D-Link®

Version 1.0 | November 18, 2013

User Manual

Wireless AC750
Dual Band Router

DIR-803

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	November 18, 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. iPhone, iPad, and iPod touch are registered trademarks of Apple Inc. Android is a trademark of Google, Inc. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2013 by D-Link Systems, Inc.

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

Table of Contents

Preface i
Manual Revisions i
Trademarks i

Product Overview 1
Package Contents 1
System Requirements 2
Introduction 3
Hardware Overview 4
Connections 4
LEDs 5

Installation 6
Before you Begin 6
Wireless Installation Considerations 7
Connect to your Network 8
Connect to an Existing Router 11

Configuration 13
Quick Setup Wizard 14
QRS Mobile App 19
Web-based Configuration Utility 20
Internet Connection Setup 21
Static (assigned by ISP) 22
Dynamic (Cable) 23
PPPoE (DSL) 24
PPTP 25
L2TP 27
DS-Lite 29
Internet Connection Setup Wizard 30
Wireless Settings 35
Wireless Connection Setup Wizard 36
Add Wireless Device with WPS Wizard 38
Manual Wireless Settings 40
802.11n/g (2.4GHz) 40
802.11ac/n/a (5GHz) 41
Wireless Security 42
What is WPA? 42
WPA/WPA2-Personal (PSK) 43
Configure WPA/WPA2-Enterprise (RADIUS) 44
Network Settings 46
Router Settings 46
DHCP Server Settings 47
DHCP Reservation 49
IPv6 50
IPv6 Internet Connection Setup Wizard 52
IPv6 Manual Setup 57
Auto Detection 57
Static IPv6 58
Autoconfiguration 59
PPPoE 60
IPv6 in IPv4 Tunneling 62
6 to 4 Tunneling 63

6rd 64
Local Connectivity 65
Advanced 66
Virtual Server 66
Port Forwarding 67
Application Rules 68
QoS Engine 69
Network (MAC) Filters 71
Inbound Filters 72
Access Control 73
Access Control Wizard 73
Website Filters 76
Firewall Settings 77
Routing 79
Advanced Wireless 80
Wi-Fi Protected Setup (WPS) 81
WPS Button 82
Advanced Network Settings 83
Guest Zone 84
Tools 85
Admin 85
Time 86
SysLog 87
Email Settings 88
System 89
Firmware 90
Language Pack Upgrade 90
Dynamic DNS 91
System Check 93
Schedules 94
Status 95
Device Info 95
Logs 96
Statistics 97
Internet Sessions 98
Wireless 99
Routing 100
IPv6 101
Support 102

Connect a Wireless Client to your Router 103
WPS Button 103
Windows® 8 104
Windows® 7 106
WPA/WPA2 106
WPS 109
Windows Vista® 113
WPA/WPA2 114
WPS/WCN 2.0 116
Windows® XP 117
WPA/WPA2 118

Troubleshooting 120
Reset Router/Forgot Password 121

Wireless Basics 124
What is Wireless? 125

Tips..... 127
Wireless Modes..... 128

Networking Basics 129
Check your IP address..... 129
Windows® 8 Users..... 129
Windows® 7/Vista® Users..... 129
Windows® XP Users..... 129
Statically Assign an IP Address 130
Windows® 8 Users 130
Windows® 7/ Vista® Users 131
Windows® XP Users..... 132

Technical Specifications 133

Contacting Technical Support 134

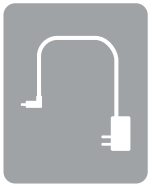
GPL Code Statement.....135

Warranty.....147

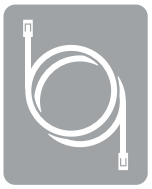
Registration 154

Package Contents

DIR-803 Wireless AC750 Dual Band Router



Power Adapter



Ethernet Cable

Wi-Fi Configuration Card

Quick Install Guide

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

Note: *Using a power supply with a different voltage rating than the one included with the DIR-803 will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based broadband modem • IEEE 802.11ac, 802.11a, 802.11n, or 802.11g wireless clients
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows® 8, 7, Vista®, XP SP2, Mac OS® X (v10.4) • An installed Ethernet adapter or wireless adapter **Supported Browsers:** • Internet Explorer 7 or higher • Firefox • Safari 4 or higher • Chrome **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
Mobile Requirements	**QRS Mobile App Requires:** • iOS 4.3 or higher • Android 2.0 or higher

Introduction

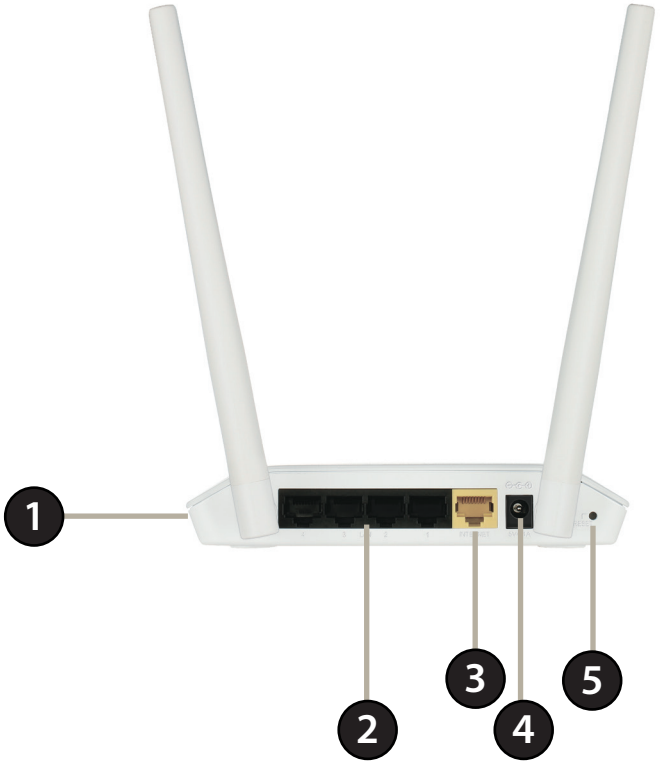
The DIR-803 Wireless AC750 Dual Band Router delivers revolutionary wireless speed, up to three times faster than 802.11n, while staying backward compatible with 802.11a/g/b devices. Connect the DIR-803 to a Cable or DSL modem for high-speed Internet access to multiple computers, video game consoles, and media players. Powered by the 802.11ac technology, this router provides wireless coverage for users running bandwidth-intensive applications.

The DIR-803 supports the latest wireless security features to help prevent unauthorized access over a wireless network or over the Internet. Support for WPA™ and WPA2™ standards ensure that you will be able to use the best possible encryption regardless of your client devices. In addition, this router utilizes Dual Active Firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

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

Hardware Overview

Connections



1	WPS Button	Press to start the WPS process. The Power LED will start to blink.
2	LAN Ports (1-4)	Connect Ethernet devices such as computers, switches, Network Attached Storage (NAS), and video game consoles.
3	Internet Port	Connect your broadband modem to this port using an Ethernet cable.
4	Power Receptor	Connect the supplied power adapter.
5	Reset Button	Press and hold the reset button with a paper clip for six seconds to reset the router to the factory default settings.

Hardware Overview

LEDs

1	Power LED	A solid green light indicates a proper connection to the power supply. The light will blink during boot-up.
2	Internet LED	A solid green light indicates a connection to your broadband modem.
3	WPS LED	This LED will blink during the WPS process.
4	Wireless LED	A solid light indicates that the wireless segment is ready. The light blinks during wireless data transmission.
5	LAN LEDs (1-4)	A solid green light indicates a connection to an Ethernet device, such as a computer, switch or video game console.

Installation

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

Before you Begin

- Please configure the router with the computer that was last connected directly to your modem.
- **Users with DSL providers** - If you are using a PPPoE connection, you will need your PPPoE user name and password. If you do not have this information, contact your Internet provider. Do not proceed until you have this information.
- **Users with Cable providers** - Make sure you unplug the power to your modem. In some cases, you may need to turn it off for up to five minutes.
- **Advanced Users** - If your ISP provided you with a modem/router combo, you will need to set it to "bridge" mode so the DIR-803 router can work properly. Please contact your ISP or refer to the user manual for your modem/router device.

Wireless Installation Considerations

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

1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

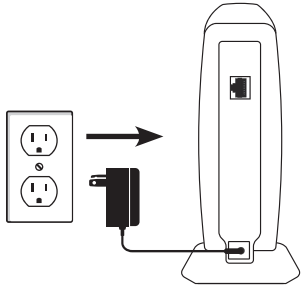
3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

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

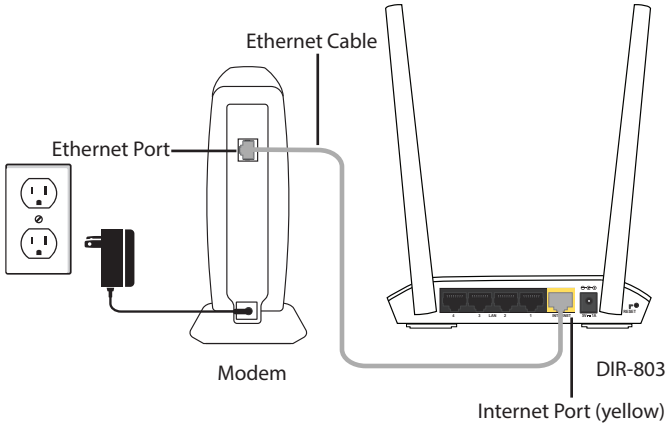
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits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

Connect to your Network

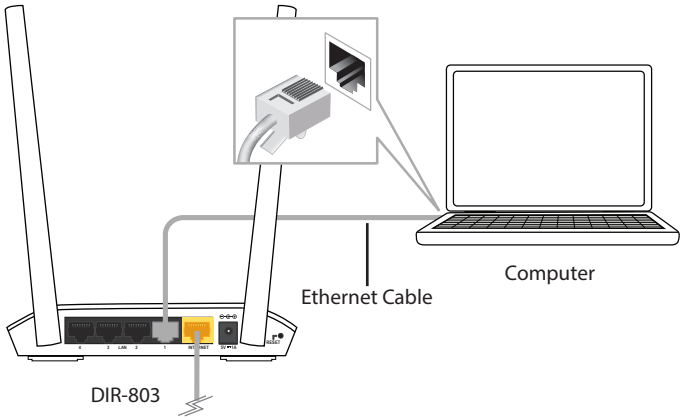
1. Turn off and unplug your DSL or Cable modem. This is required. If you have an existing router, it is strongly recommended that you replace it with the DIR-803, instead of using both. (Refer to "Connect to an Existing Router" on page 11 if your modem is a combo router.)



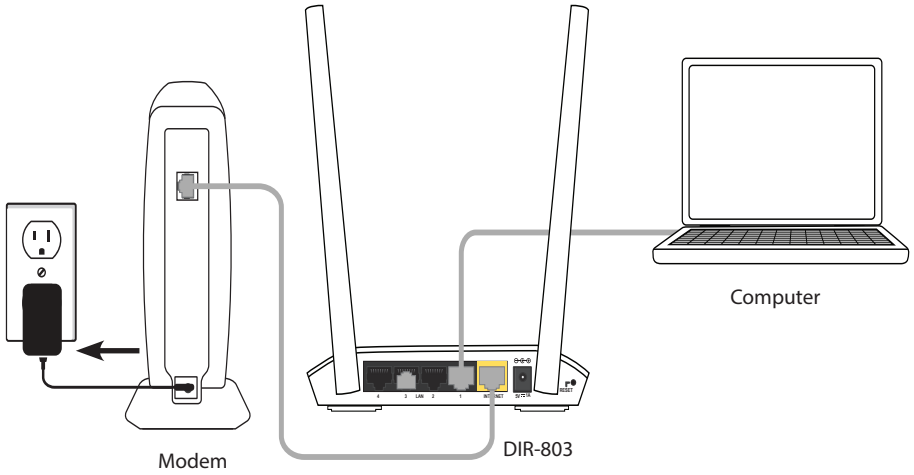
2. Connect an Ethernet cable from the yellow port labeled INTERNET on the back of the router to the Ethernet port on your DSL or Cable modem.



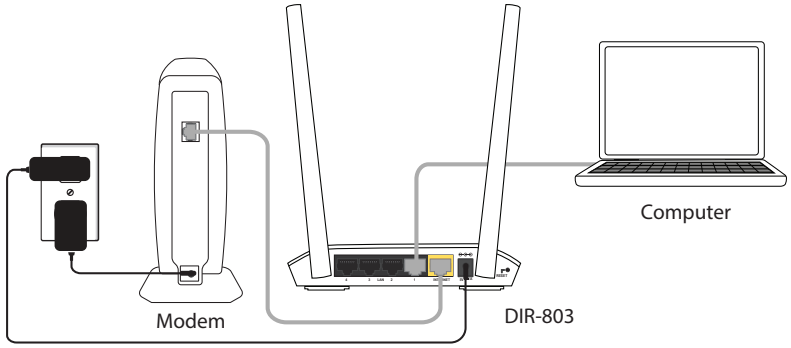
3. Connect another Ethernet cable from the Ethernet port on your computer to one of the LAN ports on the back of your router.



4. Plug the power back into your DSL or Cable modem. Please wait at least one minute before continuing.



5. Plug the power adapter into the power receptor on the back of your router and connect to an available power outlet or surge protector.



6. After the router has powered up, verify that the power and Internet LEDs are both lit. Please skip to "Configuration" on page 13 for your router configuration choices. If you did not connect to the Internet, you can use the *D-Link Setup Wizard* (refer to "Quick Setup Wizard" on page 14).

Connect to an Existing Router

Note: *It is strongly recommended that you replace your existing router with the DIR-803 instead of using both. If your modem is a combo router, you may want to contact your ISP or review the manufacturer's user guide so you can put the router into Bridge mode, which will 'turn off' the router's (NAT) functions.*

If you are connecting the DIR-803 router to an existing router to use as a wireless access point and/or switch, you will have to do the following to the DIR-803 before connecting it to your network:

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

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

1. Plug the power into the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). Please see the **Networking Basics** section for more information. If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.

2. Open a web browser, enter **http://192.168.0.1** (or **http://dlinkrouter.local./**) and press **Enter**. When the login window appears, set the user name to **Admin** and leave the password box empty. Click **Log In** to continue.

3. Click on **Advanced** and then click **Advanced Network**. Uncheck the **Enable UPnP** checkbox. Click **Save Settings** to continue.

4. Click **Setup** and then click **Network Settings**. Uncheck the **Enable DHCP Server** checkbox. Click **Save Settings** to continue.

5. Under Router Settings, enter an available IP address and the subnet mask of your network. Click **Save Settings** to save your settings. Use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 1.

6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.

7. Connect an Ethernet cable in one of the **LAN** ports of the router and connect it to your other router. Do not plug anything into the Internet (WAN) port of the D-Link router.

8. You may now use the other three LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the **Configuration** and **Wireless Security** sections for more information on setting up your wireless network.

Configuration

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

- **QRS Mobile App** - Use your iPhone, iPad, or Android device to configure your router. Refer to "QRS Mobile App" on page 19.
- **D-Link Setup Wizard** - This wizard will launch when you log into the router for the first time. Refer to "Quick Setup Wizard" on page 14.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to "Internet Connection Setup" on page 21.

Quick Setup Wizard

If this is your first time installing the router, launch your web browser (e.g., Internet Explorer), and you will automatically be directed to the **Setup Wizard** screen.

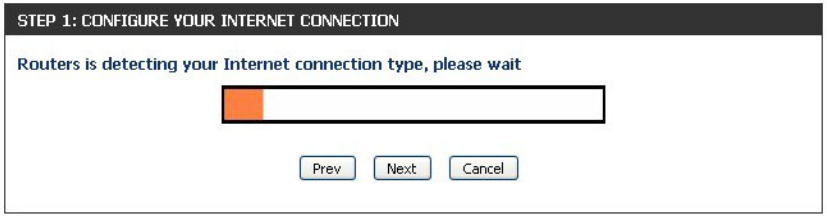
If you have already completed the initial setup, and you would like to access the configuration utility, refer to "Web-based Configuration Utility" on page 20.

If this is your first time logging into the router, and the wizard does not start automatically, enter **http://192.168.0.1**.

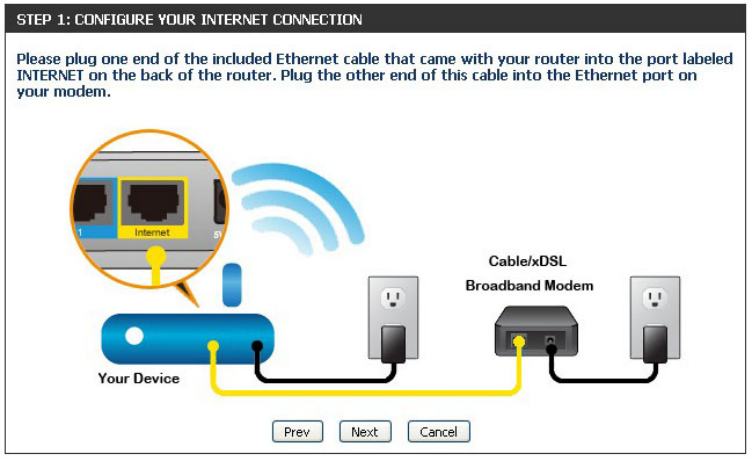
The wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

Click **Next** to continue.

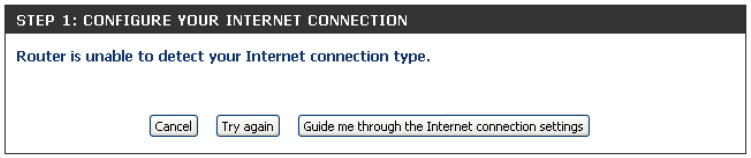
Please wait while your router detects your internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password. (See instructions on page 16 for PPPoE, PPTP and L2TP).



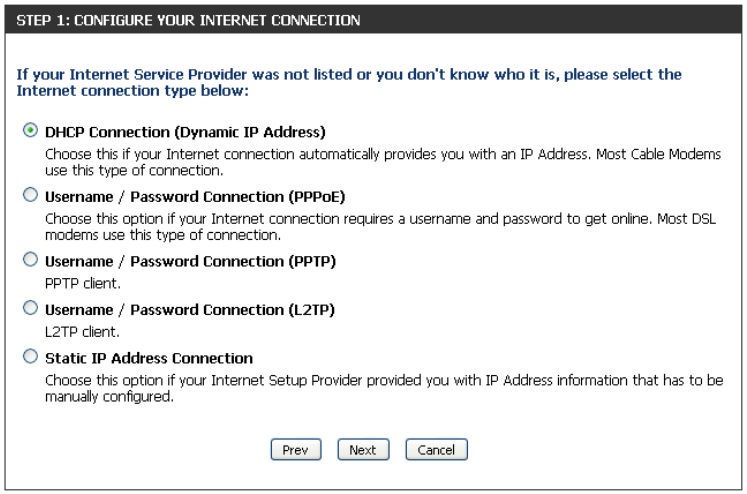
If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Connect your broadband modem to the Internet port and then click **Connect**.



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

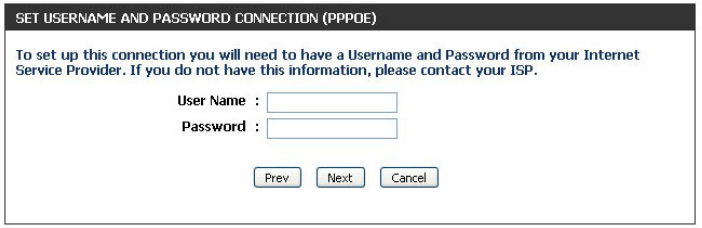


Select your Internet connection type and click **Next** to continue. You can select **DHCP Connection (Dynamic IP Address)** if your Internet connection automatically provides you with an IP Address. This option is commonly used for cable modem services. Click **Next** to continue.

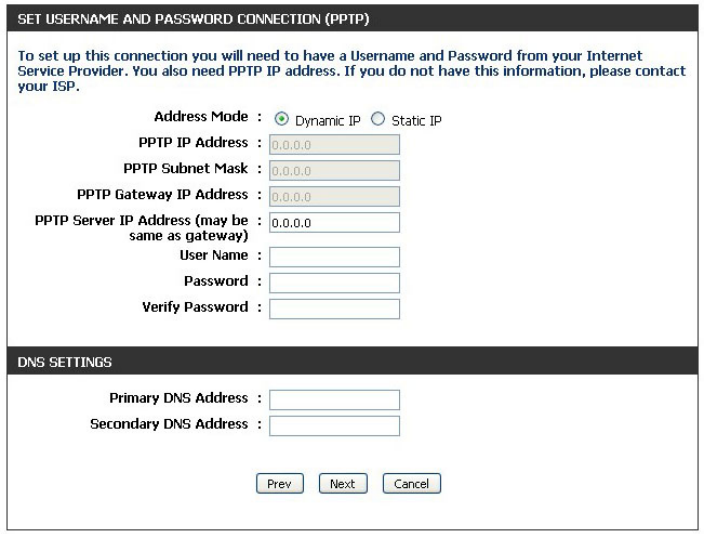


If the router detected or you selected **PPPoE**, enter your PPPoE **User Name** and **Password** and click **Next** to continue.

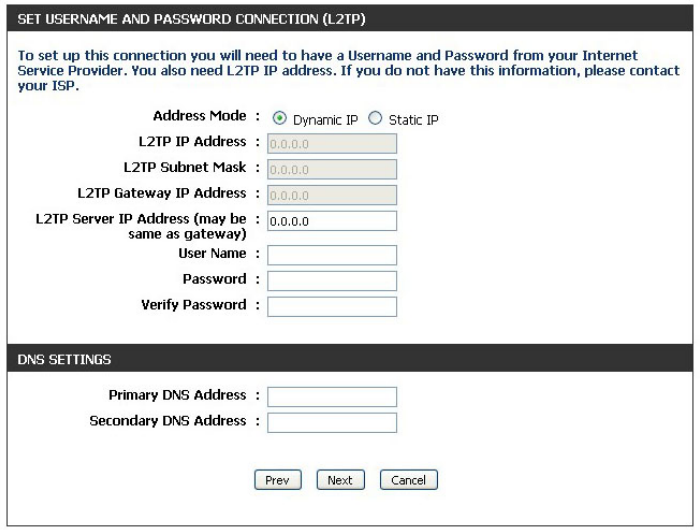
Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*



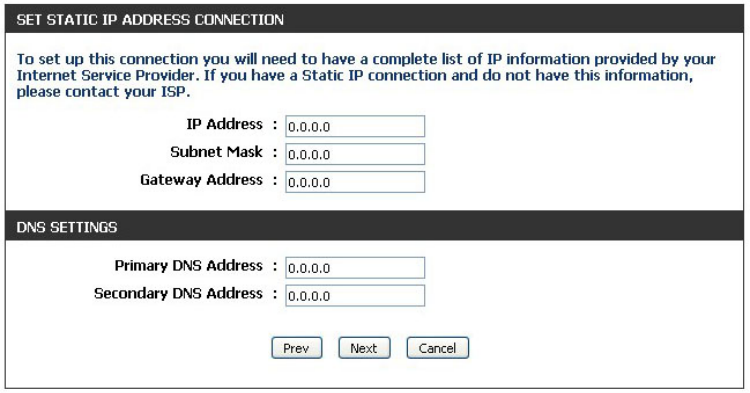
If the router detected or you selected **PPTP**, enter your PPTP **User Name**, **Password**, and other information supplied by your ISP. Click **Next** to continue.



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.



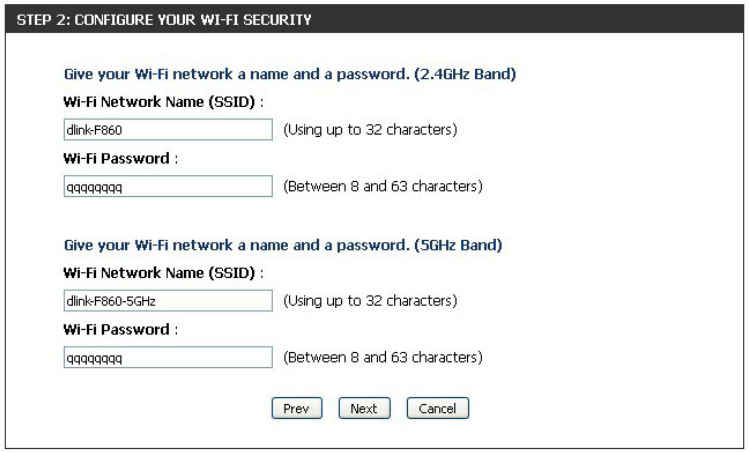
If the router detected or you selected **Static**, enter the IP and DNS settings supplied by your ISP. Click **Next** to continue.



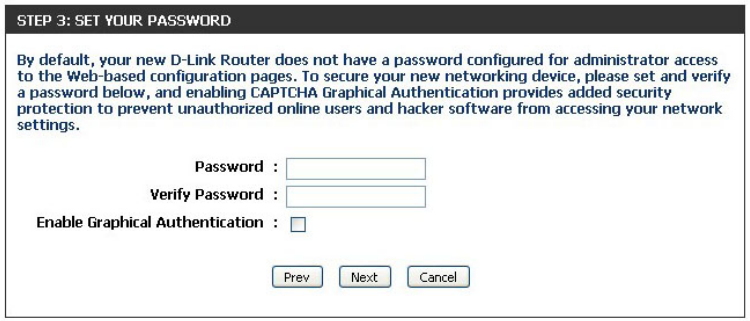
For both the 2.4GHz and 5GHz segments, create a wireless network name (SSID) using up to 32 characters.

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

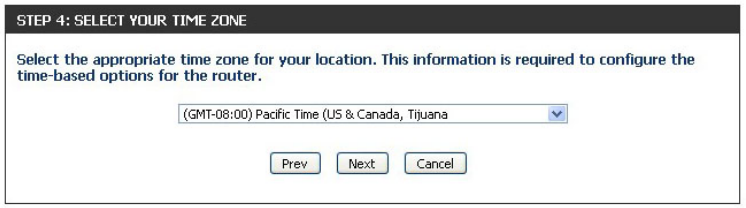
Click **Next** to continue.



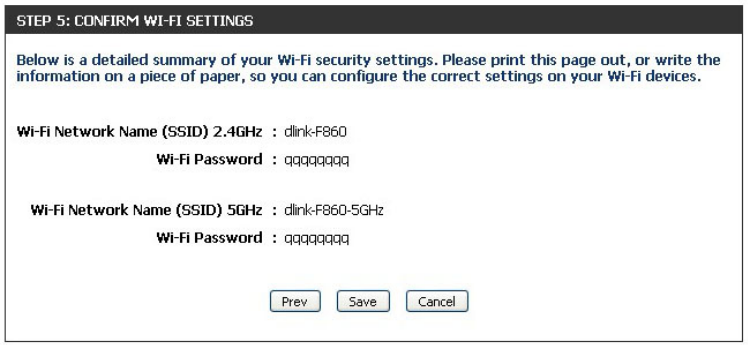
In order to secure your router, enter a new **Password**. Check the **Enable Graphical Authentication** box if you want to enable CAPTCHA authentication for added security. Click **Next** to continue.



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

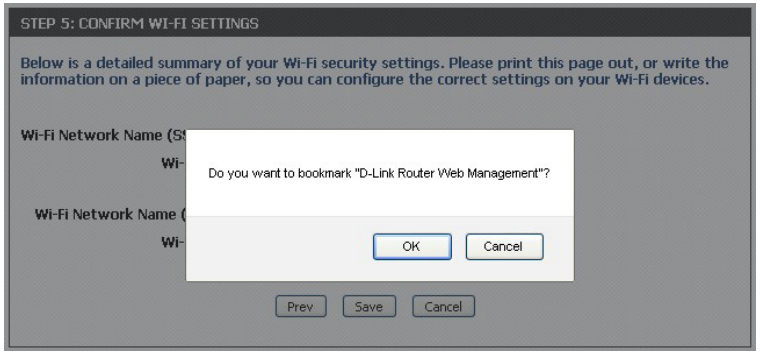


The *Confirm Wi-Fi Settings* window will display your wireless settings. Make a note of this information so you can configure your Wi-Fi devices. Click **Next** to continue.



The *Saving Settings* window will appear.

If you would like to create a bookmark to *D-Link Router Web Management*, click **OK**. Otherwise, click **Cancel**.



QRS Mobile App

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

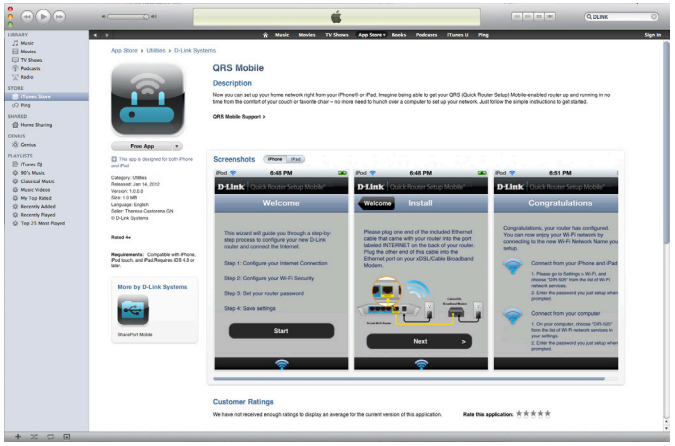
Step 1

From your iPad, iPhone, or Android device, go to the iTunes Store and search for *D-Link*. Select **QRS Mobile** and then download it.

You may also scan this code to download.

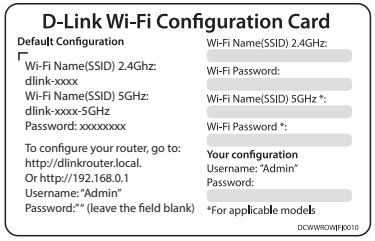
iOS

Android



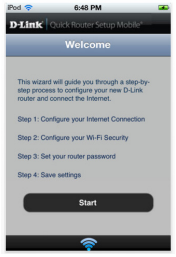
Step 2

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



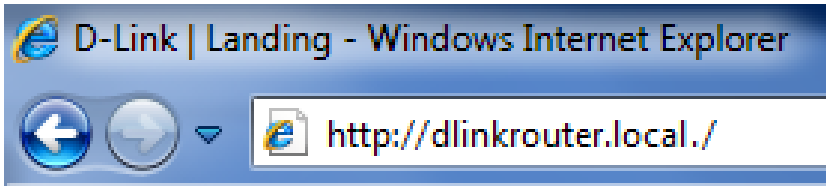
Step 3

Once you connect to the router, launch the *QRS Mobile* app and it will guide you through the installation process for your router.



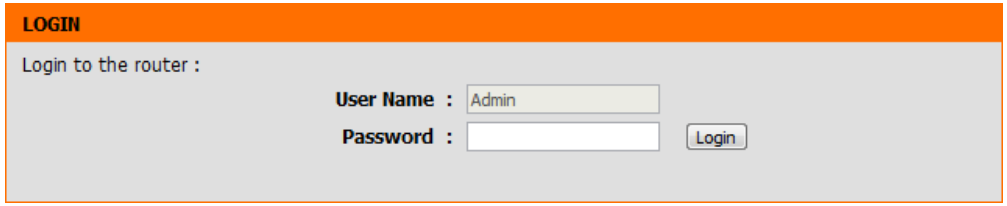
Web-based Configuration Utility

Open a web browser (e.g., Internet Explorer, Chrome, Firefox , or Safari) and enter **http://dlinkrouter.local./** or **http://192.168.0.1**. Windows XP users may use **http://dlinkrouter**.



Enter your password and click **Login**.

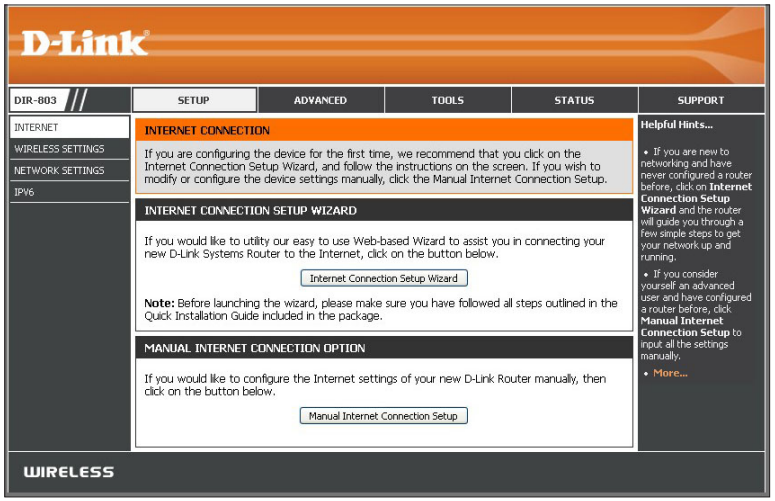
Note: *If you did not create a password with the Setup Wizard, leave the password blank by default.*



Internet Connection Setup

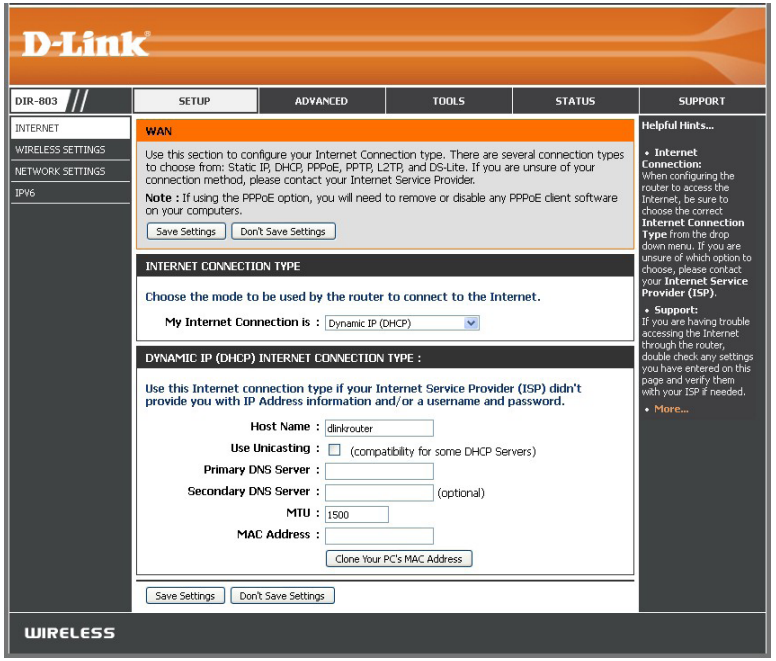
If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard**. Refer to "Internet Connection Setup Wizard" on page 30.

If you consider yourself an advanced user, click **Manual Internet Connection Setup** to configure your connection manually. (Instructions for manual setup begin below.)



The next few pages will explain each of the ISP connection types you can select from the **My Internet Connection is** drop-down menu.

At any given time, you can save the configuration by clicking on the **Save Settings** button. If you would like to discard any changes made, click on **Don't Save Settings**.



Manual Internet Setup

Static (assigned by ISP)

Select **Static IP** if all the IP information is provided to you by your ISP (Internet Service Provider).

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

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

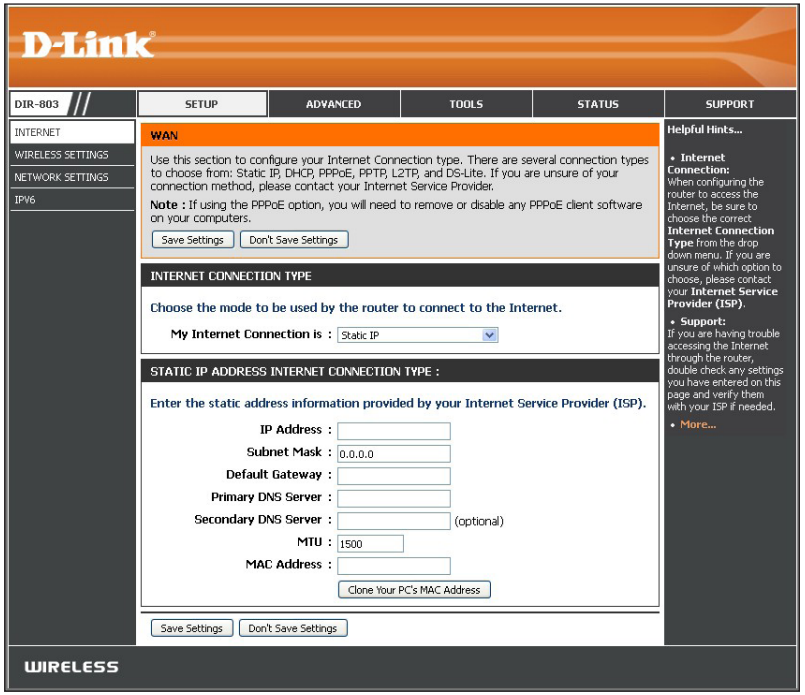
Subnet Mask: Enter the **Subnet Mask** assigned by your ISP.

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

DNS Servers: Enter the **DNS Server** information supplied by your ISP.

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

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



Internet Setup
Dynamic (Cable)

My Internet Connection is: Select **Dynamic IP (DHCP)** to obtain IP Address information automatically from your ISP. This option is commonly used for cable modem services.

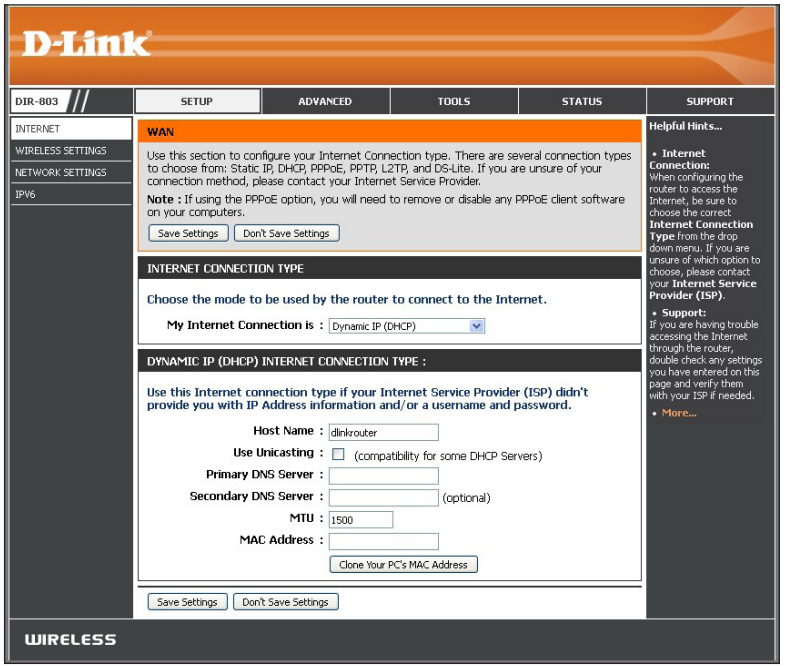
Host Name: The **Host Name** is optional but may be required by some ISPs. Leave blank if you are not sure.

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

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

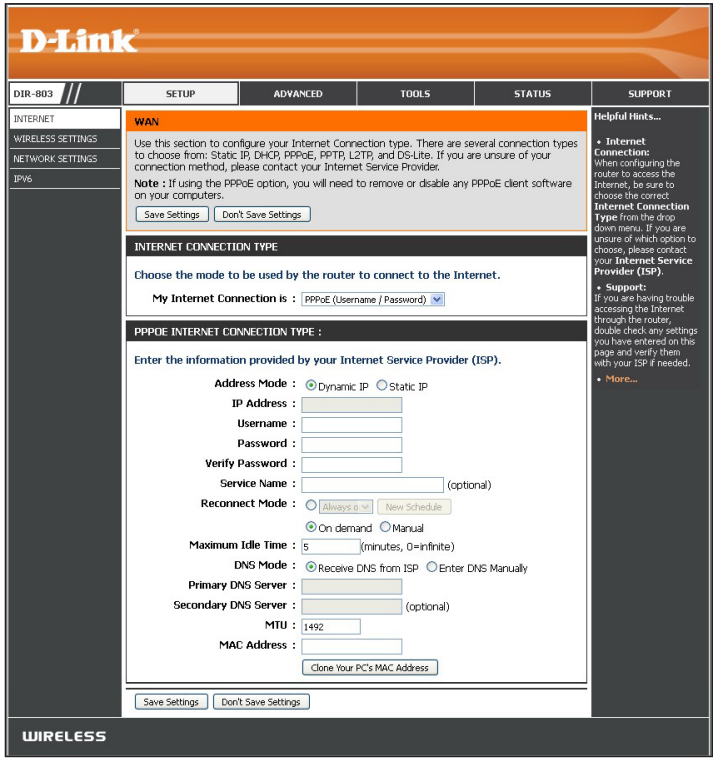
MTU: Maximum Transmission Unit - you may need to change the **MTU** for optimal performance with your specific ISP. 1500 is the default MTU.

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



Internet Setup
PPPoE (DSL)

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



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

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

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

Username: Enter your PPPoE **Username**.

Password: Enter your PPPoE **Password** and 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. Enable Auto-reconnect to disable this feature.

DNS Mode: Allows the router to obtain the DNS IP address from the ISP when **Receive DNS from ISP** is selected.

DNS Servers: Enter the Primary and Secondary **DNS Server** Addresses of your choice or 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. 1492 is the default MTU.

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

Internet Setup
PPTP

Choose PPTP (Point-to-Point-Tunneling Protocol) if your ISP (Internet Service Provider) uses a PPTP connection. Your ISP will provide you with a username and password.

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

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

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

PPTP Subnet Mask: Enter the **Subnet Mask** (Static PPTP only).

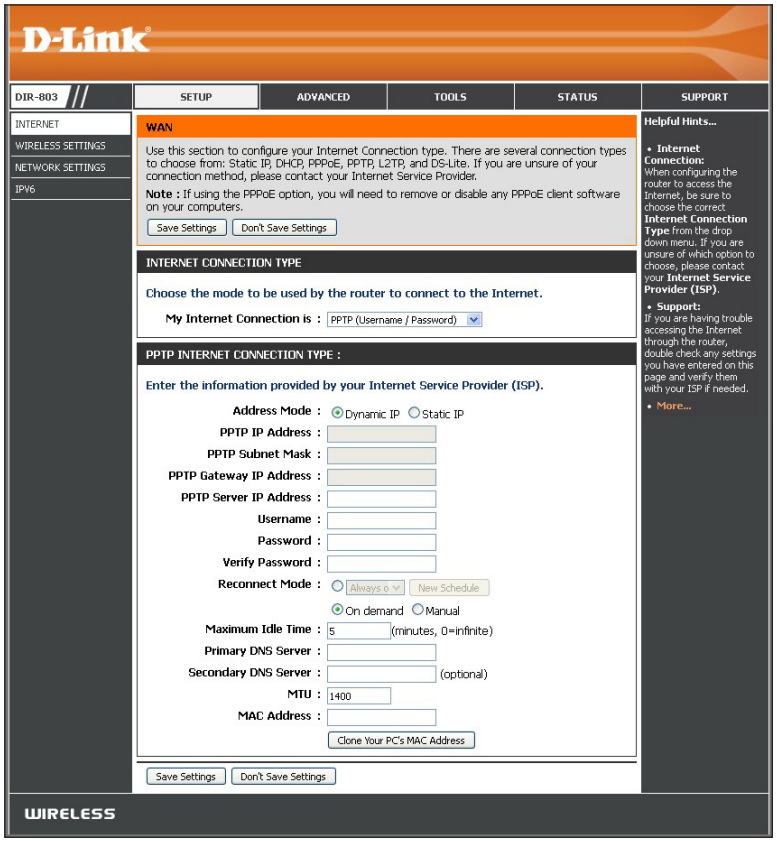
PPTP Gateway IP Address: Enter the **Gateway IP Address** provided by your ISP.

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

Username: Enter your PPTP **Username**.

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

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



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

DNS Servers: Enter the Primary and Secondary **DNS Server** Addresses. The DNS server information will be supplied by your ISP.

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

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

Internet Setup
L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP uses a L2TP connection. Your ISP will provide you with a username and password.

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

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

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

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

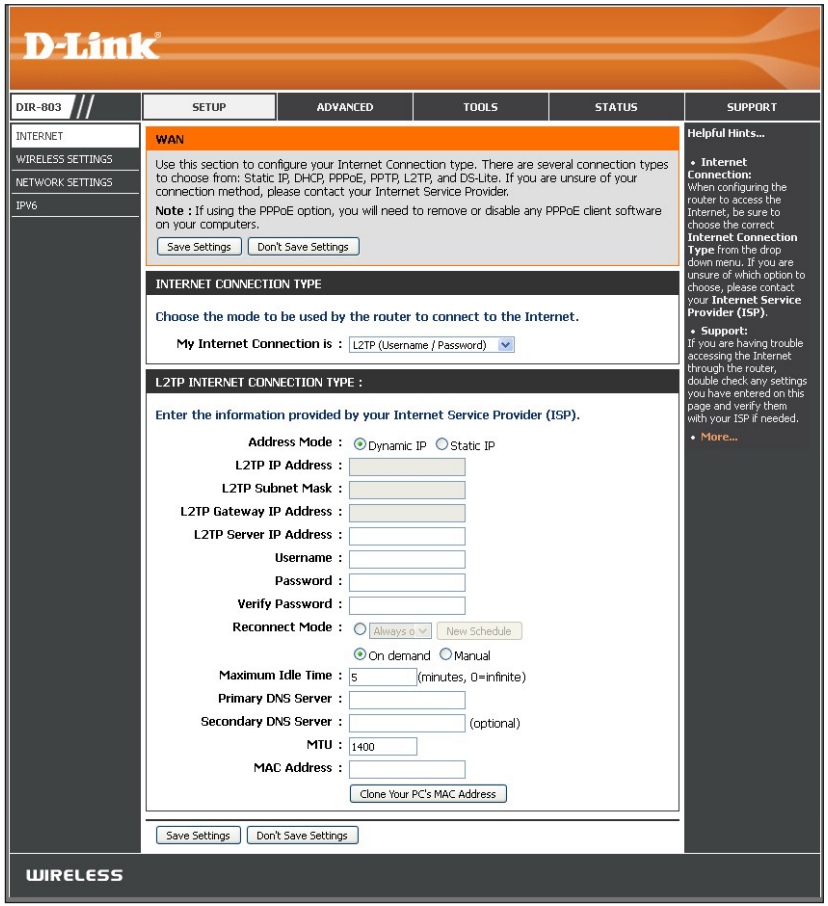
Username: Enter your L2TP **Username**.

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

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

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

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



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

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

Internet Setup
DS-Lite

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

My Internet Connection is: Select **DS-Lite** from the drop-down menu.

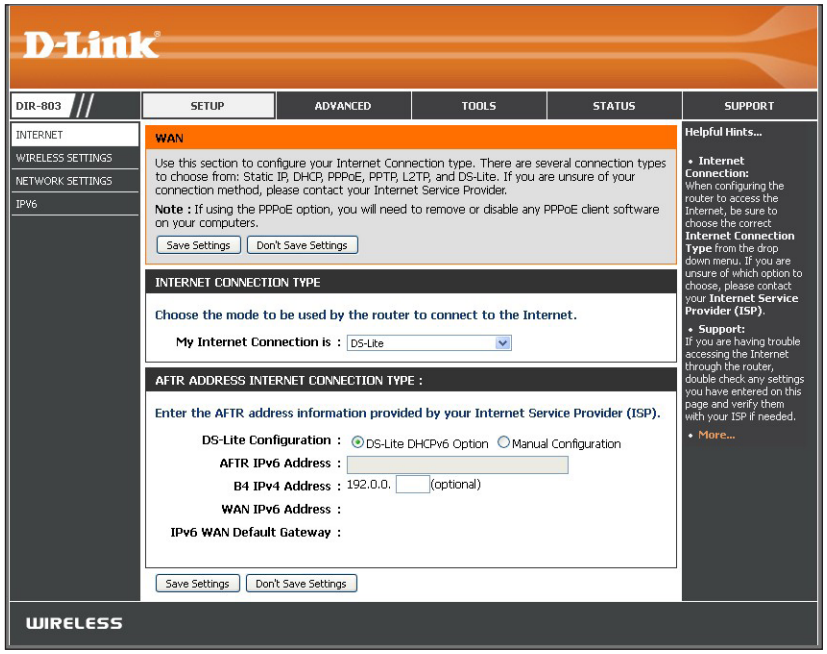
DS-Lite Configuration: Select the **DS-Lite DHCPv6 Option** to let the router allocate the AFTR IPv6 address automatically. Select the **Manual Configuration** option to enter the AFTR IPv6 address in manually.

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

B4 IPv4 Address: Enter the **B4 IPv4 Address** here. (Optional.)

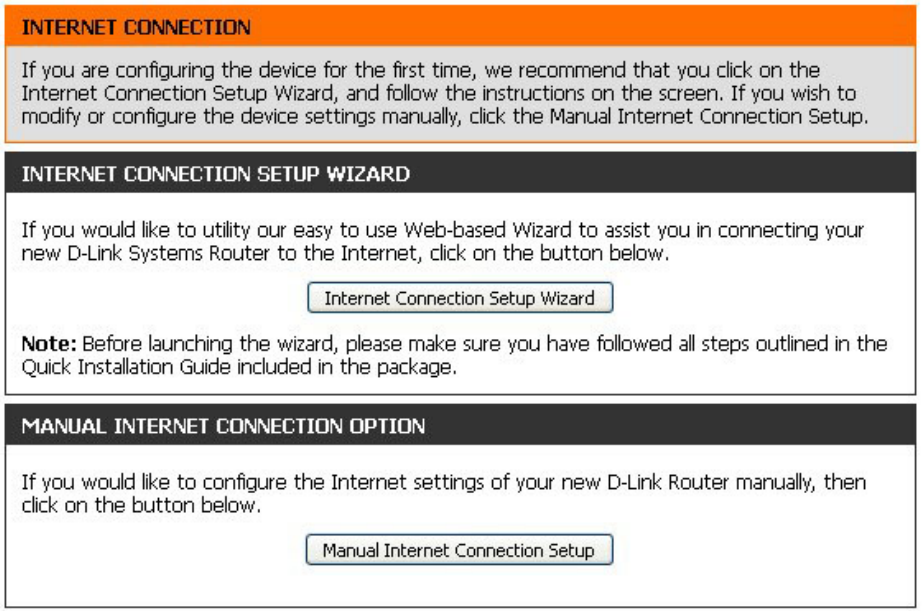
WAN IPv6 Address: Once connected, the *WAN IPv6 Address* will be displayed here.

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



Internet Connection Setup Wizard

If you did not initially choose to install your router with the *Quick Setup Wizard*, you can click on **Internet Connection Setup Wizard** from the **Setup** > **Internet** screen.

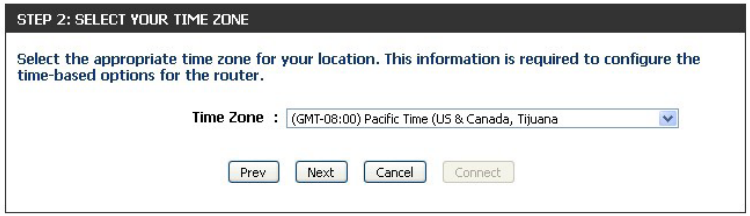


This wizard is designed to guide you through a step-by-step process to configure your new D-Link router and connect to the Internet.

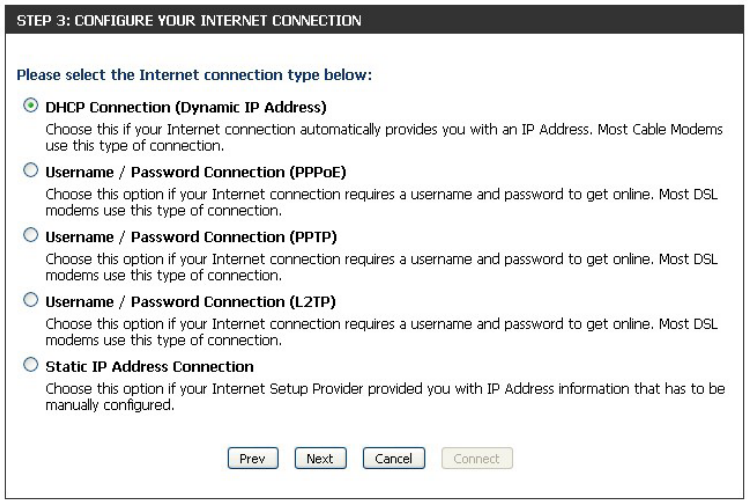
Click **Next** to continue.

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

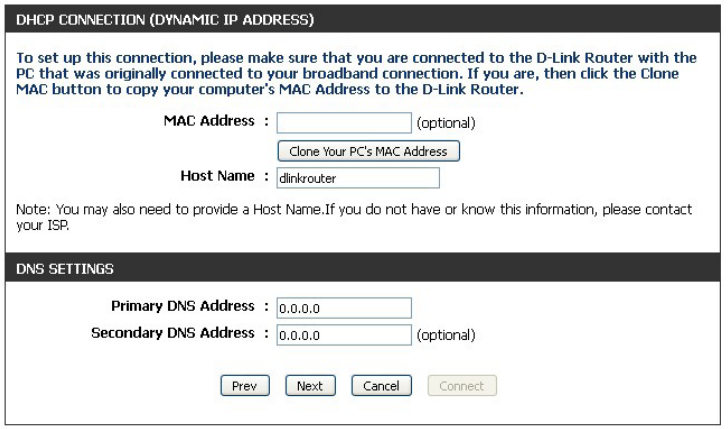
Select your **Time Zone** from the drop-down menu and click **Next** to continue.



Select your Internet connection type. You can select **DHCP Connection (Dynamic IP Address)** if your Internet connection automatically provides you with an IP Address. This option is commonly used for cable modem services. Click **Next** to continue.

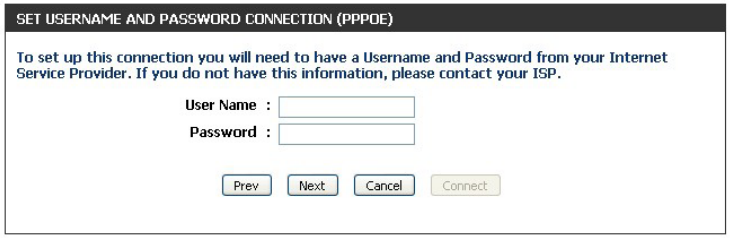


If you selected **DHCP Connection (Dynamic IP Address)** you can click on **Clone Your PC's MAC Address** to copy your computer's MAC address to your router. Click **Next** to continue.

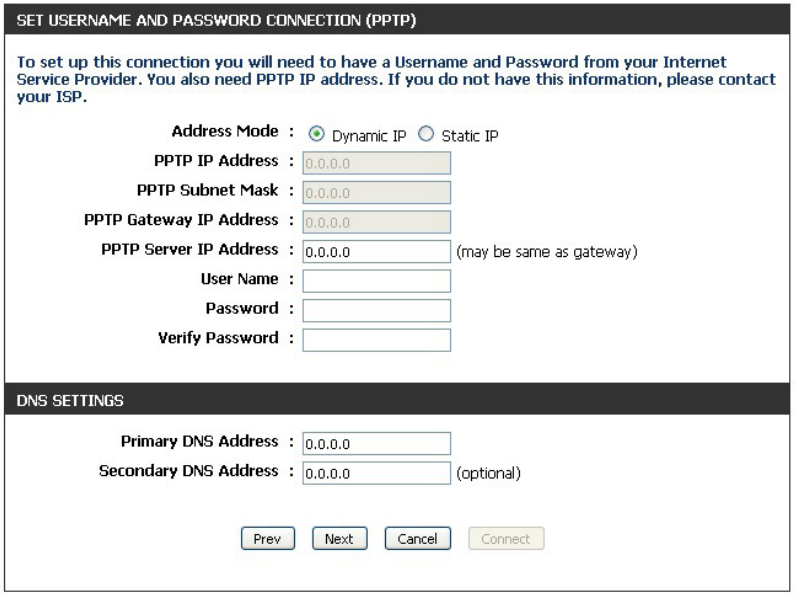


If you selected **PPPoE**, enter your PPPoE **User Name** and **Password**. Click **Next** to continue.

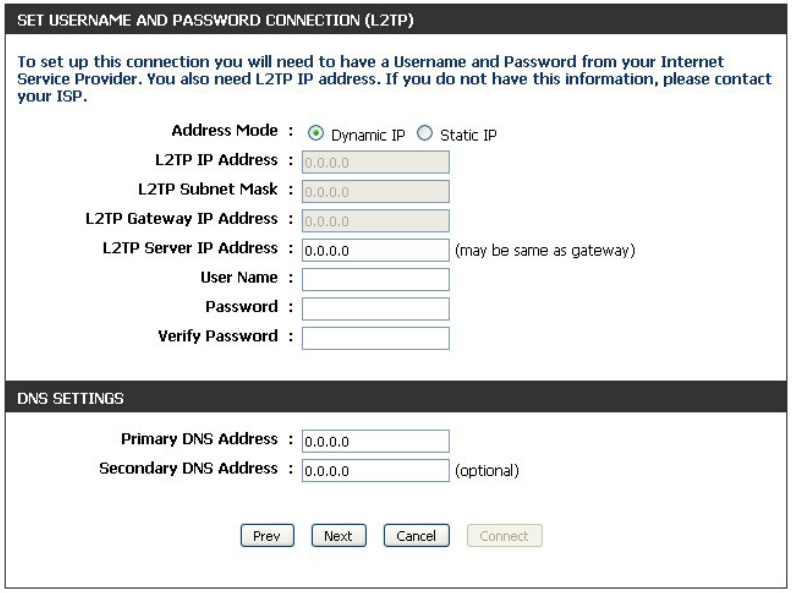
Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*



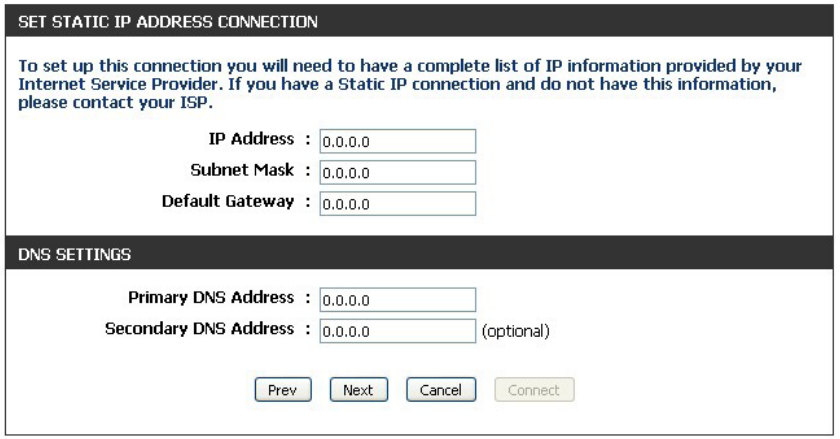
If you selected **PPTP**, enter your PPTP **User Name**, **Password**, and other information supplied by your ISP. Click **Next** to continue.



If you selected **L2TP**, enter your L2TP **User Name**, **Password**, and other information supplied by your ISP. Click **Next** to continue.



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



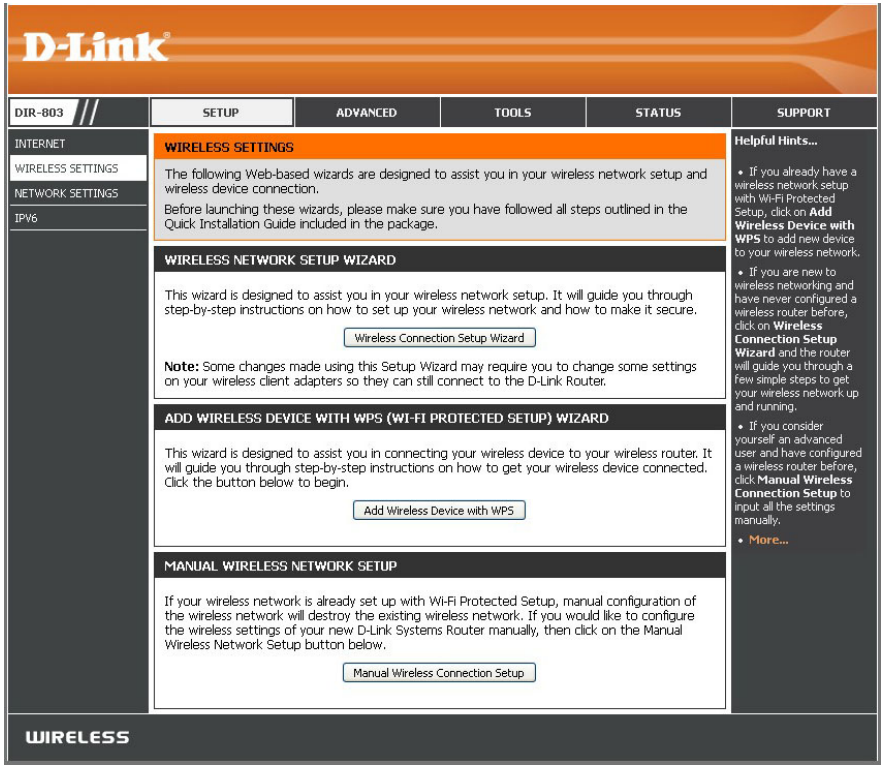
When the setup process is complete, you will see this screen. Click on **Connect** to save your settings.

Wireless Settings

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

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS). Refer to "Add Wireless Device with WPS Wizard" on page 38.

Click **Manual Wireless Connection Setup** if you want to manually configure the wireless settings on your router. Refer to "Manual Wireless Settings" on page 40.



Wireless Connection Setup Wizard

To run the security wizard, click on **Setup** > **Wireless Settings**. Click on **Wireless Connection Setup Wizard**.

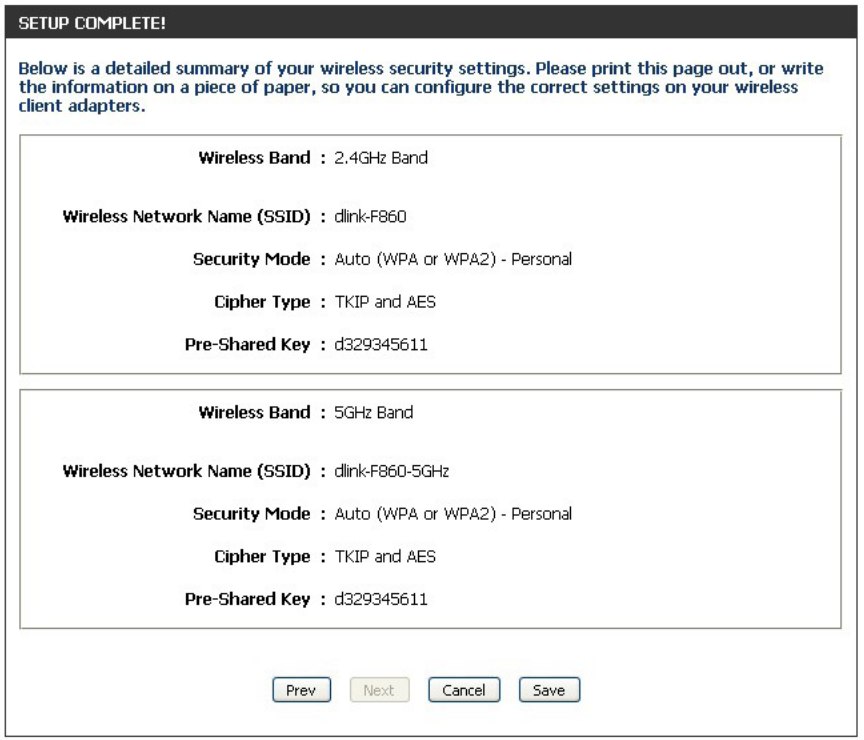
Enter a **Network Name** for your wireless network (SSID). Do not use personal information as your SSID since users with wireless devices within range of your router will be able to see this information.

Then select one of the following options:

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.

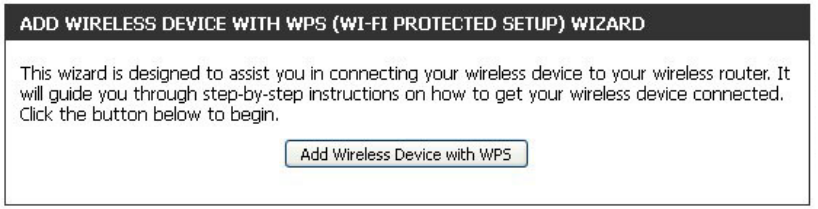


If you selected **Manually**, the following screen will appear. Create a passphrase for your **Wireless Security Password**. Click **Next** to continue. You will see a *Setup Complete* screen like the one above.

Note: *The security password/passphrase must be between 8 and 63 characters and is case-sensitive. You will need to enter this passphrase on your wireless clients exactly or it will not connect.*

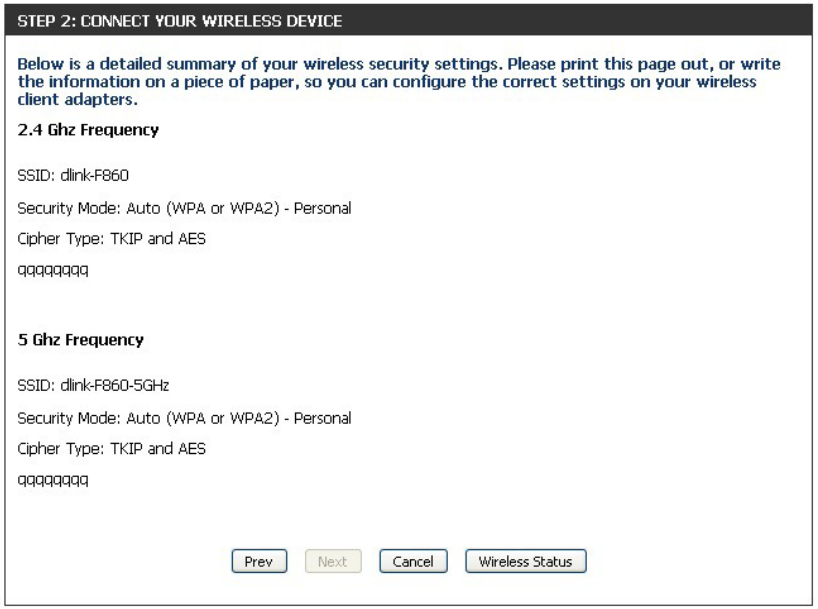
Add Wireless Device with WPS Wizard

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



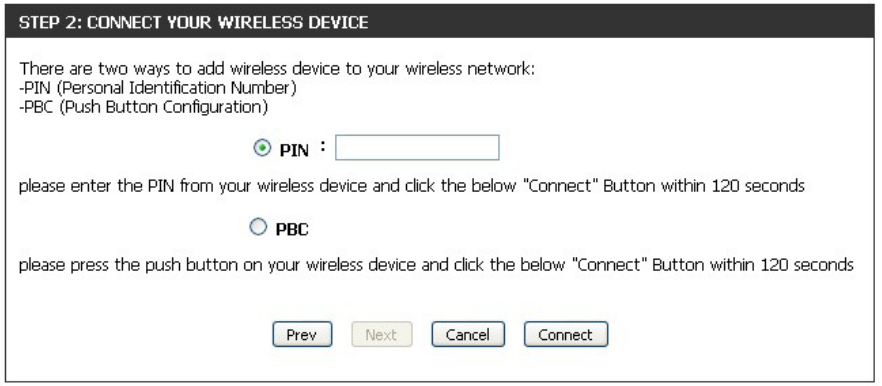
Select **Auto** to add a wireless client using WPS (*Wi-Fi Protected Setup*) and then click **Next**. Skip to the next page.

If you selected **Manual**, a settings summary screen will appear. Write down the security key and enter this on your wireless clients. Click **Wireless Status** to finish. This will take you to the *Wireless Status* screen. Skip to the bottom of the next page.

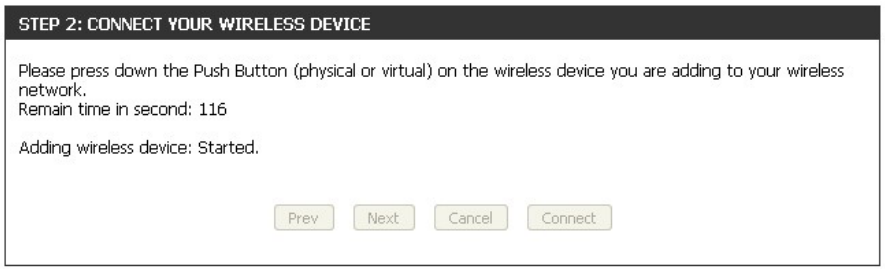


PIN: Select this option to use the Personal Identification Number (PIN) method. In order to use this method, you must enter the wireless client's eight digit PIN code. Click **Connect**.

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

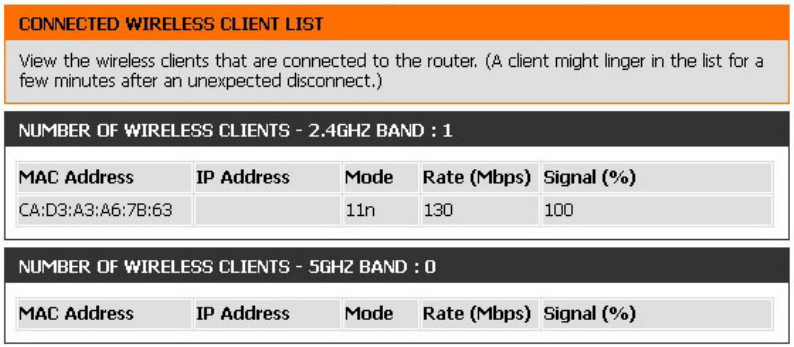


Once you click **Connect**, you will have a 120 second time limit to press the **Push Button** (physical or virtual) on your wireless client(s) and successfully establish a connection.



Click **Wireless Status** to finish. This will take you to *Wireless Status* screen.

View the *Wireless Status* screen.



Manual Wireless Settings

802.11n/g (2.4GHz)

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

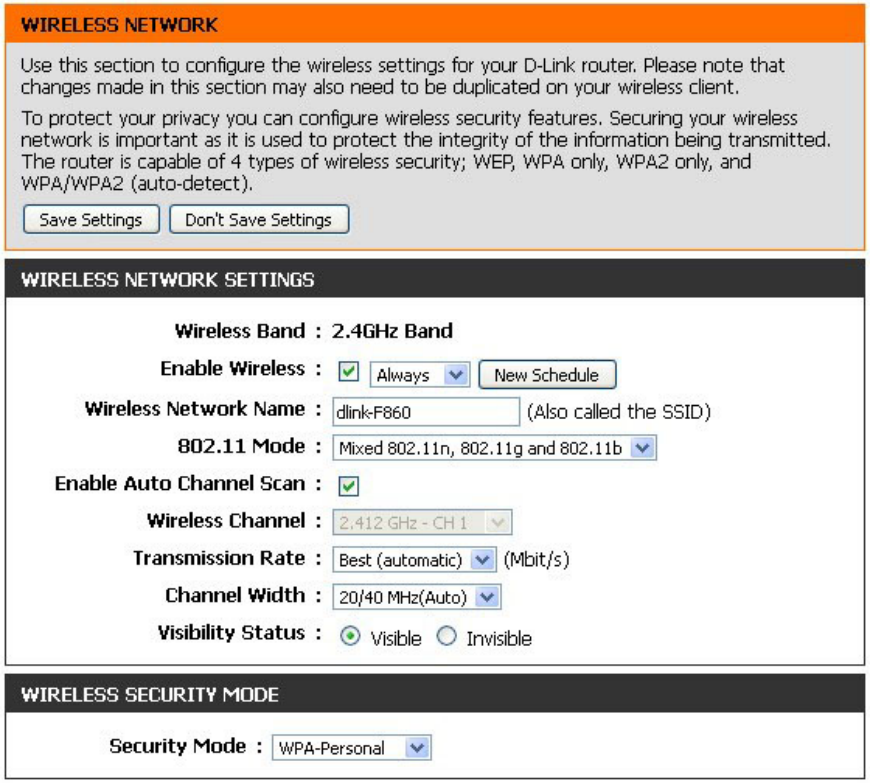
Schedule: Select the time frame that you would like your wireless network enabled. The schedule may be set to **Always**. Any schedule you create will be available in the drop-down menu. Click **New Schedule** to create a schedule.

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

802.11 Mode: Select one of the following:
802.11b Only - Select only if all of your wireless clients are 802.11b.
802.11g Only - Select only 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, 802 11g, and 802 11b - Select if you are using a mix of 802.11n, 802.11g, and 802.11b wireless clients.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be enabled to allow the DIR-803 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-803. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you check **Enable Auto Channel Scan**, this option will be greyed out.



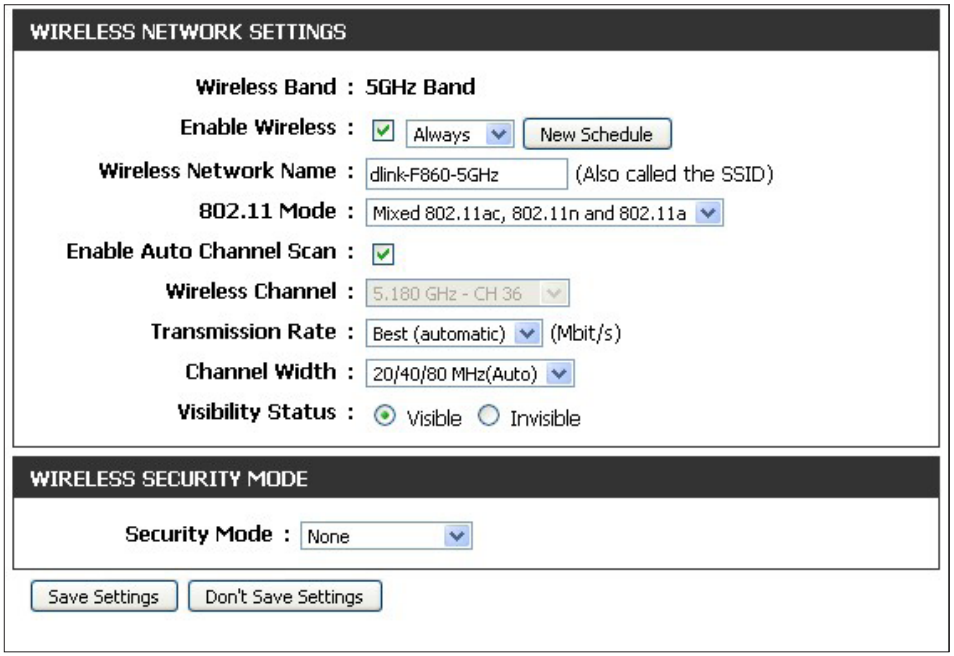
Transmission Rate: **Best (automatic)** is selected by default, or you can select a channel from the drop-down menu.

Channel Width: Select the **Channel Width**:
20/40MHz (**Auto**)- 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.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcast by the DIR-803. If Invisible is selected, the SSID of the DIR-803 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-803 in order to connect to it.

Wireless Security: Refer to "Wireless Security" on page 42 for more information regarding wireless security.

802.11ac/n/a (5GHz)



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

Schedule: Select the time frame that you would like your wireless network enabled. The schedule may be set to **Always**. Any schedule you create will be available in the drop-down menu. Click **New Schedule** to create a schedule.

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

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

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be enabled to allow the DIR-803 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-803. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you check **Enable Auto Channel Scan**, this option will be greyed out.

Transmission Rate: **Best (Automatic)** is selected by default, or you can select a channel from the drop-down menu.

Channel Width: Select the **Channel Width**:
20MHz - Select if you are not using any 802.11n wireless clients.
20/40MHz (Auto) - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.
20/40/80MHz (Auto) - Select if you are using 802.11ac, 802.11n and non-802.11n wireless devices. This option is only available when the 802.11 Mode is set to Mixed 802.11ac.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-803. If Invisible is selected, the SSID of the DIR-803 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-803 in order to connect to it.

Wireless Security: Refer to "Wireless Security" on page 42 for more information regarding 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-803 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

What is WPA?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.

- User authentication, 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.

WPA/WPA2-Personal (PSK)

It is recommended that you enable wireless security on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption.

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

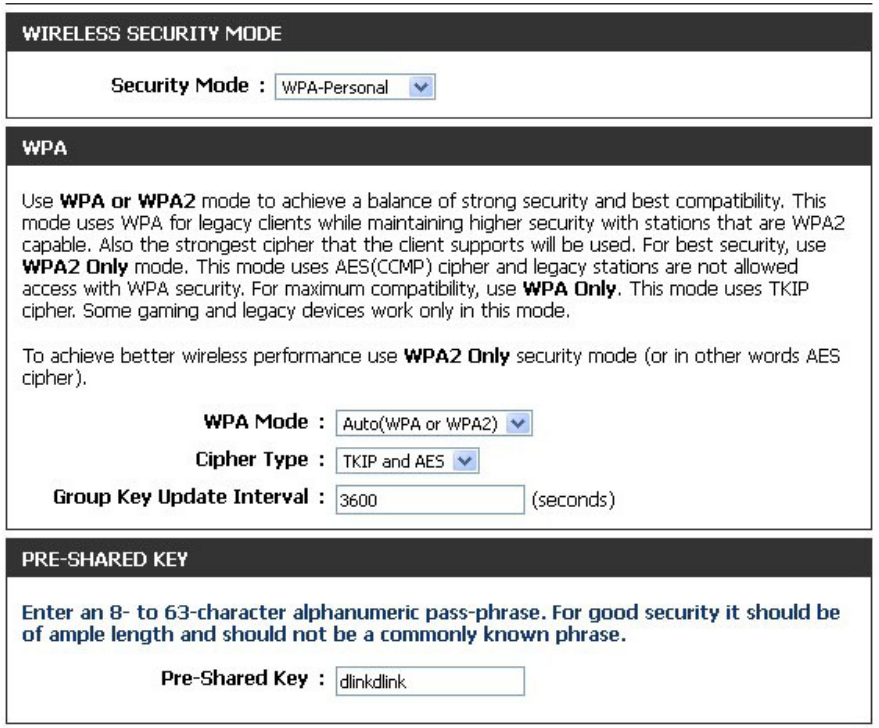
2. Next to **Security Mode**, select **WPA-Personal**.

3. Next to **WPA Mode**, select **Auto (WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

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

5. Next to **Group Key Update Interval**, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

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



7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

Configure WPA/WPA2-Enterprise (RADIUS)

It is recommended that you enable wireless security on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption.

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

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

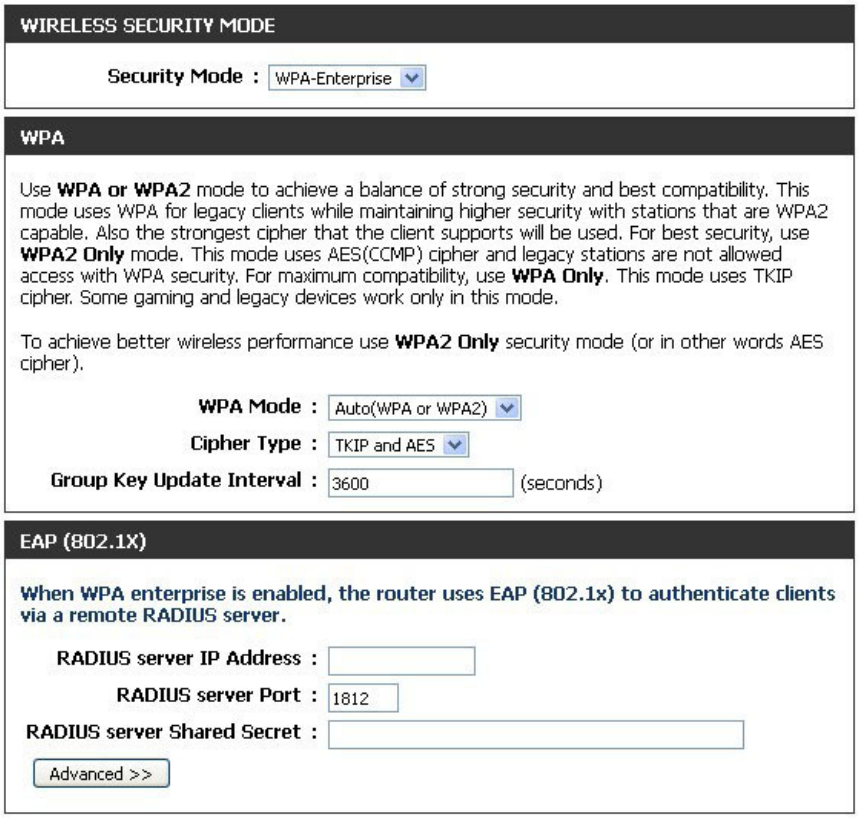
3. Next to **WPA Mode**, select **Auto(WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

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

5. Next to **Group Key Update Interval**, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

6. Next to **RADIUS Server IP Address** enter the **IP Address** of your RADIUS server.

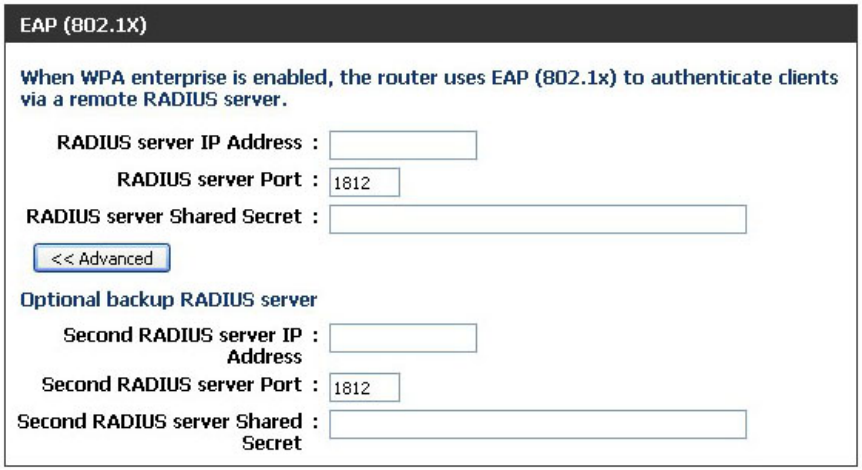
7. Next to **RADIUS Server Port**, enter the port you are using with your RADIUS server. 1812 is the default port.



8. Next to **RADIUS Server Shared Secret**, enter the security key.

9. Click **Advanced** to enter settings for a secondary RADIUS Server.

10. 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.

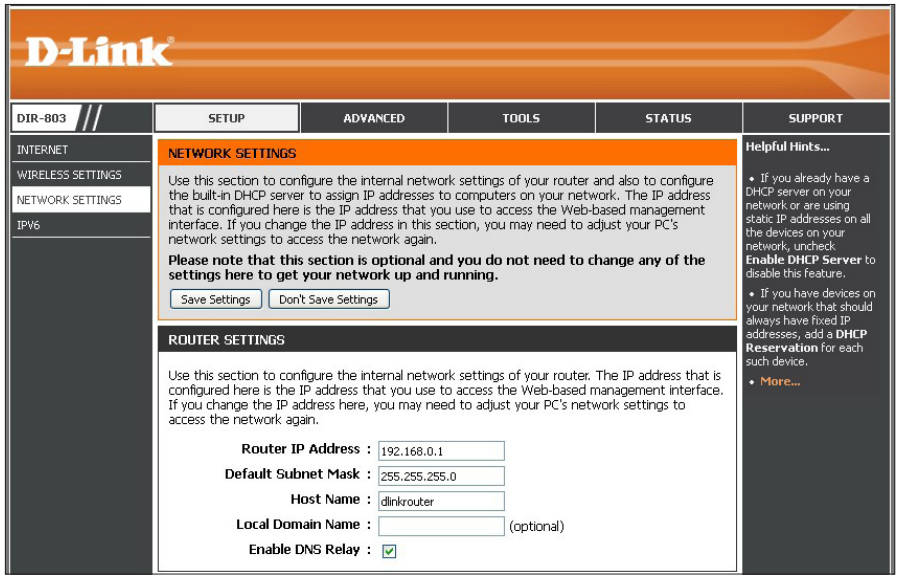
If you change the **IP Address**, once you click **Save Settings**, you will need to enter the new address in your browser to get back into the configuration utility.

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

Host Name: Enter a name for the router.

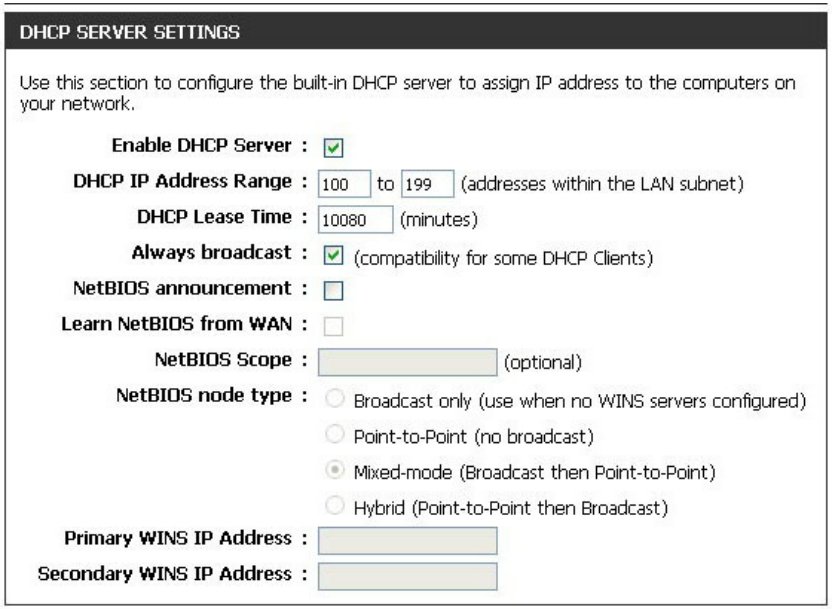
Local Domain Name: Enter the **Domain Name** (Optional).

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



DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-803 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-803. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.



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

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

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

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

Always Broadcast: Enable this feature to broadcast your network's DHCP server to LAN/WLAN clients.

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

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

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

NetBIOS Node Type: This field indicates how network hosts are to perform NetBIOS name registration and discovery. Select the type of **NetBIOS Node**: **Broadcast only**, **Point-to-Point**, **Mixed-mode**, or **Hybrid**. This setting has no effect if the *Learn NetBIOS from WAN* option is enabled.

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

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: 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.

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

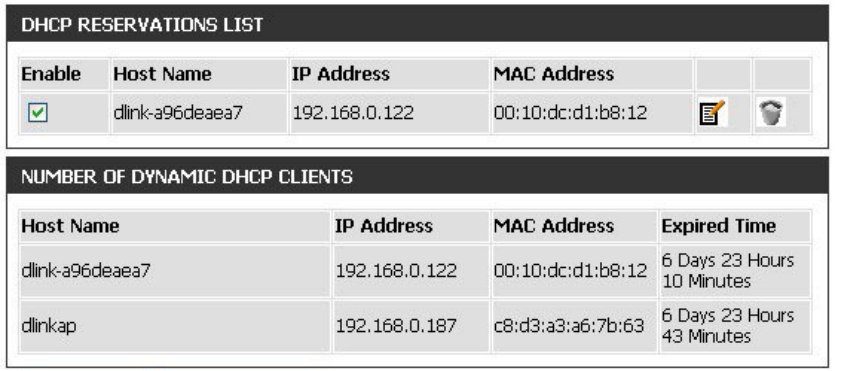
DHCP Reservations List

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

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

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

Delete: Click the trash icon to remove the reservation from the list.



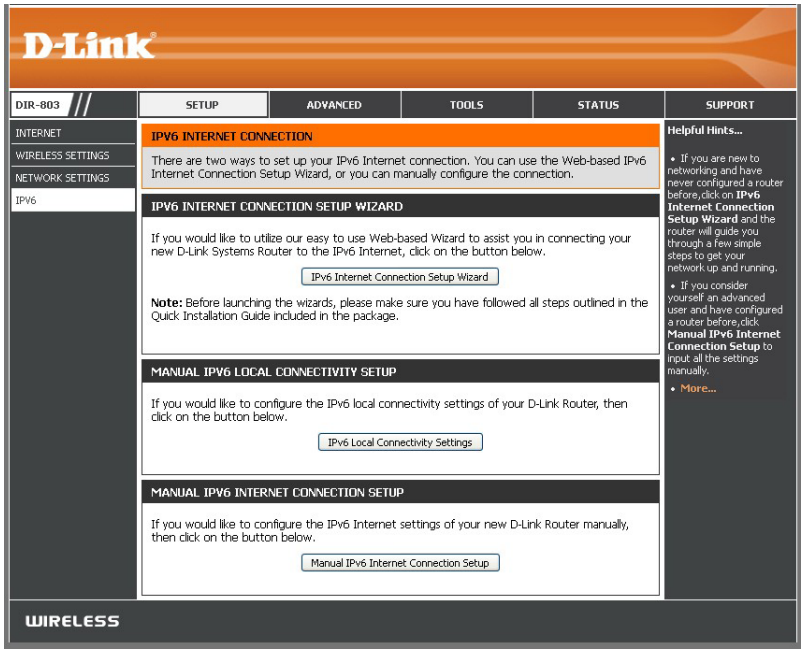
IPv6

On this page, the user can configure the IPv6 Connection type. There are three ways to set up the IPv6 Internet connection.

For the beginner user that has never configured a router before, click on the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running. (Refer to "IPv6 Internet Connection Setup Wizard" on page 52.)

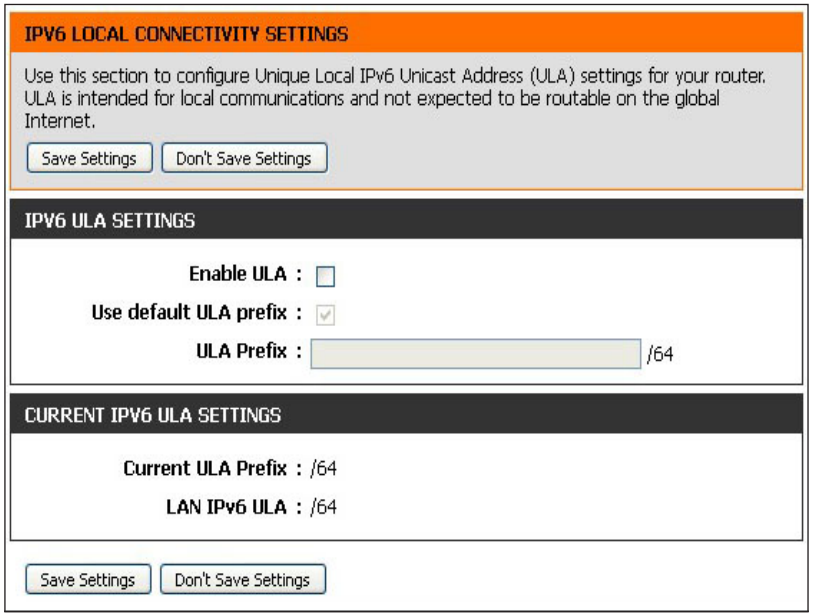
For the advanced user that has experience with configuring a router, click on the **Manual IPv6 Internet Connection Setup** button to input all the settings manually. (Refer to "IPv6 Manual Setup" on page 57.)

If you would like to manually configure the IPv6 local connectivity settings of your router, click on **IPv6 Local Connnectivity Settings**.



Click on **Enable ULA.** You can check **Use default ULA prefix**, or you can leave the box unchecked and enter the prefix manually in the **ULA Prefix** text box.

Click on **Save Settings**.



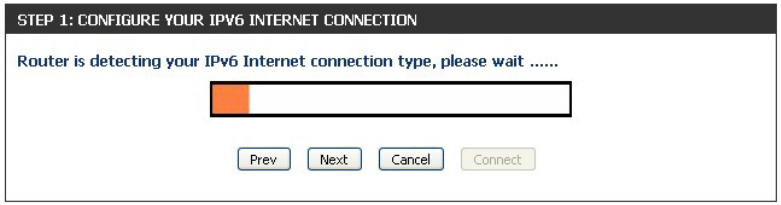
IPv6 Internet Connection Setup Wizard

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

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

Click **Next** to continue to the next page.

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

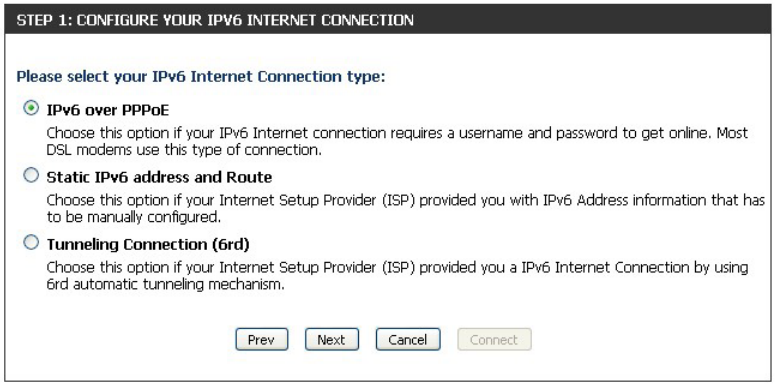


However, if the automatic detection fails, the user will be prompted to either **Try again** or to click on the **Guide me through the IPv6 settings** button to initiate the manual continual of the wizard.

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

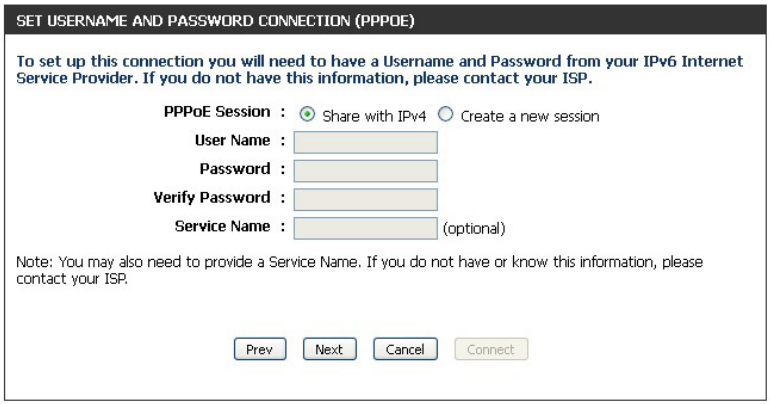
Note: *If using the PPPoE option, you will need to ensure that any PPPoE client software on your computer has been removed or disabled.*

There are three options to choose from. These connection types are explained on the pages that follow. Select **IPv6 over PPPoE, Static IPv6 address and Route,** or **Tunneling Connection (6rd)**. Click **Next** to continue.



IPv6 over PPPoE

Most DSL modems use this type of connection. If you select the **IPv6 over PPPoE** option, you will need a User Name and Password from you IPv6 Internet Service Provider (ISP). This IPv6 Internet connection type requires a username and password to get online.



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

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

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

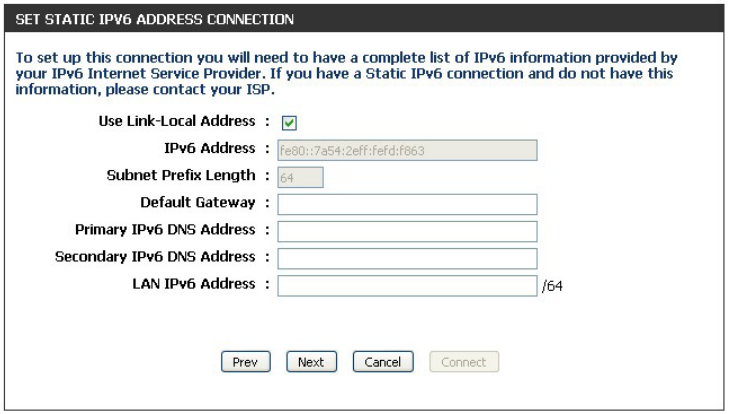
Verify Password: Re-enter the PPPoE **Password** used here.

Service Name: Enter the **Service Name** for this connection here. This field is optional.

Click **Next** to continue.

Static IPv6 Address Connection

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



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

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

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

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

Primary IPv6 DNS Address: Enter the WAN **Primary IPv6 DNS Server Address** used here.

Secondary IPv6 DNS Address: Enter the WAN **Secondary IPv6 DNS Server Address** used here.

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

Click **Next** to continue.

Tunneling Connection (6rd)

If you select the **Tunneling Connection (6rd)** option, you must obtain the information listed below from your ISP. Then you can configure the IPv6 6rd tunneling connection settings.

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

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

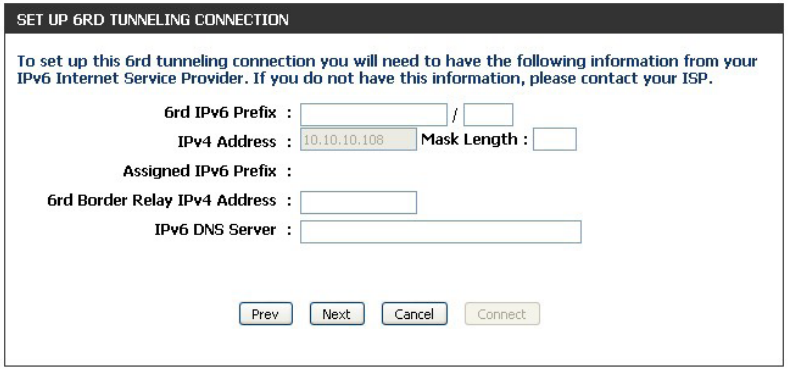
Mask Length: Enter the IPv4 **Mask Length** used here.

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

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

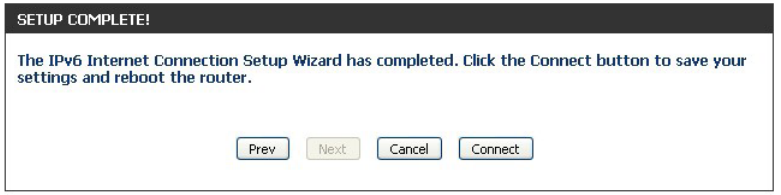
IPv6 DNS Server: Enter the primary **IPv6 DNS Server** address used here.

Click **Next** to continue.



The IPv6 Internet Connection Setup Wizard is complete. Click on the **Connect** button to save your settings and reboot the router.

If you need to make changes, click on the **Prev** button to return to the previous page. Or click on **Cancel** to discard all the changes made and return to the main page.



IPv6 Manual Setup

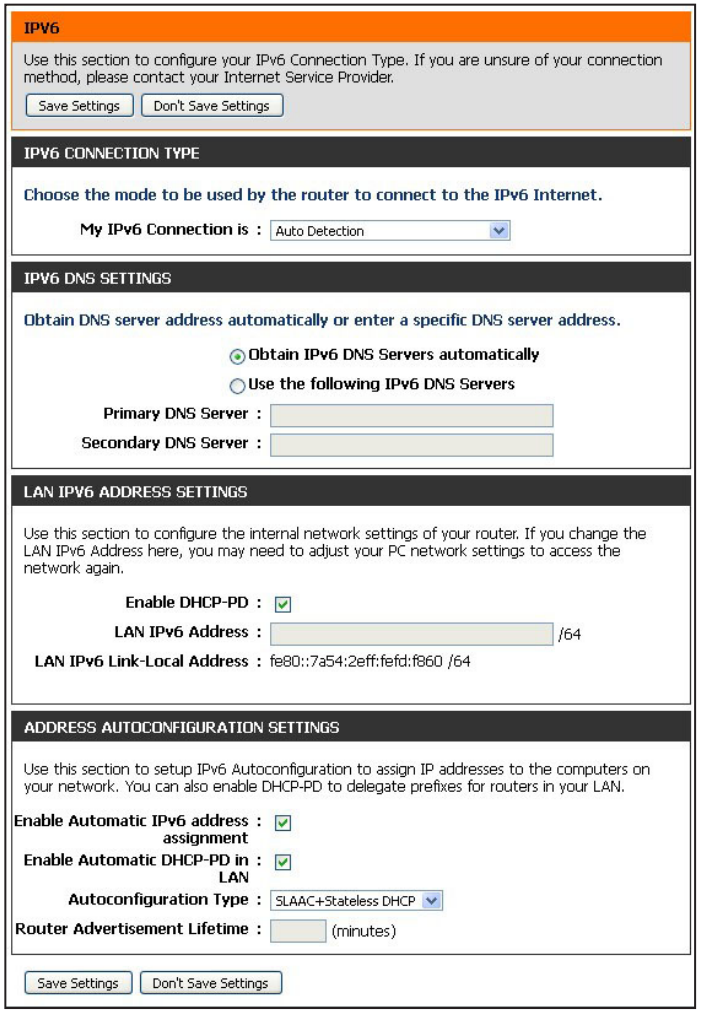
There are several connection types to choose from: **Auto Detection, Static IPv6, Autoconfiguration (SLAAC/DHCPv6), PPPoE, IPv6 in IPv4 Tunnel, 6to4, 6rd,** and **Local Connectivity Only**. If you are unsure of your connection method, contact your IPv6 Internet Service Provider (ISP).

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

Auto Detection

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

Click **Save Settings**.



Static IPv6

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

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

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

LAN IPv6 Link-Local Address: Displays the Router's *LAN IPv6 Link-Local Address*.

Enable Automatic IPv6 address assignment: Check to enable the Autoconfiguration feature.

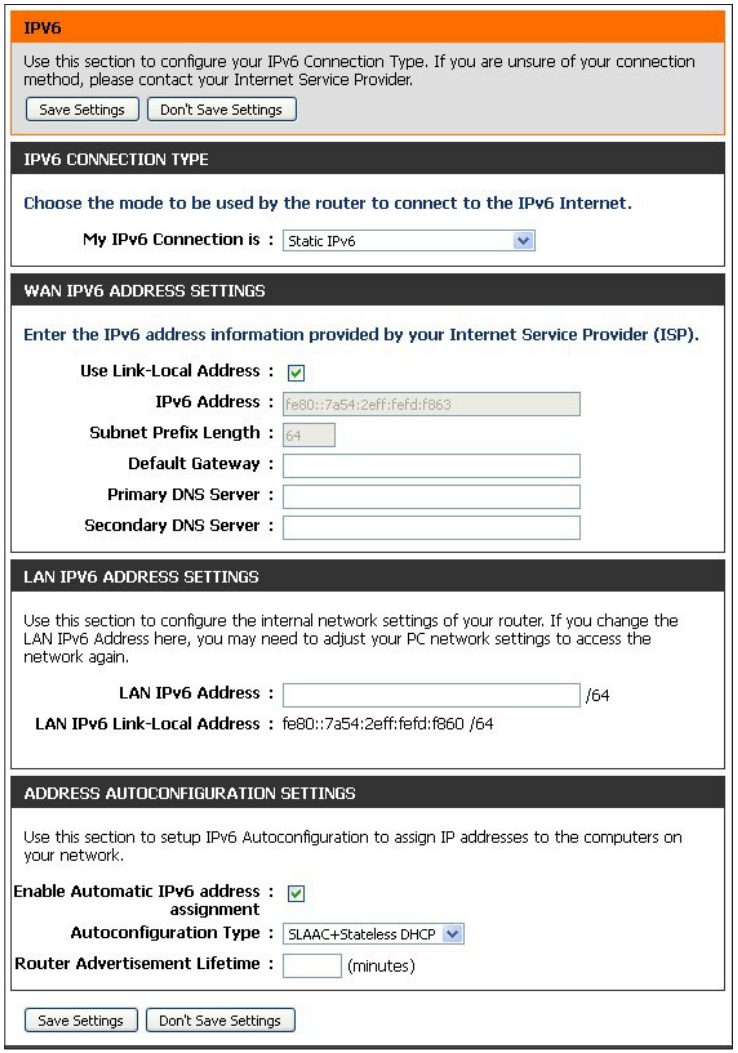
Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCP**.

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

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

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

Click **Save Settings**.



Autoconfiguration

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

IPv6 DNS Settings: Select either **Obtain IPv6 DNS Servers automatically** or **Use the following IPv6 DNS servers**.

Primary/Secondary IPv6 DNS Server: If you selected the second option above, enter the Primary and Secondary **DNS Server** addresses.

Enable DHCP-PD: Check this box to **Enable DHCP-PD** (prefix delegation).

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

LAN IPv6 Link-Local Address: Displays the Router's *LAN IPv6 Link-Local Address*.

Enable Automatic IPv6 address assignment: Check to enable the Autoconfiguration feature.

Enable Automatic DHCP-PD in LAN: Check this box to **Enable Automatic DHCP-PD in LAN**.

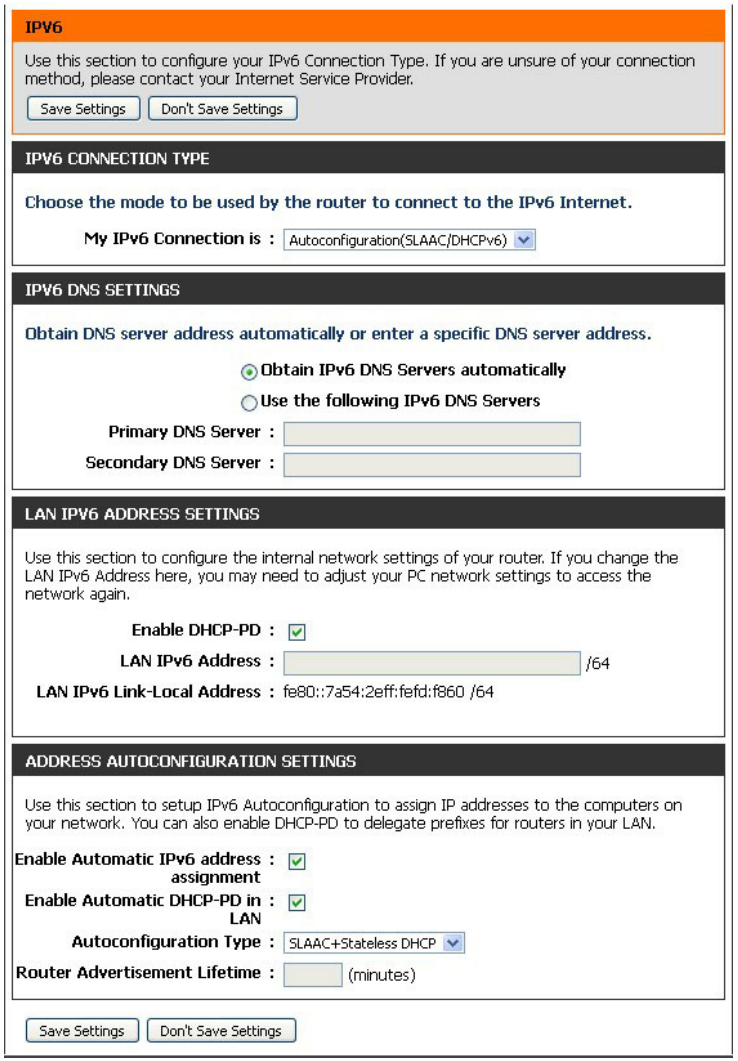
Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCP**.

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

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

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

Click **Save Settings**.



PPPoE

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

PPPoE Session: Select **Create a new session** if you have IPv6.

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

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

Username: Enter your PPPoE **Username**.

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

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

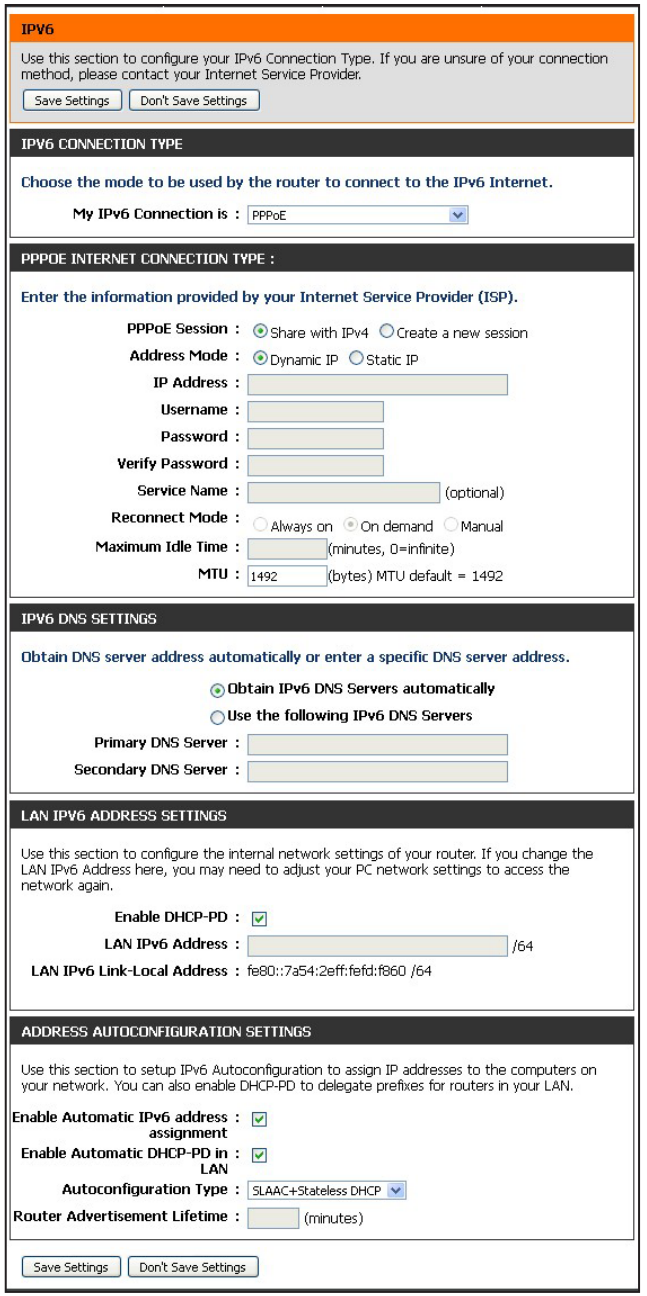
Reconnect Mode: Select either **Always-on**, **On-Demand**, or **Manual**.

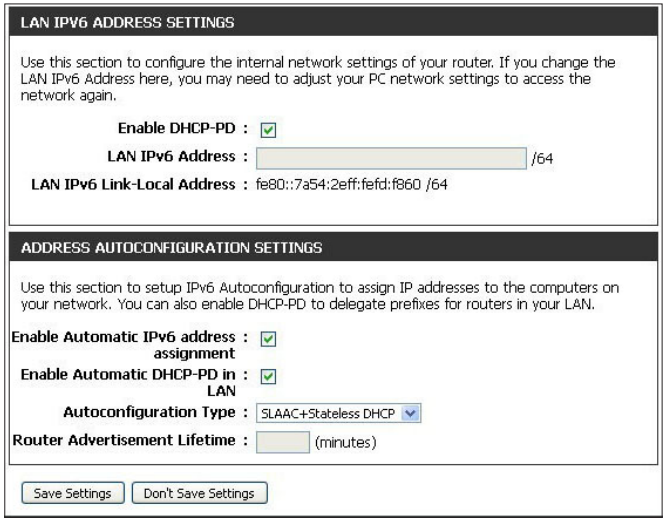
Maximum Idle Time: Enter a **Maximum Idle Time** during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

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

IPv6 DNS Settings: Select either **Obtain IPv6 DNS Servers automatically** or **Use the following IPv6 DNS servers**

Primary/Secondary IPv6 DNS Servers: If you selected the second option above, enter the Primary and Secondary **DNS Server** addresses.





Enable DHCP-PD: Check this box to **Enable DHCP** prefix delegation.

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

LAN IPv6 Link-Local Address: Displays the Router's *LAN IPv6 Link-Local Address*.

Enable Automatic IPv6 address assignment: Check to enable the IPv6 Autoconfiguration feature.

Enable Automatic DHCP-PD in LAN: Check to enable delegation of prefixes for router addresses.

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

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

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

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

Click **Save Settings**.

IPv6 in IPv4 Tunneling

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

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

IPv6 DNS Settings: Select either **Obtain IPv6 DNS Servers automatically** or **Use the following IPv6 DNS Servers.**

Primary/Secondary IPv6 DNS Servers: If you selected the second option above, enter the Primary and Secondary **DNS Server** addresses.

Enable DHCP-PD: Check this box to **Enable DHCP** prefix delegation.

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

LAN IPv6 Link-Local Address: Displays the Router's *LAN IPv6 Link-Local Address*.

Enable Automatic IPv6 address assignment: Check to enable the Autoconfiguration feature.

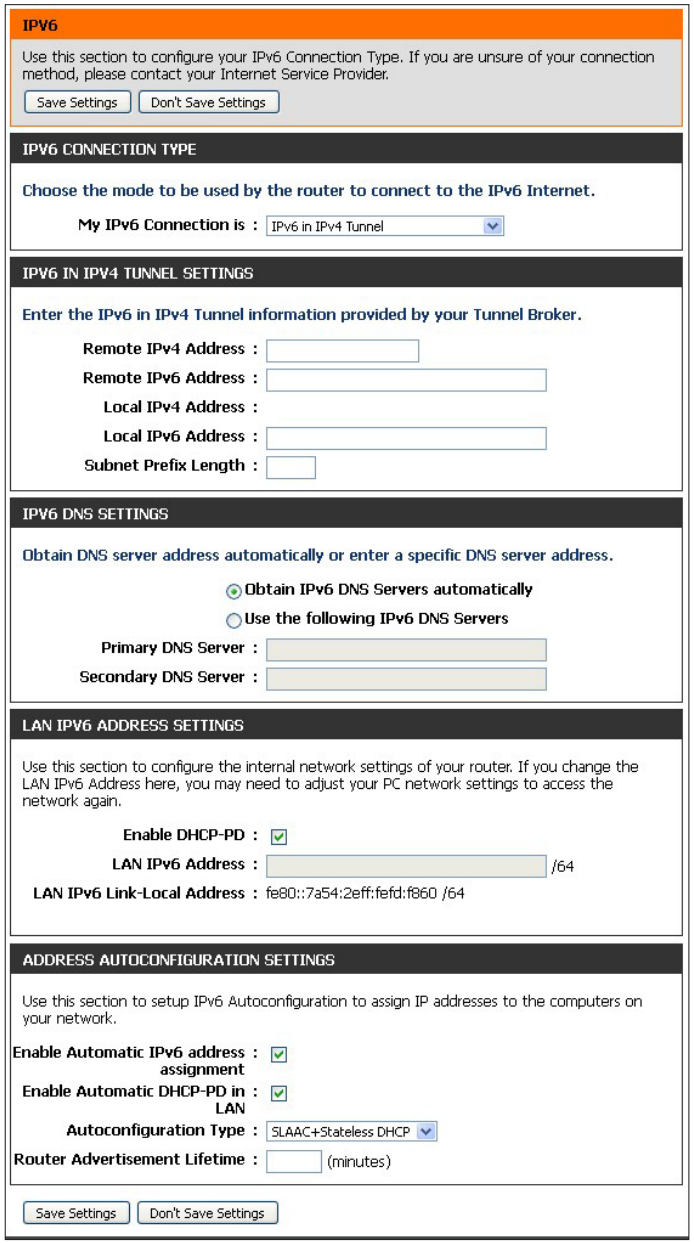
Enable Automatic DHCP-PD in LAN: Check to enable delegation of prefixes for router addresses.

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

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

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

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



6 to 4 Tunneling

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

WAN IPv6 Address Settings: Enter the IPv6 address information supplied by your Internet Service Provider (ISP).

Primary/Secondary IPv6 DNS Servers: Enter the Primary and Secondary **IPv6 DNS Server** addresses.

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

LAN IPv6 Link-Local Address: Displays the Router's *LAN IPv6 Link-Local Address*.

Enable Automatic IPv6 address assignment: Check the box to enable the Autoconfiguration feature.

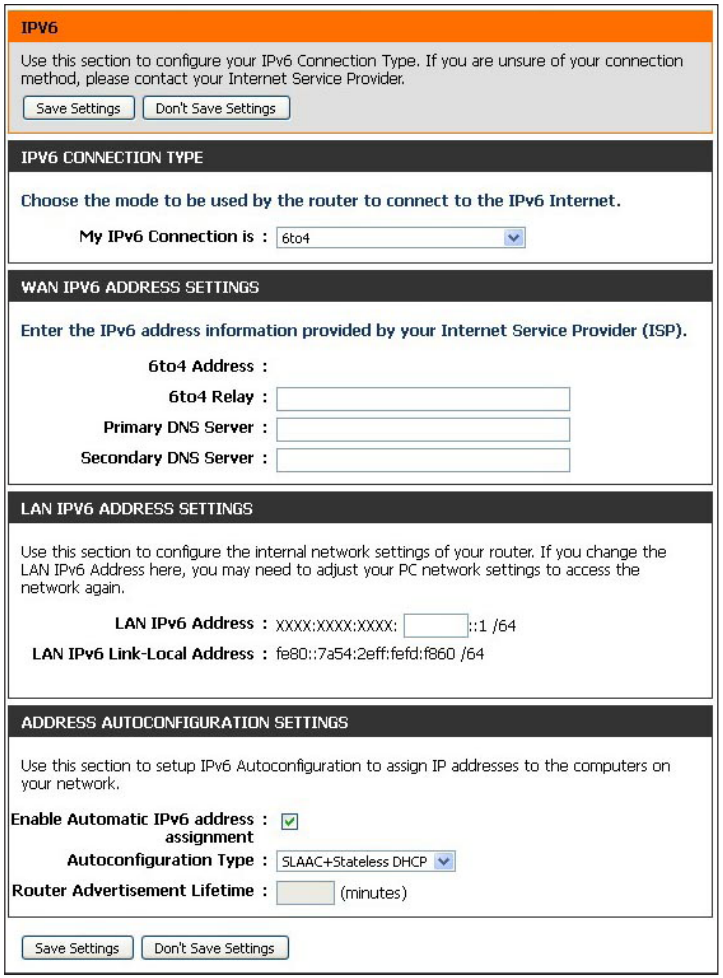
Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC + RDNSS** or **SLAAC + Stateless DHCP**.

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

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

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

Click **Save Settings**.



6rd

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

WAN IPv6 Address Settings: Enter the address information supplied by your Internet Service Provider (ISP).

Primary/Secondary IPv6 DNS Servers: Enter the Primary and Secondary **IPv6 DNS Server** addresses.

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

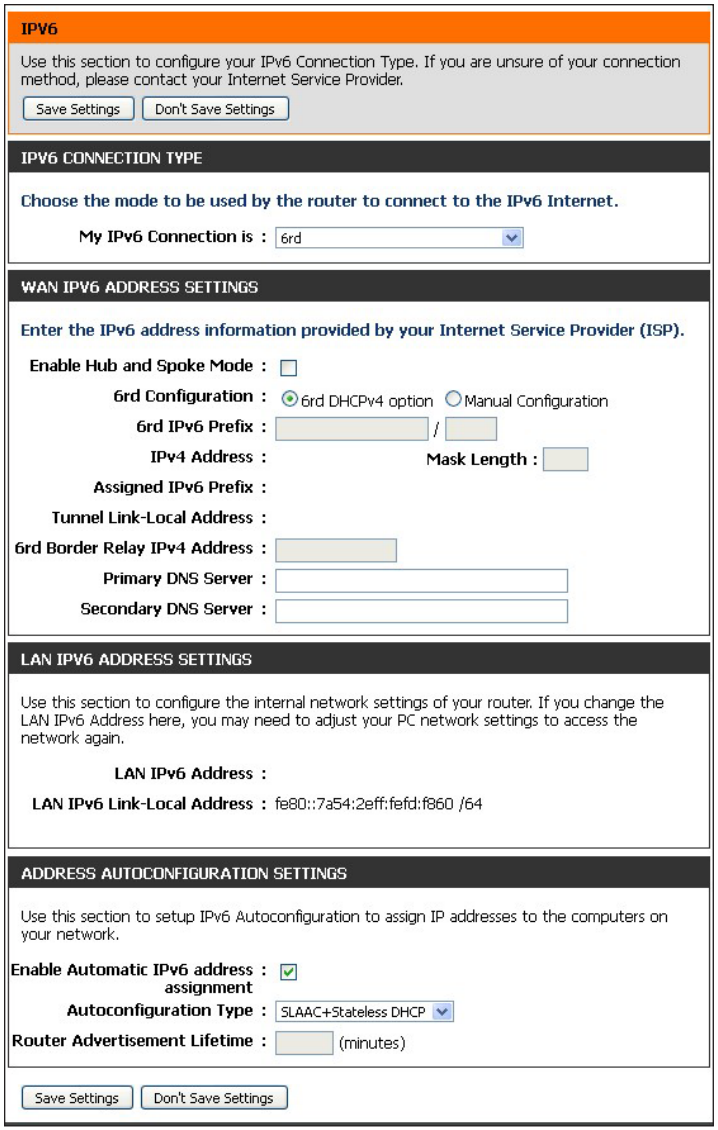
LAN IPv6 Link-Local Address: Displays the Router's *LAN IPv6 Link-Local Address*.

Enable Automatic IPv6 address assignment: Check the box to enable the Autoconfiguration feature.

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

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

Click **Save Settings**.

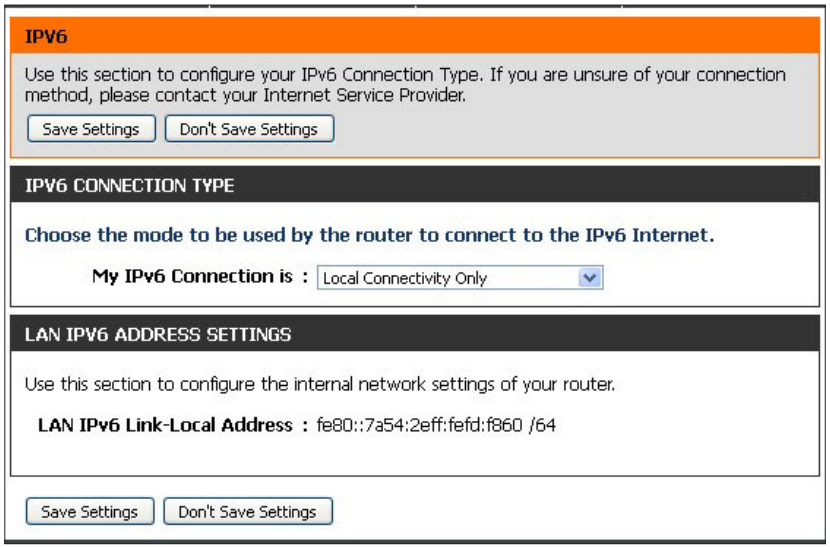


Local Connectivity

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

LAN IPv6 Link-Local Address: Displays the *LAN IPv6 Link-Local Address* of the router.

Click **Save Settings**.



Advanced

Virtual Server

If you disable UPnP™ (Universal Plug and Play), you will need to manually open ports or set up application rules for certain applications. Refer to your application's documentation or website for port information. The *Virtual Server* will allow you to open a single port. To open a range of ports, refer to *Port Forwarding* on the next page. *Application Rules* are covered on the page that follows.

Name: Enter a **Name** for the rule or select an **Application name** from the drop-down menu. When an **Application Name** is selected click **<<** to populate the field.

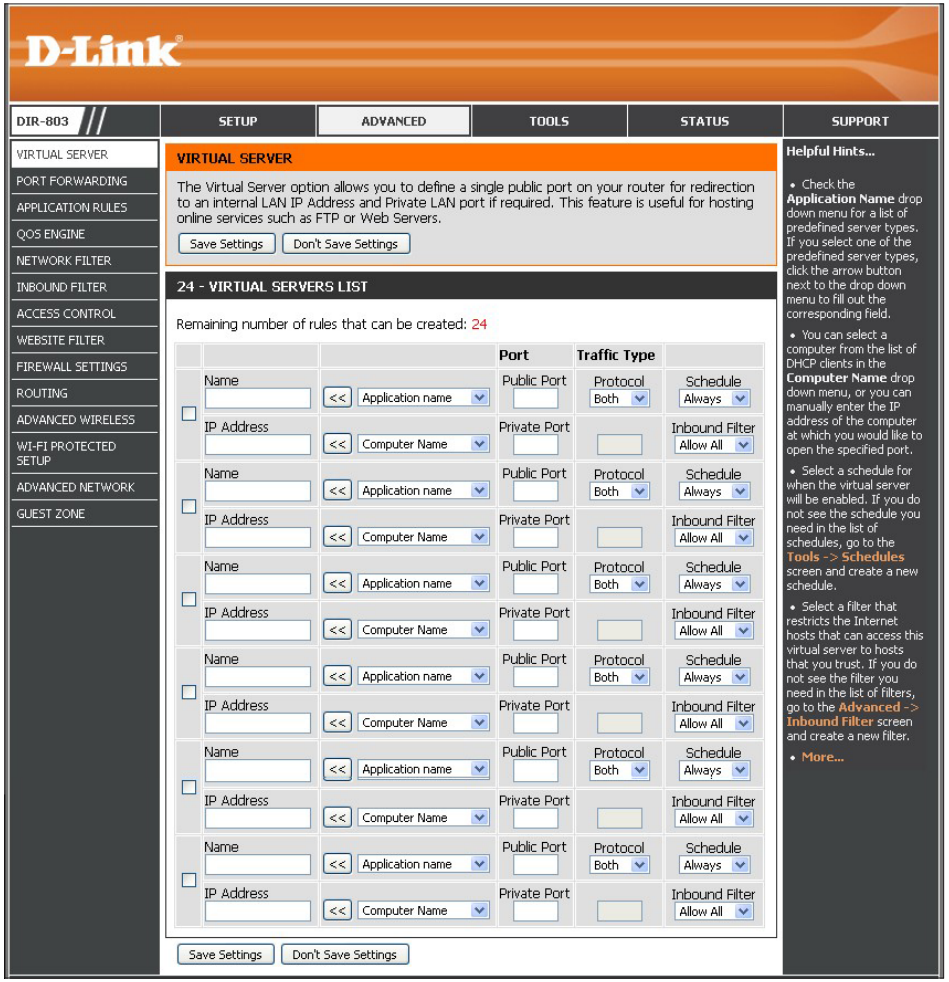
IP Address: Enter the **IP Address** of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the **Computer Name** drop-down menu. Select your computer and click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

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

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

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

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



Port Forwarding

If you disable UPnP™ (Universal Plug and Play), you will need to manually open ports or set up application rules for certain applications. Refer to your application's documentation or website for port information. *Port Forwarding* will allow you to open a single port or a range of ports in your router for specific applications. (*Application Rules* are covered in the next section.)

Name: Enter a **Name** for the rule or select an **Application Name** from the drop-down menu. When an **Application Name** is selected, click **<<** to populate the field.

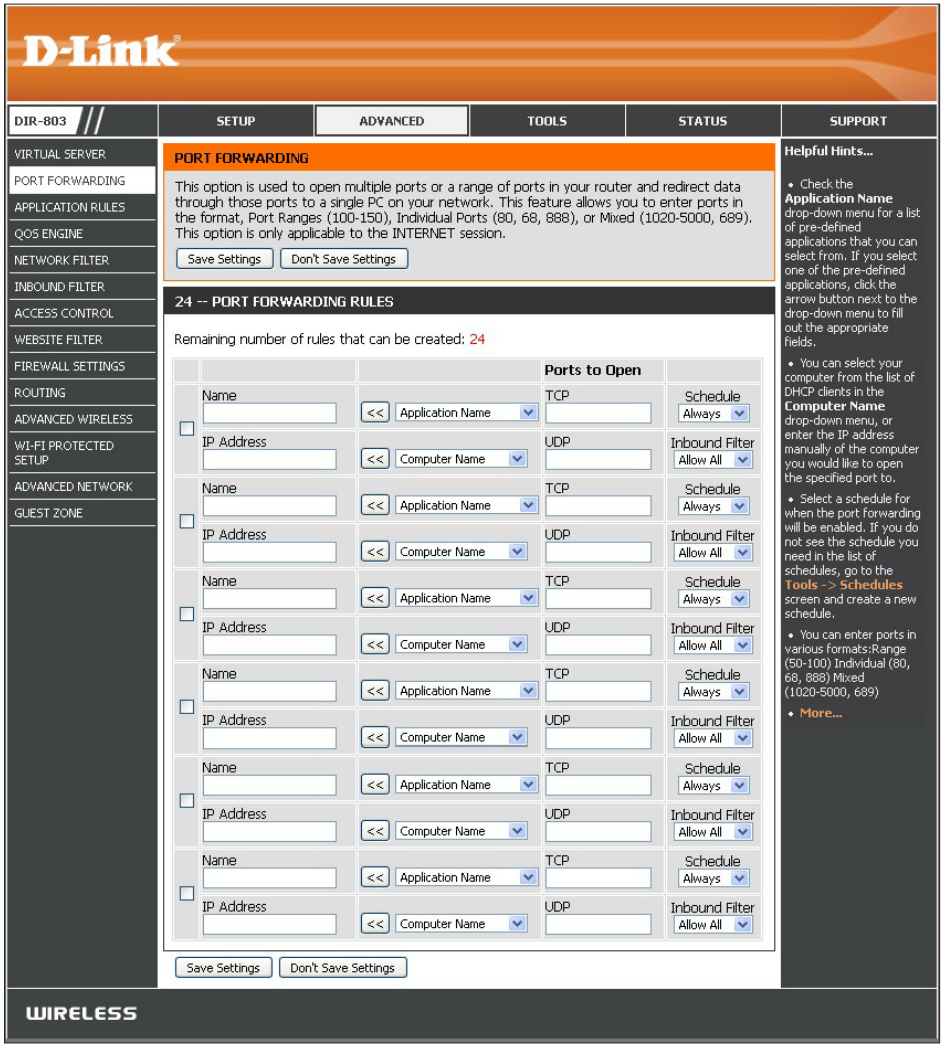
IP Address: Enter the **IP Address** of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the **Computer Name** drop-down menu. Select your computer and click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

Ports to Open TCP/UDP: Enter the **TCP** and/or **UDP** port or ports that you want to open. You can enter a single port or a range of ports. Separate ports with a comma.

Example: 24,1009,3000-4000

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

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



Application Rules

If you disable UPnP™ (Universal Plug and Play), you will need to manually open ports or set up application rules for certain applications. Refer to your application's documentation or website for port information. (Opening ports is covered in the preceding pages, under *Virtual Server* and *Port Forwarding*.)

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 **Traffic Type** as **TCP** or **UDP**, then enter the **Firewall** (public) **Port**(s) associated with the **Trigger Port** to open them for inbound traffic.

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

Note: *The DIR-803 provides some predefined applications that you can select from.*

Trigger: This is the port used to trigger the application. You can enter 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.

Example: 24,1009,3000-4000

Traffic Type: Select the protocol of each Trigger and Firewall Port (**TCP**, **UDP**, or **Both**).

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

QoS Engine

Quality of Service (QoS) assigns priority to specified applications, providing better performance of data flow. The QoS Engine option helps improve your network gaming experience by prioritizing your game traffic over other network traffic, like FTP. For most applications, automatic classification will be adequate, and specific QoS Engine Rules are not required.

Enable QoS: This option is disabled by default. Check the box to enable this option for providing better performance with online games and other interactive applications, such as VoIP.

Uplink Speed: This field displays the data transfer rate from the router to your Internet Service Provider (ISP). When the *Enable QoS* option is checked, this will allow you to enter the **Uplink Speed** manually, or select a rate from the drop-down menu that says **Select Transmission Rate**.

Downlink Speed: This field displays the speed at which data can be transferred from the Internet to your router. This is determined by your ISP.

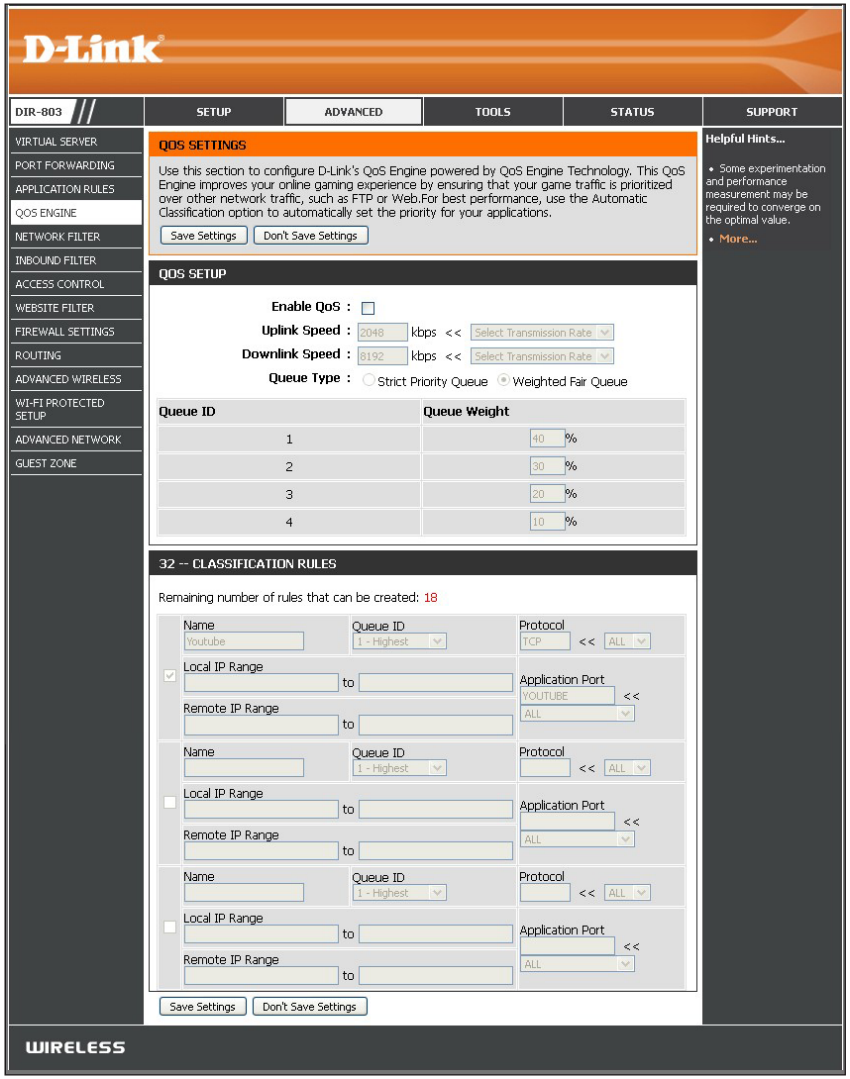
Queue Type: Select either **Strict Priority Queue** (based on traffic priority) or **Weighted Fair Queue** (based on queue weight, by percentage).

Queue ID: The Queue ID that is used will be shown in the first column.

Queue Priority: When *Strict Priority Queue* is selected, the *Queue Priority* will be displayed in the second column

Queue Weight: When *Weighted Fair Queue* is selected, you will be able to manually enter the percentages for the Queue Weight in the second column for each Queue ID.

Classification Rules: The QoS Engione supports overlaps between rules, where more than one rule can match for a specific message flow. If more than one rule is found to match, the rule with the highest priority will be used.



Name: Create a **Name** that is meaningful to you for the rule.

Queue ID: The **Priority** of the message flow is entered here -- 1 receives the highest priority (most urgent) and 255 receives the lowest priority (least urgent).

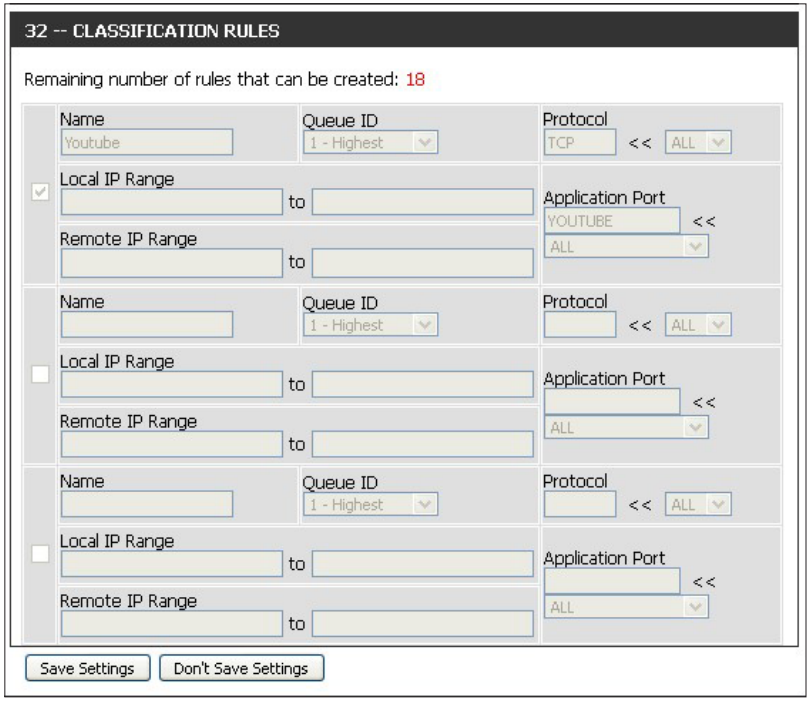
Protocol: The **Protocol** used by the messages.

Local IP Range: The rule applies to a flow of messages whose LAN-side IP address falls within the range set here.

Remote IP Range: The rule applies to a flow of messages whose WAN-side IP address falls within the range set here.

Application Port: Select an **Application Port** from the drop-down menu and click <<.

Click on **Save Settings**.



Network (MAC) Filters

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

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

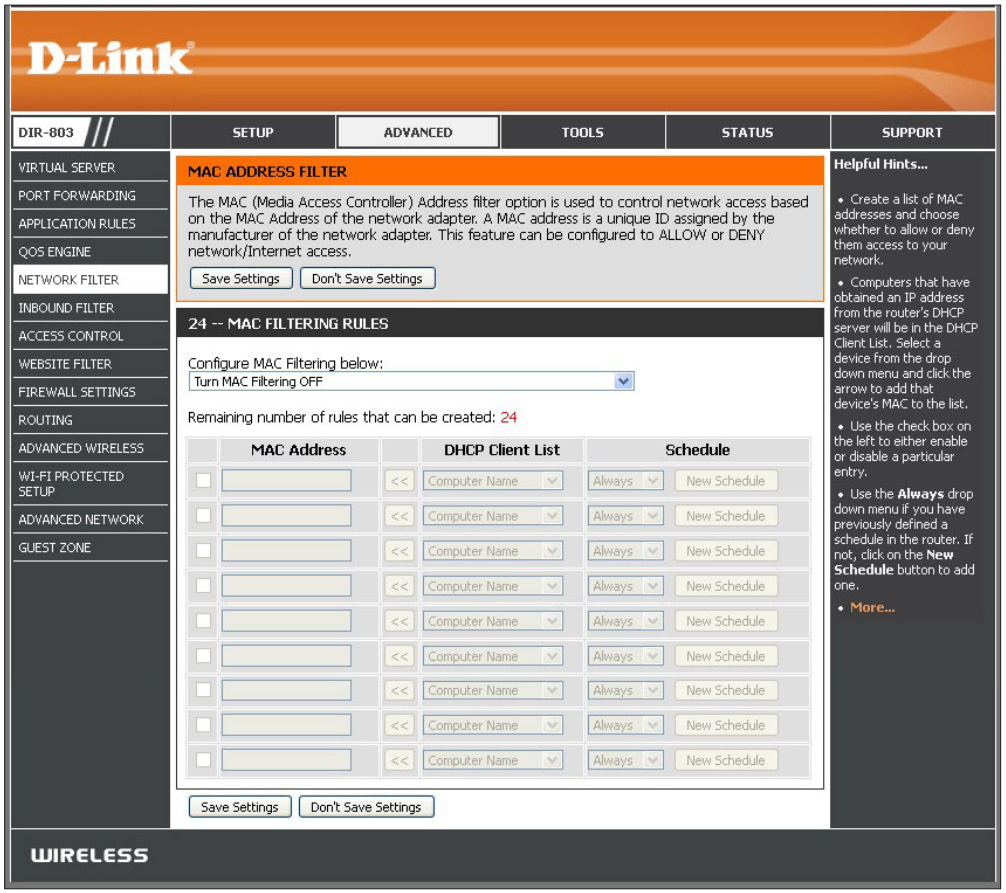
MAC Address: Enter the **MAC Address** you would like to filter, or select from the DHCP Client List (see below).

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

DHCP Client List: Devices that have obtained an IP address from the router's DHCP server will be in the **DHCP Client List**. Select a **DHCP Client** from the drop-down menu and click **<<** to copy that device's MAC Address.

Schedule: The schedule may be set to **Always**, which will allow the filtering to always be enabled. Use the drop-down menu to select a pre-defined a schedule in the router. Or, you can click on **New Schedule** to add one.

Click **Save Settings**.



Inbound Filters

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

Name: Enter a **Name** that is meaningful to you for the inbound filter rule.

Action: You may choose to **Allow** or **Deny** access.

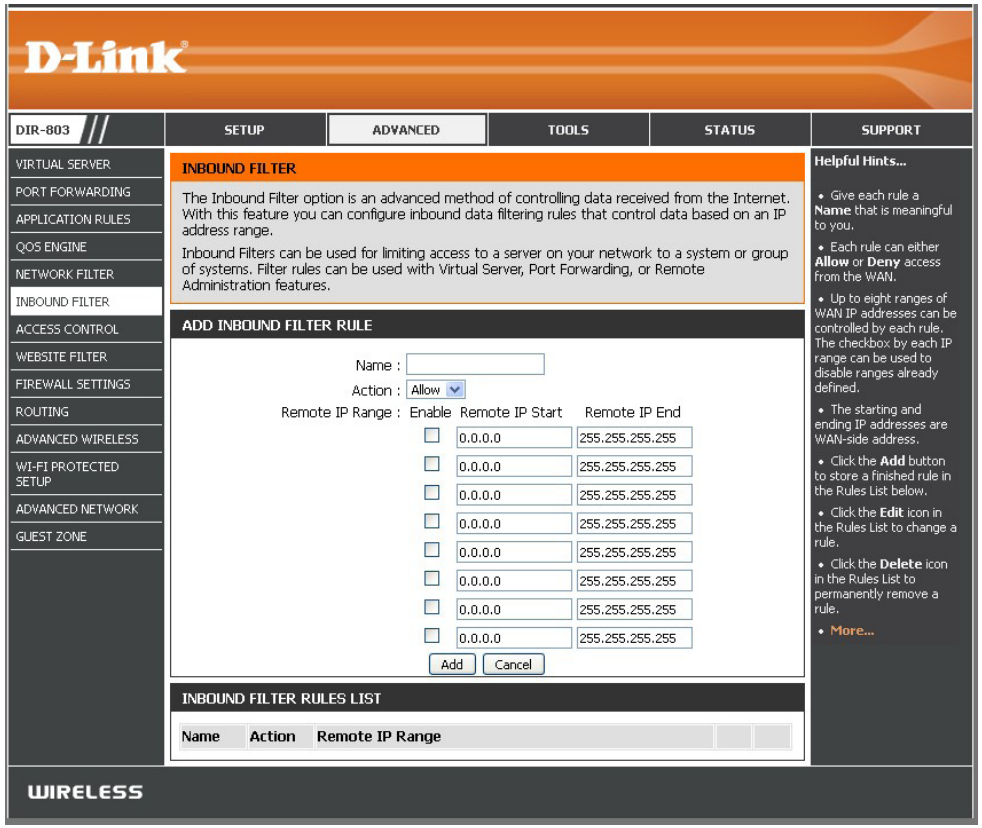
Remote IP Range: Enable: Check to **Enable** rule.

Remote IP Start: Enter the starting WAN-side IP address.

Remote IP End: Enter the ending WAN-side IP address.

Add: Click the **Add** button to apply your settings. The rule will appear in the *Inbound Filter Rules List* below.

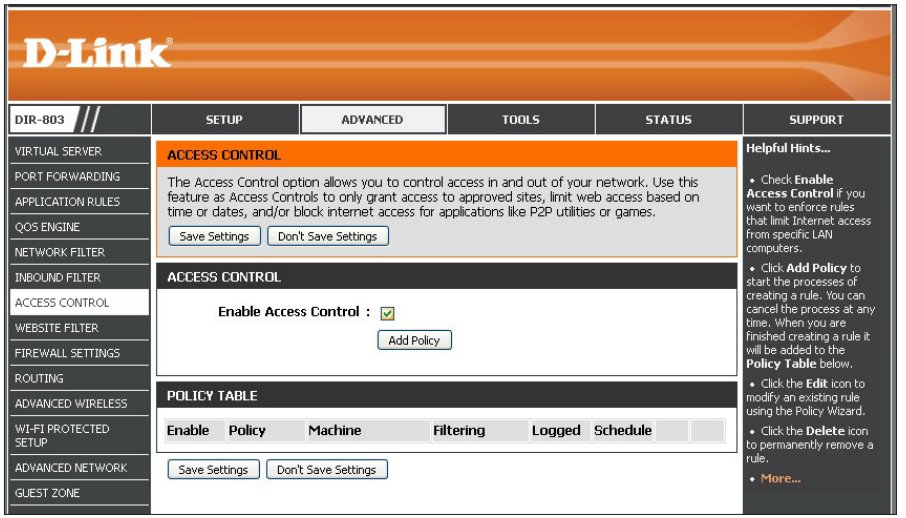
Inbound Filter Rules List: This section will list all rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Trash** icon to permanently delete the rule.



Access Control

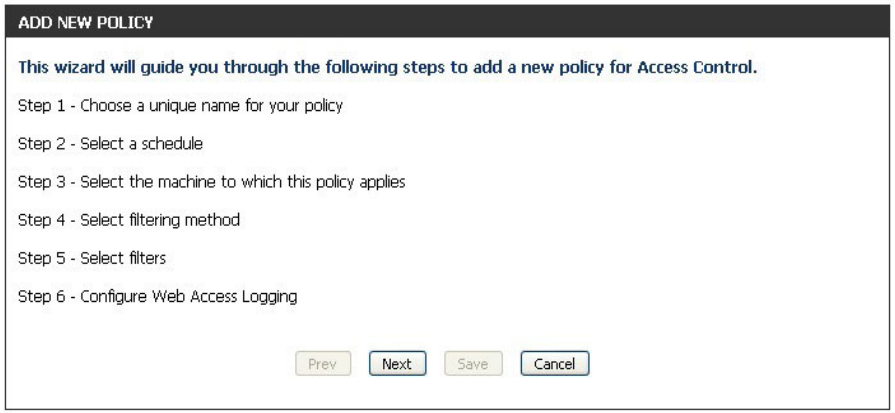
The Access Control section allows you to control access in and out of your network. Use this feature to set up parental controls. Grant access only to approved sites, limit web access based on times or dates, and/or block access from applications like P2P utilities or games.

Enable Access Control: Check the **Enable Access Control** box, and then click on **Add Policy** to start the wizard.



Access Control Wizard

The wizard will guide you through a step-by-step process for creating a rule. Click **Next** to continue.



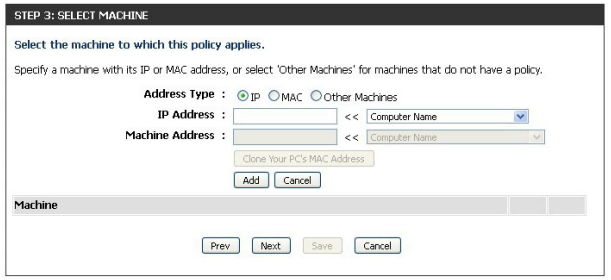
Enter a name for the policy and then click **Next** to continue.

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

Enter the following information:

- **Address Type** - Select **IP**, **MAC**, or **Other Machines**.
- **IP Address** - Enter the **IP Address** of the computer you want to apply the rule to, or select **Computer Name** and click <<.
- **Machine Address** - Enter the PC MAC address or click on **Clone Your PC's MAC Address**.

Click **Add,** and click **Next** to continue.



Select a filtering method from **Log Web Access Only**, **Block All Access** or **Block Some Access**. Click **Save**.

If you choose **Block Some Access**, check **Apply Web Filter** and/or **Apply Advanced Port Filters**.

Click **Next** to continue.

If you checked *Apply Advanced Port Filters*, add **Port Filter Rules**:

Enable - Check to **Enable** the rule.

Name - Enter a **Name** for your rule.

Dest IP Start - Enter the starting IP address.

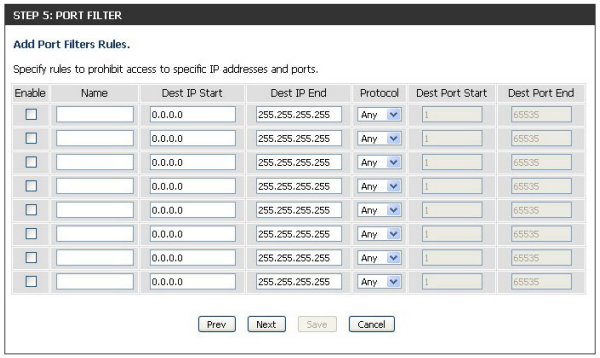
Dest IP End - Enter the ending IP address.

Protocol - Select the **Protocol** from the drop-down list.

Dest Port Start - Enter the starting port number.

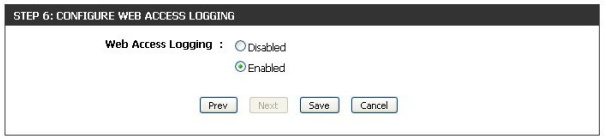
Dest Port End - Enter the ending port number.

Click **Next.**

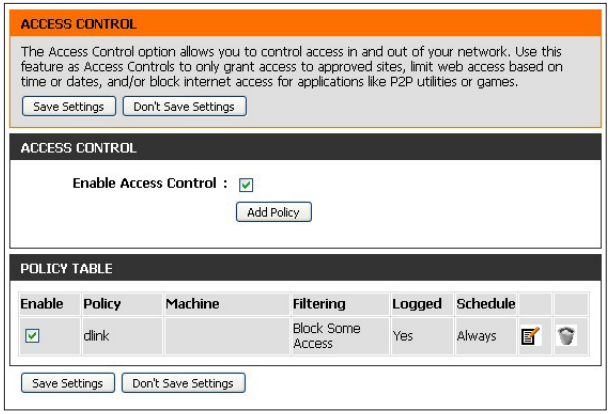


To enable **Web Access Logging**, click **Enabled**.

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



Your newly created policy will now show up under *Policy Table*. You may click the **Edit** icon to change the policy, or click the **Trash** icon to delete the policy.

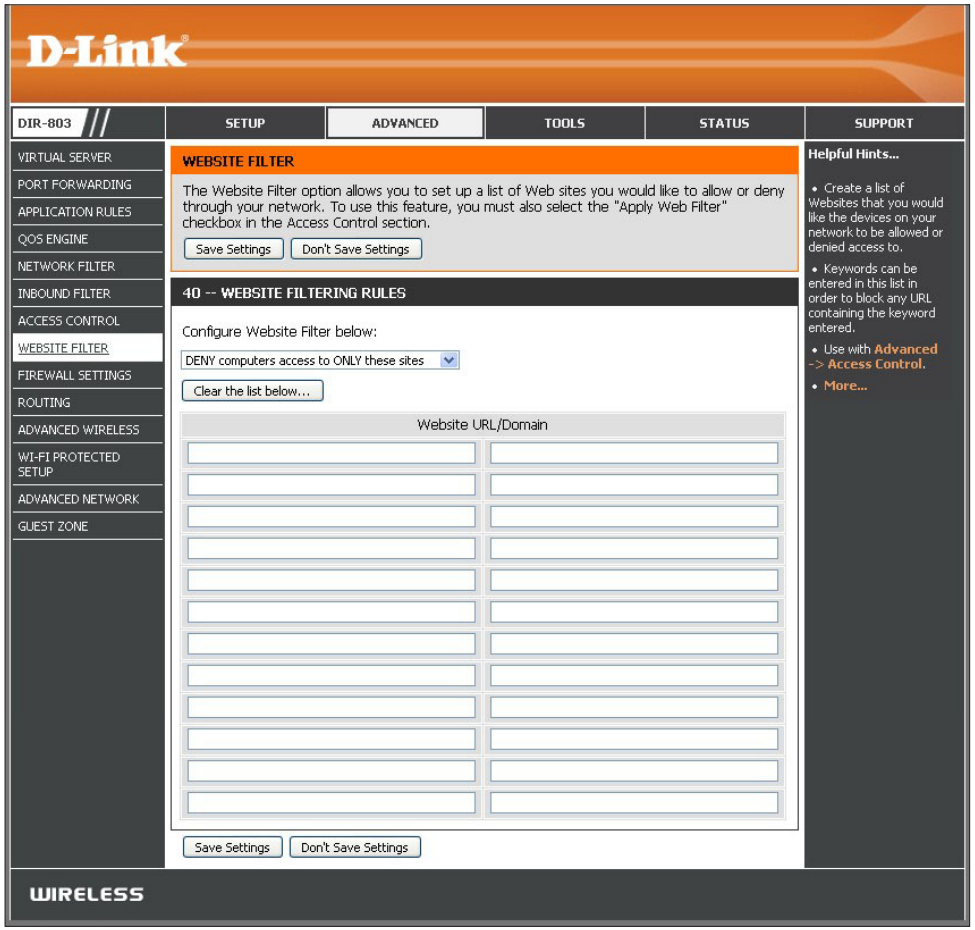


Website Filters

Website Filters are available for you to set up a list of Websites that users on your network can be allowed to view or denied access to. To use this feature select to **Allow** or **Deny**, enter the domain or website, and click **Save Settings**. Make sure you also select **Apply Web Filter** under the *Access Control* section. (Refer to "Access Control" on page 73).

Configure Website Filter: 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-803 offers a firewall type functionality. The SPI (Stateful Packet Inspection) feature helps prevent cyber attacks. There may be times when you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ.

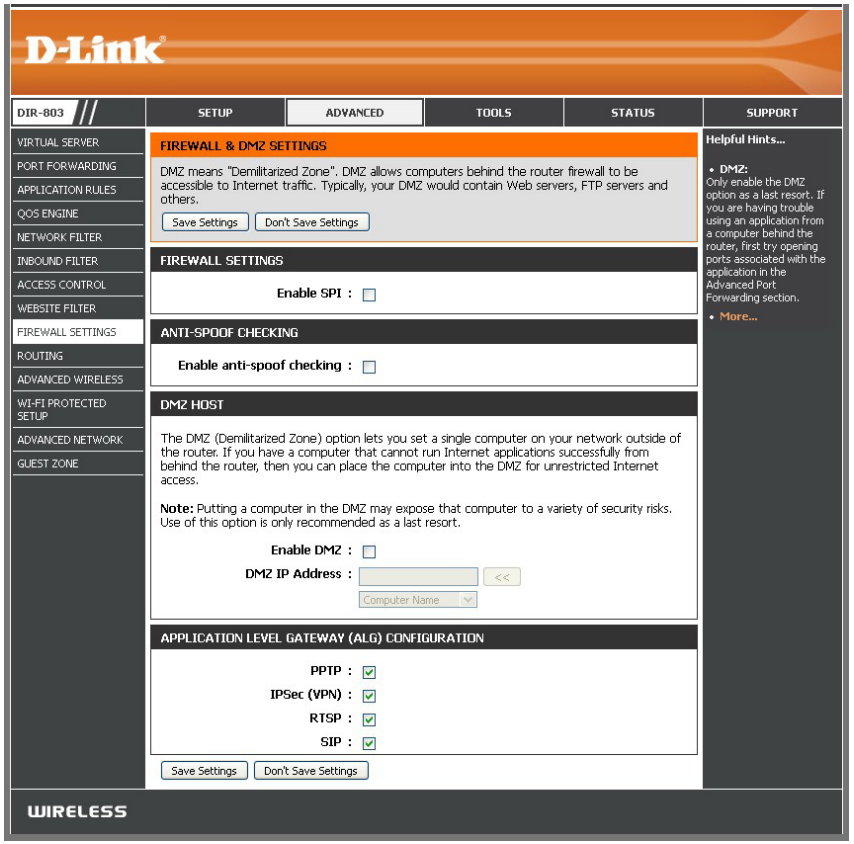
Enable SPI: SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol.

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

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

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

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



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

IPSec (VPN): Allows multiple **VPN** (Virtual Private Network) clients to connect to their corporate network using **IPSec** (Internet Protocol Security). Some VPN clients support traversal of IPSec through NAT (Network Address Translation). This ALG (Application Level Gateway) may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Check with the system administrator of your corporate network whether your VPN client supports NAT traversal.

RTSP: Allows application that uses **RTSP** (Real Time Streaming Protocol) to receive streaming media from the Internet. QuickTime and Real Player are some of the common applications using this protocol.

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

Click **Save Settings**.

Routing

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

Name: Enter a **Name** for your route.

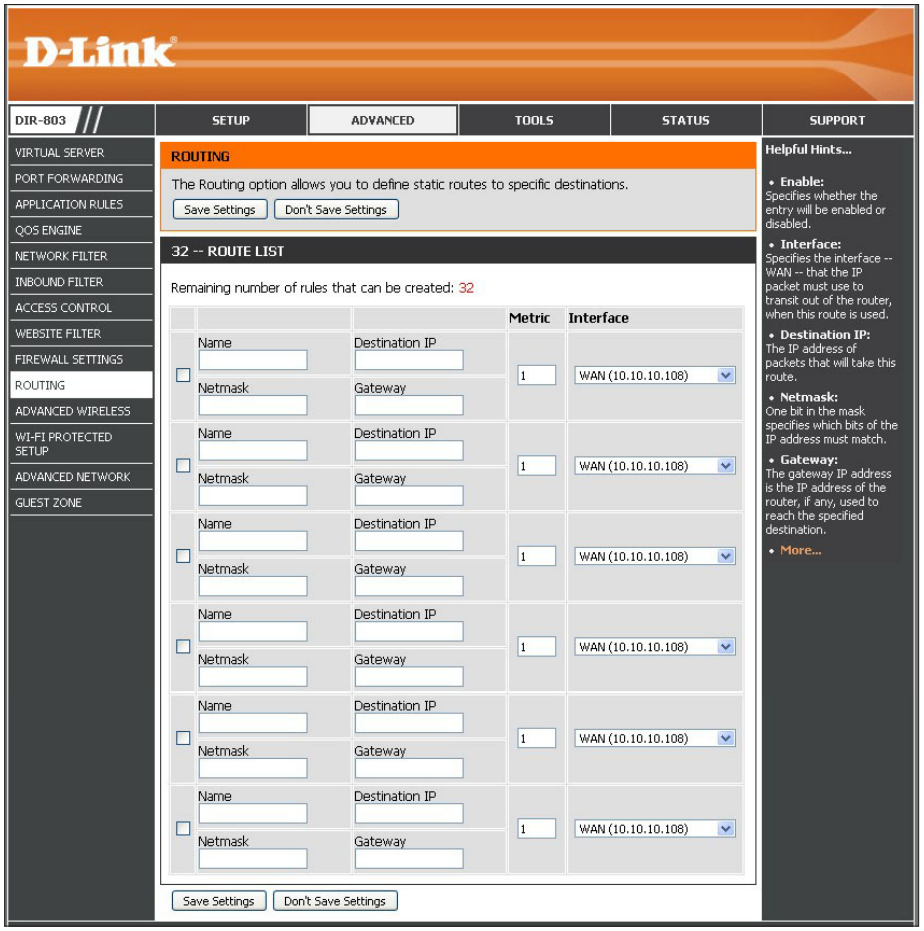
Destination IP: Enter the IP address of packets that will take this route.

Netmask: Enter the **Netmask** of the route, please note that the octets must match your destination IP address.

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

Metric: The route **Metric** is a value from 1 to 16 that indicates the cost of using this route. A value 1 is the lowest cost and 15 is the highest cost.

Interface: Select the **Interface** that the IP packet must use to transit out of the router when this route is used.



Advanced Wireless

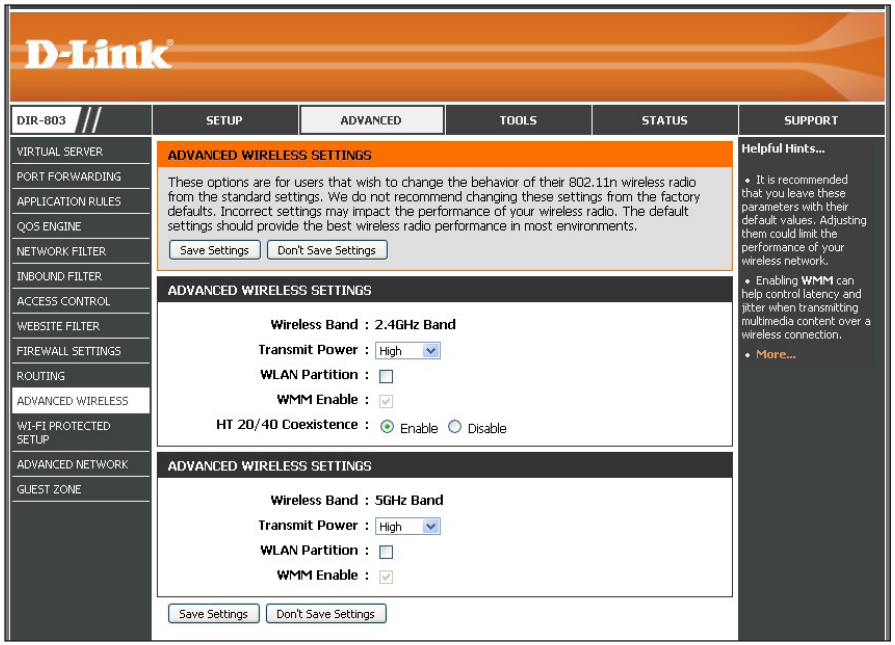
The Advanced Wireless options are available for users who wish to deviate from standard settings.

Transmit Power: Select the transmit power of the antennas from the drop-down list.

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

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

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



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 eight-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: Click to **Enable** the Wi-Fi Protected Setup feature.

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

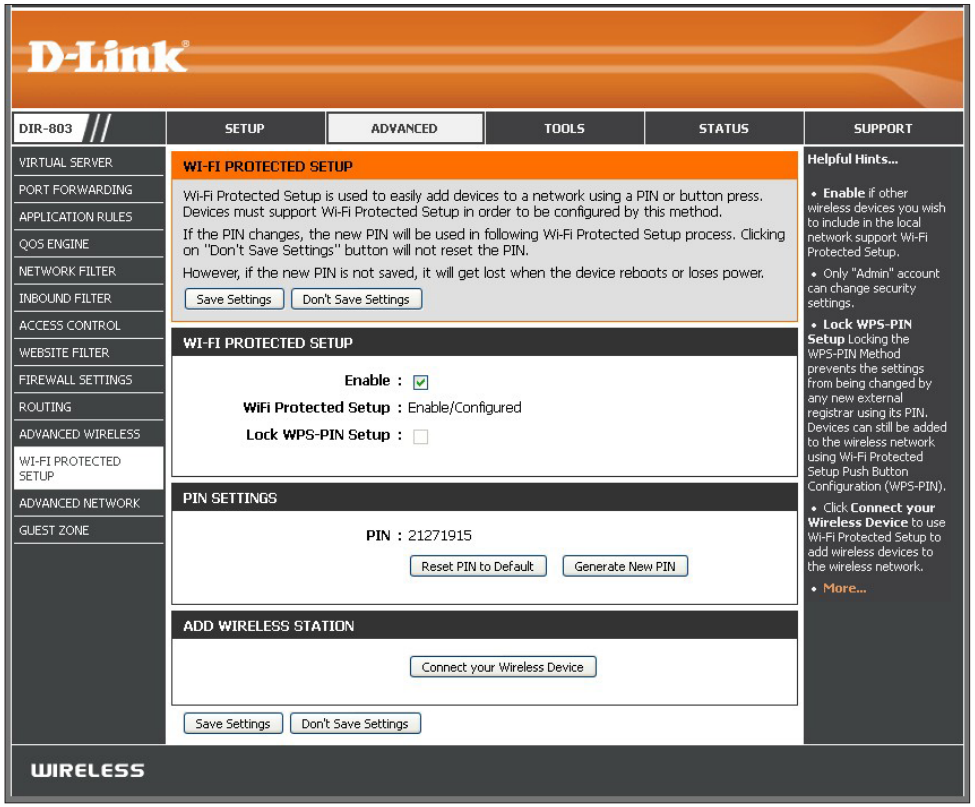
Lock WPS-PIN Setup: Locking the WPS-PIN method prevents the settings from being changed by any external registrar using its PIN. Devices can still be added to the wireless network using the Wi-Fi Protected Setup Push Button Configuration (WPS-PBC). It is still possible to change wireless networks settings 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.

PIN: Displays the current *PIN*.

Reset PIN to Default: Click to restore the default PIN of the router.

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



Add Wireless Station: This section gives you access to a Wizard that helps you add wireless devices to the wireless network.

The wizard will prompt you to select a configuration method. It will guide you through manual configuration, or allow you to choose between the Push Button (PBC) and PIN methods. If the device supports Wi-Fi Protected Setup and has a WPS button, you can add it to the network by pressing the WPS button on the device and then the on the router within 60 seconds.

Add Wireless Device with WPS: Click to start the wizard and refer to "Add Wireless Device with WPS Wizard" on page 38.

WPS Button

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

Refer to "WPS Button" on page 103 for more information about WPS.

Advanced Network Settings

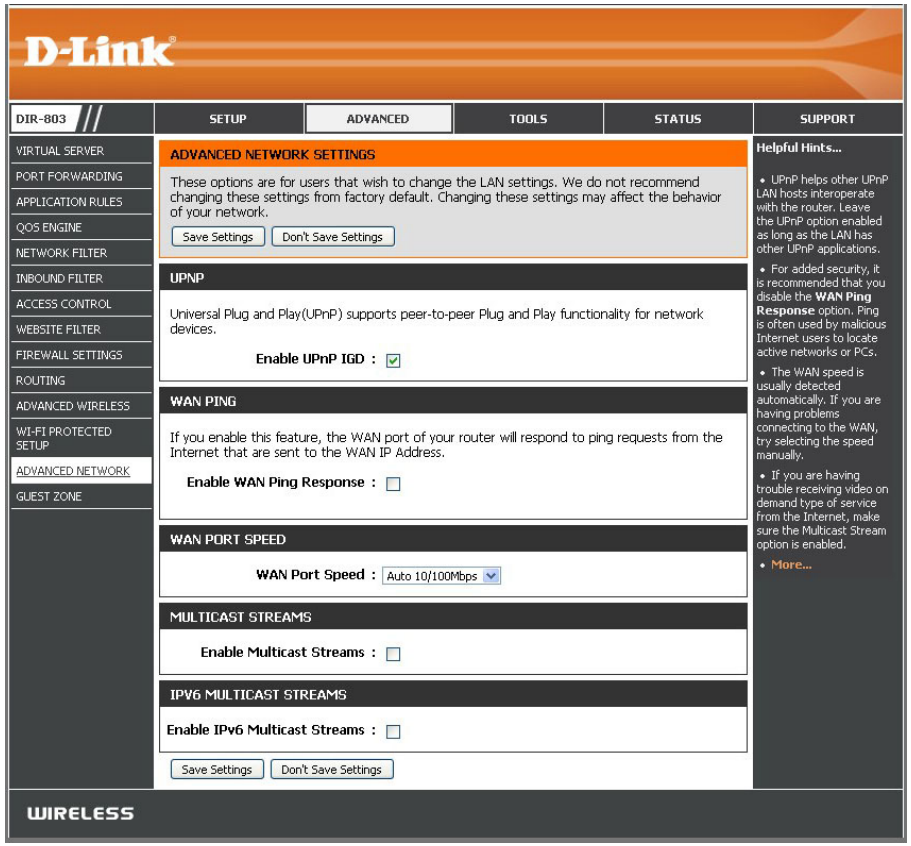
Enable UPnP IGD: **UPnP** Universal Plug and Play) allows the router to automatically open ports. For maximum security, uncheck to disable this feature. However, you will need to manually open ports for certain applications. Refer to "Port Forwarding" on page 67 and "Application Rules" on page 68.

Enable WAN Ping Response: Checking this box will allow the DIR-803 to respond to pings. Unchecking the box may provide some extra security from hackers.

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

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

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



Guest Zone

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

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

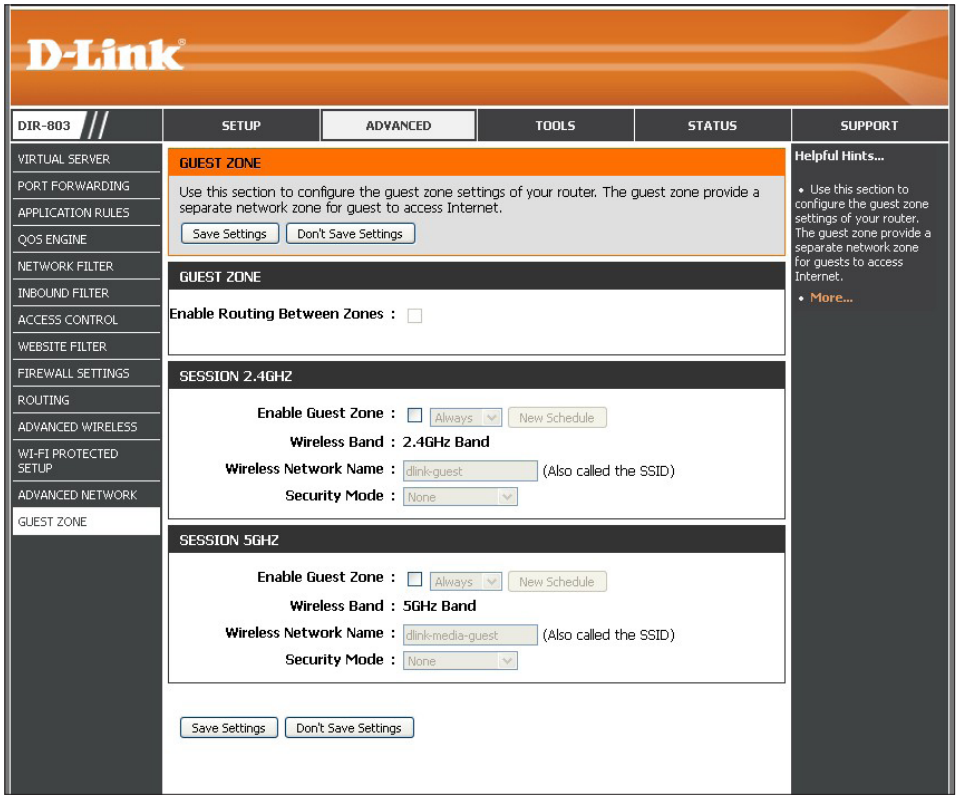
Enable Guest Zone: Check the box to enable the Guest Zone feature.

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

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

Security Mode: Select a **Security Mode** from the drop-down menu.

Click **Save Settings**.



Tools

Admin

This page will allow you to change the Administrator password and also enable Remote Management.

Password: Enter a new **Password** for the Administrator login. Enter again to verify.

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

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

Enable Remote Management: Remote management allows the DIR-803 to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

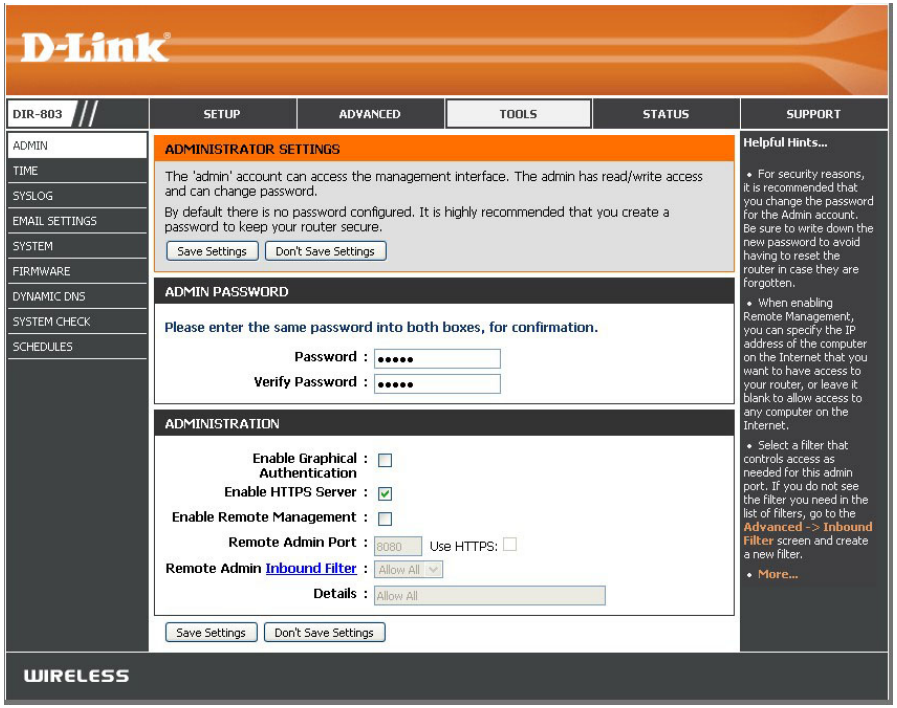
Remote Admin Port: The port number used to access the DIR-803 is used in the URL. Example: **http://x.x.x.x:8080** whereas x.x.x.x is the Internet IP address of the DIR-803 and 8080 is the port used for the Web Management interface.

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

Remote Admin Inbound Filter: Select **Allow All** or **Deny All** from the drop-down menu.

Details: This field will display the current remote admin filter.

Click **Save 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 and set the NTP (Network Time Protocol) Server. An NTP server will sync the time and date with your router. Daylight Saving can also be configured to automatically adjust the time when needed.

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

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

Enable Daylight Saving: Check to enable manual entry of daylight saving time.

Daylight Saving Offset: When daylight saving manual entry is enabled, the offset value is one hour by default.

Daylight Saving Dates: Enter a **DST Start**, and **DST End**. Select **Month**, **Week**, **Day of Week**, and **Time** for daylight saving time.

Automatically synchronize with D-Link's Internet time server: This option is strongly recommended. Check the box to synch the date and time with D-Link's Internet time server.

NTP Server Used: Select an **NTP Server** from the drop-down menu and click **Update Now**.

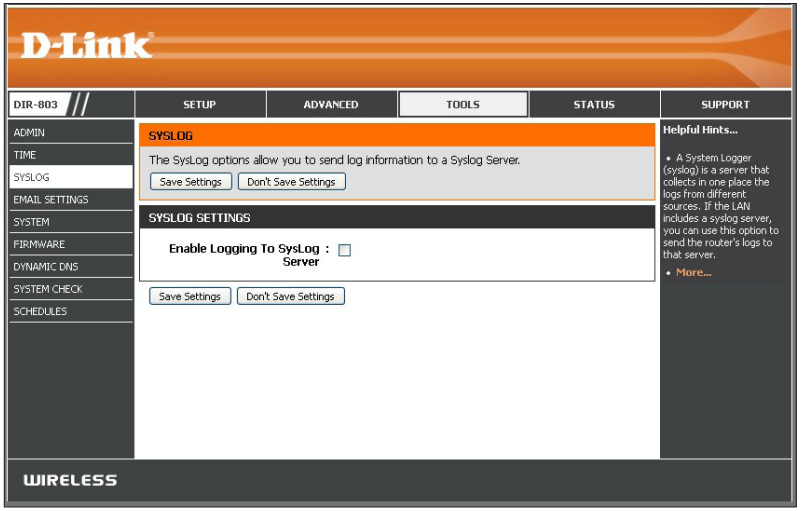
Date and Time: To manually input the **Date** and **Time**, enter the values in these fields for the **Year**, **Month**, **Day**, **Hour**, **Minute**, and **Second**.

Click **Save Settings**.

SysLog

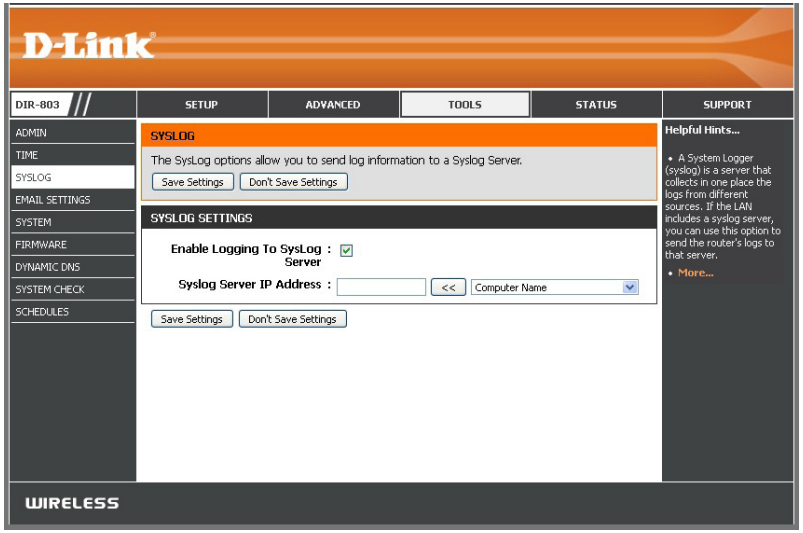
The DIR-803 keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server, which is a server that collects logs from different sources. It serves as a central repository.

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



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

Click **Save Settings**.



Email Settings

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

Enable Email Notification: When this option is enabled, router activity logs are sent to a designated e-mail address.

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

To Email Address: Enter the e-mail address where you want the email sent.

Email Subject: Enter a subject line for your e-mail.

SMTP Server Address: Enter the **SMTP Server Address** for sending e-mail.

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

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

Account Name: Enter your account for sending e-mail.

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

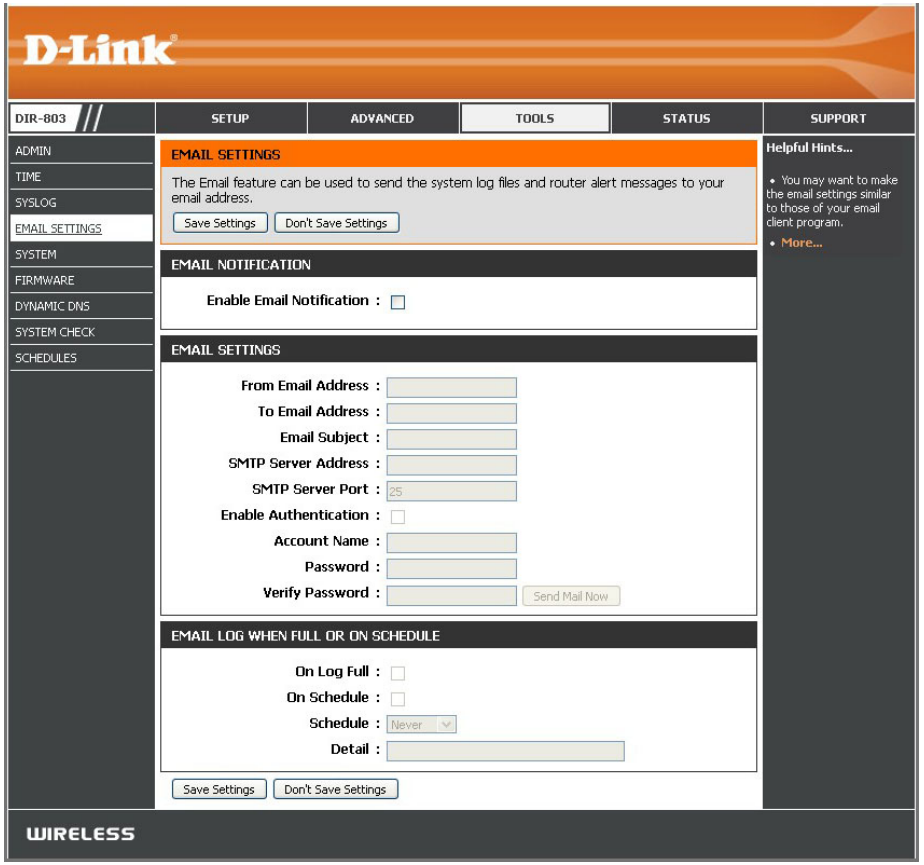
On Log Full: When this option is selected, logs will be sent via e-mail to your account when the log is full.

On Schedule: Selecting this option will send the logs via e-mail according to schedule.

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

Details: Detail will display selected schedule.

Click **Save Settings**.



System

This section allows you to save 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.

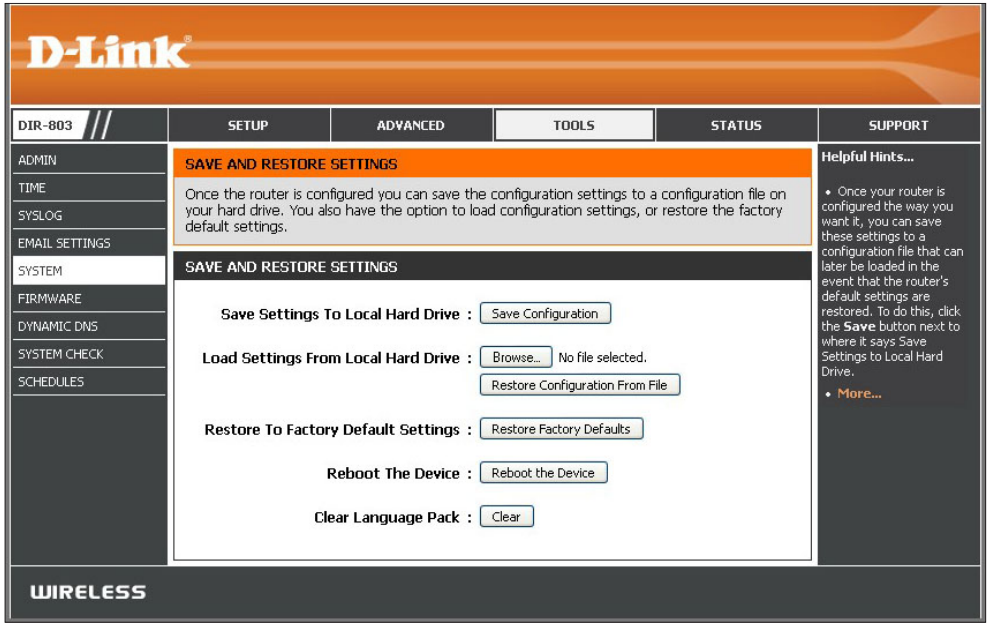
Save Settings to Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save Configuration** button. A file dialog will appear, allowing you to select a location and file name for the settings.

Load Settings from Local Hard Drive: Use this option to load previously saved router configuration settings. First, click the **Browse** button to locate a previously saved file 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. If you want to save the current router configuration settings, use the **Save Configuration** button above.

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

Clear Language Pack: Click on **Clear** to delete the Language Pack. Refer to "Firmware" on page 90 for Language Pack upgrade instructions.



Firmware

You can check for firmware updates and upgrade the firmware for your router here. Check online for the latest updates by clicking on **Check Now**. Make sure the firmware you want to use is downloaded to the local hard drive of your computer.

Firmware Upgrade

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

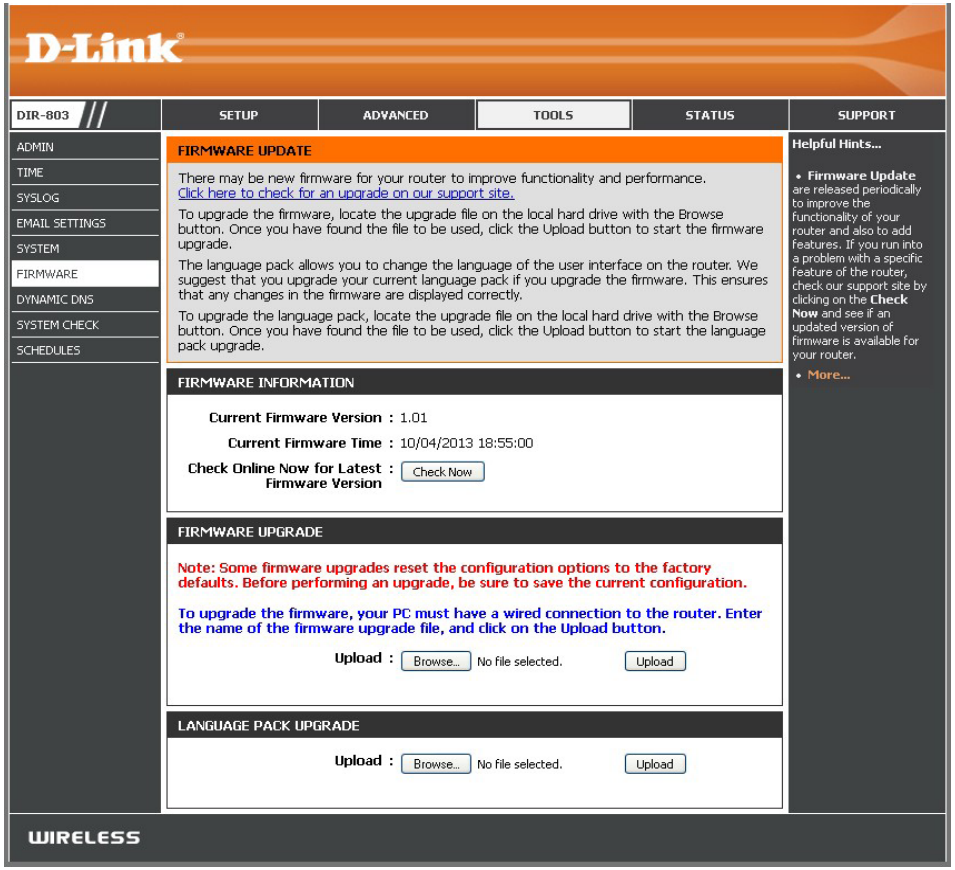
Upload: Once you have located the firmware update on your computer, click **Upload** to upgrade your firmware.

Language Pack Upgrade

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.

Upload: Once you have located the language pack update on your computer, click **Upload** to upgrade your language pack.



Dynamic DNS

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

Note: *You can sign up for D-Link's Free DDNS service by clicking on the link to* ***www.DLinkDDNS.com****.*

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 Dynamic DNS**.

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

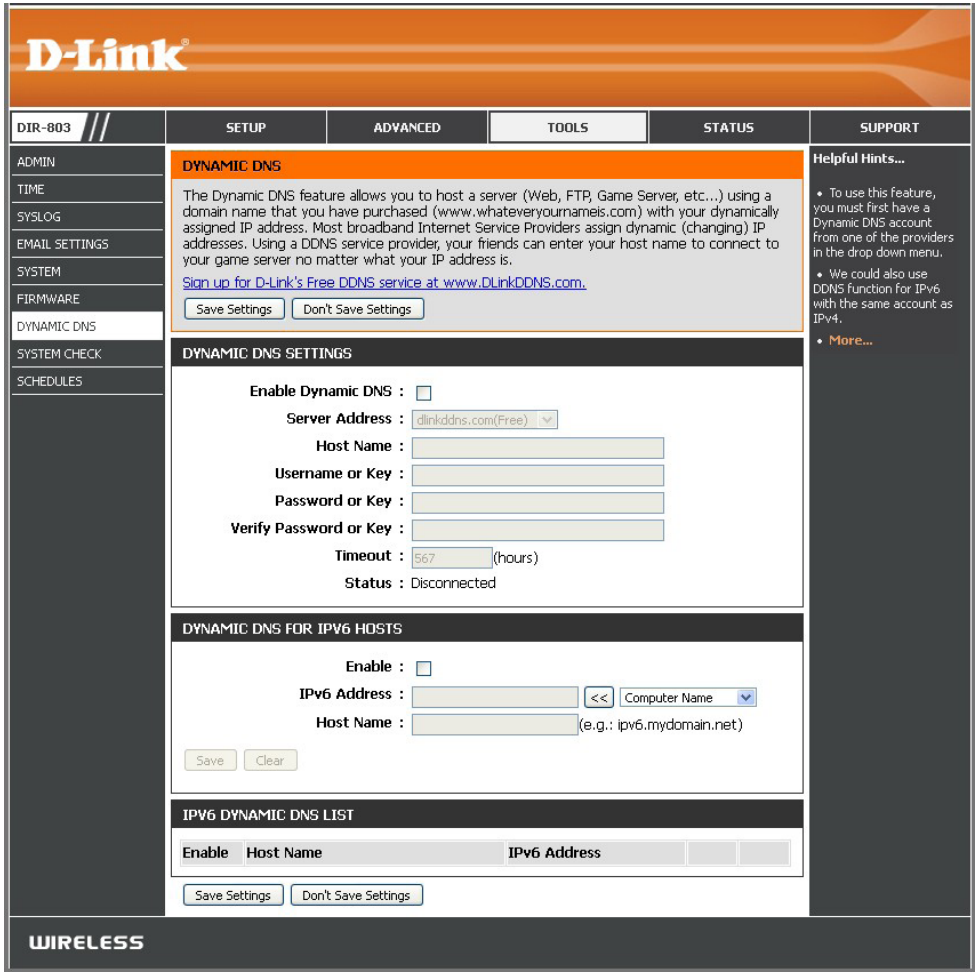
Host Name: Enter the **Host Name** that you registered with your DDNS service provider.

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

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

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

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



DDNS for IPv6 Hosts

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

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

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

IPv6 Dynamic DNS List: After you save your entry, the IPv6 DDNS host information will be displayed here.

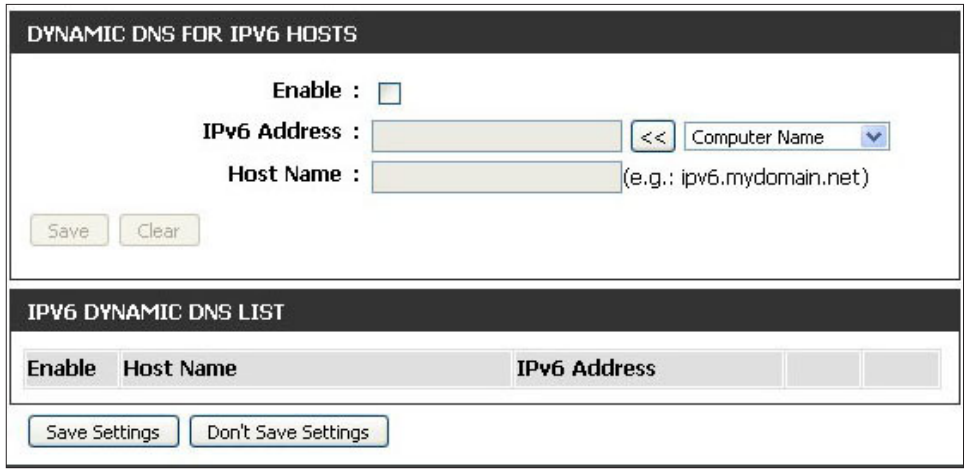
Enable: Check to **Enable** the entry.

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

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

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

Click **Save Settings**.



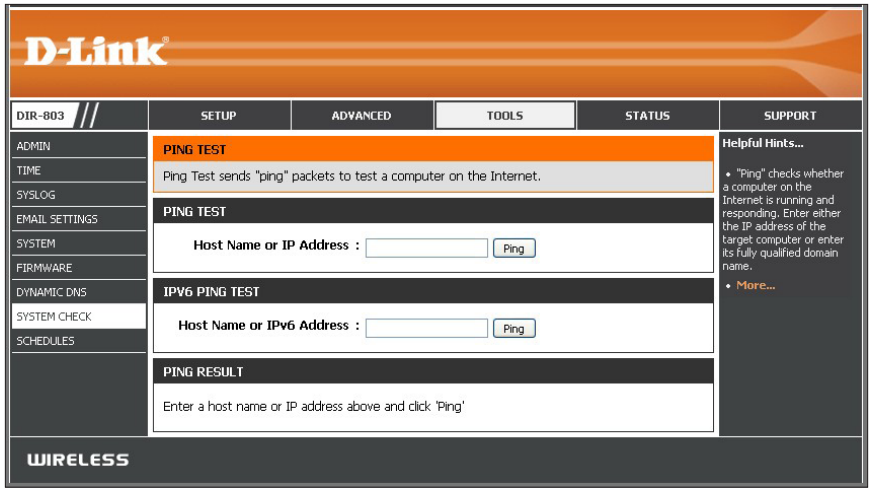
System Check

The *Ping Test* is used to send Ping packets to test if a computer on the Internet is running and responding.

Ping Test/Host Name or IP Address: Enter the **IP Address** of the computer that you wish to Ping and click **Ping**.

IPv6 Ping Test/ Host Name or IPv6 Address: Enter the **IPv6 Address** of the computer that you wish to Ping and click **Ping**.

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



Schedules

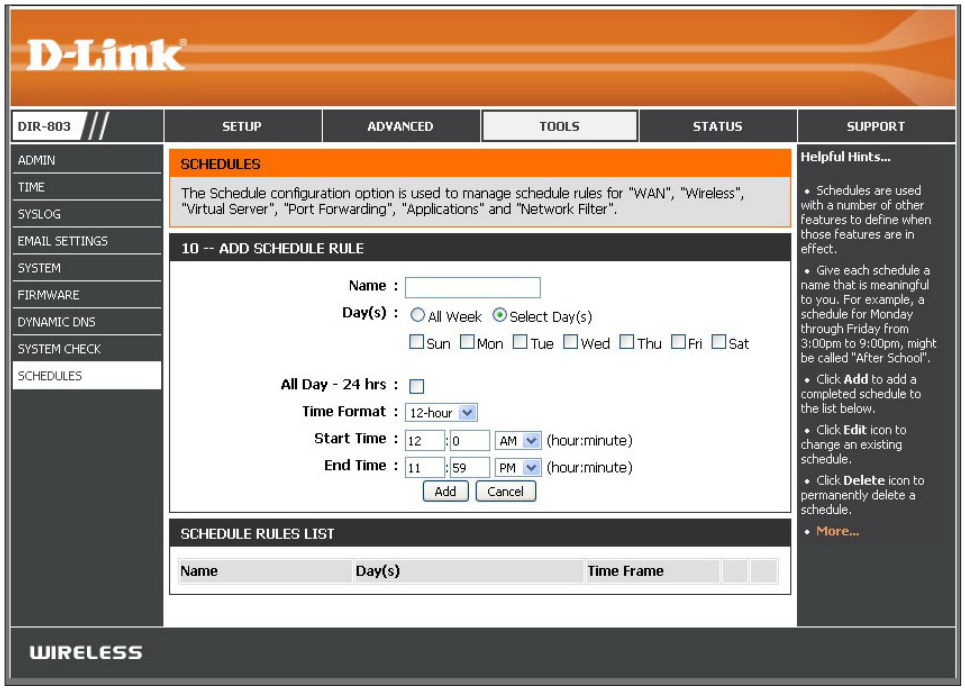
Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3:00 pm to 8:00 pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3:00 pm and End Time of 8:00 pm.

Name: Enter a **Name** that is meaningful to you for your new schedule.

Day(s): Click on **All Week** to implement your schedule every day of the week. Or, select a specific **Day** or a range of **Days** to implement your schedule.

Check **All Day - 24 hrs** or click on the arrow for the drop-down menu for **Time Format** and make a selection. Enter a **Start Time** and **End Time** for your schedule below. Click **Add** to save the schedule.

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



Status

Device Info

The Device Info page displays the connection details for the DIR-803. It will display the WAN, LAN, and Wireless LAN 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 current *Time* and *Firmware* version.

WAN: Displays the *MAC Address* and the public IP settings.

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

Wireless LAN: Displays the 2.4GHz wireless *MAC Address* and your wireless settings such as *Network Name* (*SSID*) and *Channel*.

Wireless LAN2: Displays the 5GHz wireless *MAC Address* and your wireless settings such as *Network Name* (*SSID*) and *Channel*.

LAN Computers: Displays a *MAC Address* and *IP Address* for each computer and device connected to the router via Ethernet that is receiving an IP address assigned by the router (DHCP).

IGMP Multicast Memberships: Displays IPv4 and IPv6 *Multicast Group Addresses*.

Logs

The router automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted and logs of the latest events are retained. You can define what types of events you want to view and the level of the events you would like to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

Save: Click to **Save** the log file to your local hard drive.

Log Type: Select the type of event you would like to view.

Log Level: Select the level of event you are interested in viewing.

First Page: Click to go to the **First** page of the *Log Files*.

Last Page: Click to go to the **Last** page of the *Log Files*.

Previous: Click to go back one page.

Next: Click to go to the **Next** page.

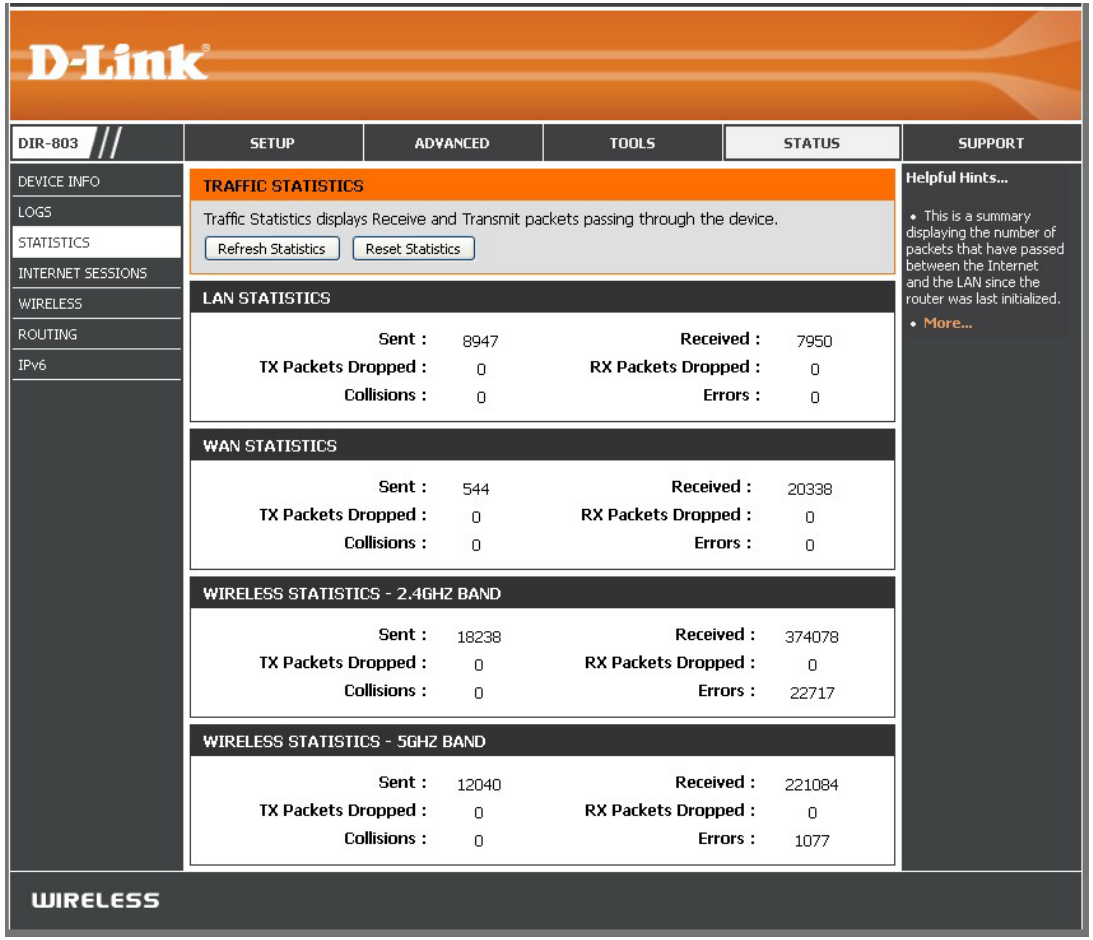
Refresh: Click to **Refresh** the page.

Clear: Clears all of the contents of the *Log Files*.

Link to Email Log Settings: Click this link to send copy of the router log to your e-mail address configured in the **Tools** > **Email Settings** page.

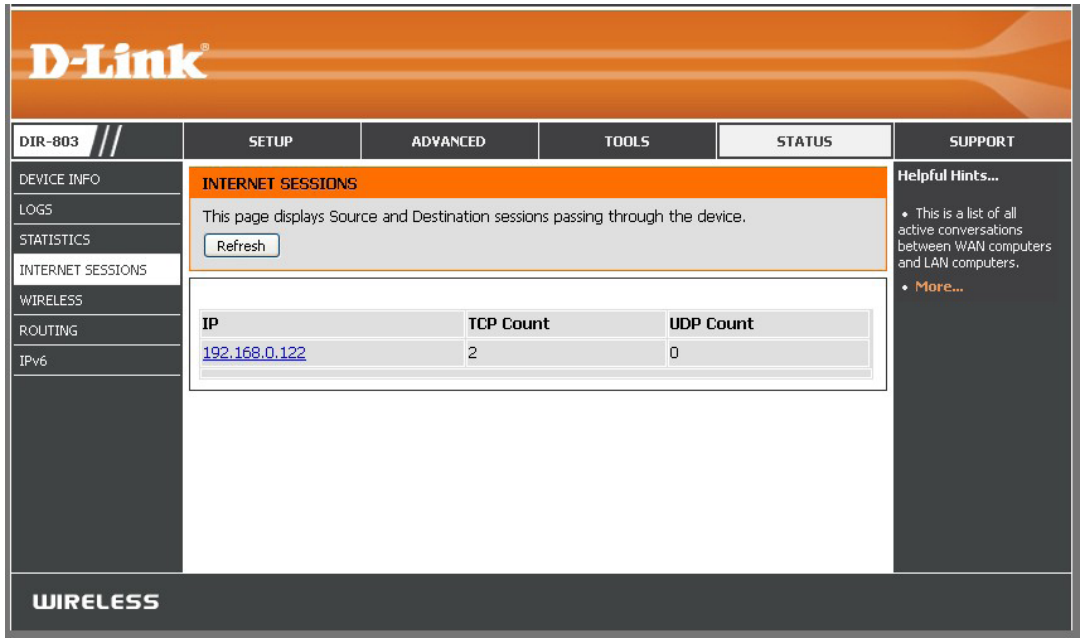
Statistics

The screen below displays the **Traffic Statistics**. Here you can view the number of packets that pass through the DIR-803 on both the LAN, WAN ports and the Wi-Fi® segments. The traffic counter will reset if the device is rebooted.



Internet Sessions

The Internet Sessions page displays full details of active Internet sessions passing 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.

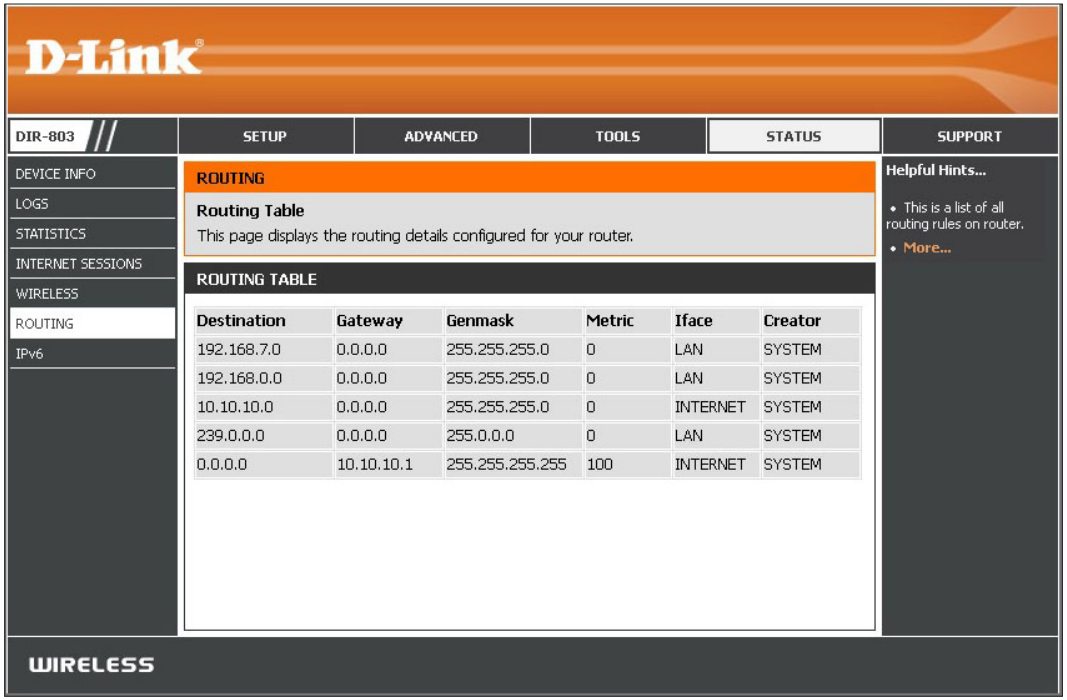


Wireless

The wireless client table displays a list of currently connected wireless clients. This table displays information including the *MAC Address* and the connection *Rate* of connected wireless clients.

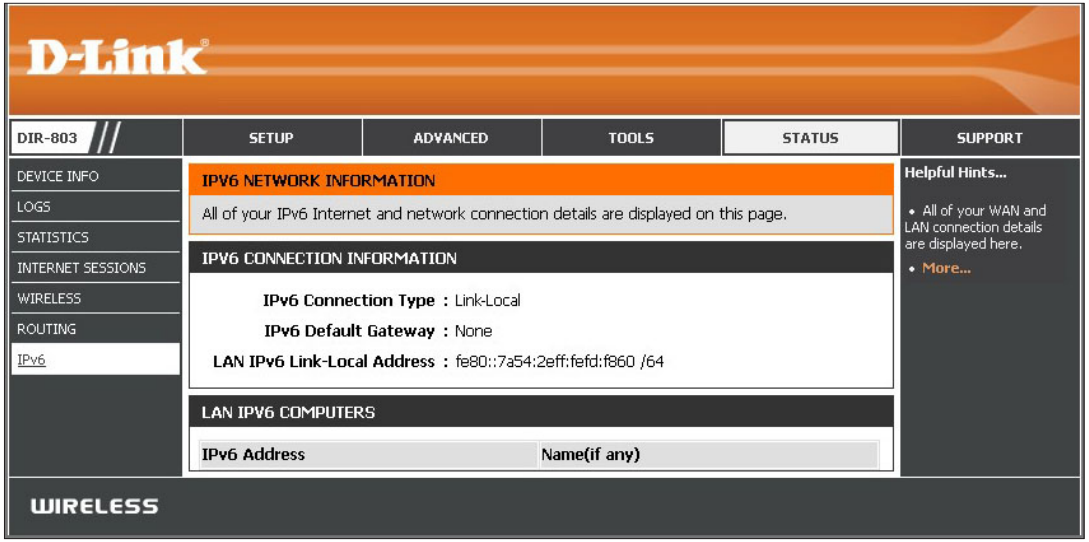
Routing

This page will display your current routing table.

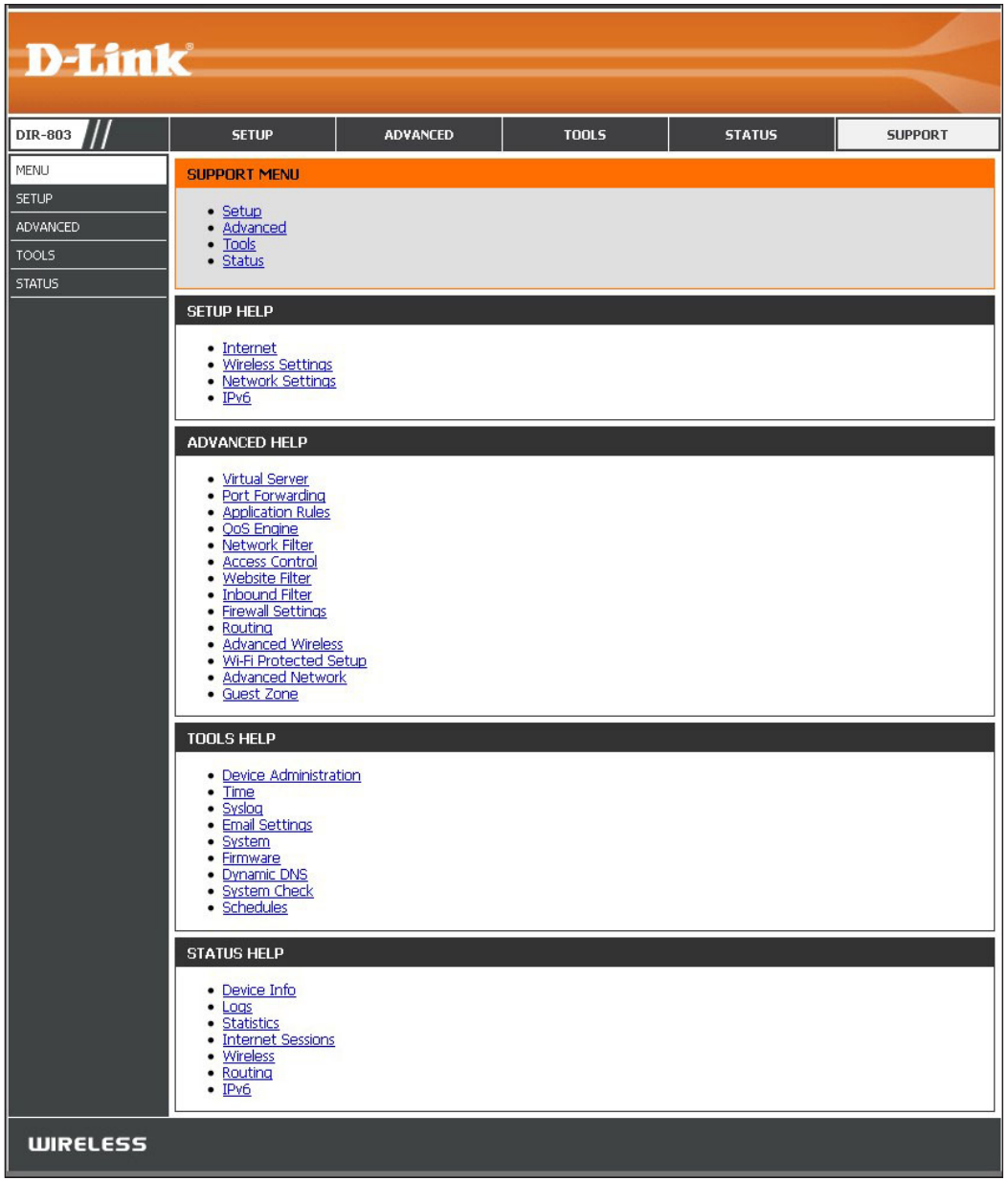


IPv6

The IPv6 Status page displays a summary of the Router's IPv6 connection details, and displays the *IPv6 Address* and host *Name* (if any) for IPv6 clients.



Support


D-Link
DIR-803
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
MENU
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT MENU
Setup
Advanced
Tools
Status
SETUP HELP
Internet
Wireless Settings
Network Settings
IPv6
ADVANCED HELP
Virtual Server
Port Forwarding
Application Rules
QoS Engine
Network Filter
Access Control
Website Filter
Inbound Filter
Firewall Settings
Routing
Advanced Wireless
Wi-Fi Protected Setup
Advanced Network
Guest Zone
TOOLS HELP
Device Administration
Time
Syslog
Email Settings
System
Firmware
Dynamic DNS
System Check
Schedules
STATUS HELP
Device Info
Logs
Statistics
Internet Sessions
Wireless
Routing
IPv6
WIRELESS

Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DIR-803 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 side of the DIR-803 for about one second. The WPS LED on the front will start to blink.

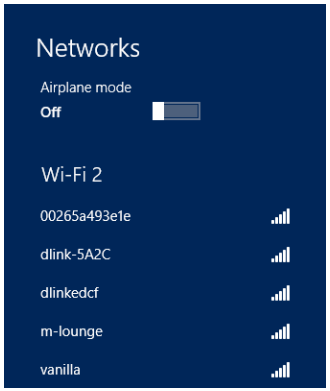
Step 2 - Within two minutes, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

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.

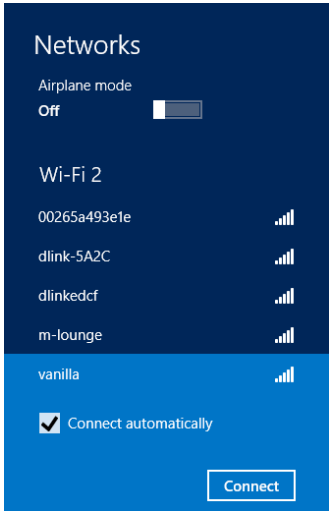
Windows® 8

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

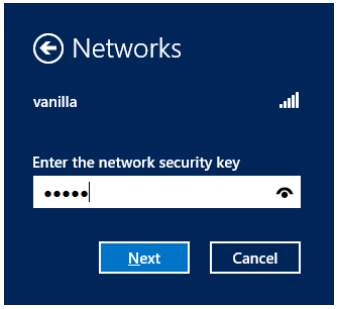
2. A list of available wireless networks will appear.



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).

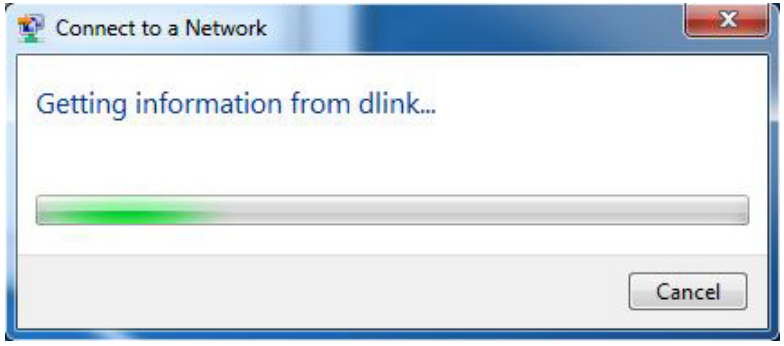
Wireless Icon

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

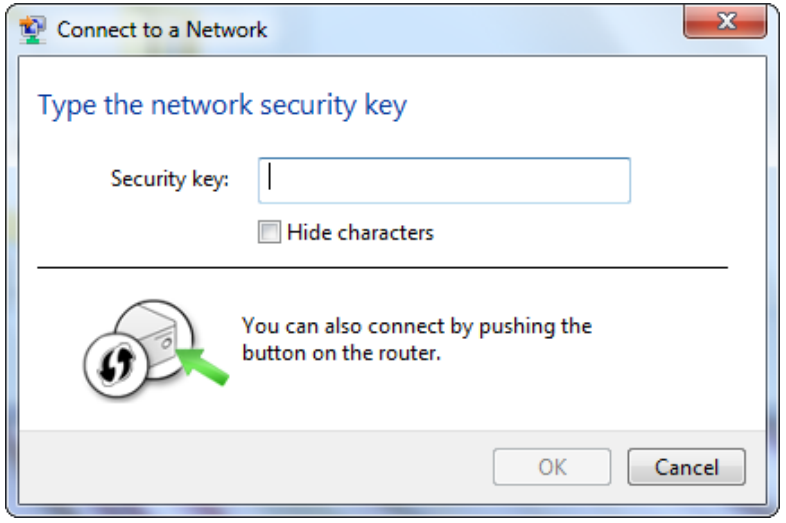
3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

   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.

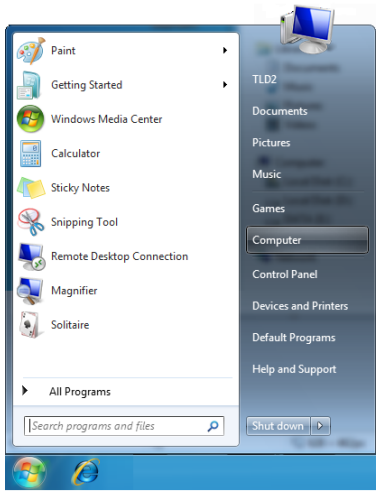


It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

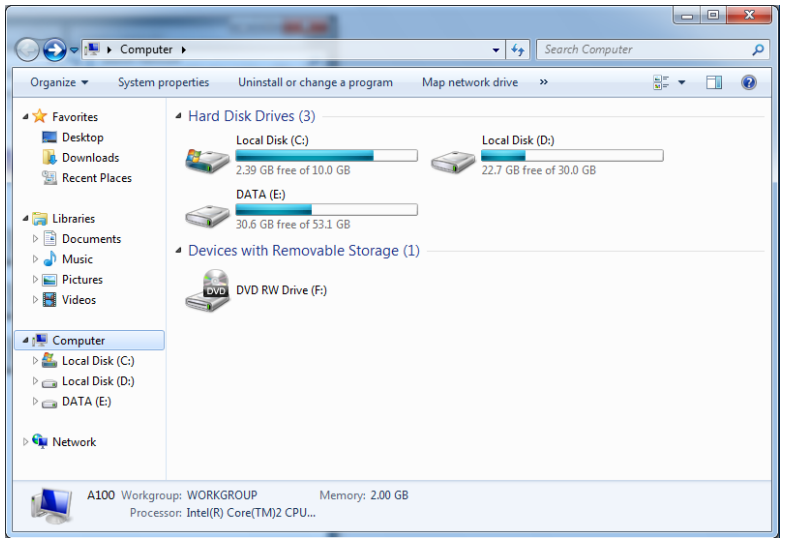
WPS

The WPS feature of the DIR-803 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

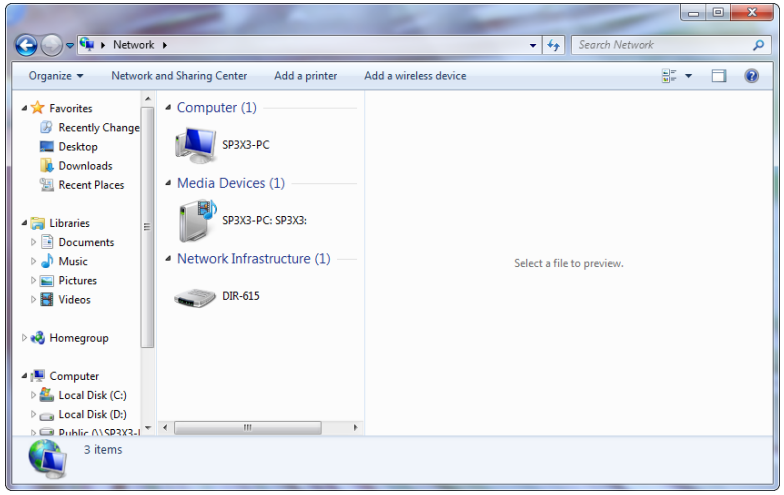
1. Click the **Start** button and select **Computer** from the Start menu.



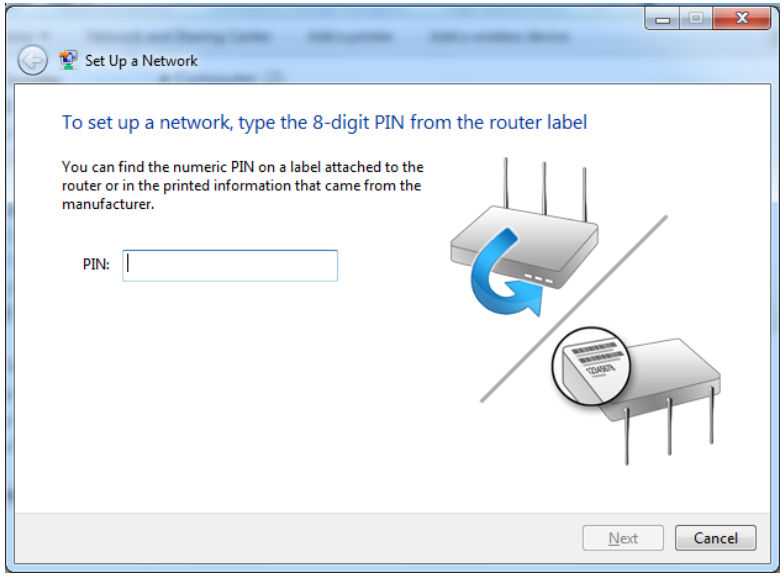
2. Click **Network** on the left side.



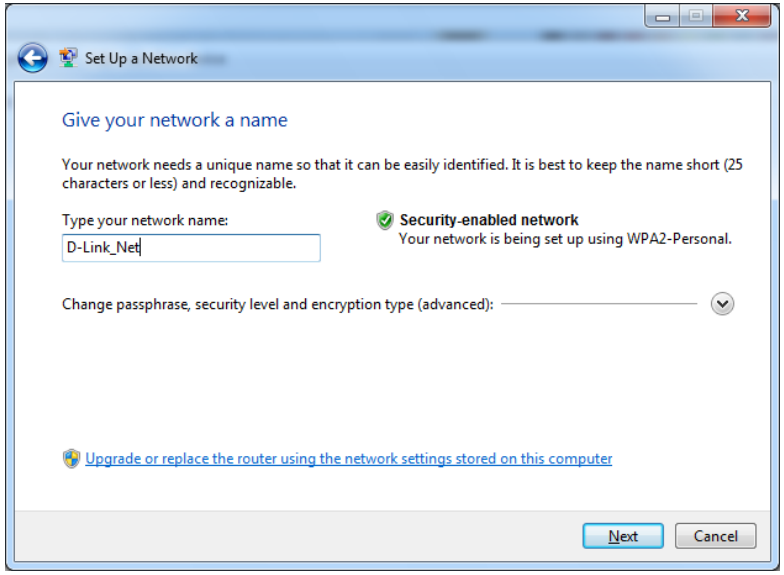
3. Double-click the DIR-803.



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**.

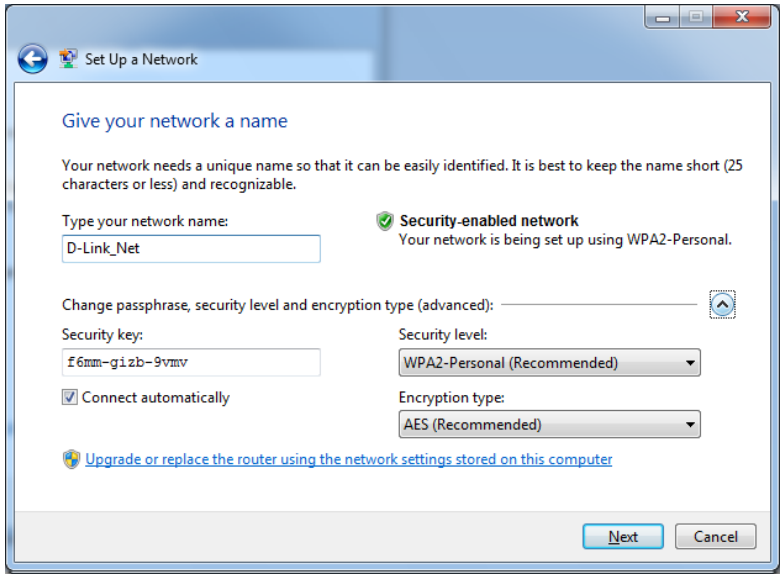


5. Type a name to identify the network.



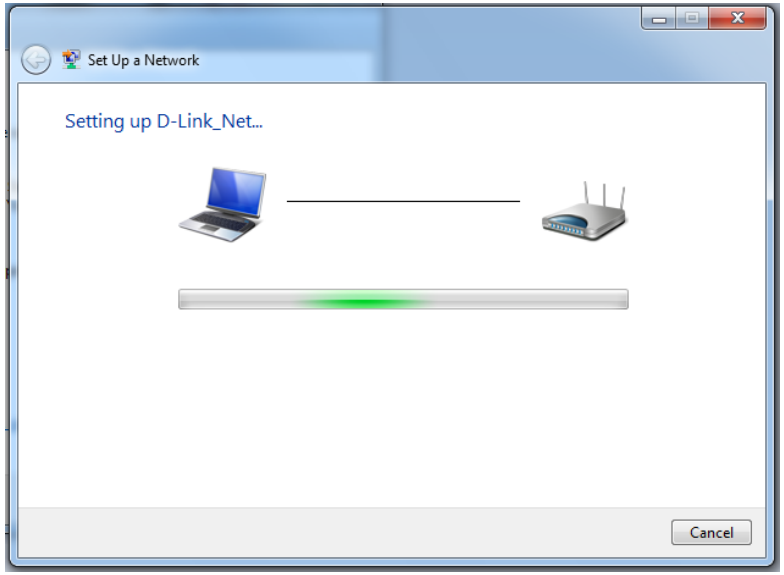
6. To configure advanced settings, click the icon.

Click **Next** to continue.



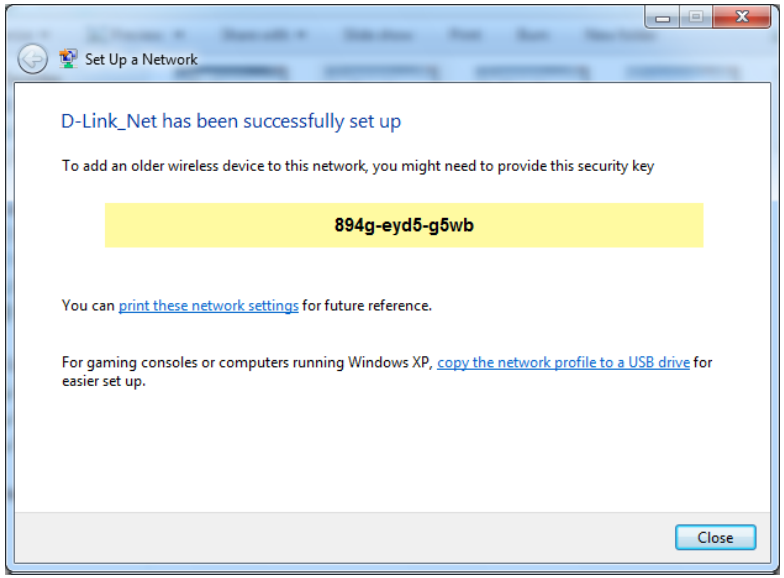
7. The following window appears while the Router is being configured.

   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.

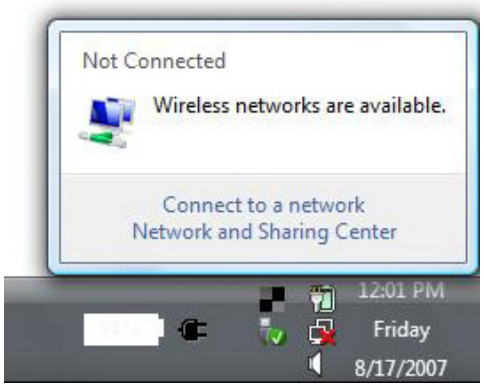
Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility, 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.

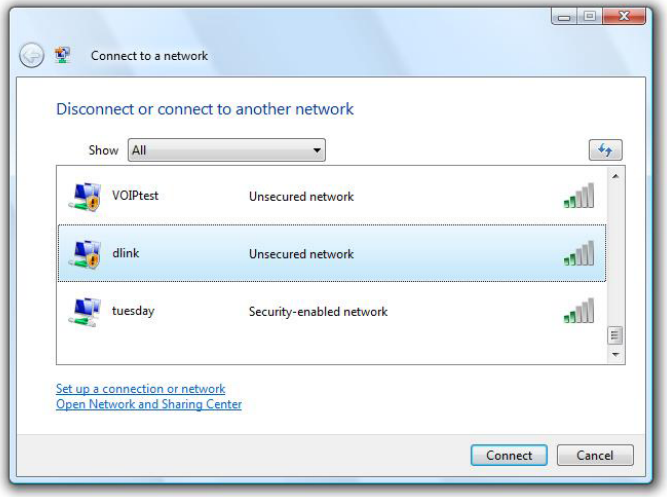
or

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.

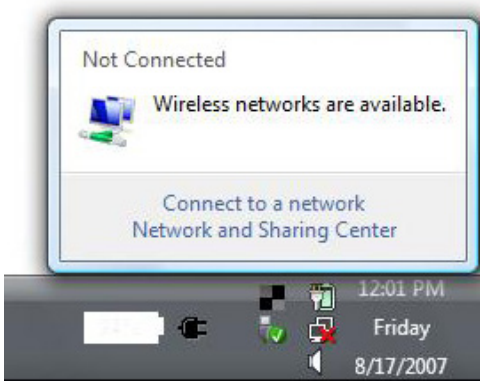
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



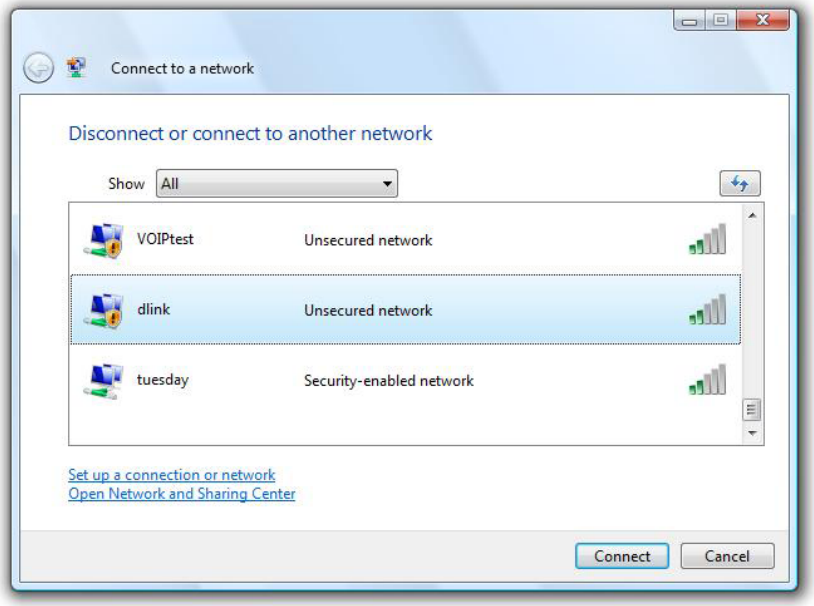
WPA/WPA2

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**.

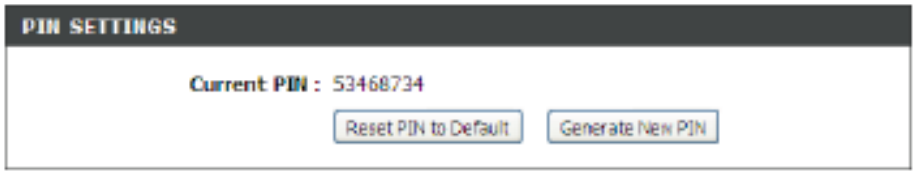
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

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.

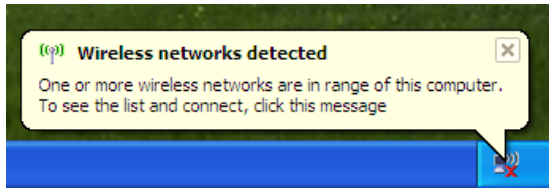


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Windows® XP

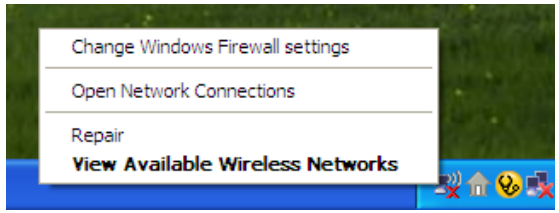
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows®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

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



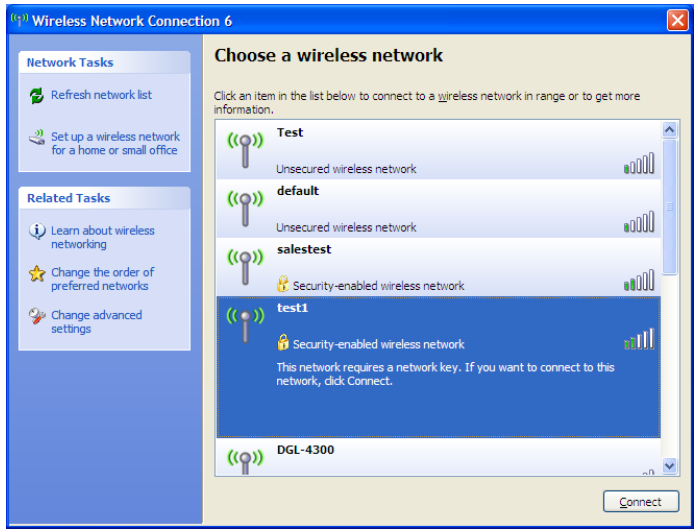
or

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.

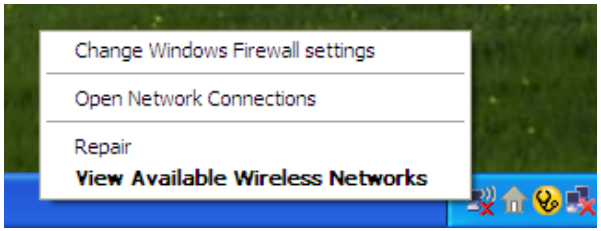
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



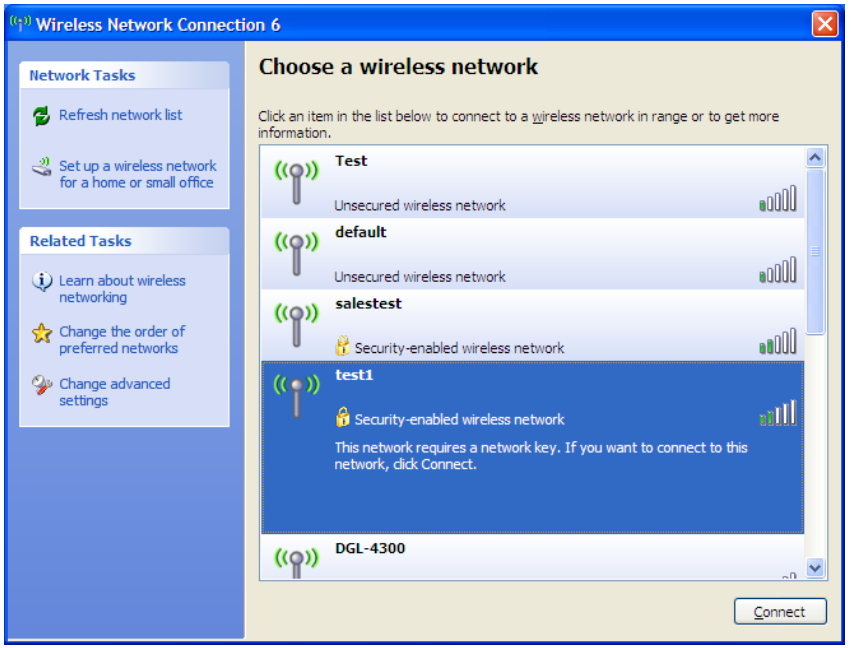
WPA/WPA2

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**.

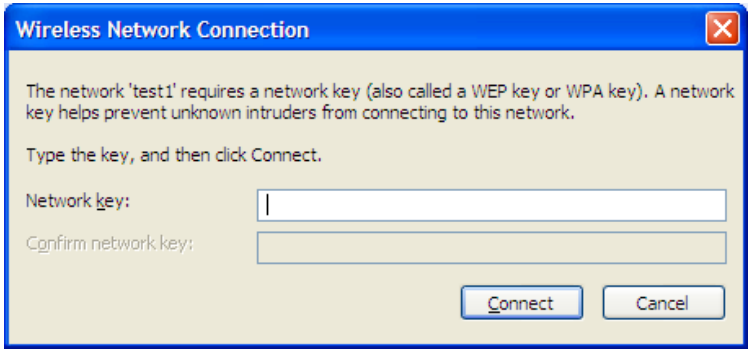


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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-803. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

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

- Make sure you have an updated Java-enabled web browser. We recommend the following:

  - Microsoft Internet Explorer® 7 and higher
  - Mozilla Firefox 9.0 and higher
  - Google™ Chrome 16.0 and higher
  - Apple Safari 4 and higher

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

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

- Configure your Internet settings:
    - Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.
    - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
    - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
    - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

To reset the router, locate the reset button (hole) on the back of the unit. With the router powered on, use a paper clip to hold the button down for at least six seconds. Release the button and the router will go through its reboot process. Wait about 30 seconds to access the router. To re-configure the router, refer to "Configuration" on page 13.

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

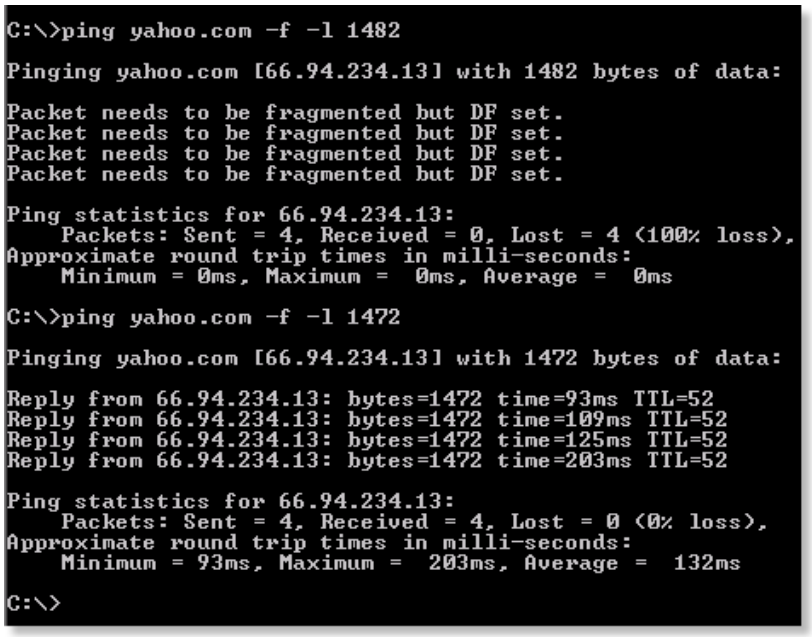
If you are having a problem sending or receiving e-mail, or connecting to secure sites such as eBay, banking sites, and Hotmail, we suggest lowering the MTU in increments of ten (Ex. 1492, 1482, 1472, etc).

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 username (admin) and password (blank by default). Click **OK** to enter the web configuration page for the device.
- Click on **Setup** and then click **Manual Configure**.
- To change the MTU enter the number in the MTU field and click **Save Settings** to save your settings.
- Test your 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 phones 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, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-803 wireless network Cardbus adapters.

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

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

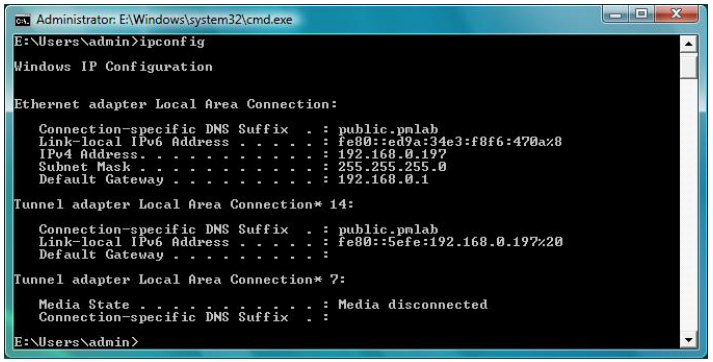
Networking Basics

Check your IP address

After you install your new D-Link 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® 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.

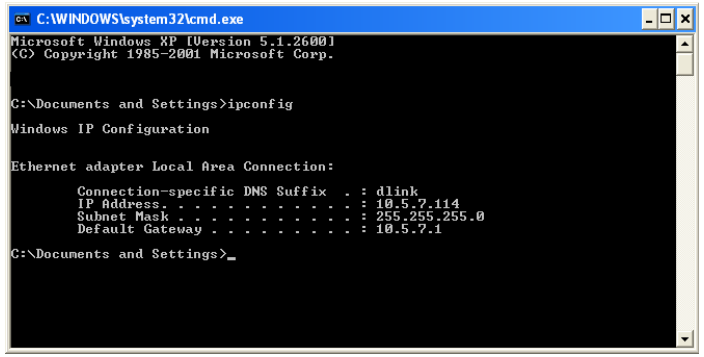


Windows® 7/Vista® Users

- 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® 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.



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.

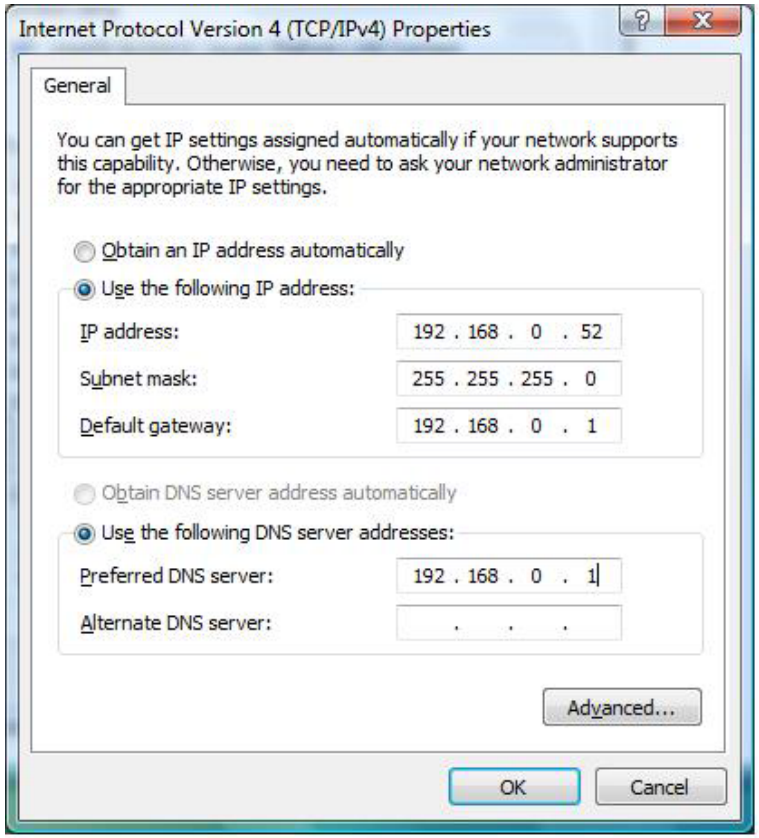
Statically Assign an IP Address

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

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.



Windows® 7/ Vista® Users

- Click on **Start** > **Control Panel** (make sure you are in Classic View). Double-click on the **Network and Sharing Center** icon. If you are using Windows Vista, click on **Manage network connections** along the left panel in the window. For Windows® 7, click on **Change adapter settings**.

- Right-click on the **Local Area Connection** which represents your D-Link wireless network adapter which will be connected to your network.

- 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.

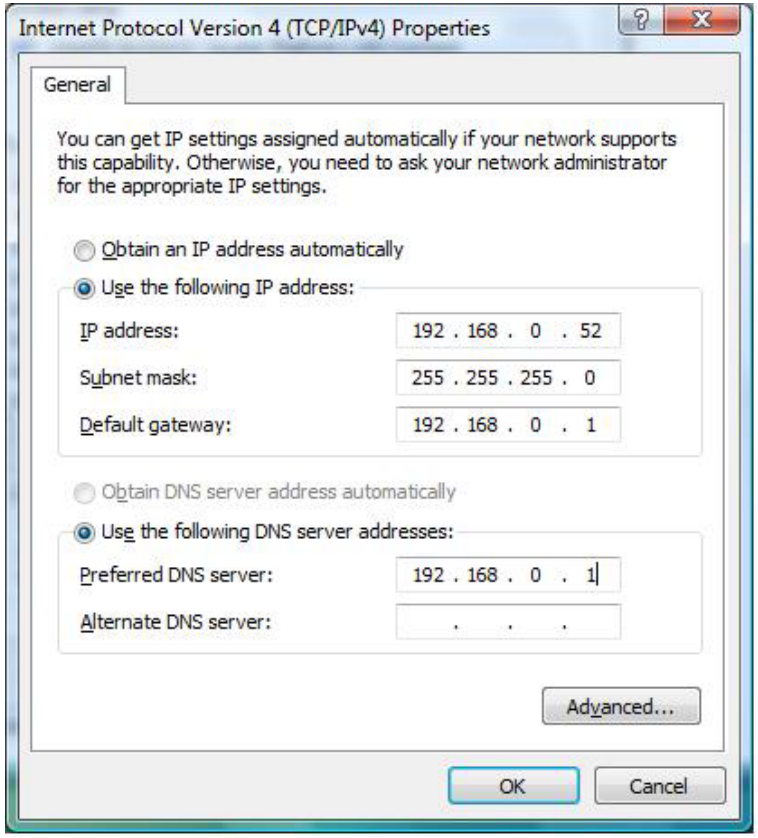
  Example: If the router's LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network.

- 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.

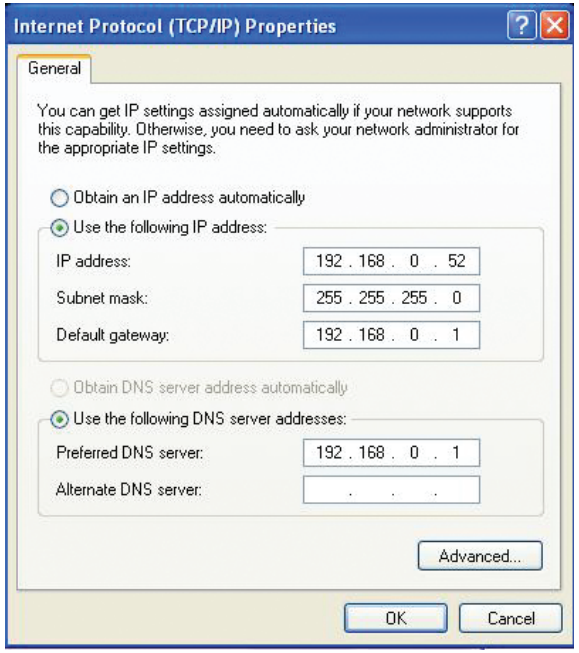


Windows® XP Users

- Click on **Start** > **Control Panel**. Make sure you are in Classic View. Double-click on the Network Connections icon.
- Right-click on the **Local Area Connection** which represents your D-Link wireless network adapter (or other adapter) which will be connected to your router.
- Highlight **Internet Protocol (TCP/IP)** 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.

  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** 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

Hardware Specifications
- LAN Interface: Four 10/100Mbps LAN ports
- WAN Interface: One 10/100Mbps Internet port
- Wireless Interface (2.4Ghz): IEEE 802.11b/g/n
- Wireless Interface (5Ghz): IEEE 802.11a/n/ac

Operating Voltage
- Input: 100~240V (±20%), 50~60Hz
- Output: DC5V, 1A

Temperature
- Operating: 32 ~ 104°F (0 ~ 40°C)
- Non-Operating: -4 ~ 149°F (-20 ~ 65°C)

Humidity
- Operating: 10% - 90% non-condensing
- Non-Operating: 5% - 95% non-condesing

Wireless Frequency Range
- IEEE 802.11a: 5180 MHz~5240 MHz, 5745 MHz~5825 MHz
- IEEE 802.11b: 2400 MHz~2483 MHz
- IEEE 802.11g: 2400 MHz~2484 MHz
- IEEE 802.11n: 2400 MHz~2484 MHz, 5180 MHz~5240 MHz, 5745 MHz~5825 MHz
- IEEE 802.11ac: 5180 MHz~5240 MHz, 5745 MHz~5825 MHz

Wireless Bandwidth Rate
- IEEE 802.11a: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11b: 11, 5.5, 2, and 1 Mbps
- IEEE 802.11g: 54, 48, 36, 24, 18, 12, 9, and 6 Mbps
- IEEE 802.11n: 6.5 to 300 Mbps
- IEEE 802.11ac(Draft): 6.5 to 433 Mbps

Antenna Type
- Two External Antennas

Wireless Security
- WPA/WPA2-Personal, WPA/WPA2-Enterprise, WPS (PIN & PBC)

Certifications
- FCC, IC, CE, and CSA

Dimensions
- 6 x 4.4 x 1.2 in (151.6 x 112 x 30.5 mm)

Weight
- 0.42 lbs (190 grams)

1 Maximum wireless signal rate derived from IEEE Standard 802.11ac (draft), 802.11a, 802.11g, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.
2 Frequency Range varies depending on country's regulation

Contacting Technical Support

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

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

- Model number of the product (e.g. DIR-803)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev B1)
- Serial Number (s/n number located on the label on the bottom of the router).

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

For customers within the United States:

Phone Support:
(877) 453-5465

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

For customers within Canada:

Phone Support:
(800) 361-5265

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

GPL Code Statement

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

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

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

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

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

Please direct all inquiries to:
Email: GPLCODE@DLink.com
Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Systems, Inc.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

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

Preamble

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

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

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

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

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

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

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

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

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

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

TERMS AND CONDITIONS

0. Definitions.

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

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

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

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

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

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

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

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

1. Source Code.

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

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

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

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

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

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

2. Basic Permissions.

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

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

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

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

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

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

4. Conveying Verbatim Copies.

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

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

5. Conveying Modified Source Versions.

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

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

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

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

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

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

6. Conveying Non-Source Forms.

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

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

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

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

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

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

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

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

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

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

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

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

7. Additional Terms.

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

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

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

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

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

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

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

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

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

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

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

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

8. Termination.

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

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

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

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

9. Acceptance Not Required for Having Copies.

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

10. Automatic Licensing of Downstream Recipients.

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

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

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

11. Patents.

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

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

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

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

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

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

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

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

12. No Surrender of Others' Freedom.

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

13. Use with the GNU Affero General Public License.

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

14. Revised Versions of this License.

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

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

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

15. Disclaimer of Warranty.

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

16. Limitation of Liability.

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

17. Interpretation of Sections 15 and 16.

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

Warranty

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

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

Limited Warranty:

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

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

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

Limited Software Warranty:

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

Non-Applicability of Warranty:

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

Submitting A Claim (USA):

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

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

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

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

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

Submitting A Claim (Canada):

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

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

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

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

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

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

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

What Is Not Covered:

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

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

Disclaimer of Other Warranties:

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

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

Limitation of Liability:

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

Governing Law:

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

Trademarks:

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

Copyright Statement:

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

Copyright ©2013 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning:

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

FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio 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
November 18, 2013