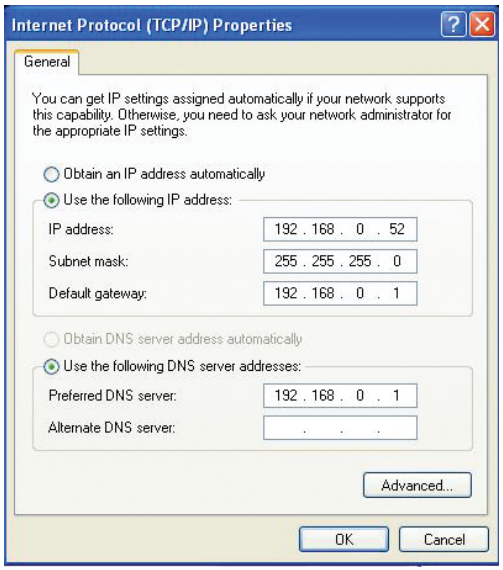
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4

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

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

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



Step 5

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

Windows® 8 Users

- Press the **Windows** key and then type **IP**. Click **Settings** on the right side and then click **View Network Connections**.
- Right-click on the adapter which represents your D-Link wireless network adapter.
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or LAN IP address on your router or network.

  Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.
- Set **Default Gateway** the same as the LAN IP address of your router or gateway.
- Set **Primary DNS** the same as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.

Technical Specifications

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

Wireless Modes
- Router Mode
- Repeater Mode
- Wi-Fi Hotspot Mode
- Access Point (AP) Mode

Wireless Frequency Range
- 2.4 GHz to 2.4835 GHz

Antennas
- Internal Antenna

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

Advanced Features
- SharePort™ Mobile app for iOS
- Quick Router Setup app for iOS
- 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
- DMZ Support

Device Management
- Web UI

Diagnostic LEDs
- Power/WPS

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

Operating Humidity
- 0% to 90% non-condensing

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

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

Weight
- 0.25 lb (113.4 grams)

Warranty
- 1-Year Limited Warranty

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

2 Frequency Range varies depending on country's regulation

Contacting Technical Support

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

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

- Model number of the product (e.g., DIR-505L)
- Hardware Revision (located on the label on the bottom of the router (e.g., rev A1))
- Serial Number (s/n number located on the label on the bottom of the router).

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

For customers within the United States:

Phone Support:
(877) 453-5465

Internet Support:
http://support.dlink.com

For customers within Canada:

Phone Support:
(800) 361-5265

Internet Support:
http://support.dlink.ca

GPL Code Statement

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

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

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

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via e-mail 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:
E-mail: GPLCODE@DLink.com
Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Systems, Inc.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

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

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

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

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

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

Developers that use the GNU GPL protect your rights with two steps:
(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

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

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

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

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

TERMS AND CONDITIONS

0. Definitions.

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

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

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

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

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

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

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

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

1. Source Code.

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

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

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

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

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

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

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

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

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

3. Protecting Users' Legal Rights From Anti-Circumvention Law.
No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

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

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

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

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

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

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

6. Conveying Non-Source Forms.

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

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

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

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

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

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

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

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

7. Additional Terms.

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

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

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

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

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

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

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

8. Termination.

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

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

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

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights

from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

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

10. Automatic Licensing of Downstream Recipients.

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

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

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

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

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

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

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

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

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

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

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

12. No Surrender of Others' Freedom.

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

13. Use with the GNU Affero General Public License.

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

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

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation. If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

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

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

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

17. Interpretation of Sections 15 and 16.

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

Warranty

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

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

Limited Warranty:

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

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

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

Limited Software Warranty:

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

Non-Applicability of Warranty:

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

Submitting A Claim (USA):

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow DLink to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package

to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

Submitting A Claim (Canada):

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

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support at 1-800-361-5265, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.ca/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will

be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

- RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

What Is Not Covered:

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

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

Disclaimer of Other Warranties:

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

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

Limitation of Liability:

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

Governing Law:

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

Trademarks:

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

Copyright Statement:

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

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.

Registration

Register your product online at registration.dlink.com

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

Version 1.0
January 24, 2013