D-Link®

Version 1.0 | 05/31/2013

User Manual

Wireless AC600 Dual Band Cloud Router

DIR-808L

Preface

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

Manual Revisions

Revision	Date	Description
1.0	May 31, 2013	• Initial release for Revision A1

Trademarks

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

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 Corporation.

Table of Contents

Preface i
Manual Revisions i
Trademarks i

Product Overview 1
Package Contents 1
System Requirements 2
Introduction 3
Features 4
Hardware Overview 5
Connections 5
LEDs 6

Installation 7
Before you Begin 7
Wireless Installation Considerations 8
Manual Setup 9

Configuration 11
Quick Setup Wizard 12
QRS Mobile App (iOS, Android) 19
Web-based Configuration Utility 20
Internet Connection Setup 21
Internet Connection Setup Wizard 22
Internet (Manual Setup) 28
Internet Connection Type 29
Static (assigned by ISP) 31
PPPoE (DSL) 33
PPTP 35
L2TP 37
DS-Lite 39
Wireless Connection Setup Wizard 40
Wi-Fi Protected Setup Wizard 43
Manual Wireless Network Setup 45
Manual Setup - 2.4 Ghz Band 46
Manual Setup - 5 Ghz Band 52
Wireless Security 57
What is WPA? 57
Network Settings 58
Router Settings 58
DHCP Server Settings 59
DHCP Reservation 61
IPv6 Internet Connection 62
IPv6 Internet Connection Setup Wizard 63
IPv6 Manual Setup 69
mydlink™ Settings 79
Advanced 82
Virtual Server 82
Port Forwarding 83
Application Rules 84
QoS Engine 85
Network Filters 87
Access Control 88

Website Filters 91
Inbound Filters 92
Firewall Settings 93
Routing 95
Advanced Wireless 96
Wi-Fi Protected Setup (WPS) 97
Advanced Network Settings 99
Guest Zone 100
IPv6 Firewall 101
IPv6 Routing 102
Tools 103
Admin 103
Time 105
SysLog 106
Email Settings 107
System Settings 108
Firmware Update 109
Language Pack 109
Dynamic DNS 110
System Check 111
Schedules 112
Status 113
Device Info 113
Logs 114
Statistics 115
Internet Sessions 116
Routing 117
Wireless 118
IPv6 119
IPV6 Routing 120
Support 121

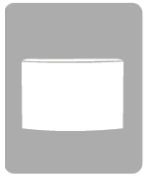
Connect a Wireless Client to your Router 122
WPS Button 122
Windows® 8 123
WPA/WPA2 123
Windows® 7 125
WPA/WPA2 125
WPS 128
Windows Vista® 132
WPA/WPA2 133
WPS/WCN 2.0 135
Windows® XP 136
WPA/WPA2 137

Troubleshooting 139
Wireless Modes 143

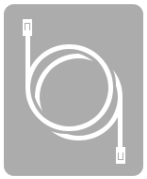
Networking Basics 144
Check your IP address 144
Assign a Static IP address 145

Technical Specifications 146

Package Contents



DIR-808L Wireless AC600 Dual Band Cloud Router



Ethernet Cable

Power Adapter

Wi-Fi Configuration Note

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-808L will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based cable or DSL modem • 802.11a, 802.11g, 802.11n, or 802.11ac wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 7 or higher • Firefox 3.5 or higher • Safari 4 or higher • Chrome 8 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.

mydlink Requirements	• iPhone/iPad/iPod Touch (iOS 3.0 or higher)
	• Android device (1.6 or higher)
	• Computer with the following browser requirements:
	  • Internet Explorer 7 or higher
	  • Firefox 3 or higher
	  • Safari 5 or higher
	  • Chrome 5 or higher
	
	iPhone, iPad, and iPod touch are registered trademarks of Apple Inc. Android is a trademark of Google, Inc.

Introduction

The D-Link DIR-808L is a draft IEEE 802.11ac compliant device that delivers speeds up to 3 times faster than 802.11n, while staying backward compatible with older 802.11b/g/n devices. Connect the DIR-808L to a cable or DSL modem and provide high-speed Internet access to multiple wireless clients. Powered by the latest 802.11ac technology, this router provides superior wireless coverage for small to medium sized homes. The DIR-808L also includes a 4-port 10/100 Fast Ethernet switch that connects Ethernet wired devices for high-speed wired connectivity.

With the DIR-808L Wireless AC600 Dual Band Cloud Router you can monitor and manage your home network right from your laptop, iOS™, or Android™ device. This cloud-enabled router can be configured to notify you whenever new devices are connected to your network or unwanted access is detected. Monitor in real-time websites that are being visited, with recent browser history displayed on the mydlink™ Lite app – which is great for parents keeping an eye on children using the Internet at home. The D-Link Cloud Service can help you to detect and block unwelcome guests who attempt to access your wireless network, and any suspicious activities will be displayed right on your mydlink Lite app or browser.

With some routers, all wired and wireless traffic, including VoIP, video streaming, online gaming, and web browsing is mixed together into a single data stream. By handling data this way, applications like video streaming could experience lags or delays. With D-Link Intelligent QoS Technology, wired and wireless traffic are analyzed and separated into multiple data streams. You can also assign priorities to different data streams to ensure that the traffic most important to you receives optimum bandwidth.

The DIR-808L supports the latest wireless security features to help prevent unauthorized access, be it from inside your wireless network or from the Internet. Support for the WPA and WPA2 standards gives you a range of security and encryption choices, based on the capabilities of your wireless clients. In addition, this router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

Features

- **Ultimate Fast Wireless Networking** - The DIR-808L provides a wireless connection up to 150 Mbps on the 2.4 GHz band, and up to 433 Mbps on the 5 GHz band. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11ac wireless router gives you the freedom of wireless networking at speeds up to three times faster than 802.11n.

- **Compatible with 802.11a/g/n Devices** - The DIR-808L remains fully compatible with the IEEE 802.11b, 802.11g and 802.11n standards, so it can connect your existing wireless clients, providing backwards compatibility for older devices.

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

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

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

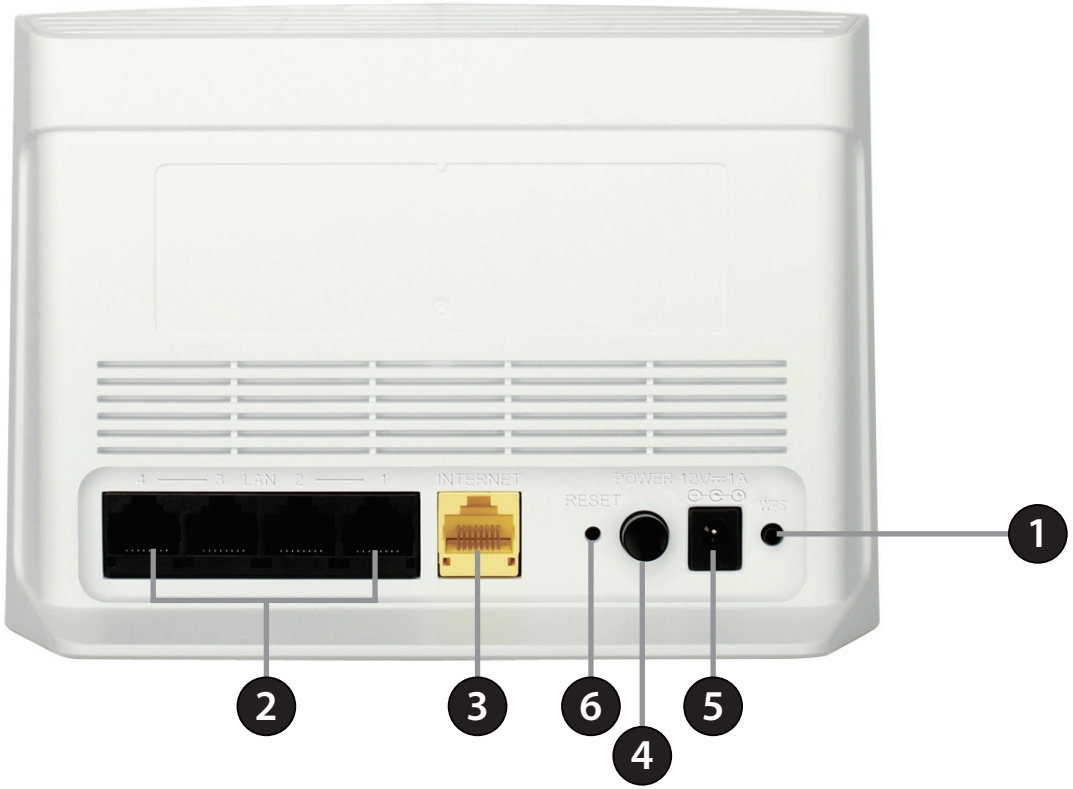
    - **Secure Multiple/Concurrent Sessions** - The DIR-808L can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-808L can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use web-based user interface, the DIR-808L guides you through the process of setting up a customized, secure wireless network, allowing you to configure your router to your specific settings within minutes.

* Maximum wireless signal rate derived from IEEE Standard 802.11b, 802.11g, 802.11n and draft 802.11ac 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 10/100 Ethernet devices such as computers, switches, storage (NAS) devices and game consoles.
3	Internet Port	Using an Ethernet cable, connect your broadband modem to this port.
4	Power Button	Press the power button to power on and off.
5	Power Receptor	Receptor for the supplied power adapter.
6	Reset Button (Hole)	Use a paperclip to depress the reset button and restore the router to its original factory settings.

Hardware Overview

LEDs

1	Power LED	A solid green light indicates a proper connection to the power supply. The light will blink green during the WPS process. The light will be solid orange during boot up.
2	Internet LED	A solid light indicates connection on the Internet port. If the LED is orange, a connection is present but the router cannot connect to the Internet.

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, an attic, or a garage.

Before you Begin

- Please configure the router with the computer that was last connected directly to your modem.
- You can only use the Ethernet port on your modem. If you were using the USB connection before using this router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the Internet port on the router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).
- If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoET, Broadjump, or Enternet 300 from your computer, or you will not be able to connect to the Internet.

Wireless Installation Considerations

The DIR-808L Wireless AC600 Dual Band Cloud 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 used 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 router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range by 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 0.5 meters thick (1.5 feet), at a 45-degree angle appears to be almost 1 meter (3 feet) thick. At a 2-degree angle it can appear over 14 meters (42 feet) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

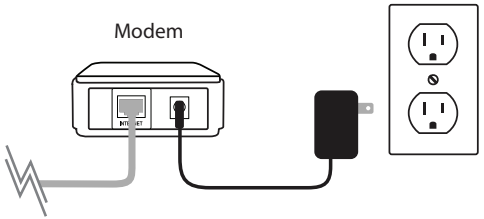
3. Building materials can affect your wireless signal. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, 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 2.4 GHz cordless phones or X-10 wireless products (such as ceiling fans, lights, and home security systems), your wireless connection may be degraded dramatically or even drop completely. Make sure your 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

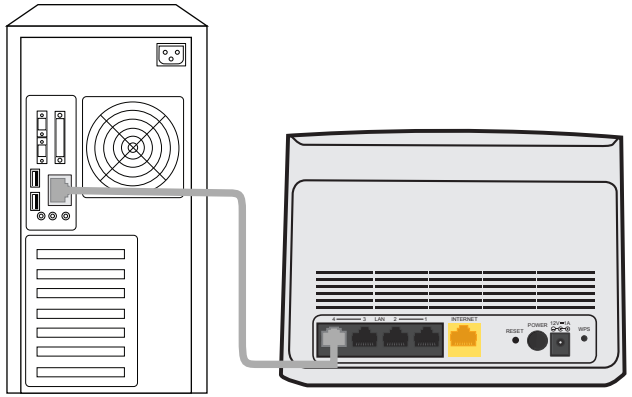
Manual Setup

1. Turn off and unplug your cable or DSL broadband modem. This is required.

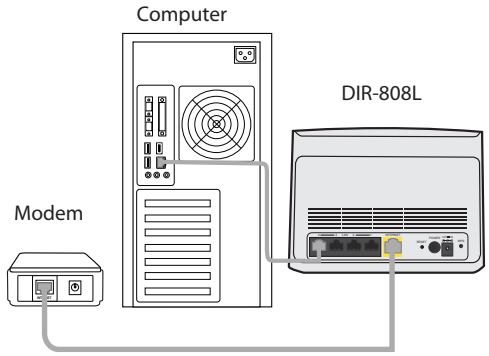


2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.

3. Unplug the Ethernet cable from your modem (or existing router if upgrading) that is connected to your computer. Plug it into the LAN port labeled **1** on the back of your router. The router is now connected to your computer.

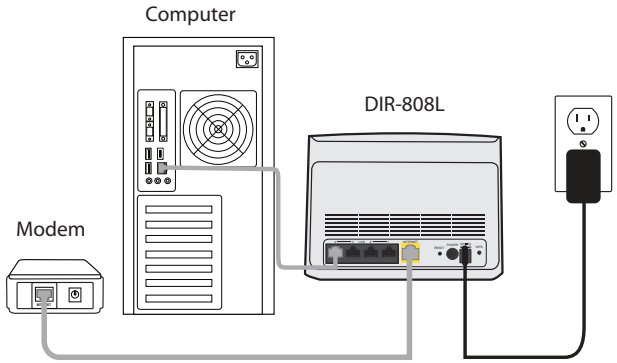


4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.



5. Reconnect the power adapter to your cable or DSL broadband modem and wait for two minutes.

6. Connect the supplied power adaptor into the power port on the back of the router and then plug it into a power outlet or surge protector. Press the power button and verify that the power LED is lit. Allow 1 minute for the router to boot up.



7. If you are connecting to a broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser and enter a web site. A solid light on the **Internet LED** indicates connection on the Internet port and the router can connect to the Internet. If the LED is orange, a connection is present but the router cannot connect to the Internet.

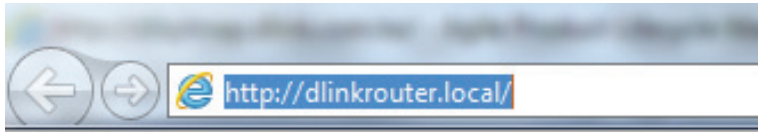
Configuration

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

- **Quick Setup Wizard** - This wizard will launch when you log into the router for the first time. Refer to "Quick Setup Wizard" on page 12.
- **QRS Mobile App** - Use your iOS or Android device to configure your router. Refer to "QRS Mobile App (iOS, Android)" on page 19.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to "Internet (Manual Setup)" on page 28.

Quick Setup Wizard

If this is your first time installing the router, open your web browser. You will automatically be directed to the Wizard Setup Screen. If not, enter "**http://dlinkrouter.local**". Then, press **Enter**.

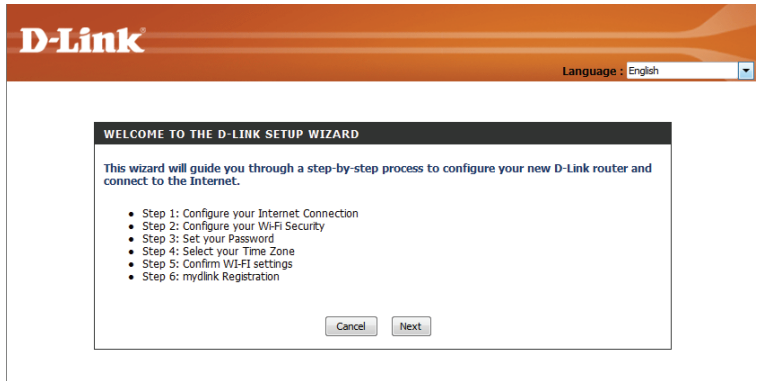


If you have already configured your settings and you would like to access the configuration utility, please refer to "Internet (Manual Setup)" on page 28.

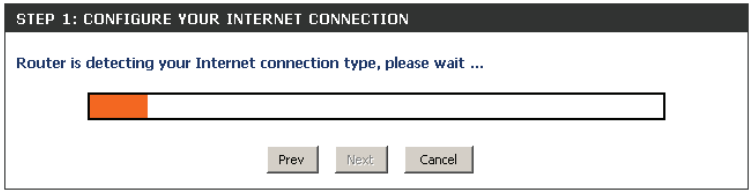
If this is your first time logging into the router, this wizard will start automatically.

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

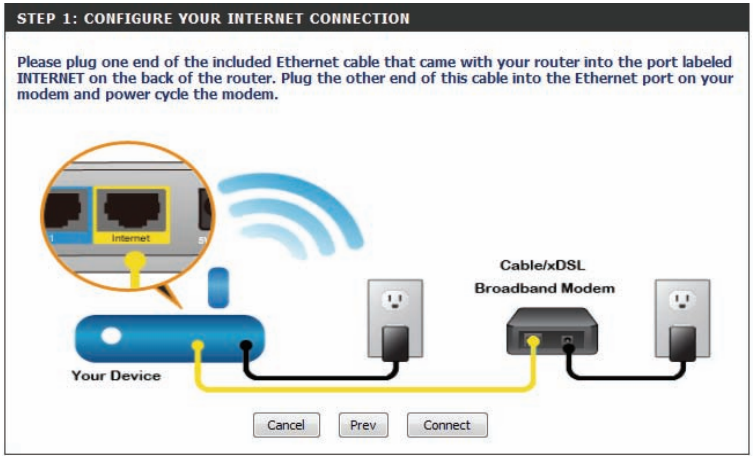
Click **Next** to continue.



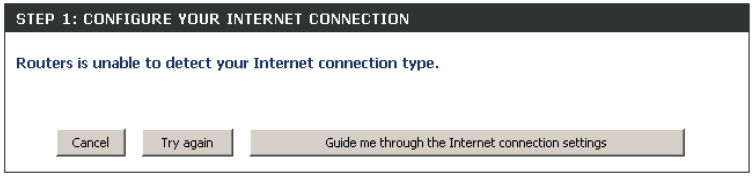
Please wait while your router detects your Internet connection type. This process may take a few minutes.



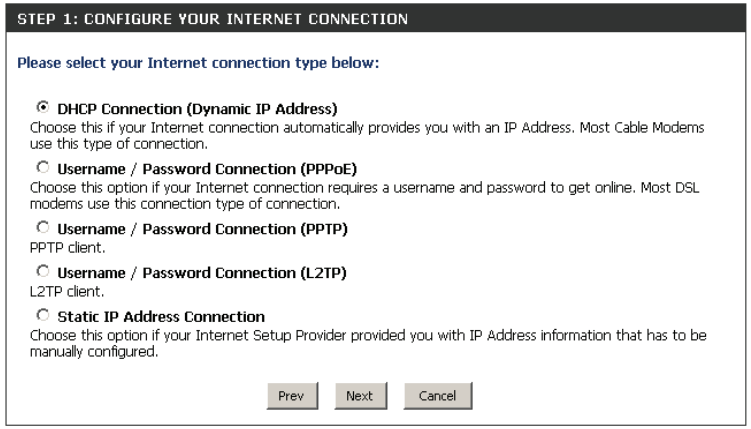
If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Check the connection between your broadband modem to the Internet port and then click **Prev** to return to the previous page and try again.



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

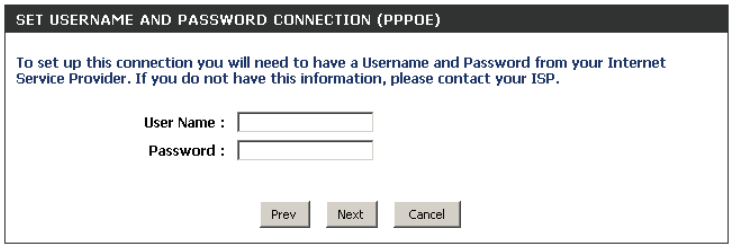


Select your Internet connection type and click **Next** to continue.

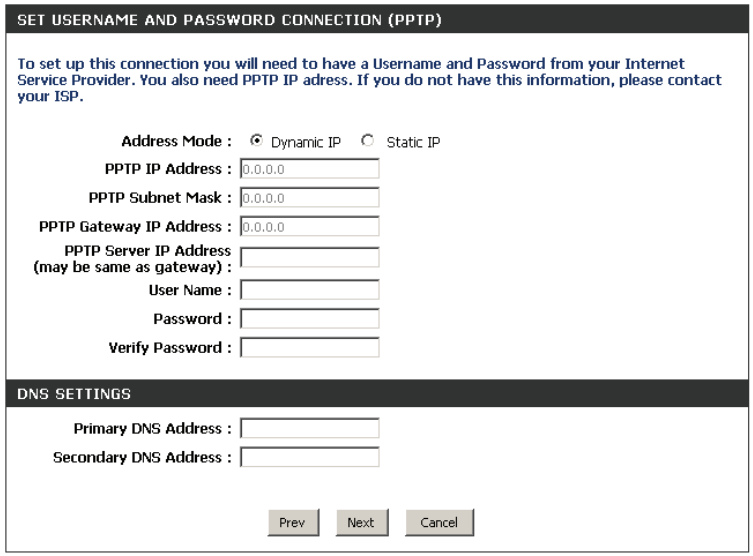


If the router detected, or you selected **PPPoE**, enter your PPPoE username and password and click **Next** to continue.

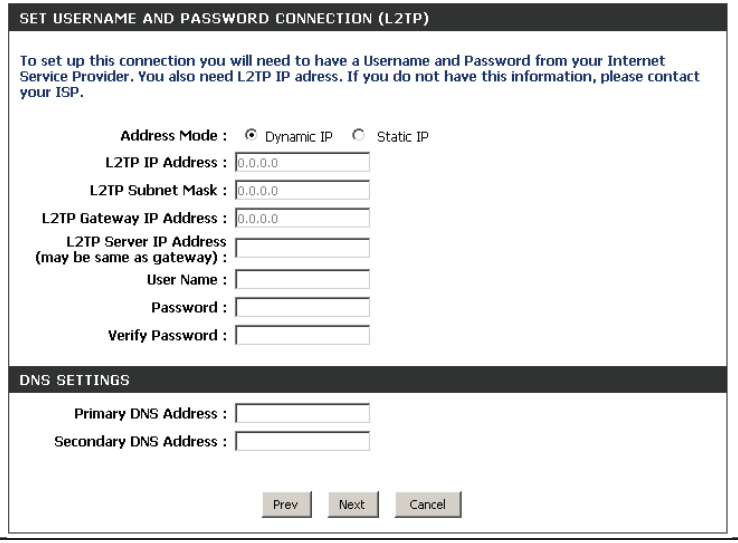
Note: *Make sure to remove any PPPoE software from your computer. The software is no longer needed and will not work through a router.*



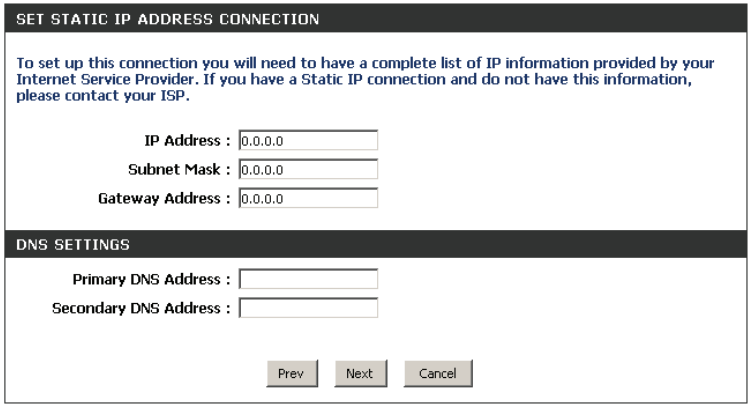
If the router detected or you selected **PPTP**, enter your PPTP username, password, and other information supplied by your ISP. Click **Next** to continue.



If the router detected, or you selected **L2TP**, enter your L2TP username, password, and other information supplied by your ISP. Click **Next** to continue.



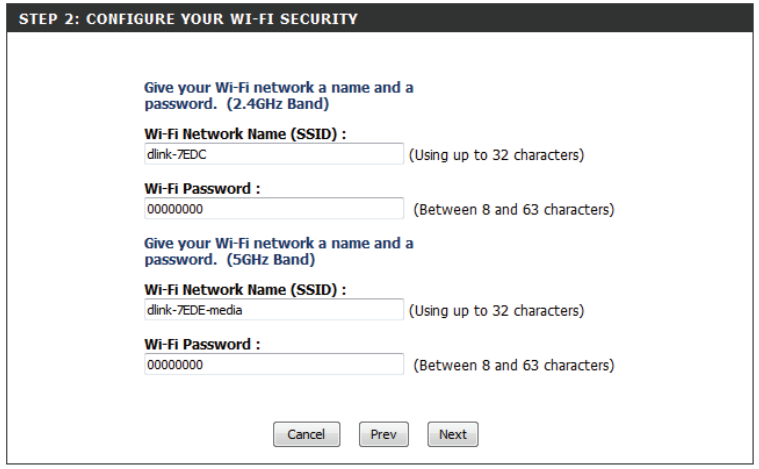
If the router detected, or you selected **Static**, enter the IP and DNS settings supplied by your ISP. Click **Next** to continue.



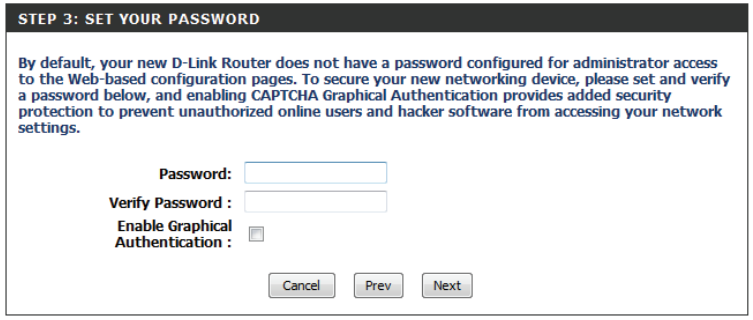
For both the 2.4 GHz and 5 GHz bands, create a Wi-Fi network name (SSID) using up to 32 characters. These names will identify your wireless network.

Create a Wi-Fi password (Network Key) (between 8-63 characters). Your wireless clients will need to have this password or key entered to be able to connect to your wireless network. It is recommended that you make a record of this information for future reference.

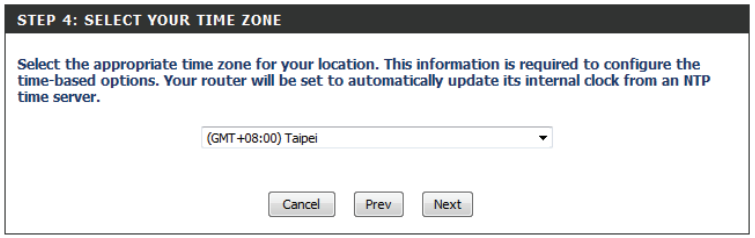
Click **Next** to continue.



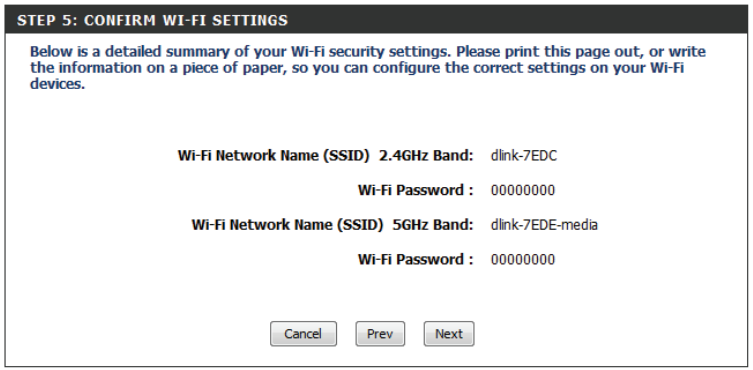
In order to secure your router, please enter a new password, which will be used to access the web-based configuration utility. Check the **Enable Graphical Authentication** box to enable CAPTCHA authentication for added security. Click **Next** to continue.



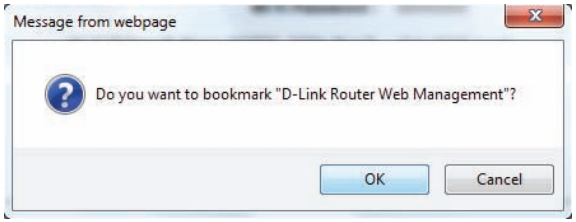
Select your time zone from the drop-down menu and click **Next** to continue.



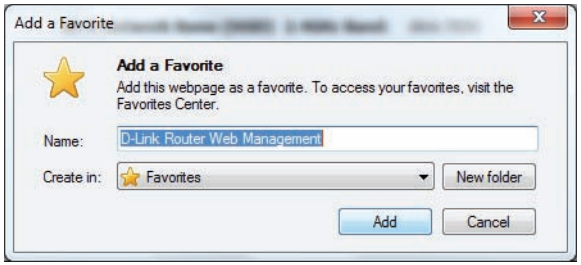
The next window will display your Wi-Fi settings and confirm the completion of the setup process. Click **Next** to continue.



If you want to create a bookmark for the router's web-based configuration utility, click **OK**. Click **Cancel** if you do not want to create a bookmark.

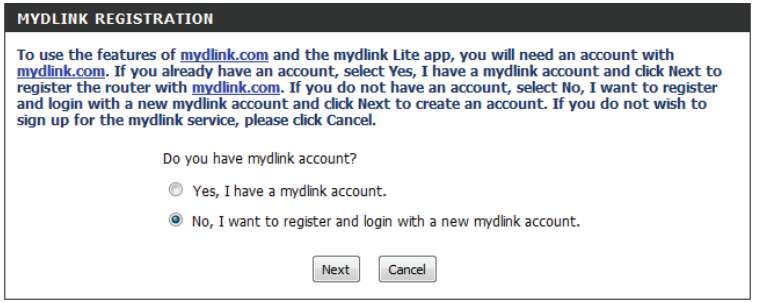


If you clicked **Yes**, a window may appear (depending on which web browser you are using) to create a bookmark.

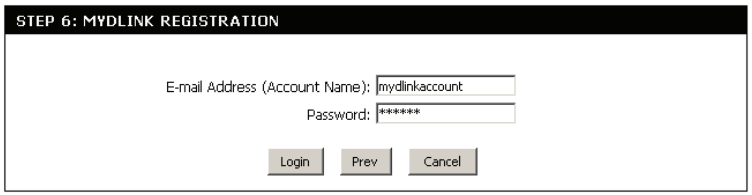


To use the mydlink service (mydlink.com or the mydlink Lite app), you must have an account. Select whether you do have a mydlink account or if you need to create one. Click **Next** to continue.

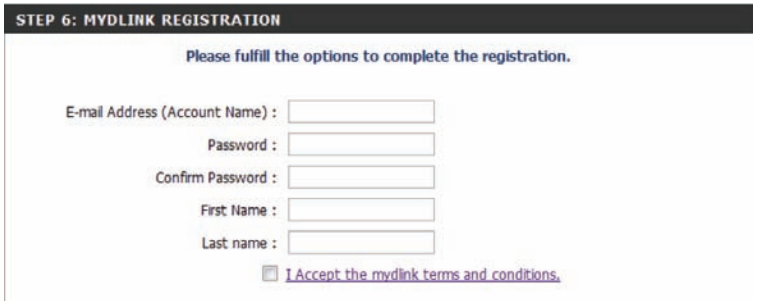
If you do not want to register at this time, click **Cancel**.



If you clicked **Yes**, enter your mydlink account name (email address) and password. Click **Login** to register your router.



If you clicked **No**, fill out the requested information, check the box to accept the terms and conditions of use, and click **Sign Up** to create your mydlink account. Click the hyperlink if you wish to read the terms and conditions before you proceed.



The mydlink app will allow you to receive notifications, browse network usage, and configure your router from an iOS (3.0 or higher), Android (1.6 or higher) device.

To download the "mydlink lite" app, visit the iOS App Store, Google Play Store, or **http://mydlink.com/Lite**.

PC and Mac users can use the mydlink portal at **http://mydlink.com**.

QRS Mobile App (iOS, Android)

D-Link offers an app for your iOS or Android device which will assist you to install and configure your router.

Step 1
From an iOS device, go to the iOS App Store. From an Android device go to the Google Play Store. Search for 'D-Link', select **QRS Mobile**, and download the app to your device. You may also scan the appropriate code on the right to locate the app download page.

iOS

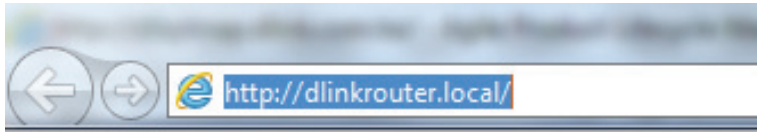
Android

Step 2
Once you have installed the app, you can now configure your router. Connect to the router wirelessly by going to your wireless utility on your device. Scan for the Wi-Fi name (SSID) as listed on the supplied info card. Select and then enter your Wi-Fi password.

Step 3
Once you have connected to the router, launch the QRS mobile app and it will guide you through the installation of your router.

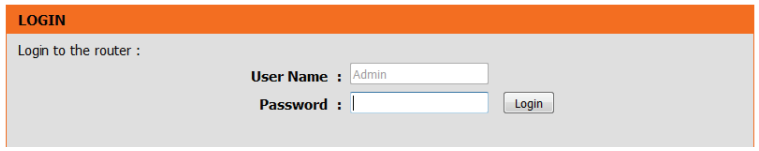
Web-based Configuration Utility

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



Non-Windows and Non-Mac users may also connect by typing **http://192.168.0.1** in the address bar.

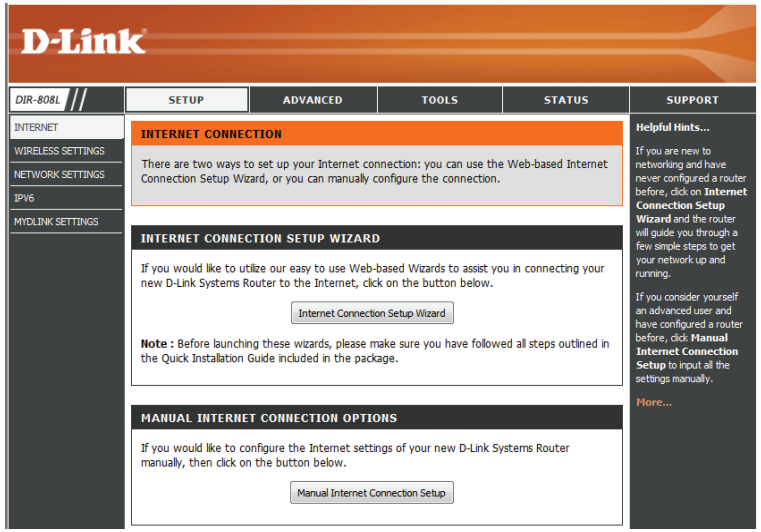
Enter "Admin" as the administrator login name. Leave the password blank by default. Click **Login** to continue.



Internet Connection Setup

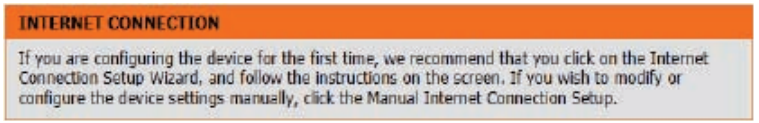
If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard.** You will be directed to the Quick Setup Wizard.

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



Internet Connection Setup Wizard

When configuring the router for the first time, we recommend that you use the **Internet Connection Setup Wizard**, and follow the instructions on the screen. This wizard is designed to provide users with a quick and easy method to configure the Internet connectivity of this router.



At any time during the Internet Connection Setup Wizard, users can click on the **Cancel** button to discard any changes made and return to the main Internet page. Also, users can click on the **Prev** button to return to the previous window for re-configuration.

Welcome:

This 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.

Step 1: Set Your Password

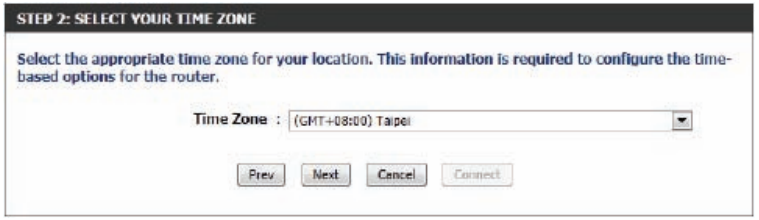
By default, the router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please enter and verify a password in the spaces provided. The two passwords must match. You should also make a record of this password for future reference.

Click **Next** to continue.

Step 2: Select Your Time Zone

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

Click **Next** to continue.



Step 3: Internet Connection

Here the user will be able to configure the Internet connectivity used by this device. If your ISP connection is listed in the drop-down menu, select it and click **Next**. If your ISP connection is not listed then you can proceed to select any of the other manual Internet connection methods listed below.

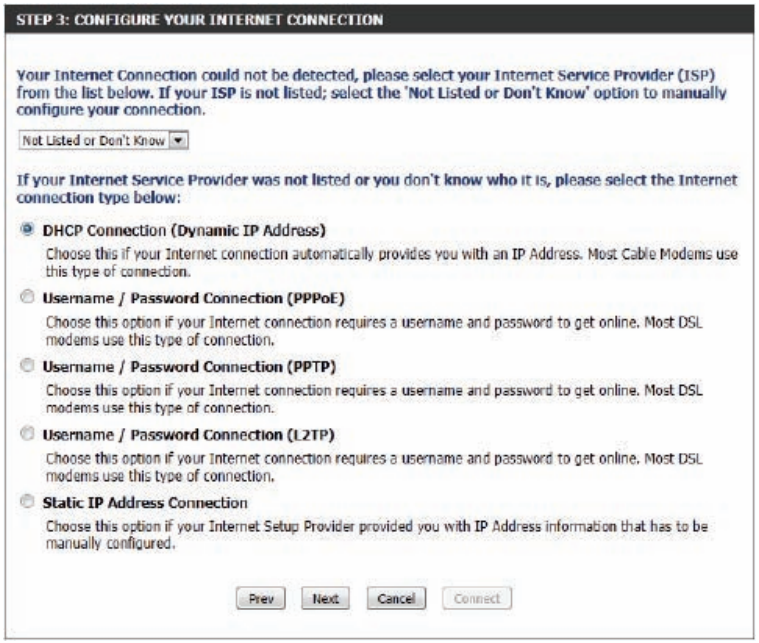
Dynamic IP Address: Choose this if your Internet connection automatically provides you with an IP address. Most cable modems use this type of connection.

PPPoE: Choose this option if your Internet connection requires a PPPoE username and password to access the Internet. Most DSL modems use this type of connection.

PPTP: Choose this option if your Internet connection requires a PPTP username and password to access the Internet.

L2TP: Choose this option if your Internet connection requires an L2TP username and password to access the Internet.

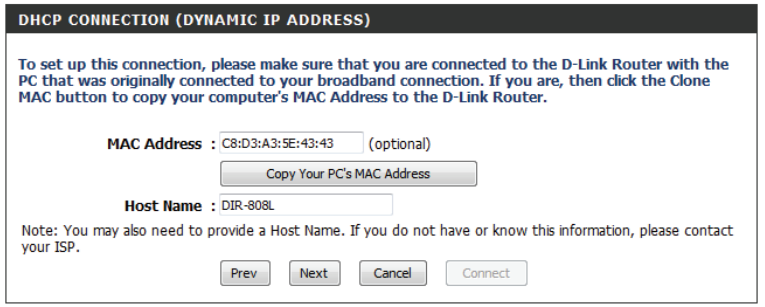
Static IP Address: Choose this option if your Internet Service Provider provided you with IP Address information that has to be manually configured.



Step 3: Internet Connection (Dynamic IP Address)

After selecting the **Dynamic IP Address** Internet connection method, the following page will appear.

The following parameters will be available for configuration:



MAC Address: Enter the MAC address of the Internet gateway (plugged into the Internet port of this device) here.

Copy Button: If the configuration PC also acts as the Internet gateway, then click on the **Copy Your PC's MAC Address** button to copy the PC's MAC address into the space provided. If you're not sure, leave the MAC address field blank.

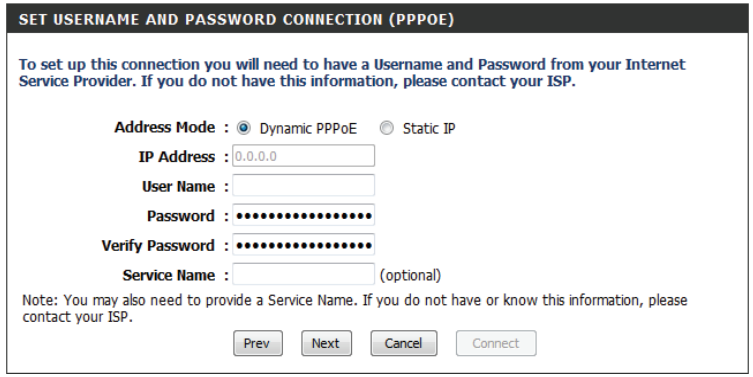
Host Name: Enter the host name used here. You may also need to provide a host name. If you do not have or know this information, please contact your ISP.

Click **Next** to continue.

Step 3: Internet Connection (PPPoE)

After selecting the PPPoE Internet connection method, the following page will appear:

The following parameters will be available for configuration:



Address Mode: Choose the IP address mode for your PPPoE connection.

IP Address: If you are using **Static PPPoE**, enter the IP address provided by your ISP.

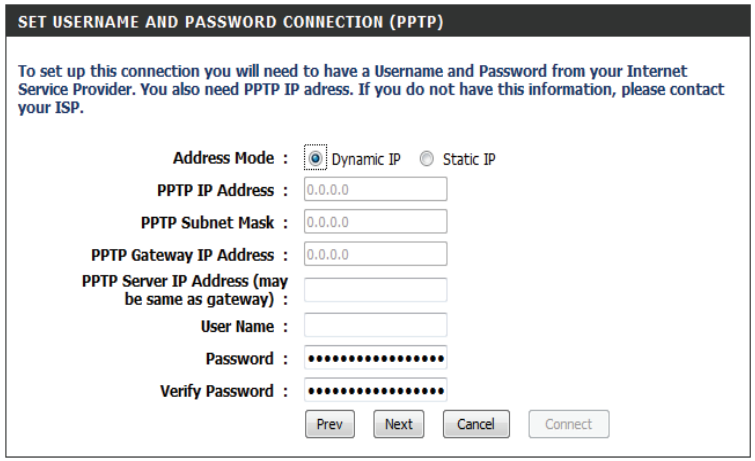
User Name: Enter the PPPoE account user name used here. This information is given by the ISP.

Password: Enter the PPPoE account password used here. This information is given by the ISP.

Service Name: You may be required to enter a service name by your ISP.

Step 3: Internet Connection (PPTP)

After selecting the PPTP Internet connection method, the following page will appear:



The following parameters will be available for configuration:

Address Mode: Here the user can specify whether this Internet connection requires the use of a dynamic or static IP address. PPTP usually requires a dynamic IP configuration.

PPTP IP Address: Enter the PPTP IP address used here. This option is only available if **Static IP** is selected.

PPTP Subnet Mask: Enter the PPTP subnet mask used here.

PPTP Gateway IP Address: Enter the PPTP gateway IP address used here.

PPTP Server IP Address: Enter the PPTP server IP address used here. This is normally the same a the PPTP gateway IP address.

User Name: Enter the PPTP username used here.

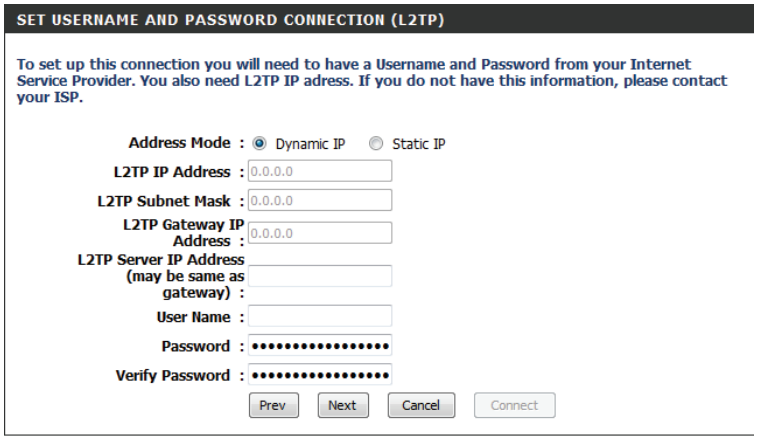
Password: Enter the PPTP password used here.

Verify Password: Re-enter the PPTP password used here.

Click **Next** to continue.

Step 3: Internet Connection (L2TP)

After selecting the **L2TP Internet** connection method, the following page will appear:



The following parameters will be available for configuration:

Address Mode: Here the user can specify whether this Internet connection requires the use of a dynamic or static IP address. L2TP usual requires a dynamic IP configuration.

L2TP IP Address: Enter the L2TP IP address used here. This option is only available if **Static IP** is selected.

L2TP Subnet Mask: Enter the L2TP subnet mask used here.

L2TP Gateway IP Address: Enter the L2TP gateway IP address used here.

L2TP Server IP Address: Enter the L2TP server IP address used here. This is normally the same a the L2TP gateway IP address.

User Name: Enter the L2TP username used here.

Password: Enter the L2TP password used here.

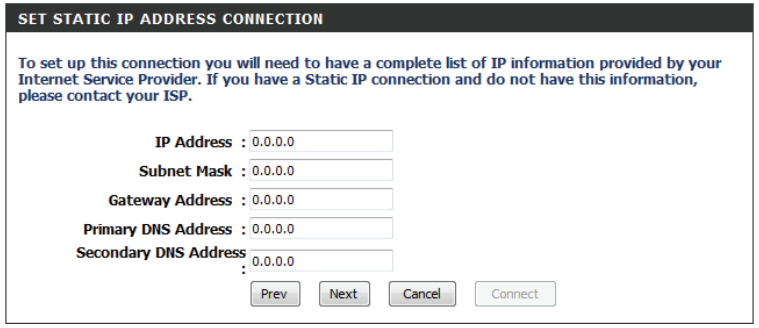
Verify Password: Re-enter the L2TP password used here.

Click **Next** to continue.

Step 3: Internet Connection (Static IP Address)

After selecting the **Static IP Address** Internet connection method, the following page will appear:

The following parameters will be available for configuration:



IP Address: Enter the static IP address provided by the ISP here.

Subnet Mask: Enter the subnet mask provided by the ISP here.

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

Primary DNS Address: Enter the primary DNS IP address used here.

Secondary DNS Address: Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

Click **Next** to continue.

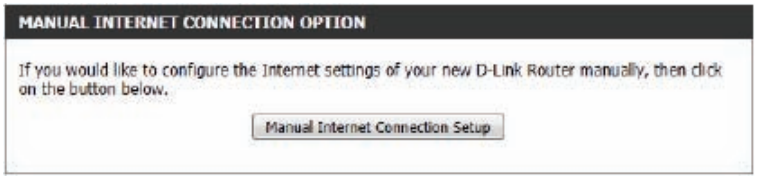
Setup Complete!

This is the last page of the Internet Connection Setup Wizard.

Click the **Connect** button to save your settings.

Internet (Manual Setup)

On this page the you can configure the Internet connection settings manually. To access the Manual Internet Connection Setup page, click on the **Manual Internet Connection Setup** button. On this page there are multiple parameters that can be configured regarding the Internet connection setup.



At any stage throughout the wizard, you can save the current configuration by clicking on the **Save Settings** button. If you wish to discard the changes made, click on the **Don't Save Settings** button.

Internet Connection Type

In this section, you can select from a list of Internet connection types that can be configured and used on this router. Options to choose from are **Static IP**, **Dynamic IP**, **PPPoE**, **PPTP**, **L2TP**, and **DS-Lite**.

After selecting a specific Internet connection type, this page will automatically refresh and provide unique fields to configure related to the specified Internet connection type.

<u>My Internet Connection is: Dynamic IP (DHCP)</u>

The default WAN configuration for this router is **Dynamic IP (DHCP)**. This option allows the router to obtain an IP address automatically from the device that is connected to the Internet port.

Note: If you're not sure about the type of Internet connection you have, please contact your Internet Service Provider (ISP) for assistance.

After selecting **Dynamic IP**, the following parameters will be available for configuration:

Enable Advanced DNS Service: Check the box to enable advanced DNS service

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

Use Unicasting: Tick this option if your ISP uses the unicast method to provide IP addresses.

Primary DNS: Enter the primary DNS IP address used here.

Secondary DNS: Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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

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

Manual Internet Setup
Static (assigned by ISP)

Select **Static IP Address** if your Internet Service Provider has supplied you with IP settings. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets each separated by a dot (x.x.x.x). The router will not accept the IP address if it is not in this format.

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

Enable Advanced DNS Service: Check the box to enable advanced DNS service.

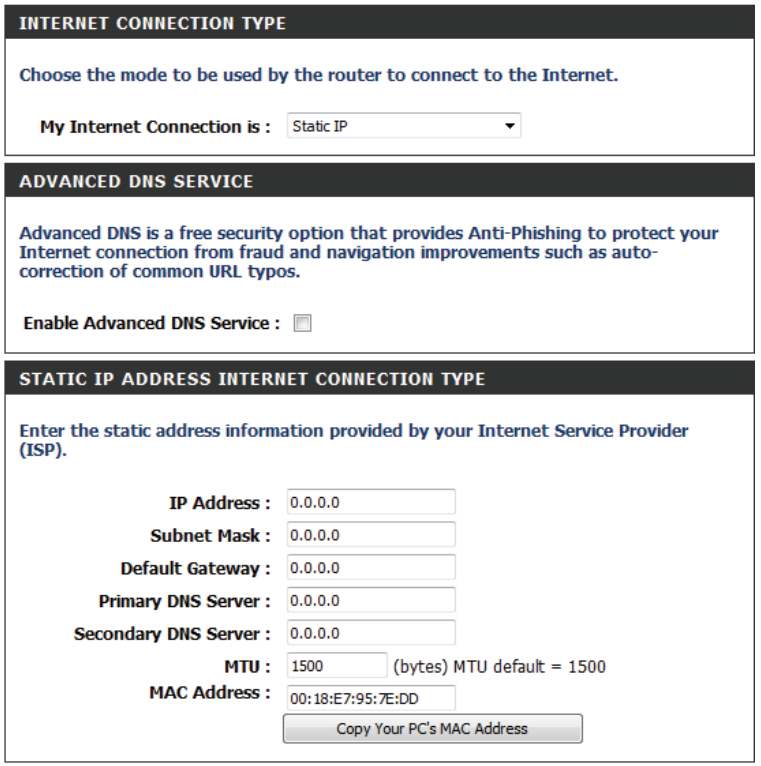
IP Address: Enter the IP address assigned by your ISP.

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

Default Gateway: Enter the gateway assigned by your ISP.

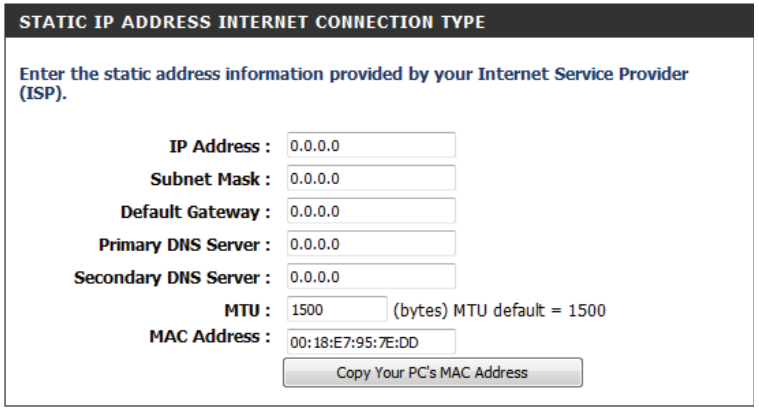
Primary DNS Server: Enter the primary DNS IP address used here

Secondary DNS Server: Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.



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

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



Internet Setup
PPPoE (DSL)

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

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

Advanced DNS Service: Check the box to enable advanced DNS service.

Address Mode: Here the user can specify whether this Internet connection requires the use of a **Dynamic** or **Static IP** address. PPPoE usually requires a Dynamic IP configuration.

IP Address: Enter the PPPoE IP address used here. This option is only available if **Static IP** is selected.

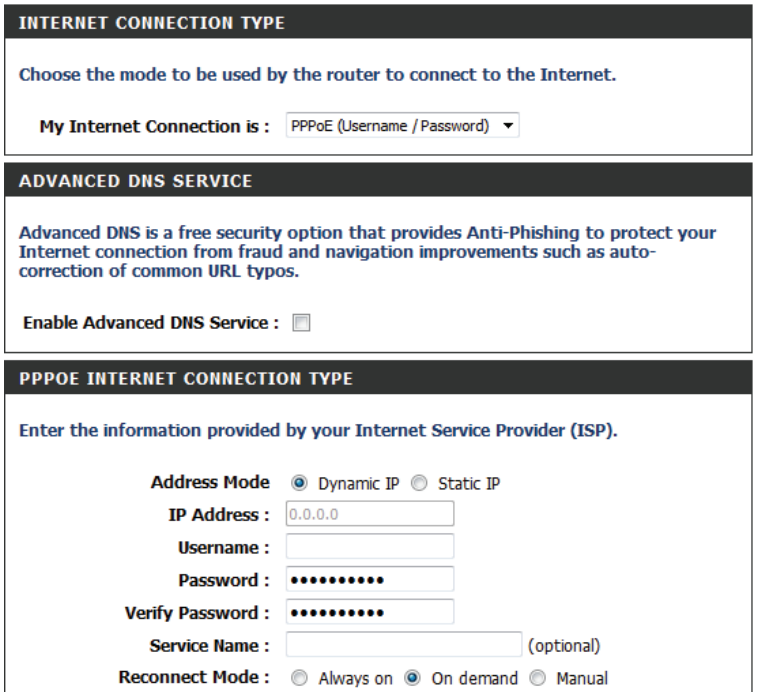
Username: Enter the PPPoE account user name used here. This information is given by the ISP.

Password: Enter the PPPoE account password used here. This information is given by the ISP.

Verify Password: Re-enter the PPPoE account password used here.

Service Name: This optional field enables the user to enter a service name to identify this Internet connection here.

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page.



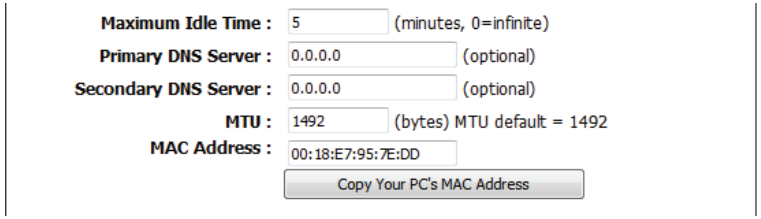
Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, set the reconnect mode to **Always on**.

Primary DNS Server: Enter the primary DNS IP address used here.

Secondary DNS Server: Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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

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



Internet Setup
PPTP

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

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

Advanced DNS Service: Check the box to enable advanced DNS service.

Address Mode: Here the user can specify whether this Internet connection requires the use of a **Dynamic** or **Static IP** address. PPTP usually requires a dynamic IP configuration.

PPTP IP Address: Enter the PPTP IP address used here. This option is only available if static IP is selected.

PPTP Subnet Mask: Enter the PPTP subnet mask used here.

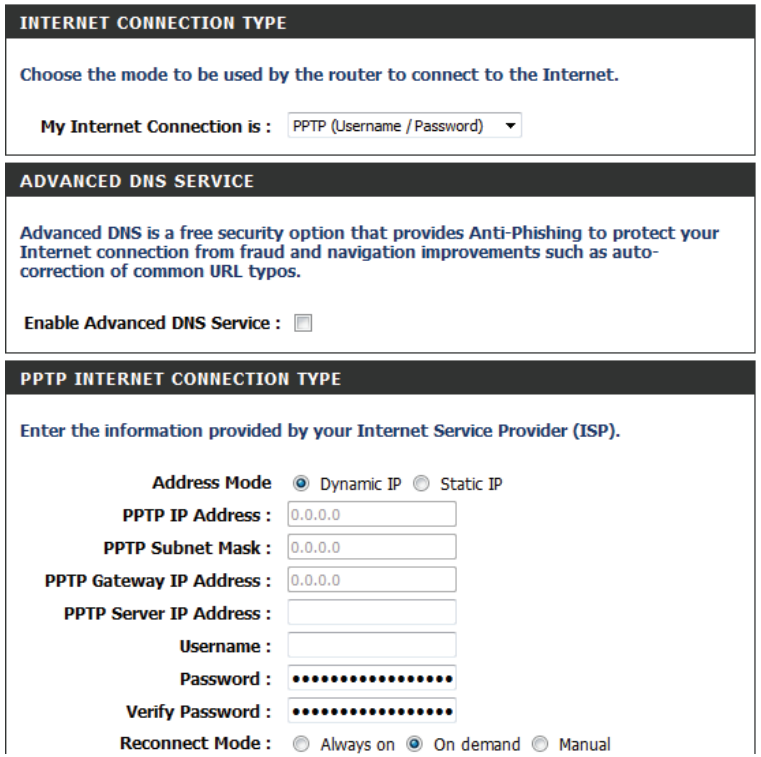
PPTP Gateway IP Address: Enter the PPTP gateway IP address used here.

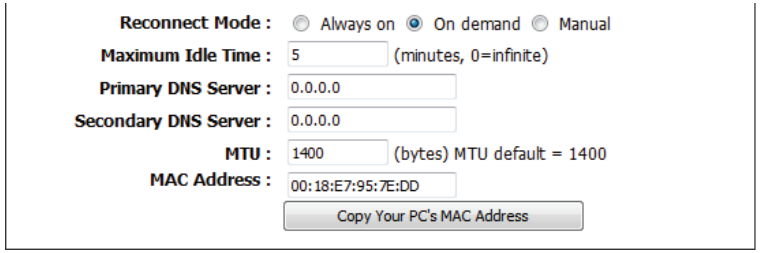
PPTP Server IP Address: Enter the PPTP server IP address used here. This is normally the same a the PPTP gateway IP address.

Username: Enter the PPTP username used here.

Password: Enter the PPTP password used here.

Verify Password: Re-enter the PPTP password used here.





Reconnect Mode: Use the radio buttons to specify the reconnect mode. You can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the **New Schedule** button to open the Schedules page.

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

Primary DNS Server: Enter the primary DNS IP address used here.

Secondary DNS Server: Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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 **Copy Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Internet Setup
L2TP

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

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

Advanced DNS Service: Check the box to enable advanced DNS service.

Address Mode: Here the user can specify whether this Internet connection requires the use of a dynamic or static IP address. L2TP usual requires a dynamic IP configuration.

L2TP IP Address: Enter the L2TP IP address used here. This option is only available if **Static IP** is selected.

L2TP Subnet Mask: Enter the L2TP subnet mask used here.

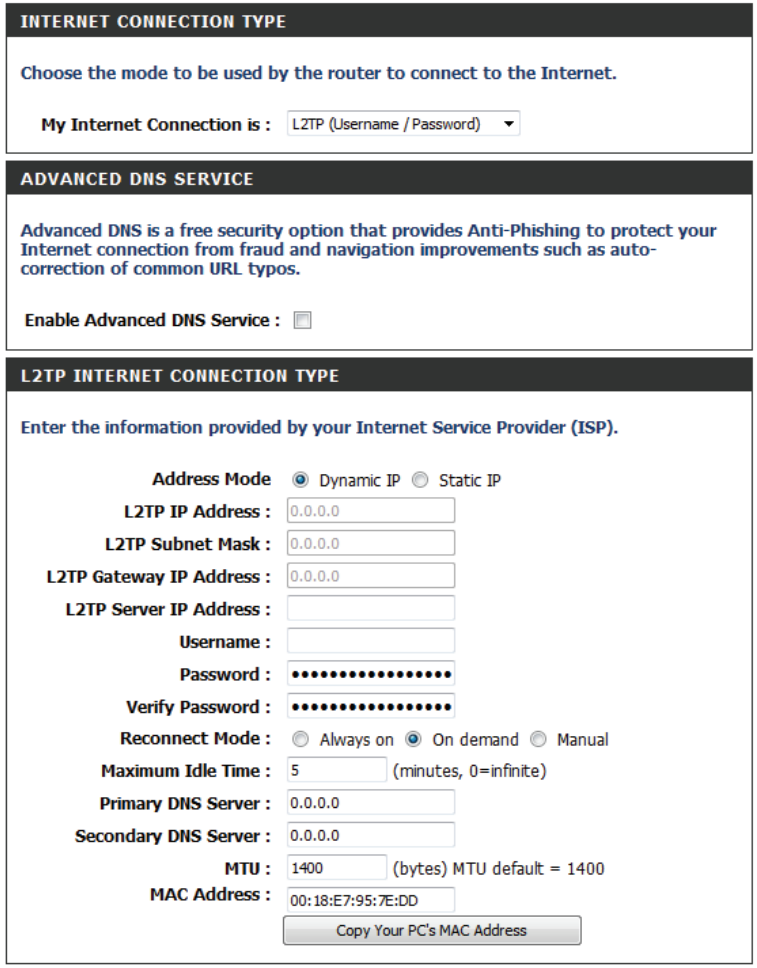
L2TP Gateway IP Address: Enter the L2TP gateway IP address used here.

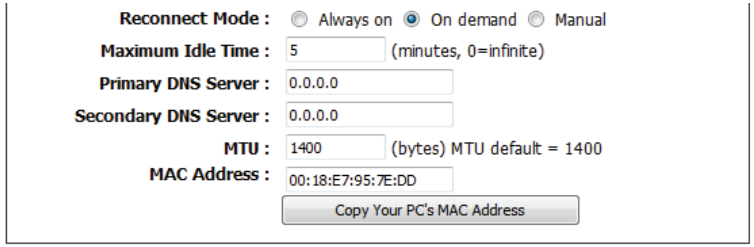
L2TP Server IP Address: Enter the L2TP server IP address used here. This is normally the same a the L2TP gateway IP address.

Username: Enter the L2TP username used here.

Password: Enter the L2TP password used here.

Verify Password: Re-enter the L2TP password used here.





Reconnect Mode: Use the radio buttons to specify the reconnect mode. You can specify a custom schedule or specify the **On Demand**, or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the Schedules page. To create a new schedule, click the **New Schedule** button to open the Schedules page.

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

Primary DNS Server: Enter the primary DNS IP address used here.

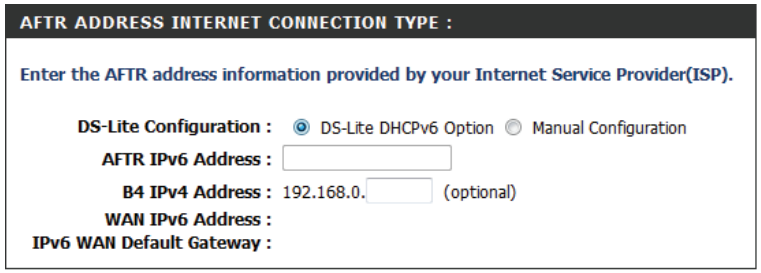
Secondary DNS Server: Enter the secondary DNS IP address used here. This field is normally optional. Only one DNS address is required for a functional Internet connection, but using a second DNS address provides more stability.

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 **Copy Your PC's MAC Address** button to replace the Internet port's MAC address with the MAC address of your Ethernet card.

Internet Setup
DS-Lite

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



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

AFTR IPv6 Address: After selecting the Manual Configuration option above, the user can enter the AFTR IPv6 address used here.

B4 IPv4 Address: Enter the B4 IPv4 address value used here.

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

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

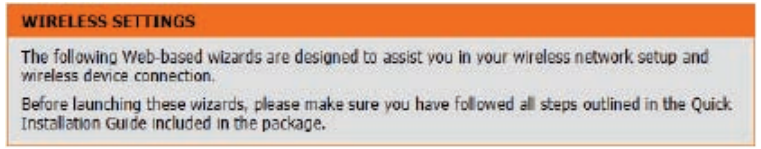
Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

Wireless Connection Setup Wizard

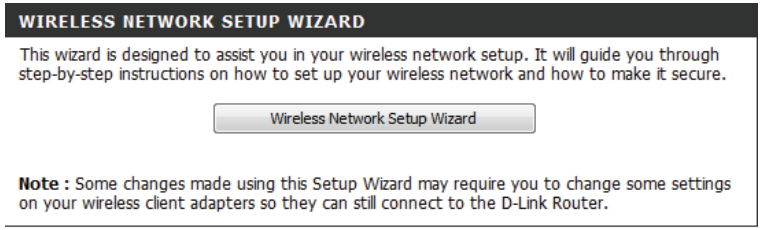
On this page you can configure the wireless settings for this device. There are three ways to configure wireless using this router. Firstly, the user can make use of the quick and easy Wireless Connection Setup Wizard. Secondly, the user can choose Wi-Fi Protected Setup. Lastly, the user can configure the wireless settings manually.

Wireless Settings: Wireless Connection Setup Wizard

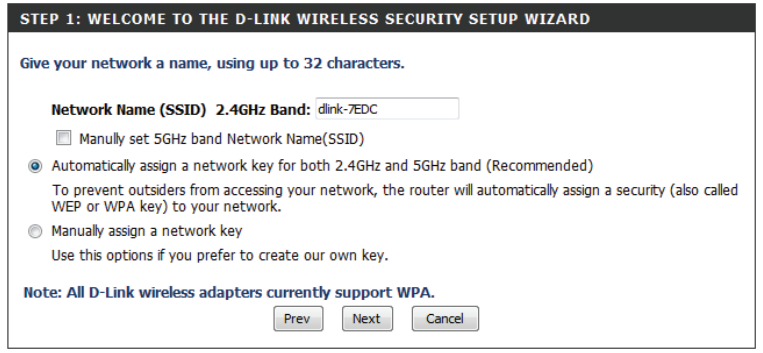
The Wireless Connection Setup Wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to configure the wireless settings of this router. It is highly recommended to customize the wireless network settings to fit into your environment and to add higher security.



To initiate the Wireless Connection Setup Wizard click on the **Wireless Network Setup Wizard** button.



Step 1: In this step, you must enter a custom wireless network name or SSID. Enter the new Network Name (SSID) in the appropriate space provided.
By default, the SSID selected for the 2.4 GHz network name will be the same for the 5 GHz network name. Users can check the **Manually set 5 GHz band Network Name(SSID)** checkbox to specify a different SSID for the 5 GHz band.

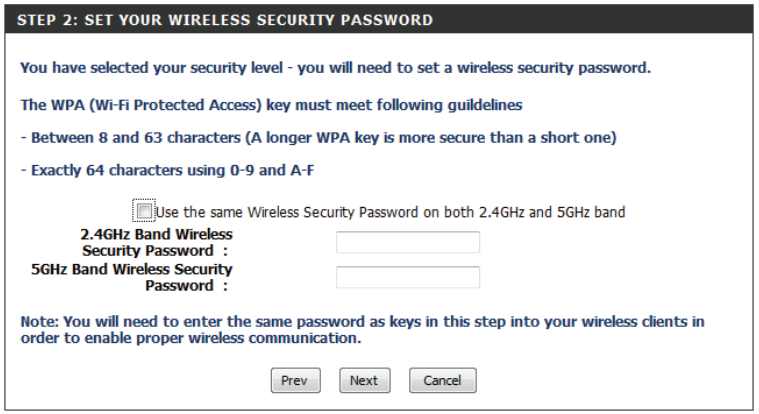


You can choose between two wireless security wizard configurations. Users can select **Automatically assign a network key**, by which the router will automatically generate a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods; or you can select **Manually assign a network key** by which you will be prompted to manually enter a WPA/WPA2 pre-shared key using the TKIP and AES encryption methods.

At any stage during this wizard, you can click on the **Prev** button to return to the previous page, click on the **Next** button to continue to the next page, or click on the **Cancel** button to discard the changes made and return to the main wireless page.

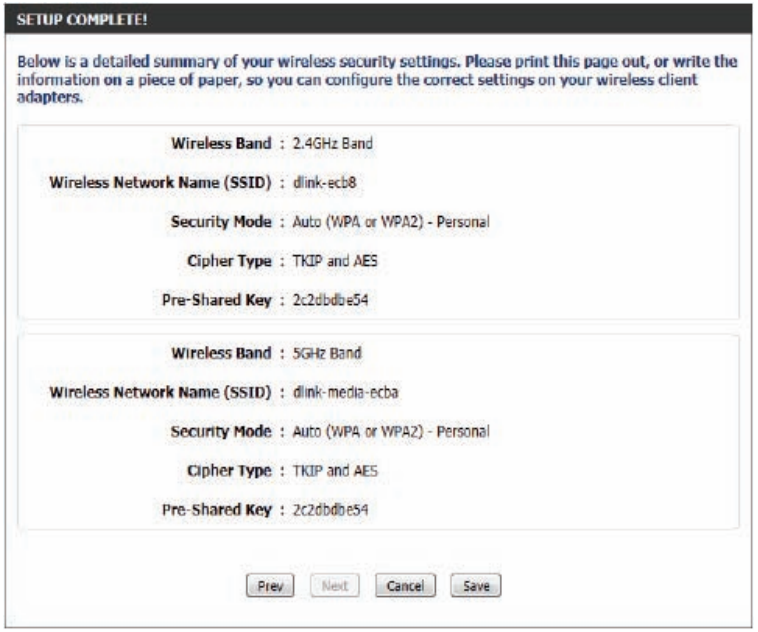
Step 2: This step will only be available if you have selected **Manually assign a network key** in the previous step. Here you can manually enter the WPA/WPA2 pre-shared key in the **Wireless Security Password** space provided. The key entered must be between 8 and 63 characters long. Remember, this key will be used when wireless clients connect to this device, so it is important to make a record of this key to prevent trouble when accessing your wireless network in the future.
If you wish to use the same Wireless Security Password for both 2.4 GHz and 5 GHz bands, check the option provided. If not selected, you need to input two separate wireless security passwords for each individual wireless band.

Click on the **Next** button to advance to the next step.



Setup Complete: The wireless configuration information will be summarized on this page. It is recommended that you check the correctness of these settings and make a record of the information listed on this page for future reference.

Click on the **Save** button to complete the setup wizard and save the changes made.



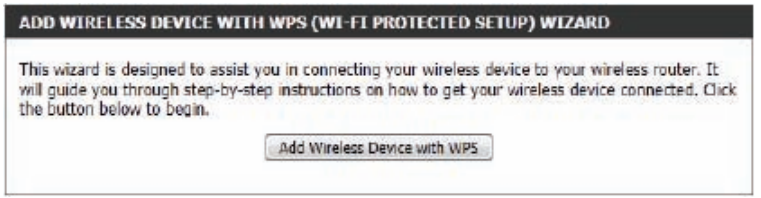
After clicking the **Save** button, the device will save the settings made and return to the main wireless page.

End of Wizard.

Wi-Fi Protected Setup Wizard

Wireless Settings: Wi-Fi Protected Setup Wizard

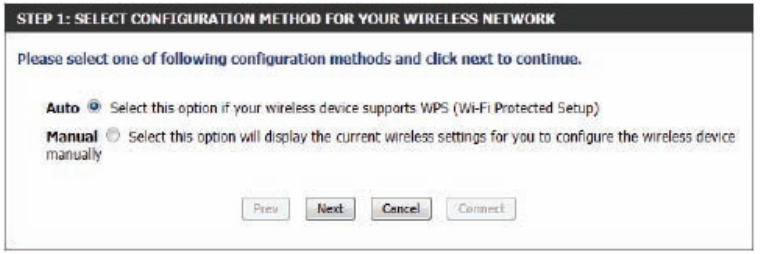
If your wireless clients support the W-Fi Protected Setup (WPS) connection method, this wizard can be used to initiate a secure wireless connection between this device and wireless clients with a simple click of the WPS button. The Wi-Fi Protected Setup wizard is specially designed to assist basic network users with a simple, step-by-step set of instructions to connect wireless clients to this router securely using the WPS method.



To initiate the Wi-Fi Protected Setup wizard click on the **Add Wireless Device with WPS** button.

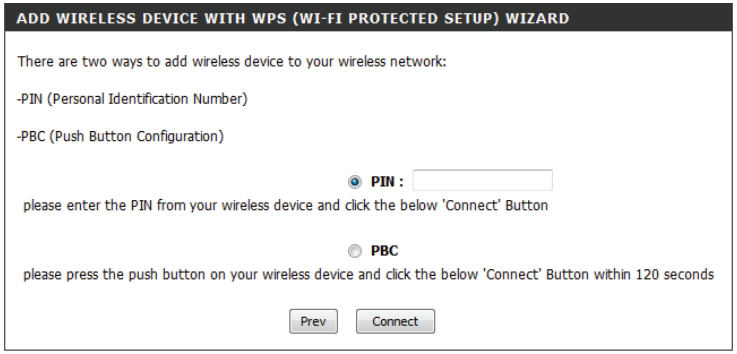
Step 1: In this step there are two options to choose from. You can choose **Auto** if the wireless client supports WPS, or **Manual** if the wireless client does not support WPS.

At any stage during this wizard, you can click on the **Prev** button to return to the previous page, click on the **Next** button to continue to the next page, or click on the **Cancel** button to discard the changes made and return to the main wireless page.



Step 2 - Auto: After selecting **Auto**, the following page will appear. There are two ways to add a wireless device which supports WPS. Firstly, the Personal Identification Number (PIN) method will prompt you to enter the PIN code which was provided with your wireless device. This PIN code should be identical on the wireless client. Secondly, the Push Button Configuration (PBC) method will allow the wireless client to connect to your router by pressing the WPS button on the client device.

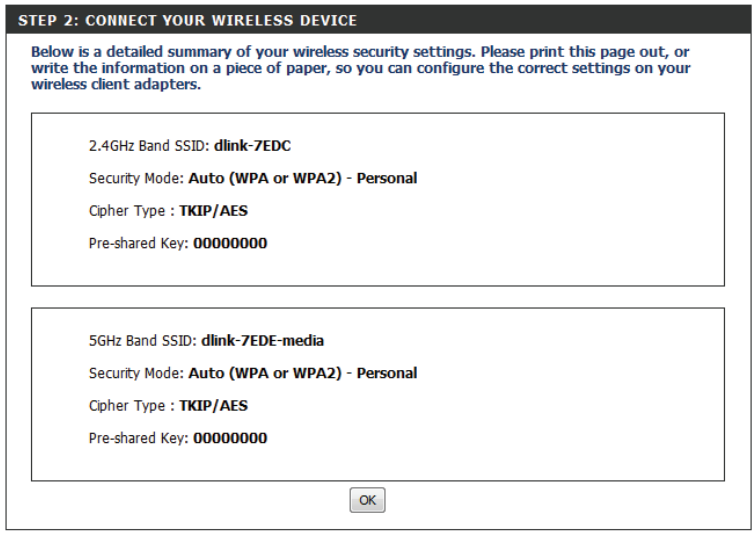
Choose the preferred method of WPS and click on the **Connect** button to establish a connection.



Step 2 - Manual: After selecting **Manual**, the following page will appear. On this page you can view the wireless configuration of this router. The wireless clients should configure their wireless settings to be identical to the settings displayed on this page for a successful connection. This option is for wireless clients that do not support the WPS Push Button method to connect to this router.

It is recommended that you make a record of this information for future reference. Click on the **OK** button to the Wireless Settings page.

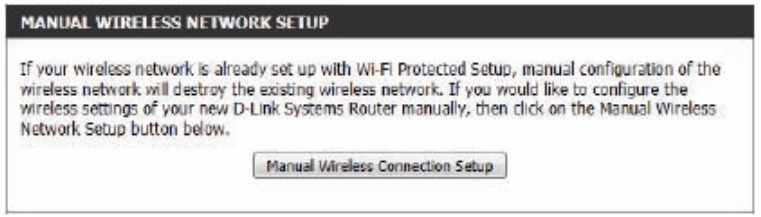
End of Wizard.



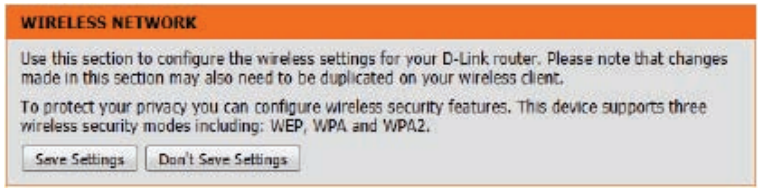
Manual Wireless Network Setup

Wireless Settings: Manual Wireless Network Setup

The Manual Wireless Network Setup option allows you to configure the wireless settings of this device manually. This option is for advanced users and includes all parameters that can be configured for wireless connectivity.



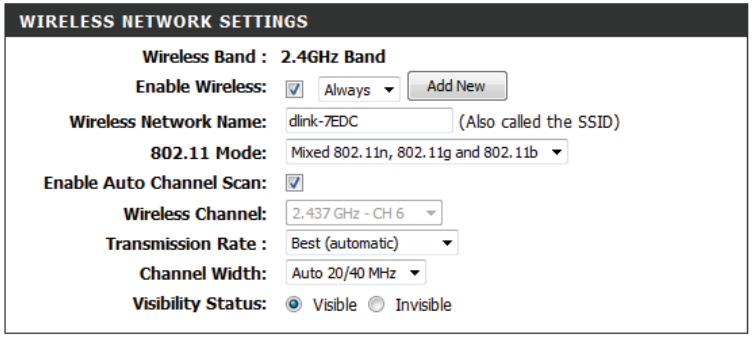
To initiate the Manual Wireless Setup page, click on the **Manual Wireless Connection Setup** button.



At any stage during setup, you can click on the **Save Settings** button to save the current configuration, or click on the **Don't Save Settings** button to discard any changes made and return to the main wireless setup page.

Manual Setup - 2.4 Ghz Band

The following parameters will be available for configuration:



Wireless Band: Displays the wireless band being configured. The following configuration relates to the **2.4 GHz** band.

Enable Wireless: Tick the box to enable the wireless function. Select **Always** from the drop-down menu to enable wireless at all times. If you do not want to use wireless, uncheck the box to disable all wireless functions. To set a schedule for the times when you want the wireless network to be available, click on the **Add New** button to specify a new schedule.

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

802.11 Mode: Here you can manually select the preferred wireless standard to use for this wireless network. You should select the 802.11 mode according to the capabilities of the wireless clients/ devices which will be accessing this network. If only 802.11n devices will be accessing your network, it is recommended to set the 802.11 mode to **802.11n only**.

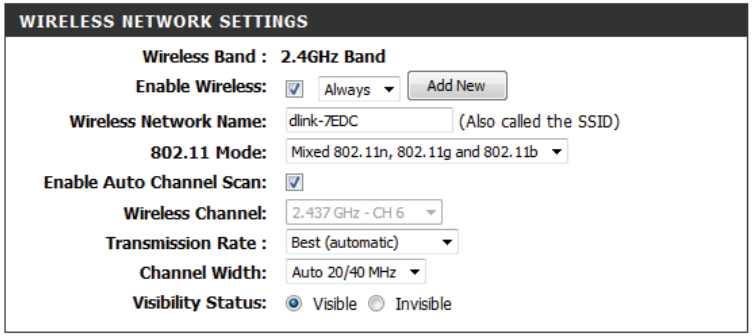
Enable Auto Channel Scan: The auto channel selection setting can be selected to allow this device to choose the wireless channel with the least amount of interference.

Wireless Channel: If auto channel scan is disabled, you can select your preferred wireless channel. By default the channel is set to 1. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Transmission Rate: Select the transmission rate. It is strongly suggested that **Best (Automatic)** is selected for best performance.

Channel Width: When using the 802.11n frequency band, you have an option to choose between a 20 MHz only, or 20/40 MHz bandwidth.

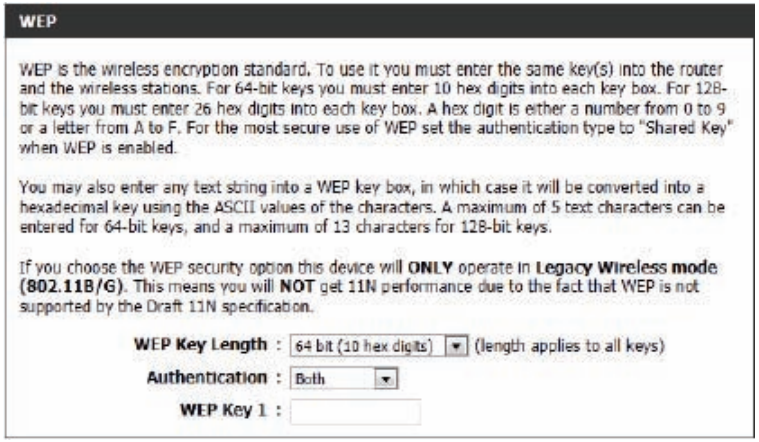
Visibility Status: This option allows you to adjust the visibility of your SSID. If **Visible** is selected, the SSID of your wireless network will be visible to any wireless clients within range of the signal. If **Invisible** mode is selected, clients must search for the SSID of your wireless network manually in order to connect to the network.



By default the wireless security of this router will be disabled. In this option you can enable or disable wireless security for the frequency band 2.4 GHz. There are two types of encryption that can be used: WEP or WPA/WPA2. For further information on these security types, please refer to "Wireless Security" on page 57.

Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. WEP is considered to be a relatively weak security method, however it provides more protection than an unsecured network. Older wireless adapters may only support WEP encryption. It is recommended that this method is used only if your wireless clients do not support WPA.



The following parameters are available for configuration:

WEP Key Length: Here the user can specify to either use a 64-bit or a 128-bit encryption key.

Authentication: Authentication is a process by which the router verifies the identity of a network device that is attempting to join the wireless network. There are two types authentication for this device when using WEP. **Open System** allows all wireless devices to communicate with the router before they are required to provide the encryption key needed to gain access to the network. **Shared Key** requires any wireless device attempting to communicate with the router to provide the encryption key needed to access the network before they are allowed to communicate with the router.

WEP Key 1: Enter the WEP key used here. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

Wireless Security Mode: WPA-Personal

Wi-Fi Protected Access (WPA) is the most advanced wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a passphrase (Pre-Shared Key) for security.

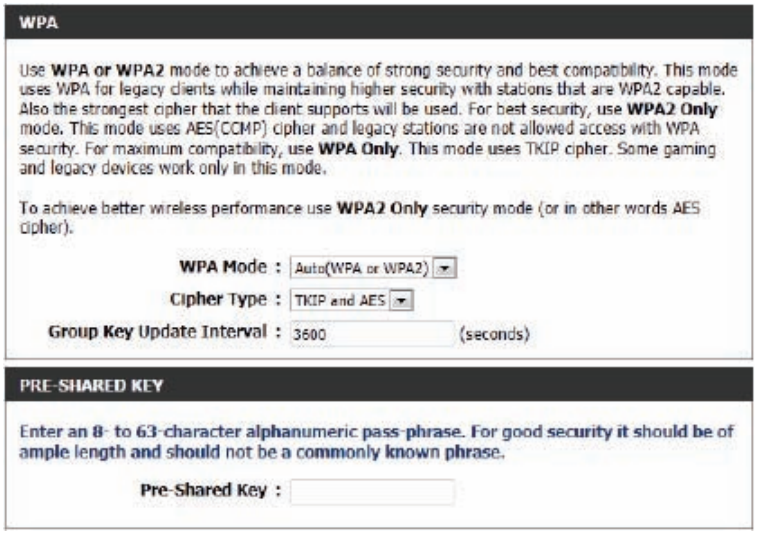
The following parameters will be available for configuration:

WPA Mode: WPA is an older standard; select this option if the clients that will be used with the router only support this older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. Select **Auto (WPA or WPA2)** to have the security set automatically depending on the compatibility of connected clients. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), or Both (**TKIP and AES**).

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Pre-Shared Key: Enter the password to be used for the wireless network here. This password is required by wireless clients for them to be able to connect to the wireless network successfully.



Wireless Security Mode: WPA-Enterprise

WPA-Enterprise is a more sophisticated level of wireless security which requires a RADIUS Authentication Server. This form of security is used primarily in medium to large-scale network environments.

The following parameters will be available for configuration:

WPA Mode: WPA is an older standard; select this option if the clients that will be used with the router only support this standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. Select **Auto (WPA or WPA2)** to have the security set automatically depending on the compatibility of connected clients. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), and Both (**TKIP and AES**).

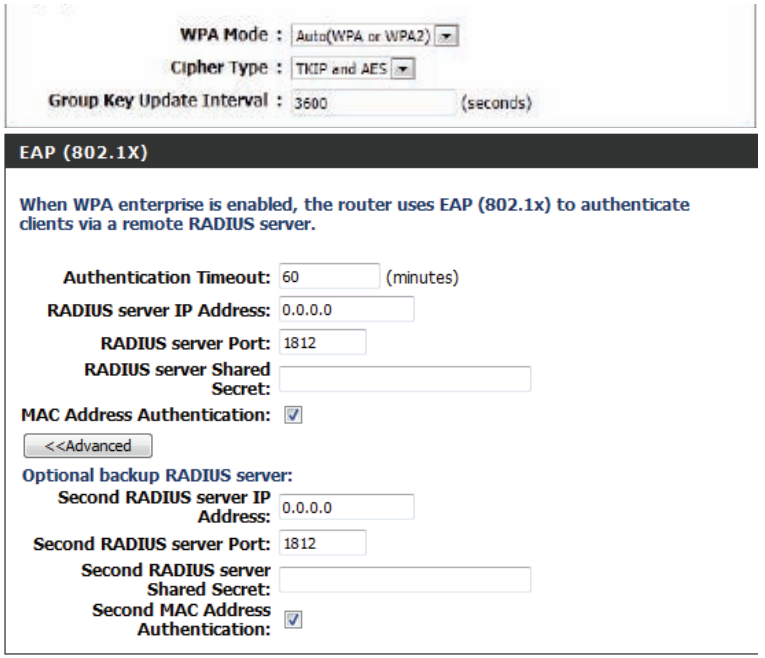
Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Authentication Timeout: Specifies the amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: When the user chooses to use the EAP authentication framework, the RADIUS server's IP address can be entered here.

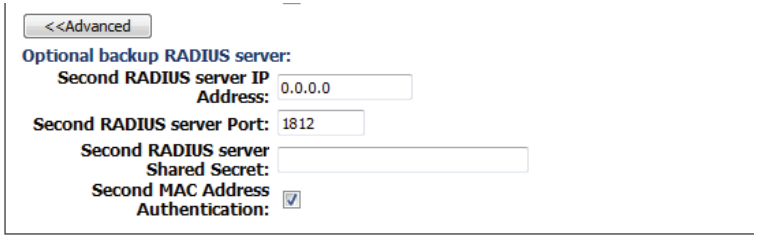
RADIUS Server Port: When you can choose to use the EAP authentication framework, the RADIUS server's port number can be entered here.

RADIUS Server Shared Secret: Enter the shared secret (password) used here. This password needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.



MAC Address Authentication: Select this option to include authentication of clients according to their MAC address.

Optional backup RADIUS server: This option allows you to specify a secondary RADIUS server to be used in the event that the primary RADIUS server fails. Enter the information for the secondary server in the same manner as the primary server described in the steps on the previous page.



Manual Setup - 5 Ghz Band

The following parameters will be available for configuration:

Wireless Band: Displays the wireless band being configured. The following configuration relates to the **5 GHz** band.

Enable Wireless: Check the box to enable the wireless function at all times. If you do not want to use wireless, uncheck the box to disable all wireless functions. To set a schedule for the times when you want the wireless network to be available, click on the **Add New** button to specify a new schedule.

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

802.11 Mode: Here you can manually select the preferred frequency band to use for this wireless network.

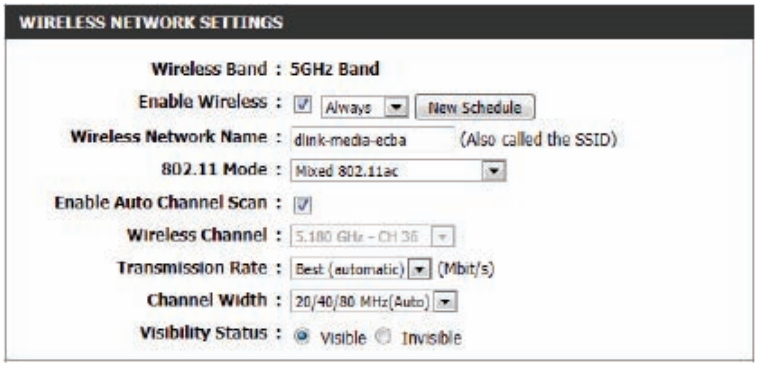
Enable Auto Channel Scan: The auto channel selection setting can be selected to allow this device to choose the channel with the least amount of interference.

Wireless Channel: If Auto Channel Scan is not enabled, you can manually select a wireless channel. By default the channel is set to 36. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network.

Transmission Rate: Select the transmission rate. It is strongly suggested to select Best (Automatic) for best performance.

Channel Width: When using the 802.11n frequency band, you have an option to choose between a 20 MHz, 20/40 MHz, or 20/40/80 MHz bandwidth for 802.11ac.

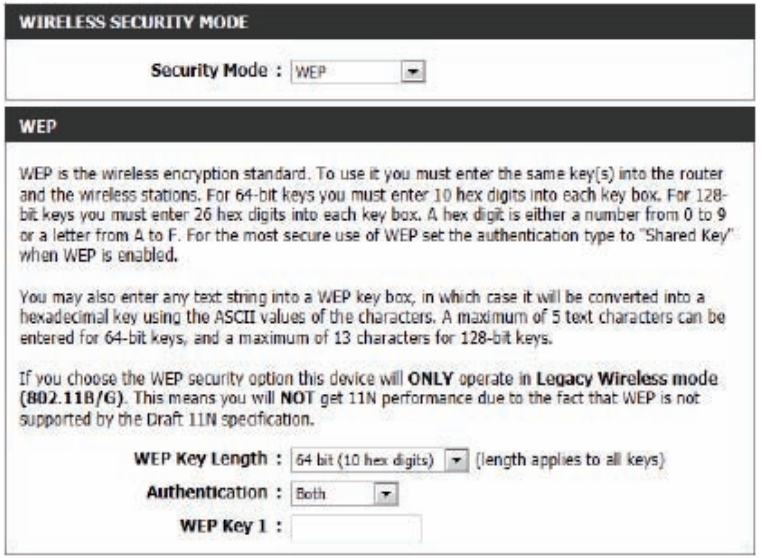
Visibility Status: This option allows you to adjust the visibility of your SSID. If **Visible** is selected, the SSID of your wireless network will be visible to any wireless clients within range of the signal. If **Invisible** mode is selected, clients must search for the SSID of your wireless network manually in order to connect to the network.



By default the wireless security of this router will be disabled. In this option you can enable or disable wireless security for the frequency band 2.4 GHz. There are two types of encryption that can be used: WEP or WPA/WPA2. For further information on these security types, please refer to "Wireless Security" on page 57.

Wireless Security Mode: WEP

Wired Equivalent Privacy (WEP) is the most basic form of encryption that can be used for wireless networks. WEP is considered to be a relatively weak security method, however it provides more protection than an unsecured network. Older wireless adapters may only support WEP encryption. It is recommended that this method is used only if your wireless clients do not support WPA.



The following parameters will be available for configuration:

WEP Key Length: Here the user can specify to either use a 64-Bit or a 128-Bit encrypted key.

Authentication: Authentication is a process by which the router verifies the identity of a network device that is attempting to join the wireless network. There are two types authentication for this device when using WEP. **Open System** allows all wireless devices to communicate with the router before they are required to provide the encryption key needed to gain access to the network. **Shared Key** requires any wireless device attempting to communicate with the router to provide the encryption key needed to access the network before they are allowed to communicate with the router.

WEP Key 1: Enter the WEP key used here. For 64-bit keys you must enter 10 hex digits into each key box. For 128-bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64-bit keys, and a maximum of 13 characters for 128-bit keys.

Wireless Security Mode: WPA-Personal

Wi-Fi Protected Access (WPA) is the most advanced wireless encryption method used today. This is the recommended wireless security option. WPA supports two authentication frameworks. Personal (PSK) and Enterprise (EAP). Personal requires only the use of a passphrase (Pre-Shared Key) for security.

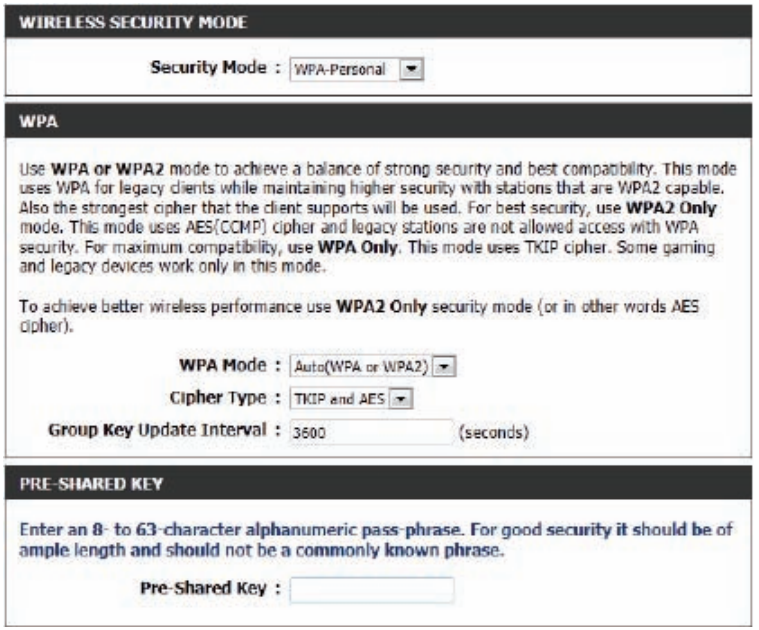
The following parameters will be available for configuration:

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support the older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. Select **Auto (WPA or WPA2)** to have the security set automatically depending on the compatibility of connected clients. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), and Both (**TKIP and AES**).

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

Pre-Shared Key: Enter the password to be used for the wireless network here. This password is required by wireless clients for them to be able to connect to the wireless network successfully.



Wireless Security Mode: WPA-Enterprise

WPA-Enterprise is a more sophisticated level of wireless security which requires a RADIUS Authentication Server. This form of security is used primarily in medium to large-scale network environments.

The following parameters will be available for configuration:

WPA Mode: WPA is the older standard; select this option if the clients that will be used with the router only support this older standard. WPA2 is the newer implementation of the stronger IEEE 802.11i security standard. Select **Auto (WPA or WPA2)** to have the security set automatically depending on the compatibility of connected clients. With the **WPA2** option, the router tries WPA2 first, but falls back to WPA if the client only supports WPA. With the **WPA2 Only** option, the router associates only with clients that also support WPA2 security.

Cipher Type: Select the appropriate cipher type to use here. Options to choose from are Temporal Key Integrity Protocol (**TKIP**), Advanced Encryption Standard (**AES**), and Both (**TKIP and AES**).

Group Key Update Interval: Enter the amount of time before the group key used for broadcast and multicast data is changed.

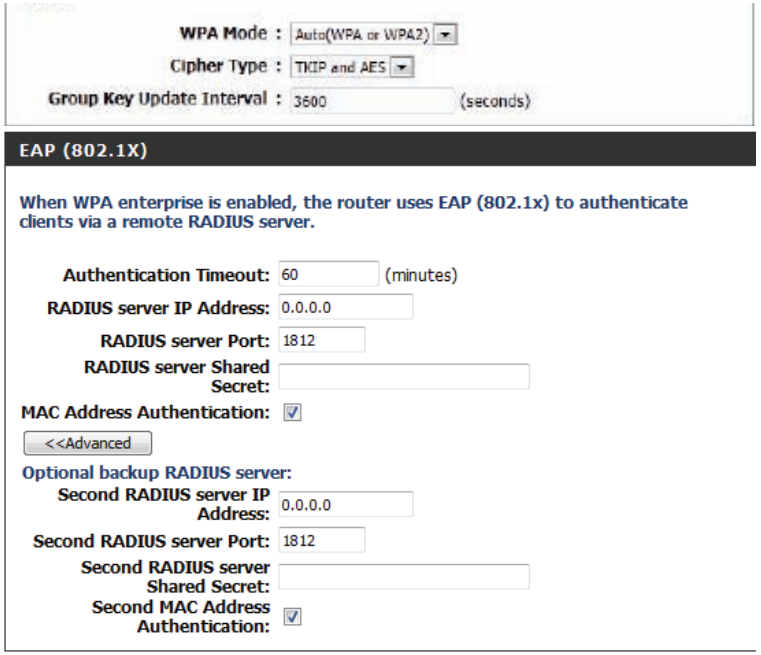
Authentication Timeout: Specifies the amount of time before a client will be required to re-authenticate.

RADIUS Server IP Address: When you choose to use the EAP authentication framework, the RADIUS server's IP address can be entered here.

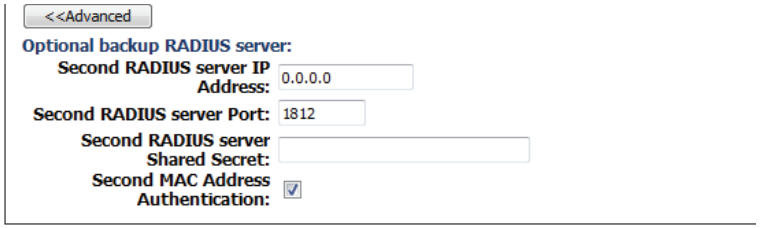
RADIUS Server Port: When the user chooses to use the EAP authentication framework, the RADIUS server's port number can be entered here.

RADIUS Server Shared Secret: Enter the shared secret (password) used here. This password needs to be the same on all of the wireless clients for them to be able to connect to the wireless network successfully.

MAC Address Authentication: Select this option to include authentication of clients according to their MAC address.



Optional Backup RADIUS Server: This option allows you to specify a secondary RADIUS server to be used in the event that the primary RADIUS server fails. Enter the information for the secondary server in the same manner as the primary server described in the steps on the previous page.



Wireless Security

This section discusses the different levels of security you can use to protect your data from intruders. The DIR-808L 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)
- Wired Equivalent Privacy (WEP)

What is WPA?

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

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.

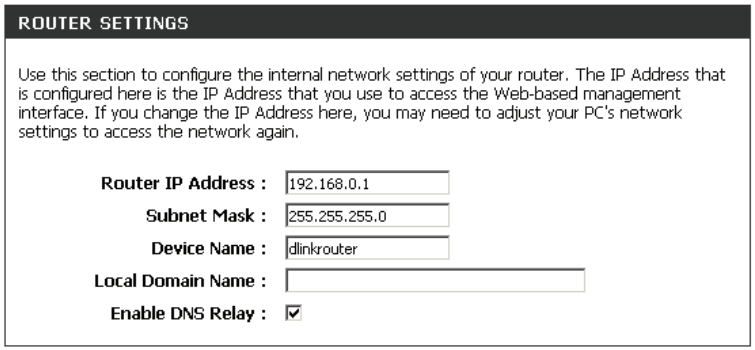
WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

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.

Network Settings

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

Router Settings



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

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

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

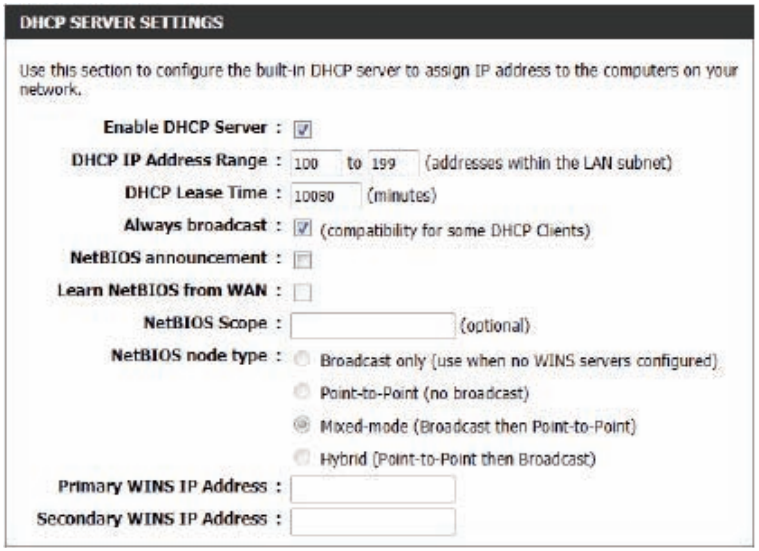
Device Name: Enter a name for the router.

Local Domain: Enter the domain name (Optional).

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

DHCP Server Settings

DHCP stands for Dynamic Host Configuration Protocol. The DIR-808L has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. If using DHCP, be sure to set your computers to be DHCP clients by setting their TCP/IP settings to **Obtain an IP Address Automatically**. When your wireless devices connect to the router, they will automatically load the TCP/IP settings provided by the DIR-808L. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting device. 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 Lease time in minutes.

Always Broadcast: If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

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

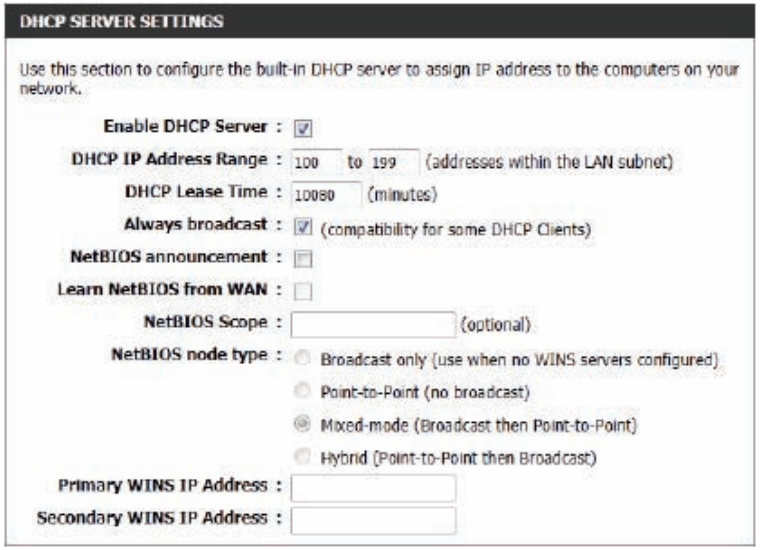
Learn NetBIOS from WAN: If NetBIOS announcement is switched on, it will cause WINS information to be learned from the WAN side, if available. Turn this setting off to configure manually.

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

NetBIOS Node Type: This field indicates how network hosts are to perform NetBIOS name registration and discovery. **Broadcast only** indicates to use local network broadcast ONLY. This setting is useful where there are no WINS servers available, however, it is recommended that you try Mixed-mode operation first. This setting has no effect if the **Learn NetBIOS information from WAN** option is activated. **Point-to-point** indicates to use WINS servers ONLY. This setting is useful to force all NetBIOS operations to the configured WINS servers. You must have configured at least the primary WINS server IP to point to a working WINS server. **Mixed-mode** (default), this indicates a Mixed-Mode of operation. First a broadcast operation is performed to register hosts and discover other hosts, if the broadcast operation fails, WINS servers are tried, if any. This mode favours broadcast operations which may be preferred if WINS servers are reachable by a slow network link and the majority of network services such as servers and printers are local to the LAN. **Hybrid** indicates a Hybrid-State of operation. First WINS servers are tried, if any, followed by local network broadcast. This is generally the preferred mode if you have configured WINS servers.

Primary WINS IP Address: Enter your primary WINS Server IP address.

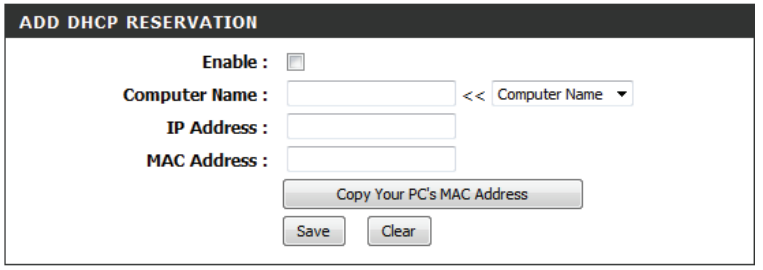
Secondary WINS IP Address: Enter your secondary WINS Server IP address.



DHCP Reservation

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

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



Enable: Check this box to enable the reservation.

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

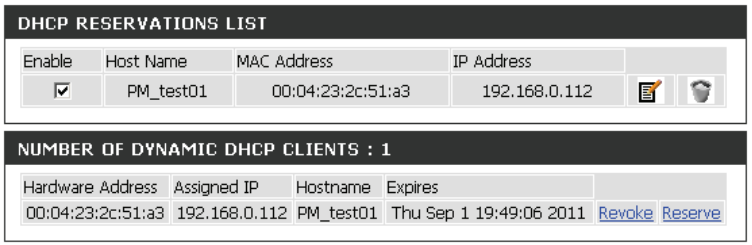
IP Address: Enter the IP address you want to assign to the computer or device. This IP address must be within the DHCP IP address range.

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

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

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

DHCP Reservations List



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

Enable: Check to enable the reservation.

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

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

IPv6 Internet Connection

On this page, you can configure the IPv6 connection type. There are two ways to set up the IPv6 Internet connection. You can use the Web-based IPv6 Internet Connection Setup Wizard, or you can manually configure the connection.

For beginner users that have not configured a router before, click on the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.

For the advanced user that has configured a router before, click on the **Manual IPv6 Internet Connection Setup** button to input all the settings manually.

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

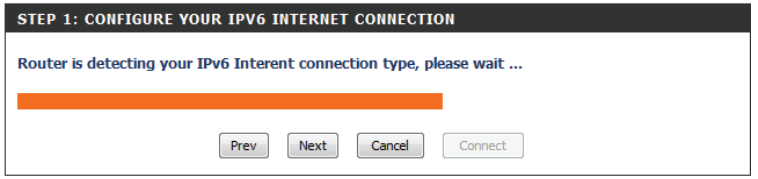
IPv6 Internet Connection Setup Wizard

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

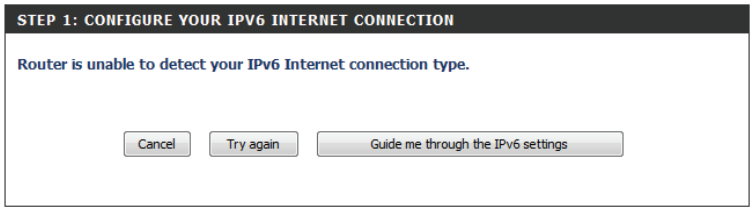
Click the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running.

Click **Next** to continue to the next page. Click **Cancel** to discard the changes made and return to the main page.

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



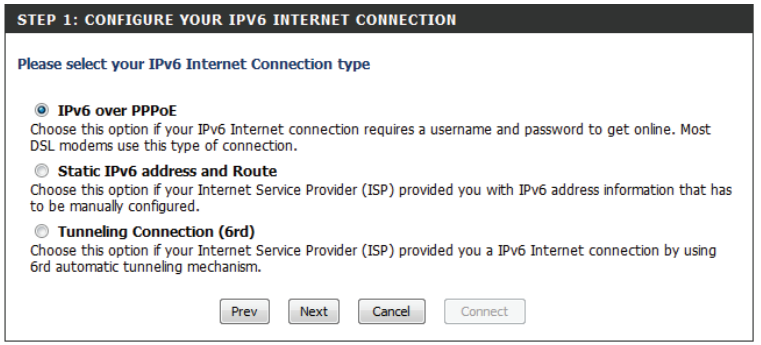
However, if the automatic detection fails, you will be prompted to either **Try again** or to click on the **Guide me through the IPv6 settings** button to manually configure the IPv6 settings using the wizard.



There are several connection types to choose from. If you are unsure of your connection method, please contact your IPv6 Internet service provider.

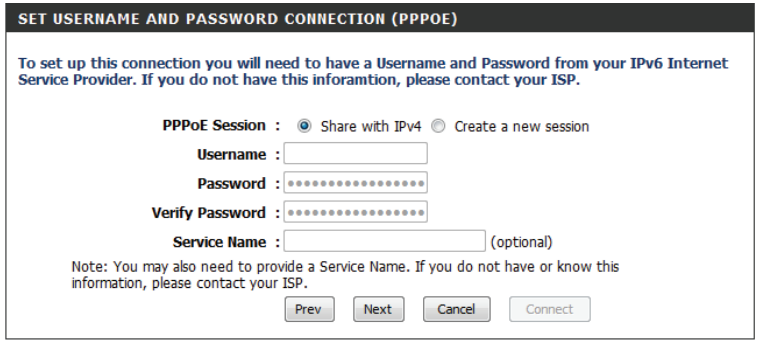
Note: If using the PPPoE option, you will need to ensure that any PPPoE client software on your computers has been removed or disabled. The 3 options available on this page are **IPv6 over PPPoE**, **Static IPv6 address and Route**, and **Tunneling Connection**.

Choose the required IPv6 Internet connection type and click on the **Next** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.



IPv6 over PPPoE

After selecting the **IPv6 over PPPoE** option, you will be able to configure the IPv6 Internet connection that requires a username and password to access the Internet. Most DSL modems use this type of connection.



The following parameters will be available for configuration:

PPPoE Session: Select the first option to share the configuration settings with those for IPv4 over PPPoE, or alternatively select the second option to configure a new session.

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 (optional).

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 this information.

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

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

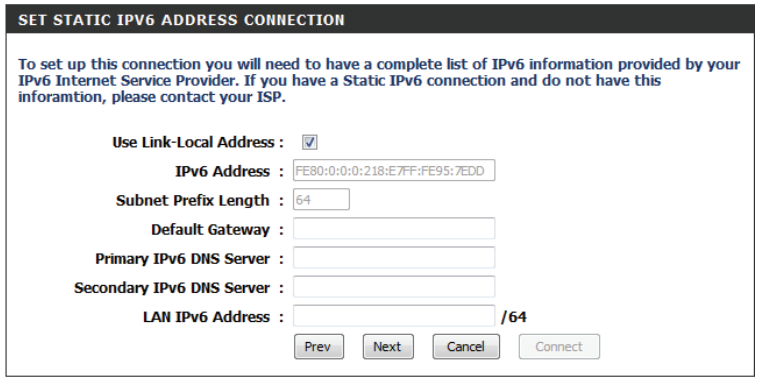
Subnet Prefix Length: Enter the WAN subnet prefix length value used here.

Default Gateway: Enter the WAN default gateway IPv6 address used here.

Primary IPv6 DNS Address: Enter the WAN primary DNS server address used here.

Secondary IPv6 DNS Address: Enter the WAN secondary DNS server address used here.

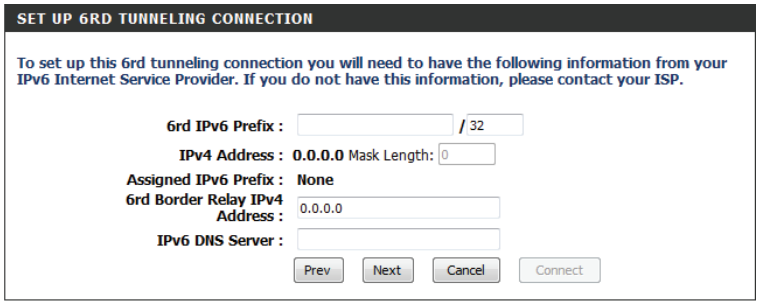
LAN IPv6 Address: These are the settings of the LAN (Local Area Network) IPv6 interface for the router. The router's LAN IPv6 Address configuration is based on the IPv6 address and subnet assigned by your ISP. (A subnet with prefix /64 is supported in LAN.)



Tunneling Connection (6rd)

After selecting the **Tunneling Connection (6rd)** option, you can configure the IPv6 6rd connection settings.

The following parameters will be available for configuration:



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

IPv4 Address: Enter the IPv4 address used here.

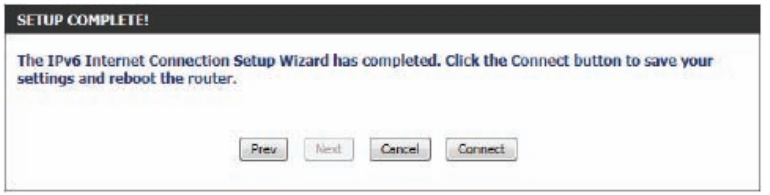
Mask Length: Enter the IPv4 mask length used here.

Assigned IPv6 Prefix: Displays the IPv6 assigned prefix value here.

6rd Border Relay IPv4 Address: Enter the 6rd border relay IPv4 address used here.

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

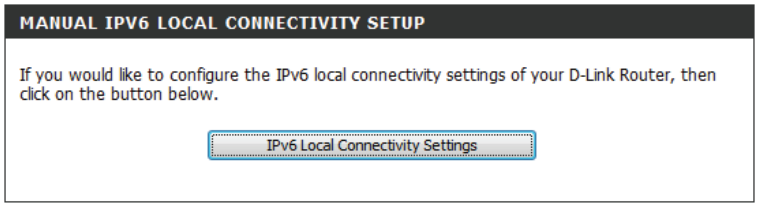
The IPv6 Internet Connection Setup Wizard is complete.



Click on the **Connect** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.

Manual IPv6 Local Connectivity Settings

This option can be used to manually configure IPv6 settings for local connectivity. These settings are used only on the local network, and will not be used to access the Internet.

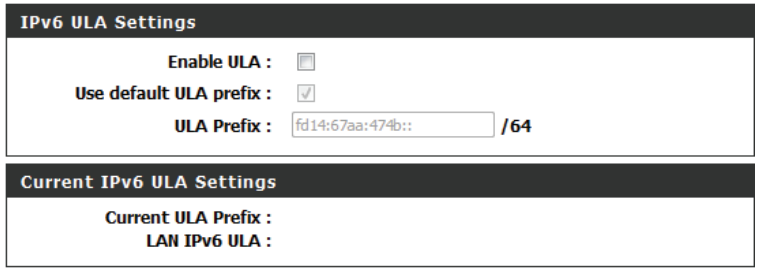


Enable ULA: Click here to enable Unique Local IPv6 Unicast Addresses settings.

Use Default ULA Prefix: Checking this box will automatically configure the ULA prefix for the default setting.

ULA Prefix: If you wish to choose your own ULA prefix, enter it here.

Current IPv6 ULA Settings: This section with display the current settings for your IPv6 ULA.



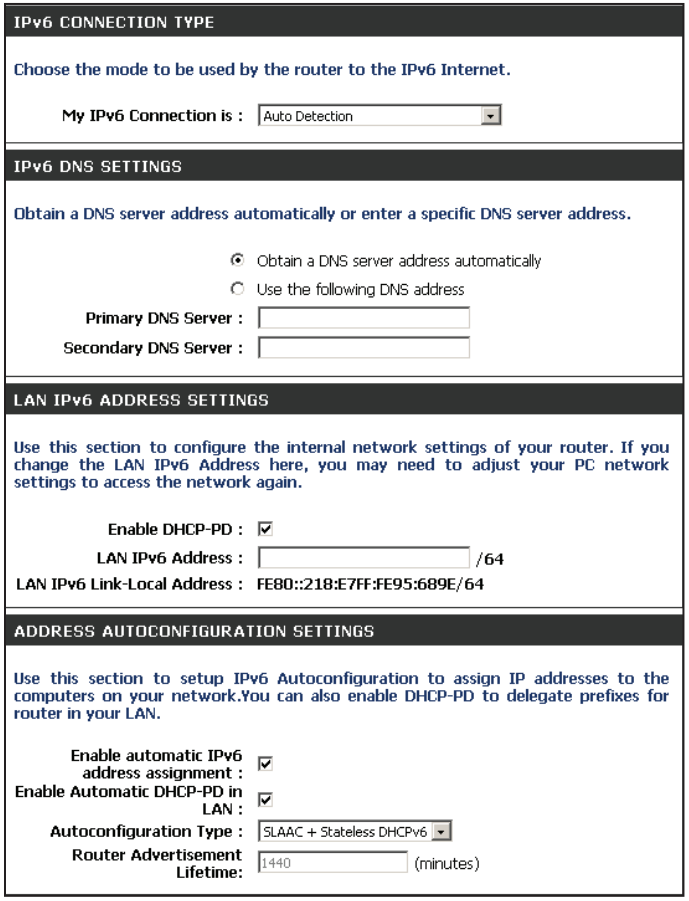
IPv6 Manual Setup

There are several connection types to choose from: Auto Detection, Static IPv6, Autoconfiguration (SLAAC/DHCPv6), PPPoE, IPv6 in IPv4 tunnel, 6to4, 6rd, and Link-local. If you are unsure of your connection method, please contact your IPv6 Internet Service Provider.

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

Auto Detection

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



Static IPv6

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

Use Link-Local Address: Tick this box to use the link-local address as the IPv6 address.

IPv6 Address: If you did no tick the box above, enter the IPv6 address provided to you by your Internet Service Provider (ISP).

Subnet Prefix Length: Enter the subnet prefix length specified by your ISP.

Default Gateway: Enter the default gateway provided by your ISP.

Primary DNS Server: Enter the primary DNS server provided by your ISP.

Secondary DNS Server: Enter the secondary DNS server provided by your ISP.

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

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

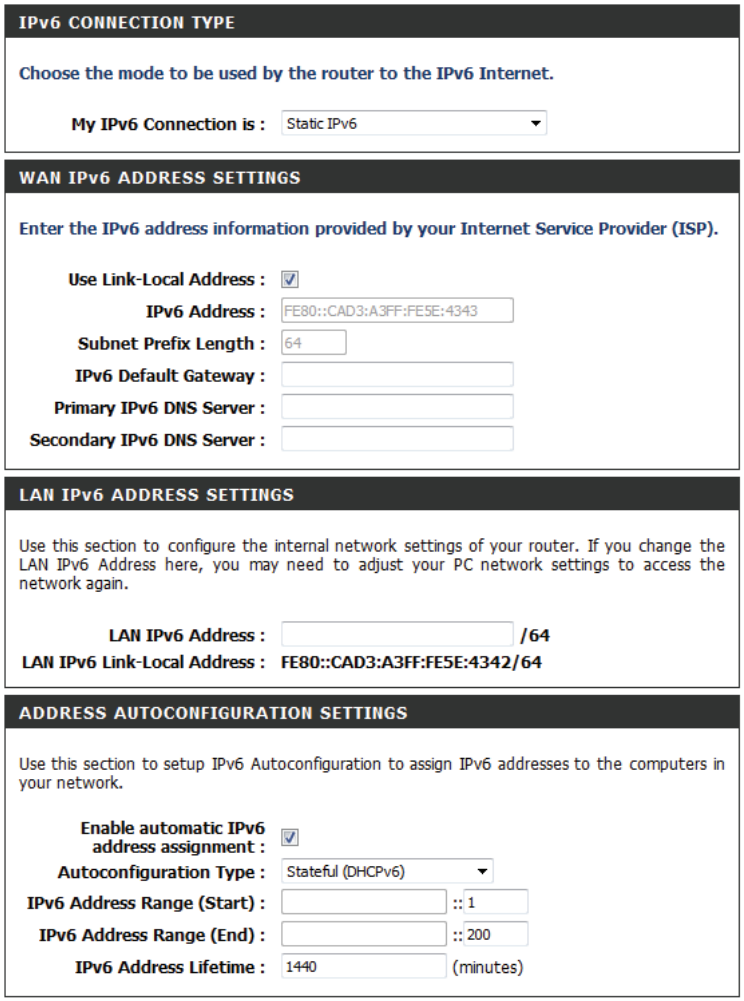
Enable Automatic IPv6 address assignment: Tick to enable the automatic assignment of IPv6 addresses to computers on your network.

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

IPv6 Address Range Start: If you selected Stateful (DHCPv6) above, enter the start IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Range End: If you selected Stateful (DHCPv6) above, enter the end IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 address lifetime (in minutes).



Autoconfiguration

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

IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

Enable DHCP-PD: Tick to enable DHCP-PD.

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

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

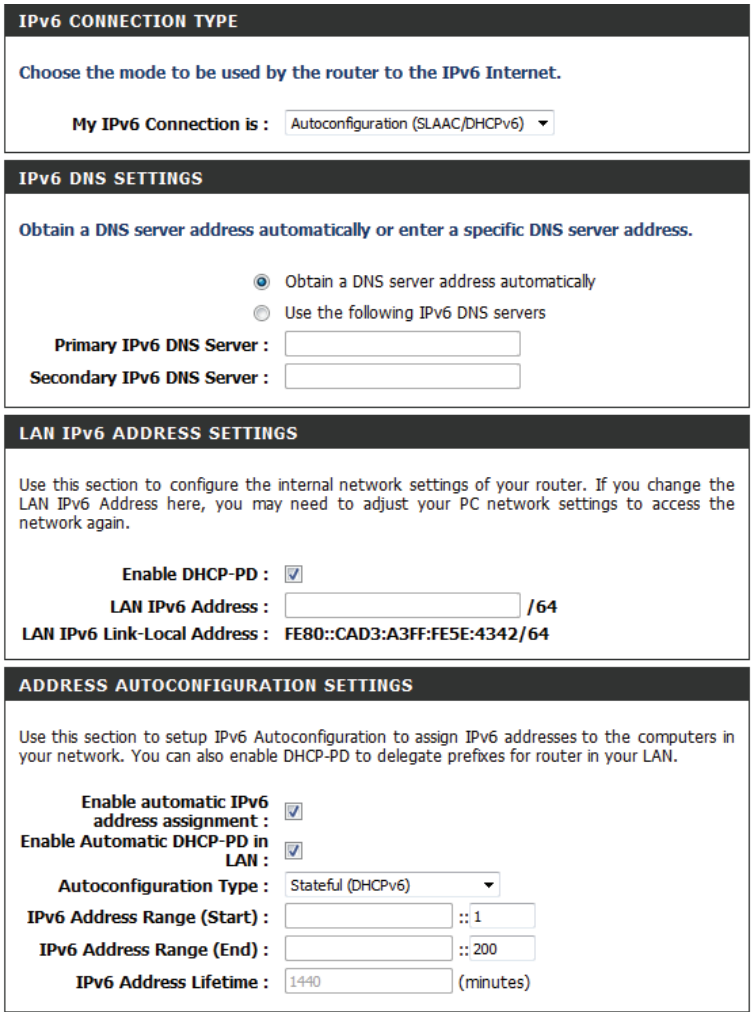
Enable Automatic IPv6 address assignment: Tick to enable the automatic assignment of IPv6 addresses to computers on your network.

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

IPv6 Address Range Start: If you selected Stateful (DHCPv6) above, enter the start IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Range End: If you selected Stateful (DHCPv6) above, enter the end IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 address Lifetime (in minutes).



PPPoE

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

PPPoE Session: Enter the PPPoE account settings supplied by your Internet provider (ISP).

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

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

Username: Enter your PPPoE user name.

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

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

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

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

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

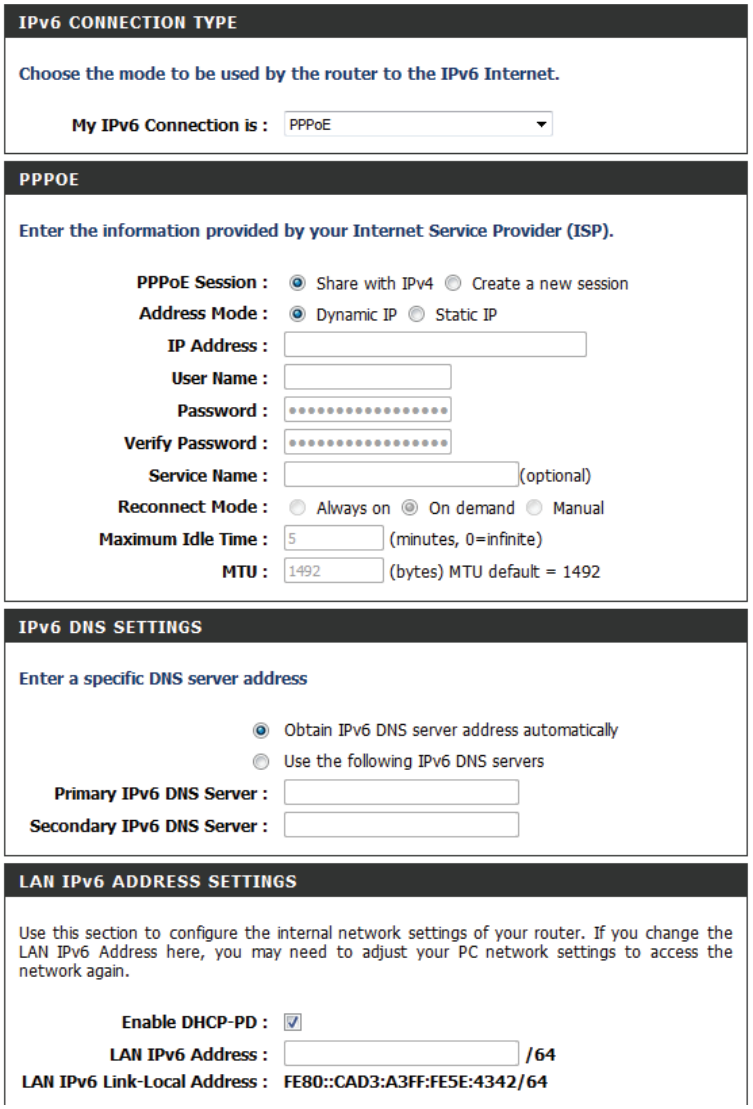
IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address.**

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses.

Enable DHCP-PD: Tick to enable DHCP-PD.

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

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



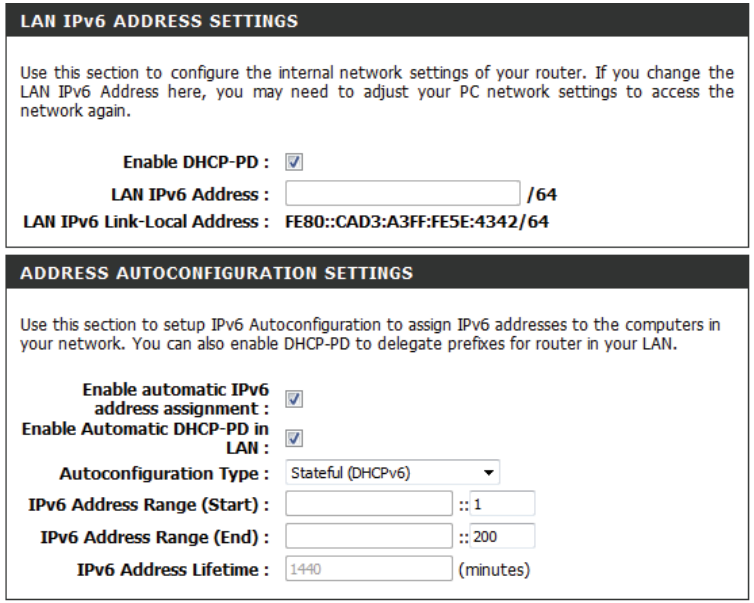
Enable Automatic IPv6 address assignment: Tick to enable the automatic assignment of IPv6 addresses to computers on your network.

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

IPv6 Address Range Start: If you selected Stateful (DHCPv6) above, enter the start IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Range End: If you selected Stateful (DHCPv6) above, enter the end IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 address lifetime (in minutes).



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 remote and local IPv4 and IPv6 settings supplied by your Internet Service Provider (ISP).

IPv6 DNS Settings: Select **Obtain a DNS server address automatically**, or **Use the following IPv6 DNS servers**. If you chose to use IPv6 DNS servers, enter the primary and secondary DNS server addresses provided to you by your ISP.

LAN IPv6 Address:

Enable DHCP-PD: Tick to enable DHCP-PD.

LAN IPv6 Address Enter the LAN (local) IPv6 address for the router.

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

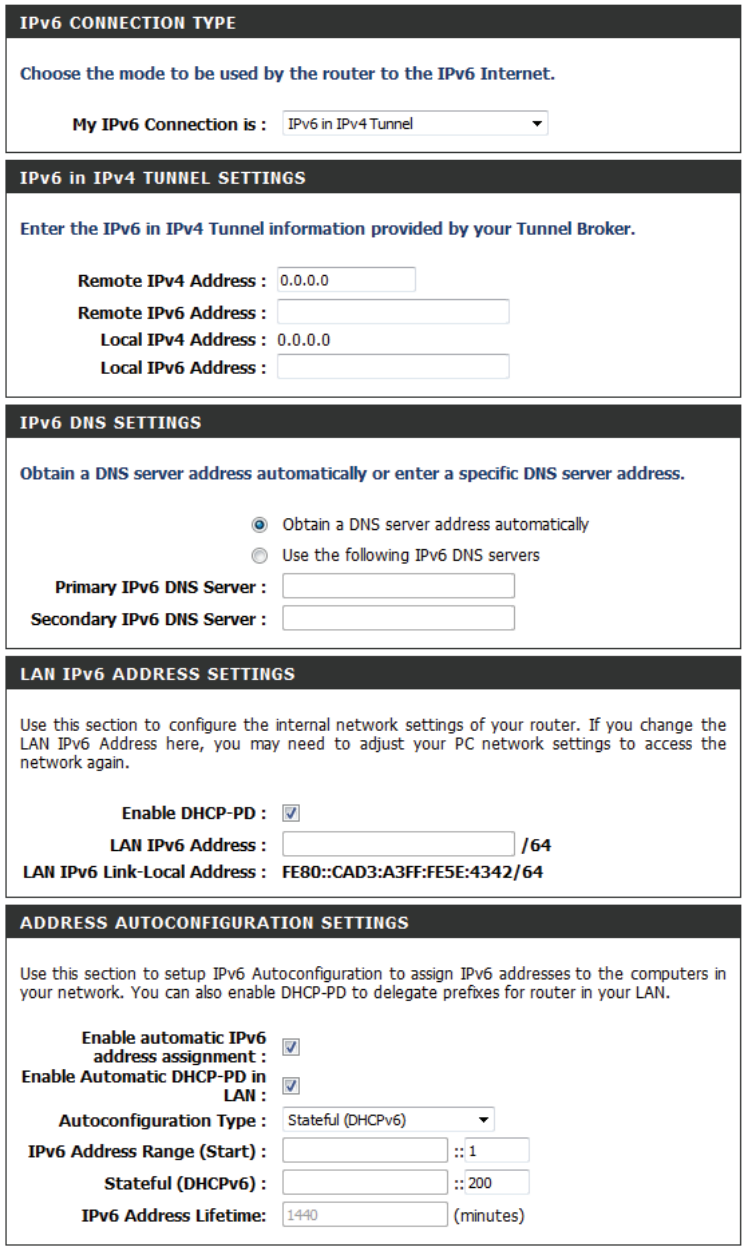
Enable Automatic IPv6 address assignment: Tick to enable the automatic assignment of IPv6 addresses to computers on your network.

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

IPv6 Address Range Start: If you selected Stateful (DHCPv6) above, enter the start IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Range End: If you selected Stateful (DHCPv6) above, enter the end IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the router advertisement lifetime (in minutes).



6 to 4 Tunneling

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

6 to 6 Address Displays the 6 to 4 address of the router.

6 to 4 Relay: Enter the 6 to 4 relay address provided by your Internet Service Provider (ISP).

Primary/Secondary DNS Address: Enter the primary and secondary DNS server addresses provided by your ISP.

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

LAN IPv6 Link-Local Address: Displays the router's LAN link-local address.

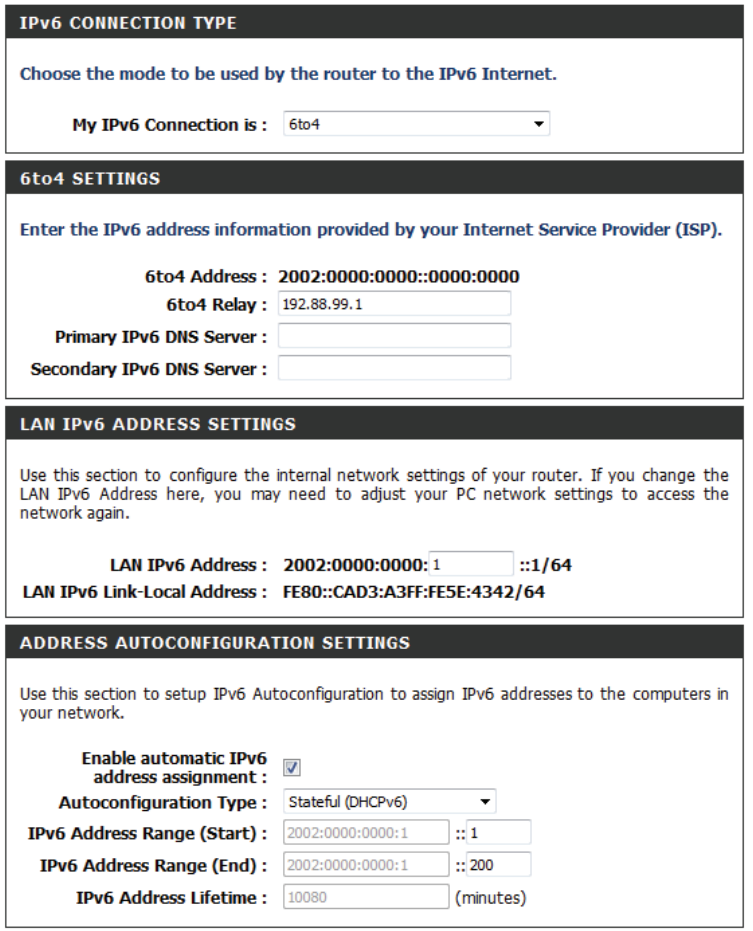
Enable Automatic IPv6 address assignment: Tick to enable the automatic assignment of IPv6 addresses to computers on your network.

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

IPv6 Address Range Start: If you selected Stateful (DHCPv6) above, enter the start IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Range End: If you selected Stateful (DHCPv6) above, enter the end IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Lifetime: Enter the IPv6 address lifetime (in minutes).



6rd

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

Enable Hub and Spoke Mode: Tick to enable hub and spoke mode.

6rd Configuration: Select either **6rd DHCPv4 Option** or **Manual Configuration**. If you select manual, there will be additional fields available for configuration.

6rd IPv6 Prefix: Enter the 6rd IPv6 prefix provided by your Internet Service Provider (ISP)

IPv4 Address/ Mask Length: Displays the IPv4 address. Enter the mask length provided by your ISP.

Assigned IPv6 Prefix: Displays the assigned IPv6 prefix.

6rd Border Relay IPv4 Address: Enter the 6rd border relay IPv4 address provided by your ISP.

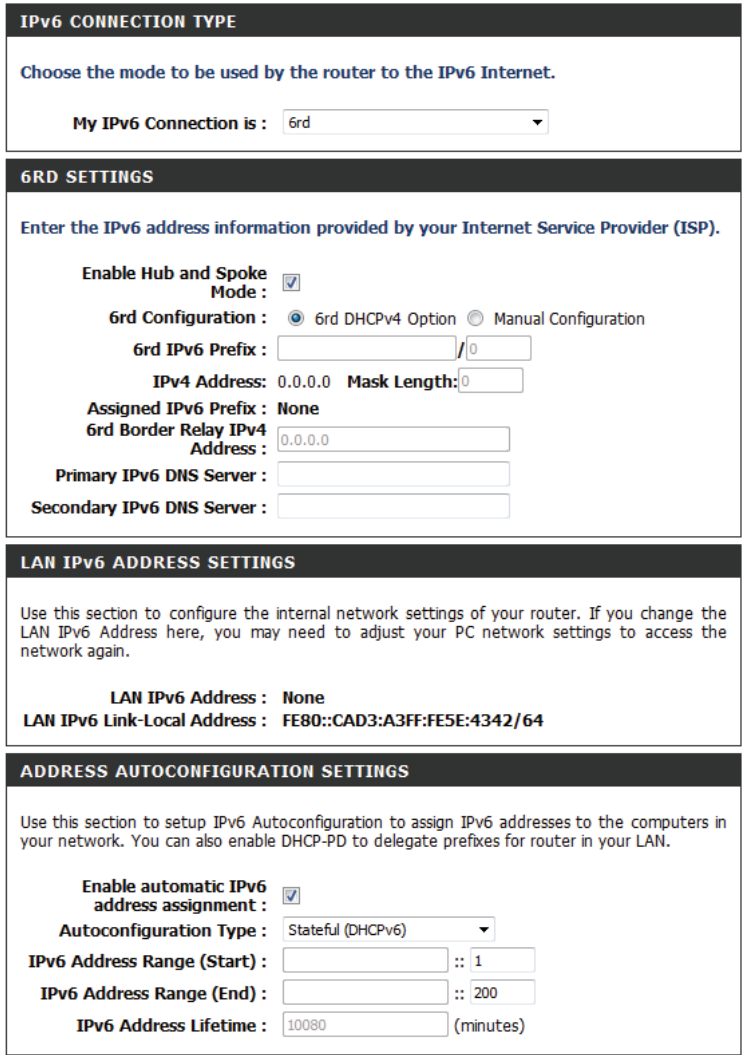
Primary IPv6 DNS Server: Enter the primary IPv6 DNS server address provided by your ISP.

Secondary IPv6 DNS Server: Enter the secondary IPv6 DNS server address provided by your ISP.

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

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

Enable Automatic IPv6 address assignemtn: Tick to enable the automatic assignment of IPv6 addresses to computers on your network.

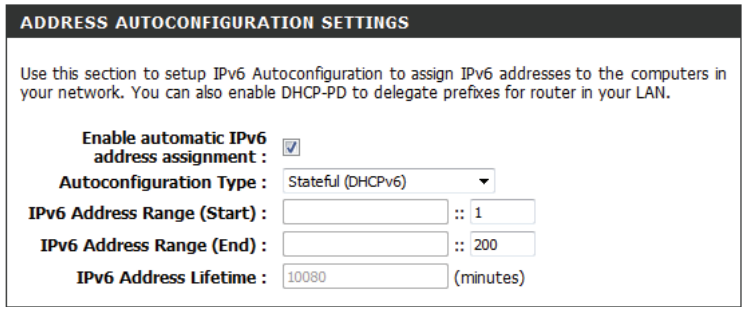


Autoconfiguration Type: Select **Stateful (DHCPv6)**, **SLAAC+RDNSS**, or **SLAAC + Stateless DHCPv6.**

IPv6 Address Range Start: If you selected Stateful (DHCPv6) above, enter the start IPv6 address for the DHCPv6 range for your local computers.

IPv6 Address Range End: If you selected Stateful (DHCPv6) above, enter the end IPv6 address for the DHCPv6 range for your local computers.

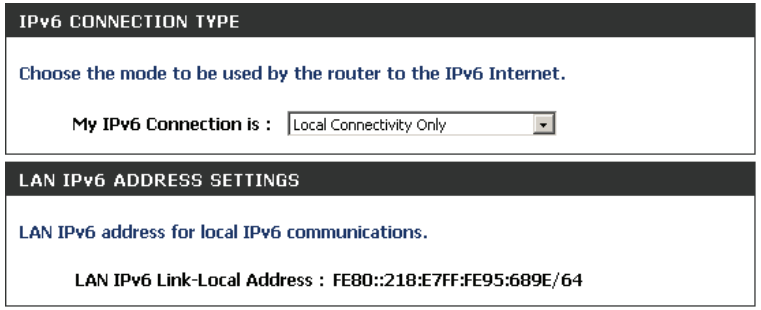
IPv6 Address Lifetime: Enter the router advertisement lifetime (in minutes).



Link-Local Connectivity

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

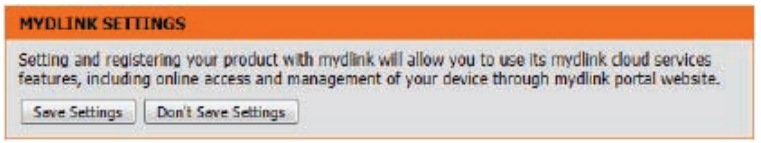
LAN IPv6 Address Settings: Displays the IPv6 address of the router.



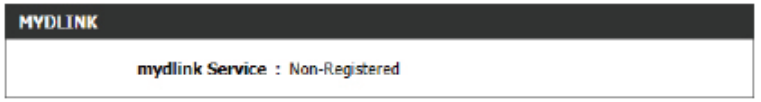
mydlink™ Settings

The DIR-808L features a new cloud service that pushes information such as firmware upgrade notifications, user activity, and intrusion alerts to the mydlink app on your Android or iOS mobile device. To ensure that your router is up to date with the latest features, mydlink will notify you when an update is available for your router. You can also monitor users' online activity with real-time website browsing history, maintaining a safe and secure environment, especially useful for monitoring your children's Internet usage at home.

On this page you can configure the mydlink settings for this router. This feature will allow you to use the mydlink cloud services, which include online access and management of this router through the mydlink portal website or the mydlink Lite app for iOS and Android mobile devices.

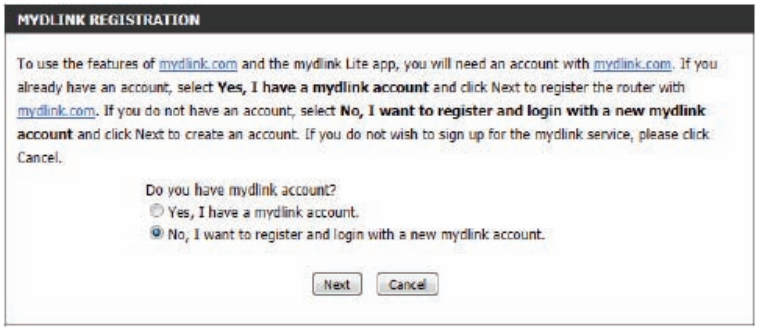


In the **mydlink** section, you can view the registration status of the mydlink account service. The **mydlink Service** field will either display **Registered** or **Non-Registered**.



In the **Register mydlink Service** section, you can register or modify a mydlink account. Click on the **Register mydlink Service** button to initiate this procedure.

After clicking the **Register mydlink Service** button, this window will appear.



Register mydlink Service Wizard: Step 1

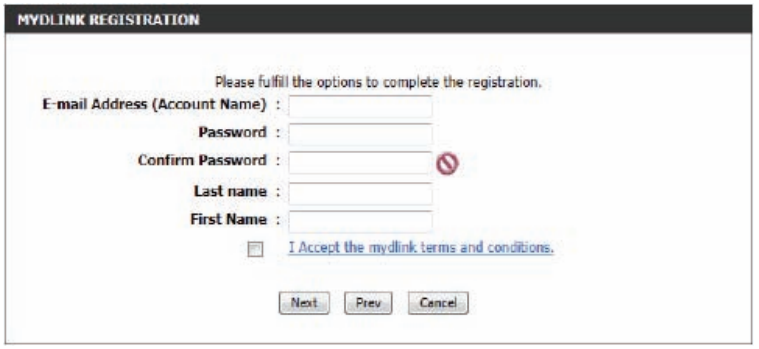
In this section you can select one of two options.

- Select the '**Yes, I have a mydlink account**' option if you already have a mydlink account that you want to use on this router.
- Select the '**No, I want to register and login with a new mydlink account**' option to register a new account and use it on this router.

Click the **Next** button to proceed to the next step.
Click the **Cancel** button to discard the changes made and return to the main page.

Register mydlink Service Wizard: Step 2

When registering a **new account**, the following page appears. The following parameters will be available for configuration:



E-mail Address (Account Name): Enter your e-mail address here. This e-mail address will also become your account name.

Password: Enter your preferred password here.

Confirm Password: Re-enter your preferred password here.

Last Name: Enter your last name here.

First Name: Enter your first name here.

Accept terms and conditions: Tick this option to accept the mydlink terms and conditions.

Click the **Next** button to proceed to the next step.
Click the **Prev** button to return to the previous step.
Click the **Cancel** button to discard the changes made and return to the main page.

When logging in with an **existing account**, the following page appears. The following parameters will be available for configuration:

E-mail Address (Account Name): Enter your e-mail address here. This e-mail address that you used to register with the mydlink service.

Password: Enter your mydlink password here.

Click the **Login** button to login using these account details.
Click the **Prev** button to return to the previous step.
Click the **Cancel** button to discard the changes made and return to the main page.

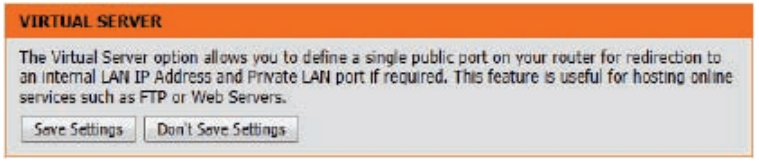
At any point during this wizard, you can change the preferred language. To change the language, select the desired language option from the **Language** drop-down menu, found on the top right of this page.

End of Wizard

Advanced

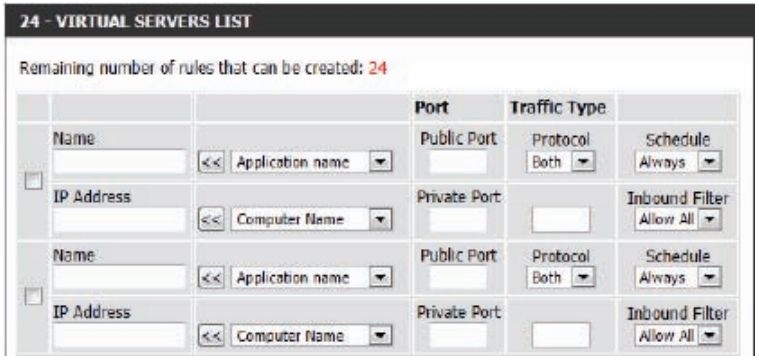
Virtual Server

This will allow you to open a single port. If you would like to open a range of ports, refer to the next page. Tick the box next to each tule to enable that rule.



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

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



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

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

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

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

Port Forwarding

This will allow you to open a single port or a range of ports. Tick the box next to each rule to enable that rule.

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

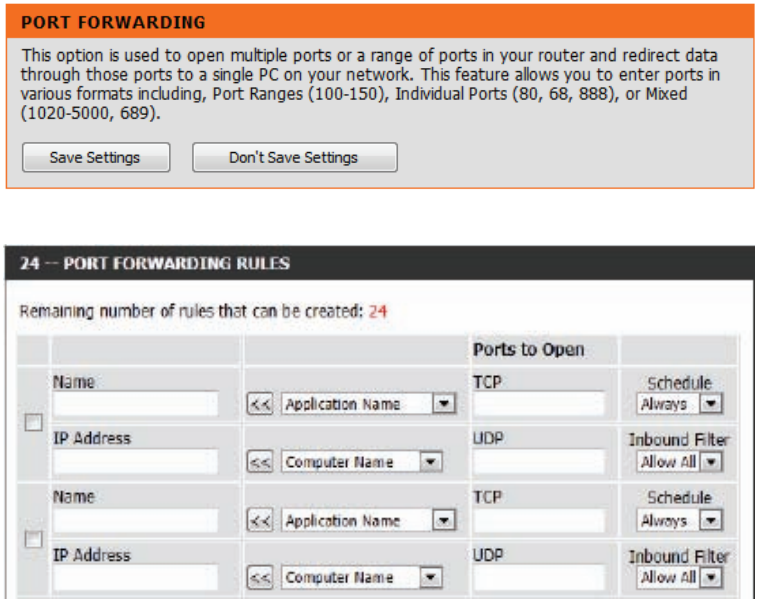
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your computer will be listed in the "Computer Name" drop-down menu. Select your computer and click 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

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

Example: 24,1009,3000-4000

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

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



Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special application rules allow some of these applications to work with the DIR-808L. If you need to run applications that require multiple connections, specify the port normally associated with an application in the **Trigger Port** field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-808L provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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

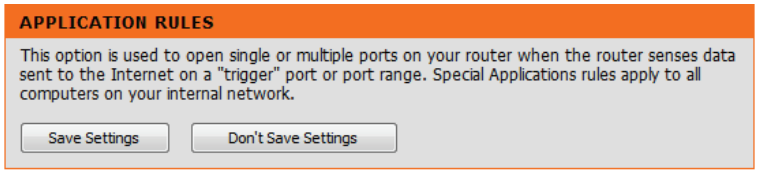
Trigger: This is the port used to trigger the application. It can be either a single port or a range of ports.

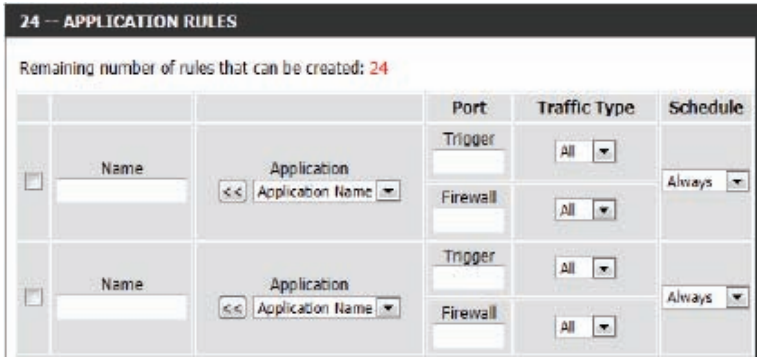
Traffic Type: Select the protocol of the trigger port (TCP, UDP, or Both).

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

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

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





QoS Engine

The QoS Engine option helps improve your network performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically. The QoS section contains a queuing mechanism, traffic shaping, and classification. It supports two kinds of queuing mechanisms: Strict Priority Queue (SPQ) and Weighted Fair Queue (WFQ). SPQ will process traffic based on traffic priority; queue 1 has the highest priority and queue 4 has the lowest priority. WFQ will process traffic based on the queue weight; you can configure each queue's weight, where the sum of all the queues' weights must be 100. When surfing the Internet, the system will do traffic shaping based on the uplink and downlink speed. The classification rules can be used to classify traffic to different queues, then SPQ or WFQ will do QoS based on the queue's priority or weight.

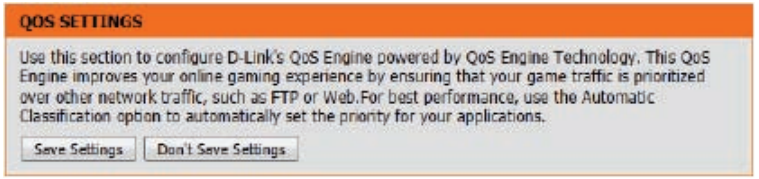
The following parameters will be available for configuration:

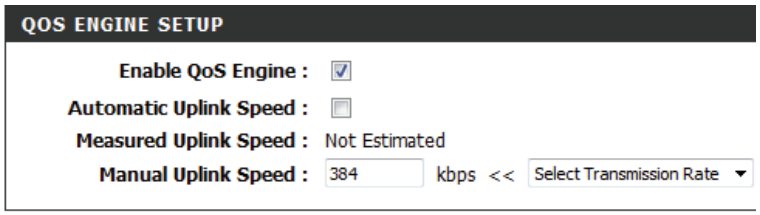
Enable QoS: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Uplink Speed: Tick this option to have the QoS engine automatically set your uplink speed.

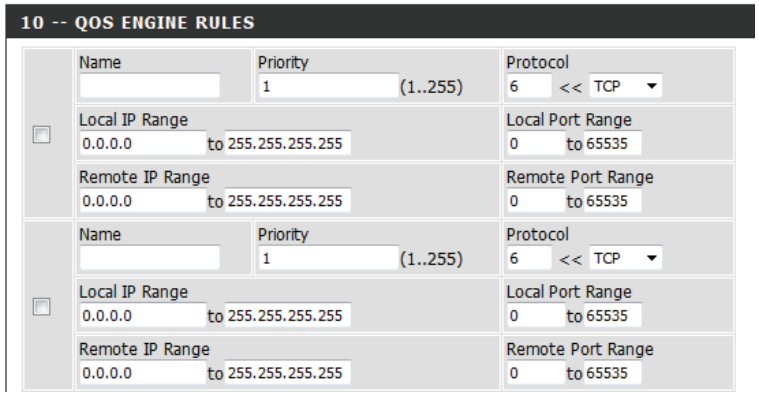
Measured Uplink Speed: Displays the uplink speed measured by the router.

Manual Uplink Speed: This section allows you to specify the speed at which data can be transferred from the ISP to the router. This is determined by your ISP. ISPs often define speed as a download/upload pair. For example, 1.5 Mbits/284 Kbits.





After specifying the QoS framework used, in the QoS setup section, the user can now create individual rules for scenarios that require the use of traffic control and data priority manipulation.



The following parameters will be available for configuration:

Checkbox: Tick this option to enable the rule specified.

Name: Enter a custom name for the rule being created here. This name is used for identification.

Priority: Select the appropriate priority requirement by entering a value between 1 and 255 in the box provided.

Protocol: Select the protocol used for the application for in the drop-down menu and it will automatically place it in the Protocol field.

Local IP Range: Enter the local IP range used here. This is the IP range of your Local Area Network. The router's IP cannot be included in this range.

Remote IP Range: Enter the remote IP range used here. This is the IP range of the public network from the Internet port side. To apply this rule to any IP addresses from the public side, enter the range 0.0.0.1 to 255.255.255.254.

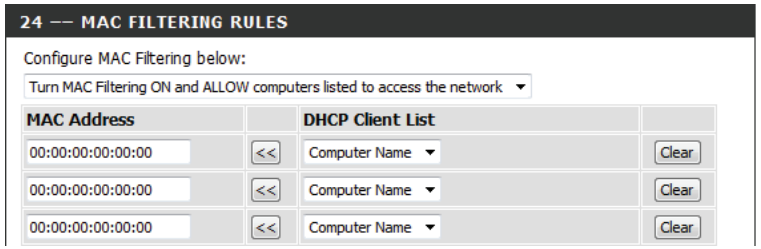
Local Port Range: Enter the local port range to be used for this rule.

Remote Port Range: Enter the remote port range to be used for this rule.

Click on the **Save Settings** button to accept the changes made.
Click on the **Don't Save Settings** button to discard the changes made.

Network Filters

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



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

MAC Address: Enter the MAC address you would like to filter.

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

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

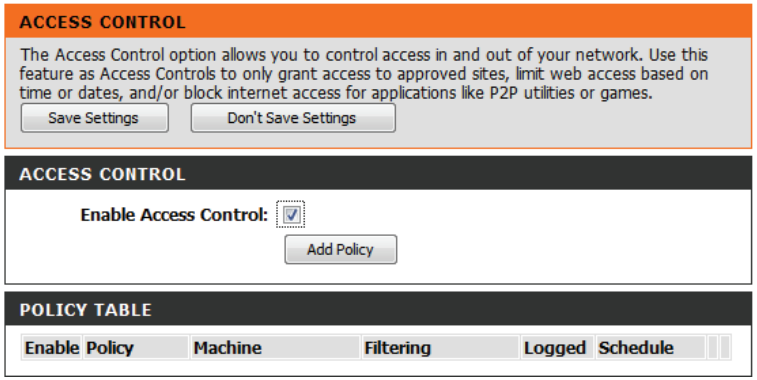
Clear: Click the **Clear** button to clear the MAC address and DHCP client list fields for each line.

Access Control

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

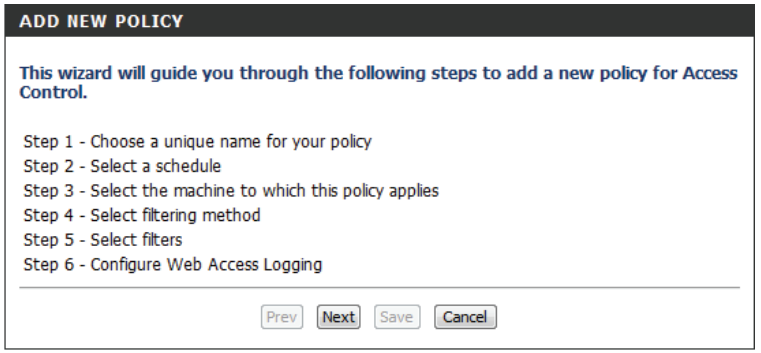
Enable Access Control: Tick the box to enable access control. Any policies specified will be enabled.

Add Policy: Click the **Add Policy** button to start the Access Control Wizard.

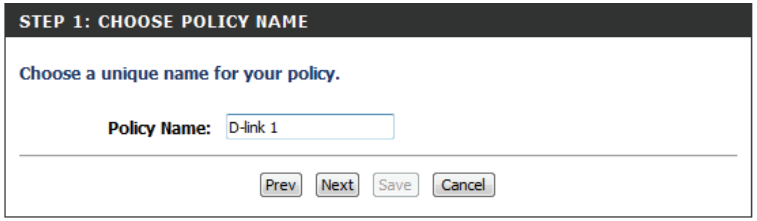


Access Control Wizard

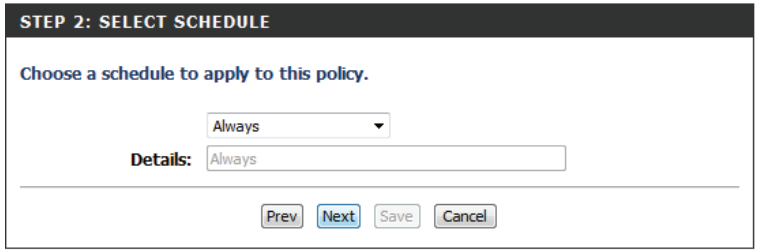
Click **Next** to continue with the wizard.



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

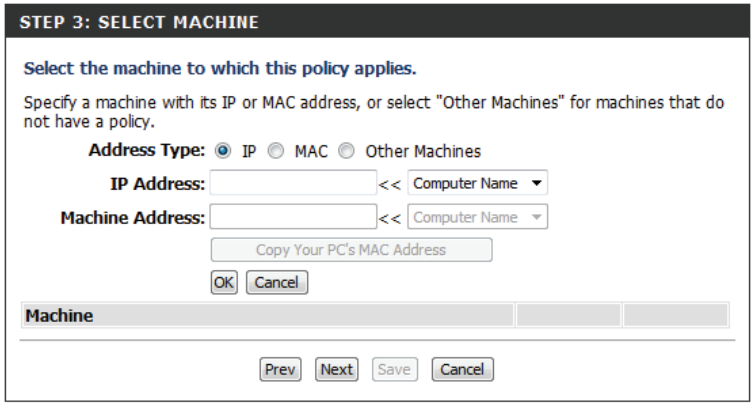


Select a schedule (eg: Always) from the drop-down menu and then click **Next** to continue.



Enter the following information and then click **Next** to continue.

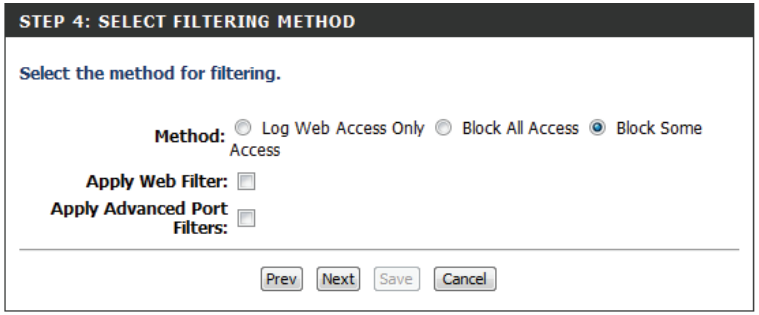
- **Address Type** - Select **IP address**, **MAC address**, or **Other Machines**.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.
- **Machine Address** - Enter the PC MAC address (i.e. 00:00.00.00.00).



Select the filtering method. If you choose **Block Some Access**, there will be two filtering options available:

- **Apply Web Filter** - This will enable the website filtering rules selected in the Advanced >> Website Filter section.
- **Apply Advanced Port Filters** - This will enable the port filtering rules, which will be specified on the subsequent page.

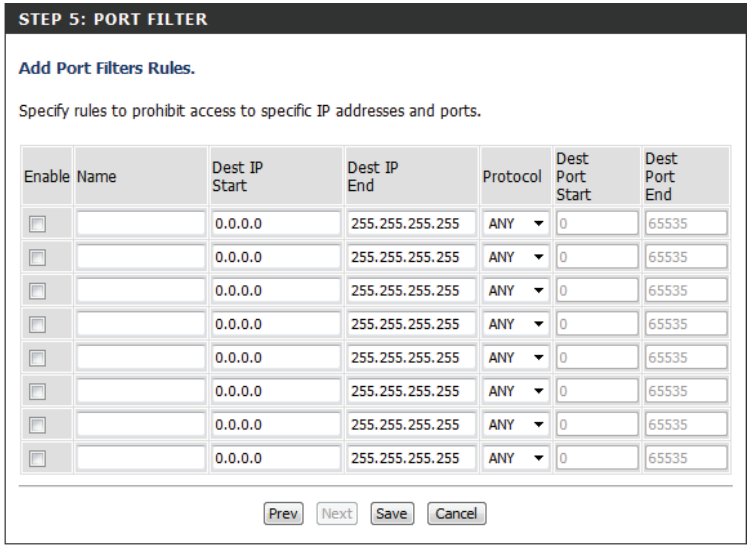
Click **Next** to continue.



Enter the rule:

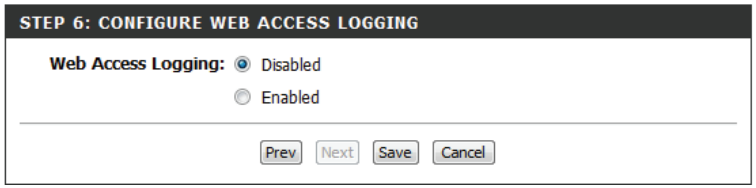
Enable - Tick to enable the rule.
Name - Enter a name for your rule.
Dest IP Start - Enter the starting IP address.
Dest IP End - Enter the ending IP address.
Protocol - Select the protocol.
Dest Port Start - Enter the starting port number.
Dest Port End - Enter the ending port number.

Click **Save** to continue.

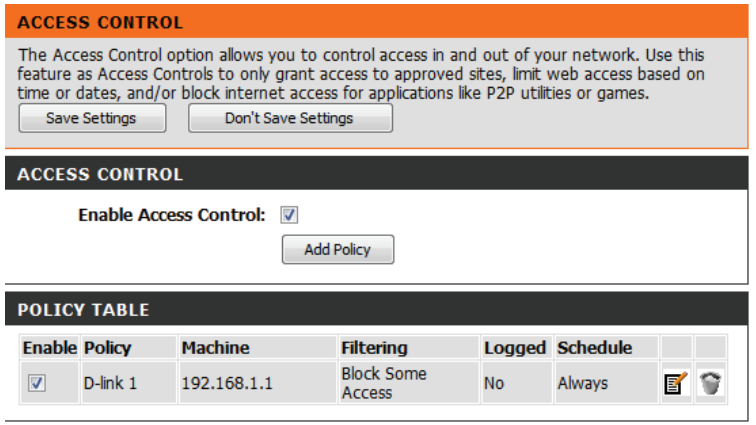


To enable web logging, click **Enable**.

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



Your newly created policy will now show up under **Policy Table**.



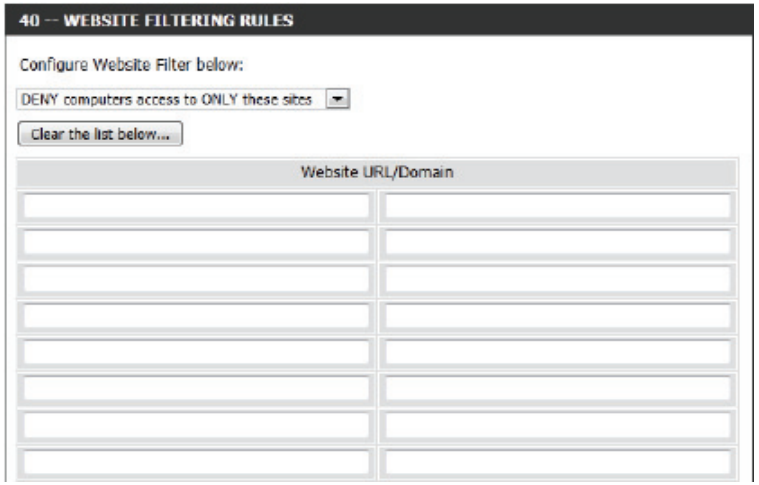
Website Filters

Website filters are used to allow you to control access to websites by users connected to the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section in order to activate this filter.

Add Website Filtering Rule: 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**.

Clear the list below: Click this button to clear the list of filtered websites.



Inbound Filters

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range. Inbound filters can be used with virtual server, port forwarding, or remote administration features.

Name: Enter a name for the inbound filter rule.

Action: Select **Allow** or **Deny**.

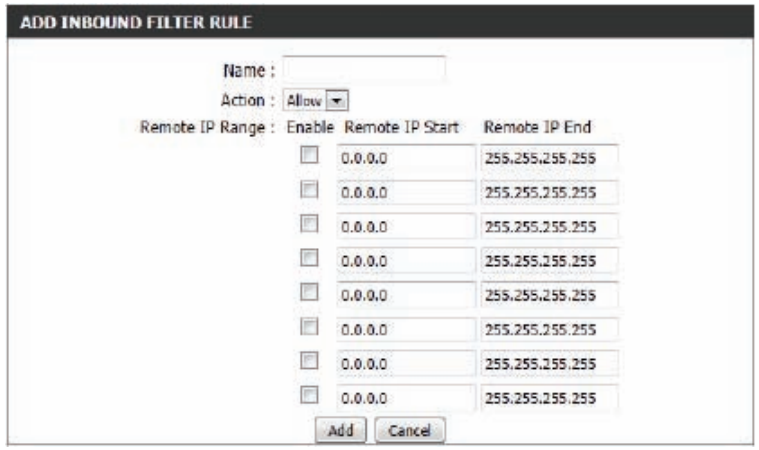
Enable: Check to enable rule.

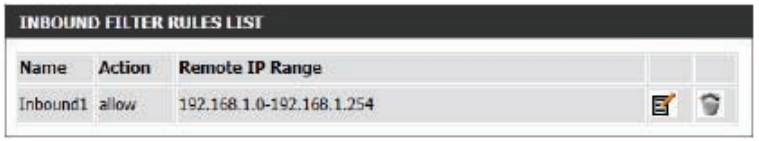
Remote IP Start: Enter the starting IP address. Enter 0.0.0.0 if you do not want to specify an IP range.

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

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

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





Firewall Settings

The DIR-808L offers a firewall which helps protect your network from external threats. The SPI feature helps prevent malicious attacks by inspecting and verifying incoming data packets. In certain cases, you may also want a computer exposed to the outside world for certain types of applications. The firewall setup also features a Demilitarized Zone (DMZ) option, which will expose the selected clients completely to the outside world.

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

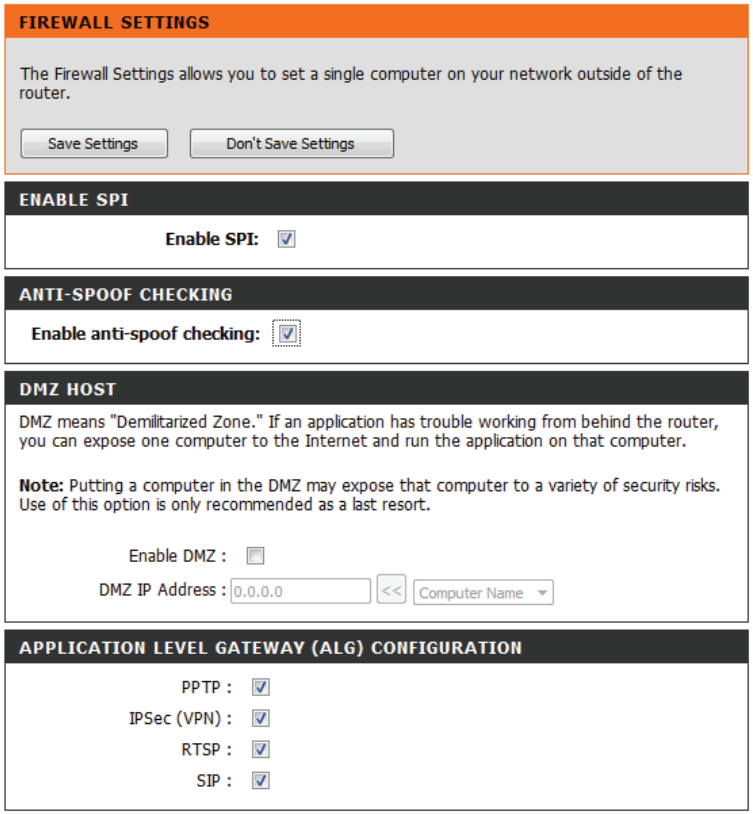
Anti-Spoof Check: Enable this feature to protect your network from certain kinds of "spoofing" attacks.

Enable DMZ: Tick the box to enable to DMZ feature.

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 its 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.

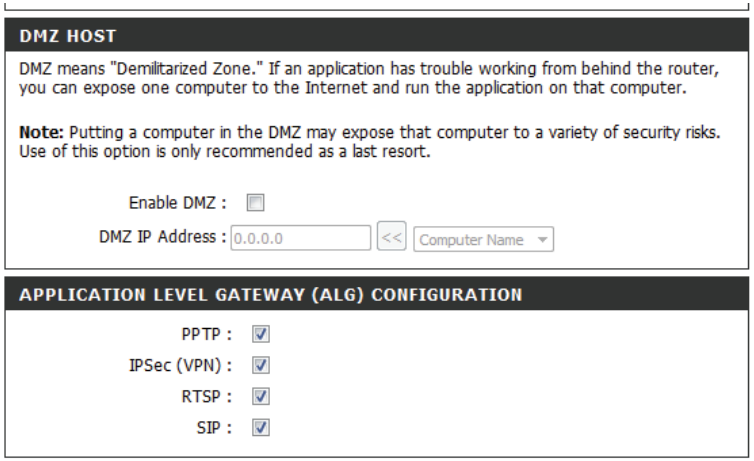
PPTP: Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

IPSEC (VPN): Allows multiple VPN clients to connect to their corporate network using IPSec. Some VPN clients support traversal of IPSec through
NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. Please check with the system administrator of your corporate network whether your VPN client supports NAT traversal.



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

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



Routing

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

Name: Enter a name for your route.

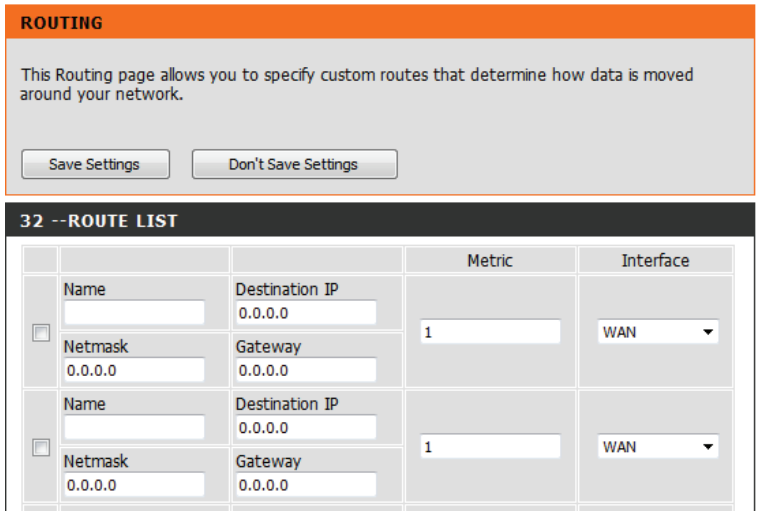
Destination IP: Enter the IP address of packets that will take this route.

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 15 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.



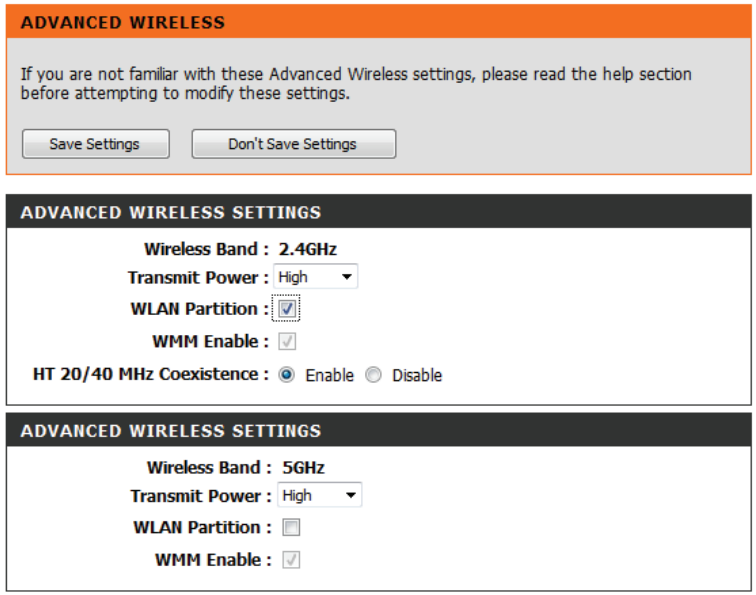
Advanced Wireless

Transmit Power: Set the transmit power of the antennas.

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

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

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



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 has certified WPS across different products as well as manufacturers. The process as simple as pressing a button for the Push Button Method or correctly entering an 8-digit code for the Pin Code Method. WPS significantly reduces the amount of time required to set up a secure wireless network, while maintaining the highest level of wireless security provided by the WPA2 standard.

Enable: Enable the Wi-Fi Protected Setup feature.

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

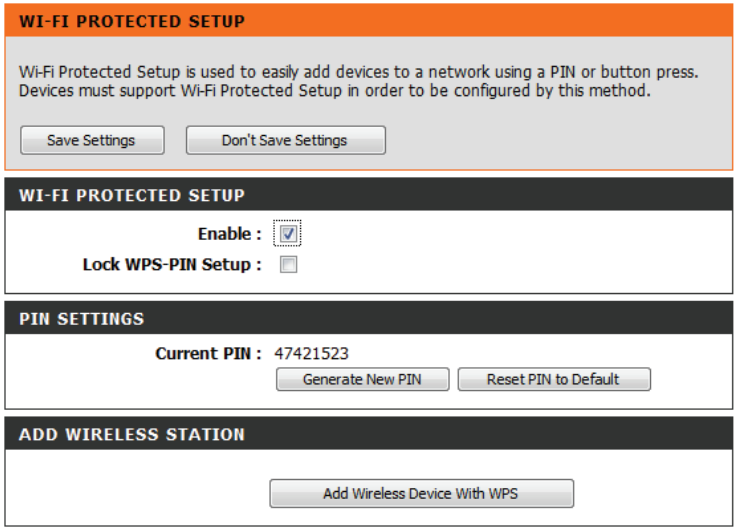
Lock WPS-PIN Setup: Tick this option to lock the use of the WPS-PIN setup feature.

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

Current PIN: Shows the current PIN.

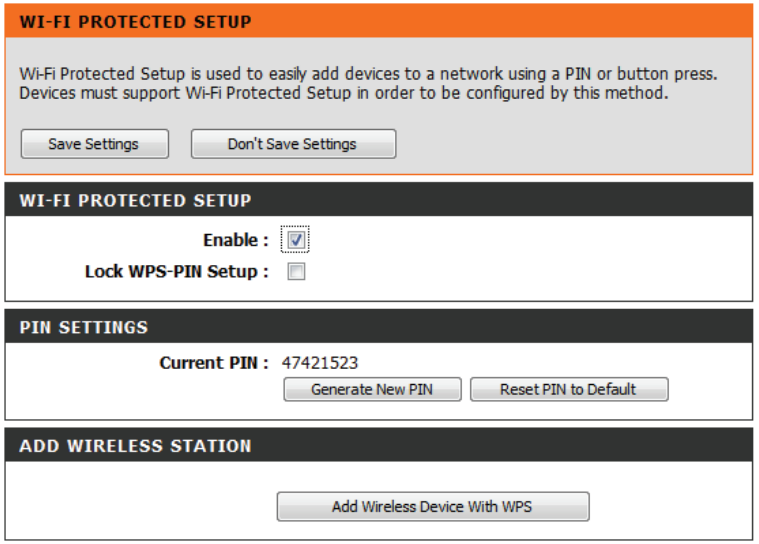
Reset PIN to Default: Restore the default PIN of the router.

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



Add Wireless Device Wizard: Click this button to begin the WPS wizard, which will guide you through the process of adding a wireless device to your network using WPS.

Click to start the wizard and refer to "Wi-Fi Protected Setup Wizard" on page 43.



WPS Button

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

Refer to "Connect a Wireless Client to your Router" on page 122 for more information.

Advanced Network Settings

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

Enable WAN Ping Respond: Checking the box will allow the DIR-808L to respond to pings, which may be required by some ISPs. If not required, unchecking the box may provide some extra security from outside intruders.

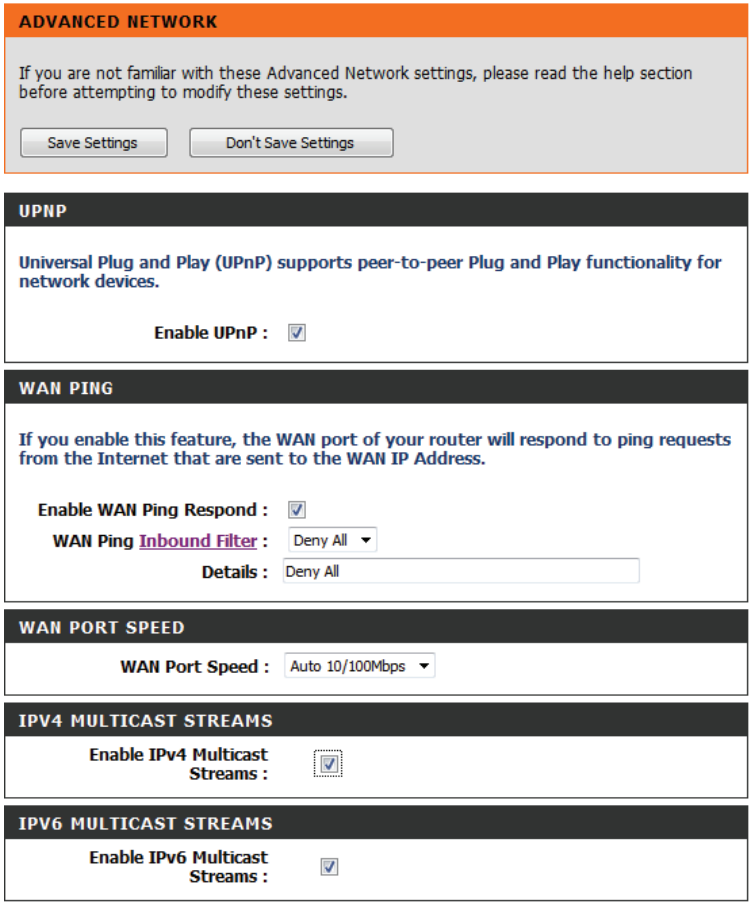
WAN Ping Inbound Filter: Choose whether to **Allow All** or **Deny All** WAN pings according to the inbound filter rules determined under the Inbound Filters section.

Details: Displays the state of the WAN ping inbound filter.

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

Enable IPV4 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, and will allow only Internet access to any clients that are connected. You may configure different zones for the 2.4 GHz and 5 GHz wireless bands.

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

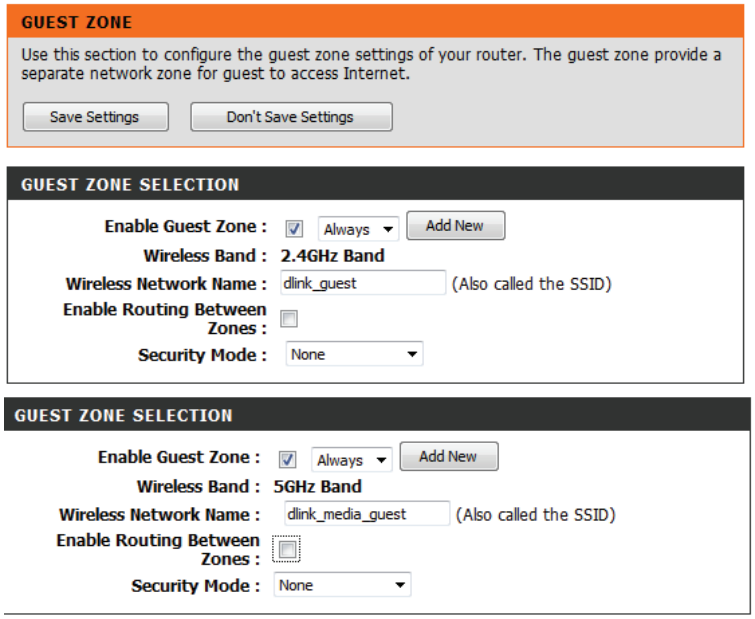
Schedule: The schedule of time when the guest zone will be active. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools** > **Schedules** section or click Add New.

Wireless Band: Indicates whether the settings are for the **2.4 GHz** or **5 GHz Wireless** band.

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

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

Security Mode: Select the type of security or encryption you would like to enable for the guest zone.



IPv6 Firewall

The DIR-808L's IPv6 firewall feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-808L's IPv6 firewall functions in a similar way to the IP Filters feature.

Enable IPv6 Ingress Filtering: Tick the box to enable ingress filtering protection for IPv6.

Enable IPv6 Simple Security: Check the box to enable the IPv6 firewall simple security.

Configure IPv6 Firewall: Select an action from the drop-down menu.

Name: Enter a name to identify the IPv6 firewall rule.

Schedule: Use the drop-down menu to select the time schedule that the IPv6 firewall rule will be enabled on. The schedule may be set to **Always**, which will allow the particular service to always be enabled. You can create your own times in the **Tools** > **Schedules** section.

Interface (Source): Use the drop-down menu to specify the interface that connects to the source IPv6 addresses of the firewall rule.

IP Address Range (Source): Enter the source IPv6 address range in the adjacent **IP Address Range** field.

Protocol: Select the protocol of the firewall port (**All**, **TCP**, **UDP**, or **ICMP**).

Interface (Dest): Use the drop-down menu to specify the interface that connects to the destination IP addresses of the firewall rule.

IP Address Range (Dest): Enter the destination IPv6 address range in the adjacent **IP Address Range** field.

Port Range: Enter the first port of the range that will be used for the firewall rule in the first box and enter the last port in the field in the second box.

IPv6 Routing

This page allows you to specify custom routes that determine how data is moved around your network.

Checkbox: Tick the box next to the route you wish to enable.

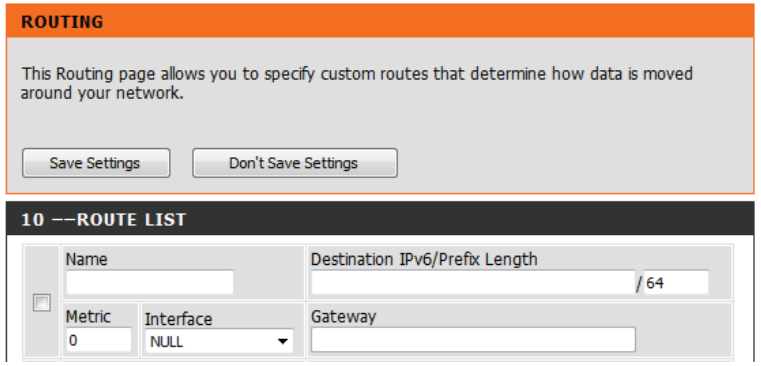
Name: Enter a specific name to identify this route.

Destination IP/ Prefix Length: This is the IP address of the router used to reach the specified destination or enter the IPv6 address prefix length of the packets that will take this route.

Metric: Enter the metric value for this rule here.

Interface: Use the drop-down menu to specify if the IP packet must use the WAN or LAN interface to transit out of the router.

Gateway: Enter the next hop that will be taken if this route is used.



Tools

Admin

This page will allow you to change the Administrator password. You can also enable remote management and specify the settings for the remote management feature.

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

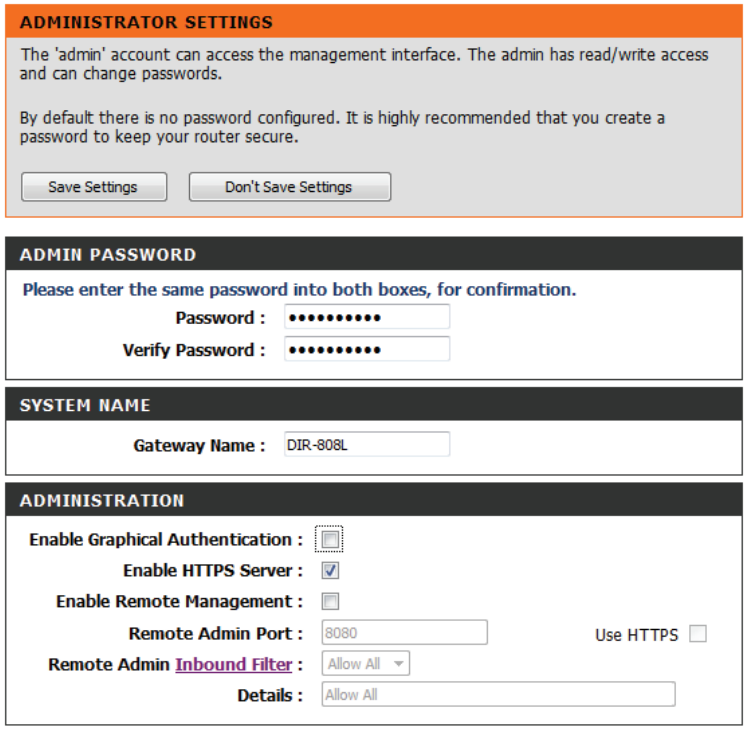
Gateway name: Enter a name for your router.

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

Enable HTTPS Server: Check to enable HTTPS to connect to the router securely. 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-808L to be configured from the Internet by a web browser. A username/password is still required to access the web management interface.

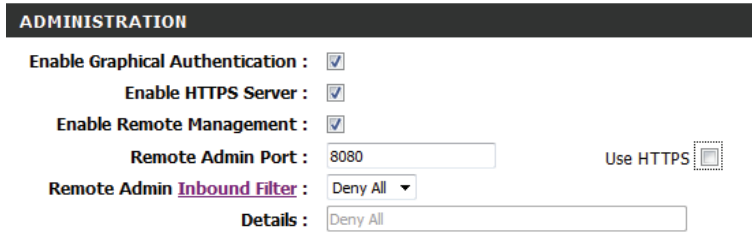
Remote Admin Port: The port number used to access the DIR-808L is used in the URL. Example: **http://x.x.x.x:8080** where x.x.x.x is the Internet IP address of the DIR-808L and 8080 is the port used for the



Web Management interface.

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

This section will list any rules that are created. You may click the **Edit** icon to change the settings or enable/disable the rule, or click the **Delete** icon to remove the rule. **Details** will display the current status.



Time

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

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

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

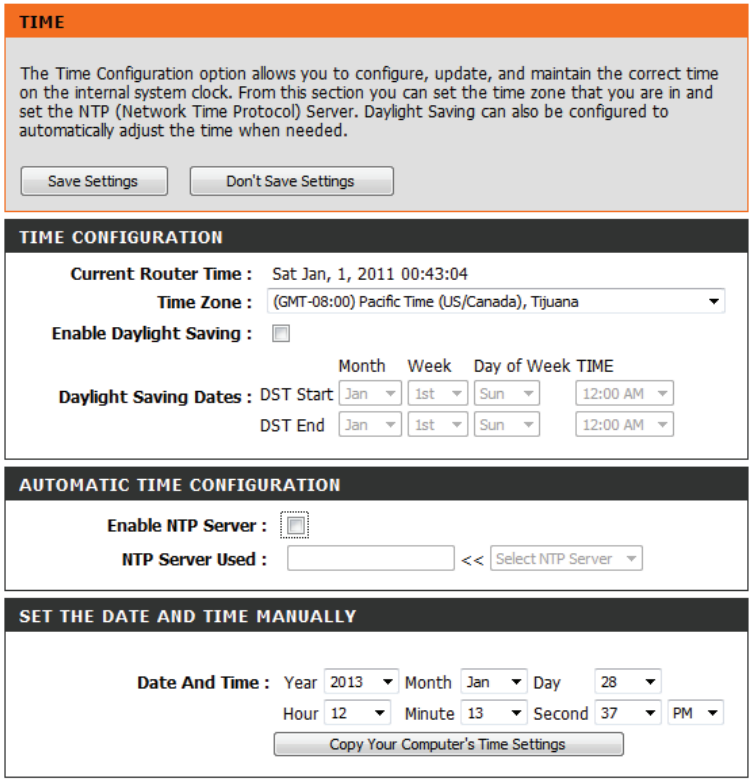
Enable Daylight Saving: To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

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

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

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

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

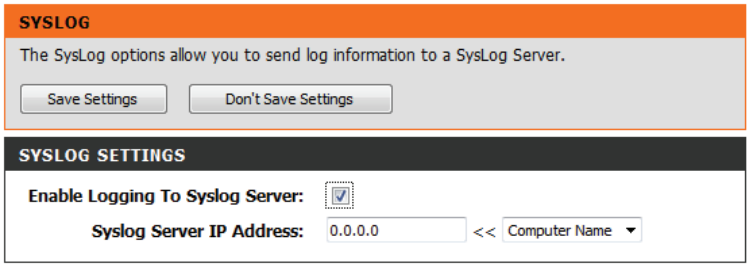


SysLog

The DIR-808L keeps a running log of events and activities occurring on the Router. You may send these logs to a SysLog server on your network.

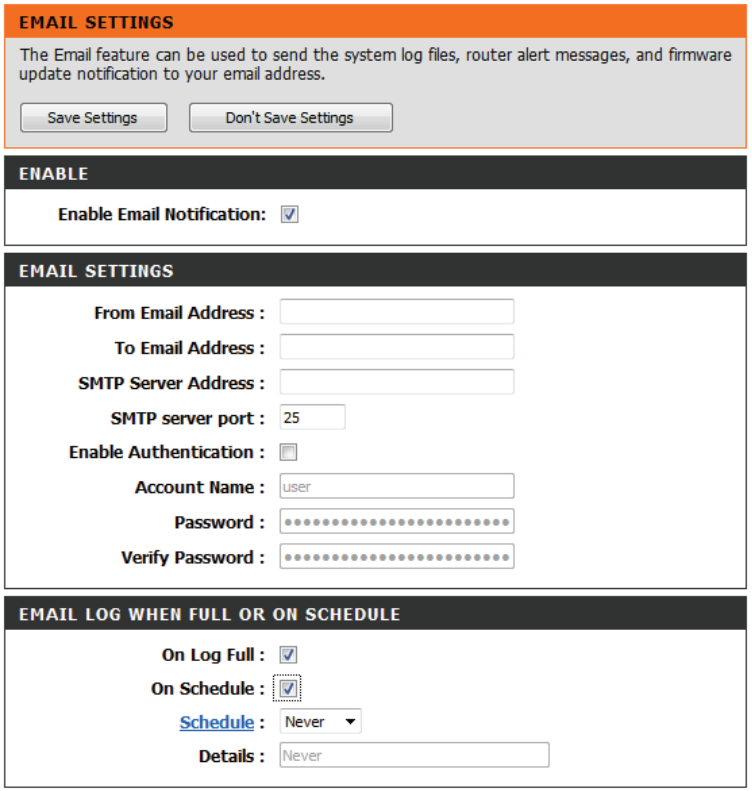
Enable Logging to SysLog Server: Check this box to send the router logs to a SysLog server.

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



Email Settings

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



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

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

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

SMTP Server Address: Enter the SMTP server address for sending email.

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 email.

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

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

On Schedule: Selecting this option will send the logs via email according to schedule.

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

Details: Lists the details of the current schedule.

System Settings

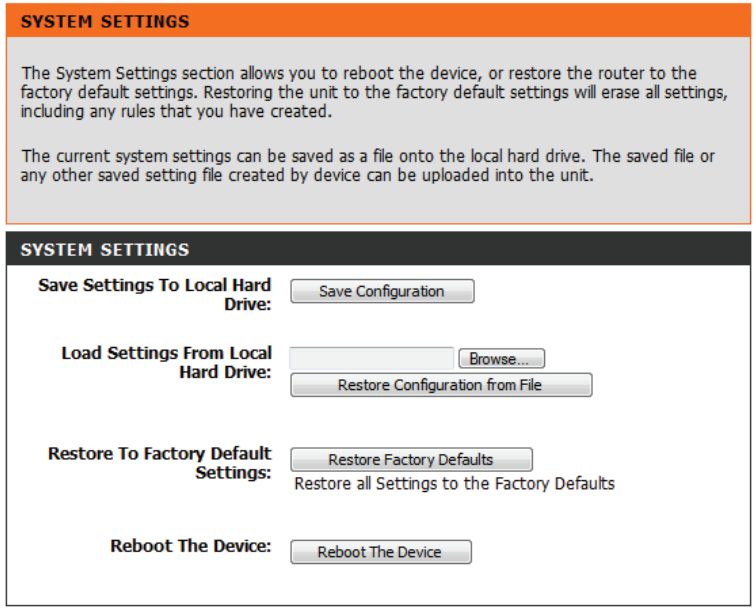
This section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

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

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

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

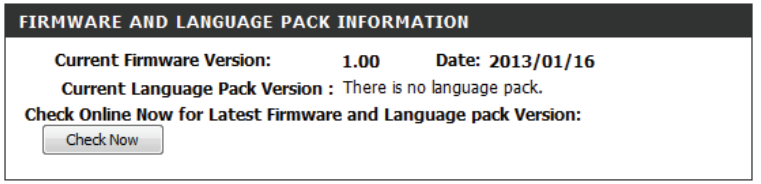
Reboot Device: Click to reboot the router.

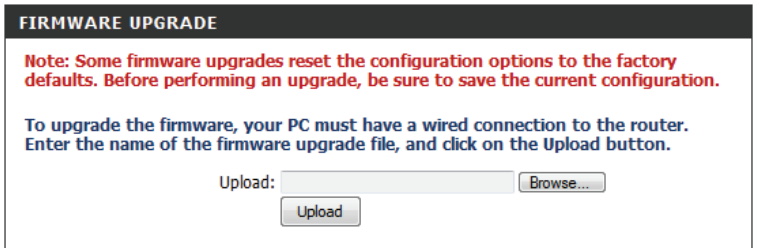


Firmware Update

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

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

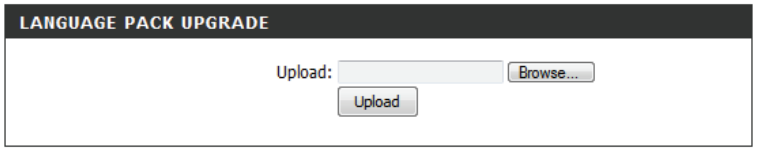




Language Pack

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

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



Dynamic DNS

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

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

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

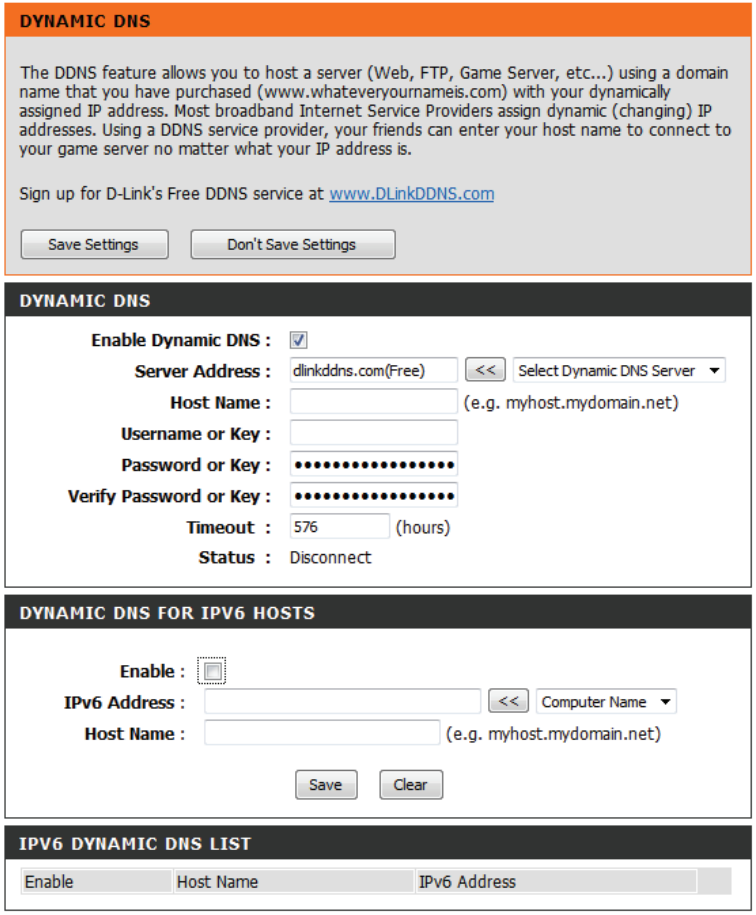
Host Name: Enter the host name that you registered with your DDNS service provider.

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.

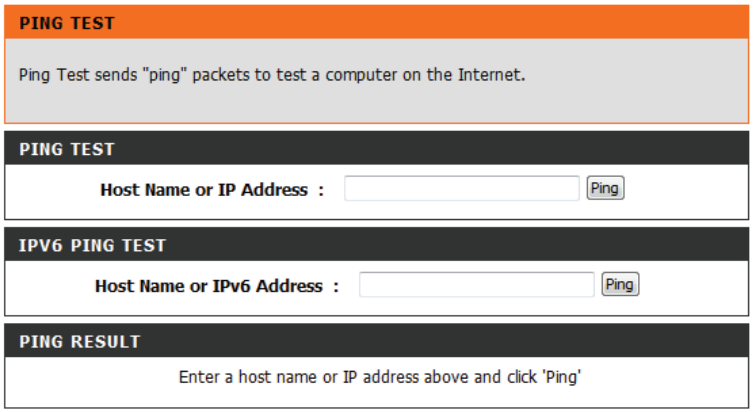


System Check

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

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

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



Schedules

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

Name: Enter a name for your new schedule.

Days: **All Week** to include every day, or choose **Select** to specify a day, or multiple days.

All Day - 24 Hours: Check **All Day - 24hrs** to have the schedule on 24-hours per day.

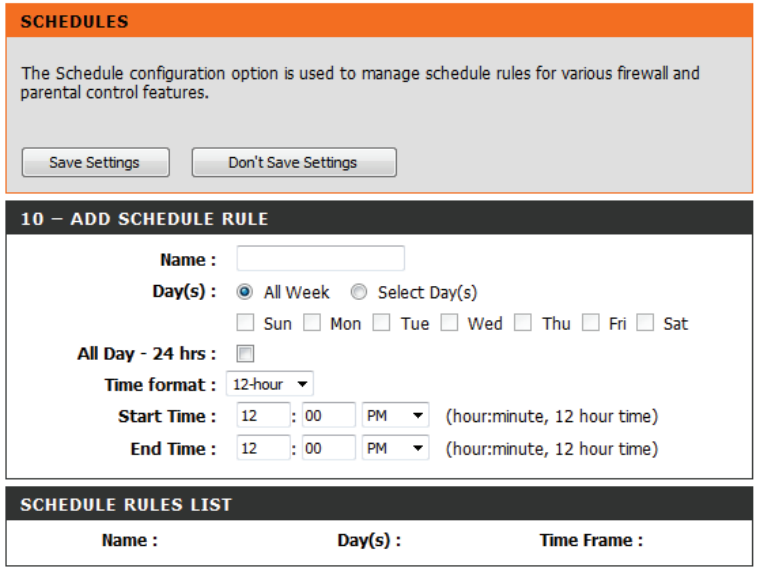
Time Format: Select **12-hour** or **24-hour** as the time format.

Start Time: Enter the starting time for the schedule each day.

End Time: Enter the end time for the schedule each day

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

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



Status

Device Info

This page displays the current information for the DIR-808L. It will display the LAN, WAN (Internet), and wireless information. If your Internet connection is set up for a Dynamic IP address, then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

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

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

WAN: Displays the MAC address and the public IP settings

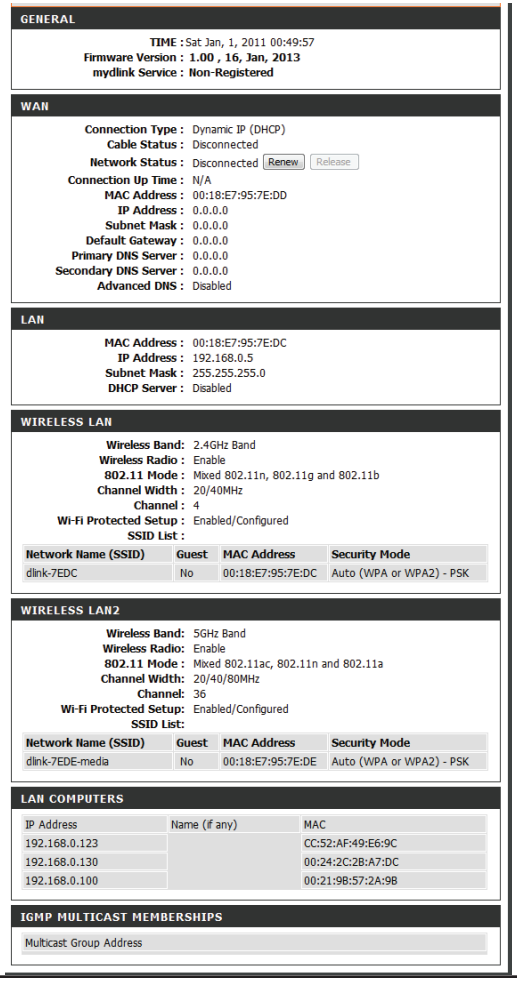
LAN: Displays the MAC address and the private (local) IP settings for the router.

Wireless LAN: Displays the 2.4 GHz wireless MAC address and your wireless settings such as SSID and channel.

Wireless LAN2: Displays the 5 GHz wireless MAC address and your wireless settings such as SSID and channel.

LAN Computers: Displays computers and devices that are connected to the router via Ethernet and that are receiving an IP address assigned by the router (DHCP).

IGMP Multicast Memberships: Shows details of current multicast connections.



Logs

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

Log Options: You can select the types of messages that you want to display from the log. System Activity, Debug Information, Attacks, Dropped Packets, and Notice messages can be selected. Click **Apply Log Settings Now** to activate your settings.

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

First Page: Click to go to the first page.

Last Page: Click to go to the last page.

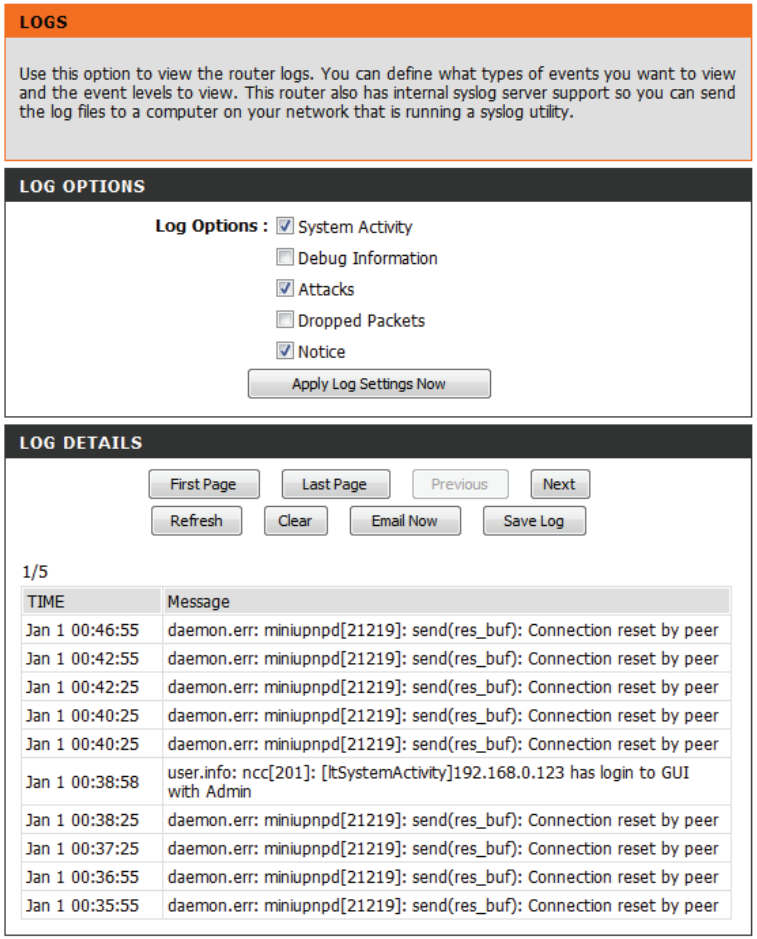
Previous: Click to go back one page.

Next: Click to go to the next page.

Clear: Clears all of the log contents.

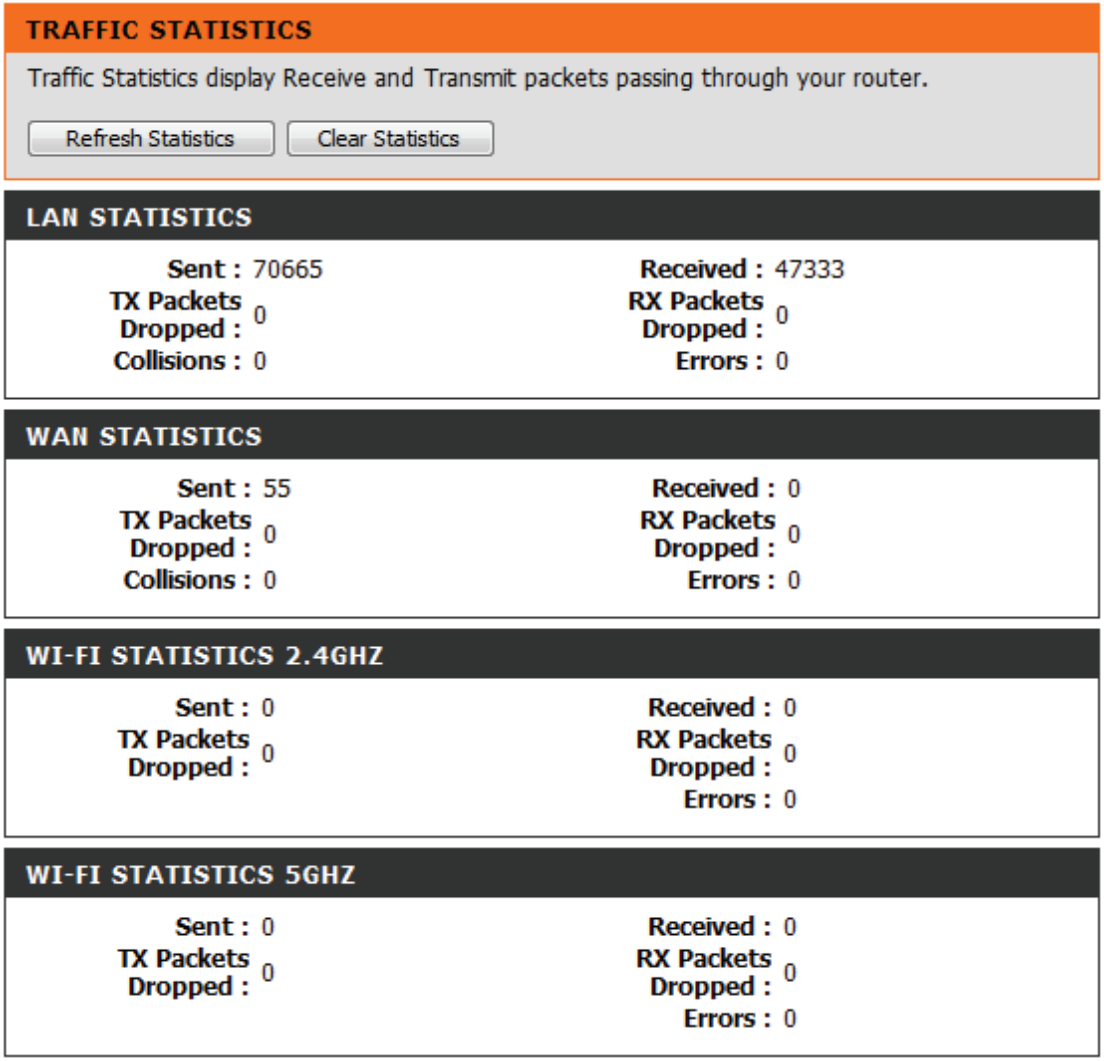
Email Now: This option will send a copy of the router log to your email address configured in the **Tools** > **Email Settings** screen.

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



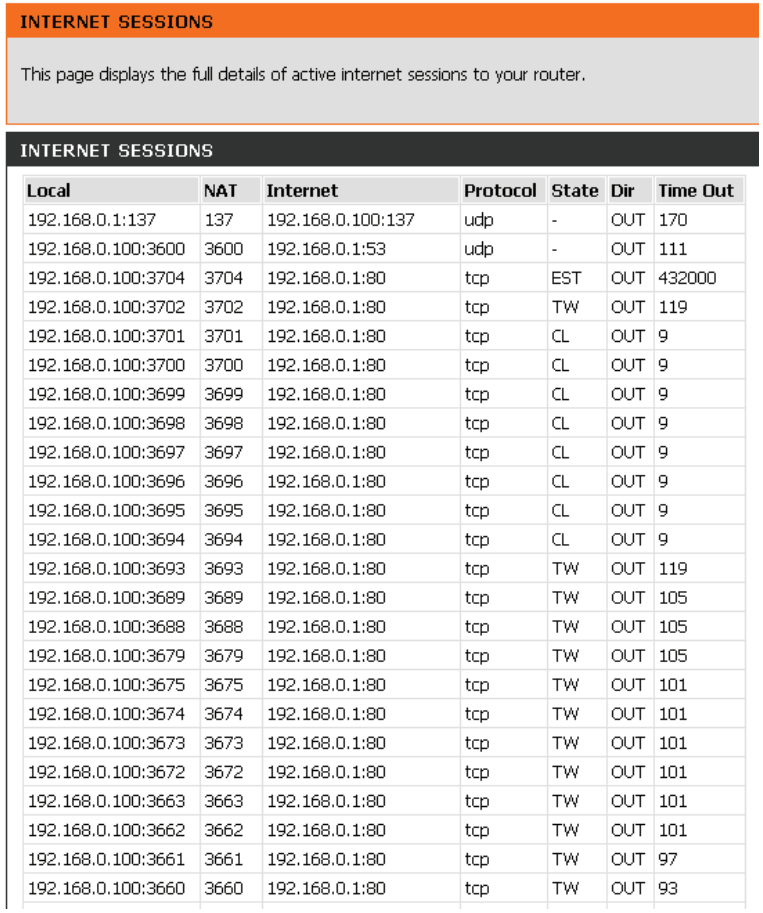
Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-808L on both the WAN and LAN ports, and the wireless segments. The traffic counter will reset if the device is rebooted.



Internet Sessions

The Internet Sessions page displays full details of active Internet sessions through your router. An Internet session is a conversation between a program or application on a LAN-side computer and a program or application on a WAN-side computer. For further information regarding the information in this table, please refer to the relevant article in the Support section of the user interface.



INTERNET SESSIONS

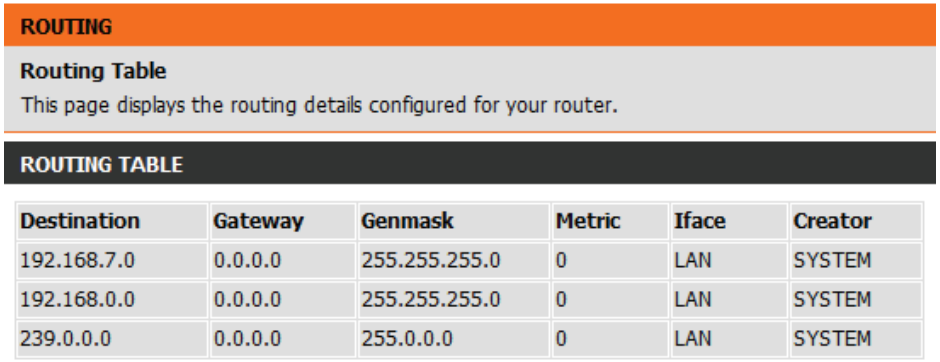
This page displays the full details of active internet sessions to your router.

INTERNET SESSIONS

Local	NAT	Internet	Protocol	State	Dir	Time Out
192.168.0.1:137	137	192.168.0.100:137	udp	-	OUT	170
192.168.0.100:3600	3600	192.168.0.1:53	udp	-	OUT	111
192.168.0.100:3704	3704	192.168.0.1:80	tcp	EST	OUT	432000
192.168.0.100:3702	3702	192.168.0.1:80	tcp	TW	OUT	119
192.168.0.100:3701	3701	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3700	3700	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3699	3699	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3698	3698	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3697	3697	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3696	3696	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3695	3695	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3694	3694	192.168.0.1:80	tcp	CL	OUT	9
192.168.0.100:3693	3693	192.168.0.1:80	tcp	TW	OUT	119
192.168.0.100:3689	3689	192.168.0.1:80	tcp	TW	OUT	105
192.168.0.100:3688	3688	192.168.0.1:80	tcp	TW	OUT	105
192.168.0.100:3679	3679	192.168.0.1:80	tcp	TW	OUT	105
192.168.0.100:3675	3675	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3674	3674	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3673	3673	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3672	3672	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3663	3663	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3662	3662	192.168.0.1:80	tcp	TW	OUT	101
192.168.0.100:3661	3661	192.168.0.1:80	tcp	TW	OUT	97
192.168.0.100:3660	3660	192.168.0.1:80	tcp	TW	OUT	93

Routing

This page will display your current routing table. This information will also reflect any routing settings configured in the Routing section of the setup.



ROUTING

Routing Table

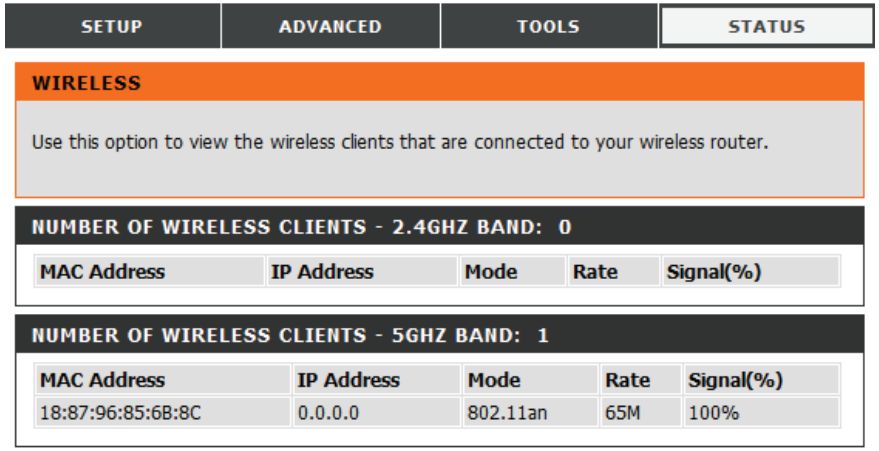
This page displays the routing details configured for your router.

ROUTING TABLE

Destination	Gateway	Genmask	Metric	Iface	Creator
192.168.7.0	0.0.0.0	255.255.255.0	0	LAN	SYSTEM
192.168.0.0	0.0.0.0	255.255.255.0	0	LAN	SYSTEM
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN	SYSTEM

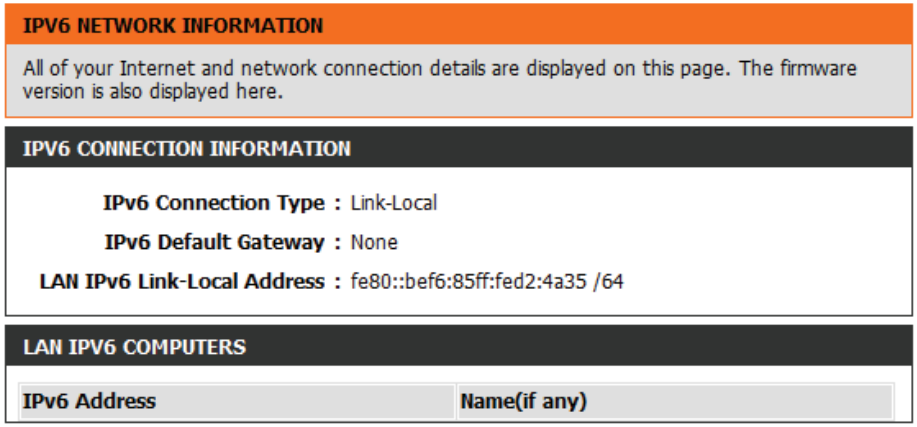
Wireless

The wireless client table displays a list of currently connected wireless clients. This table displays the MAC address of the connected wireless clients, as well as client IP address, wireless mode, connection rate, and signal strength for each client.



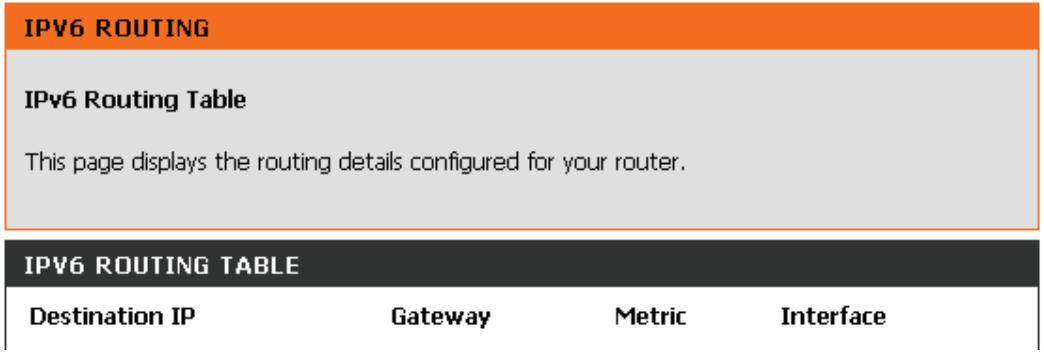
IPv6

The IPv6 page displays a summary of the router's IPv6 settings and lists the IPv6 address and host name of any IPv6 clients.

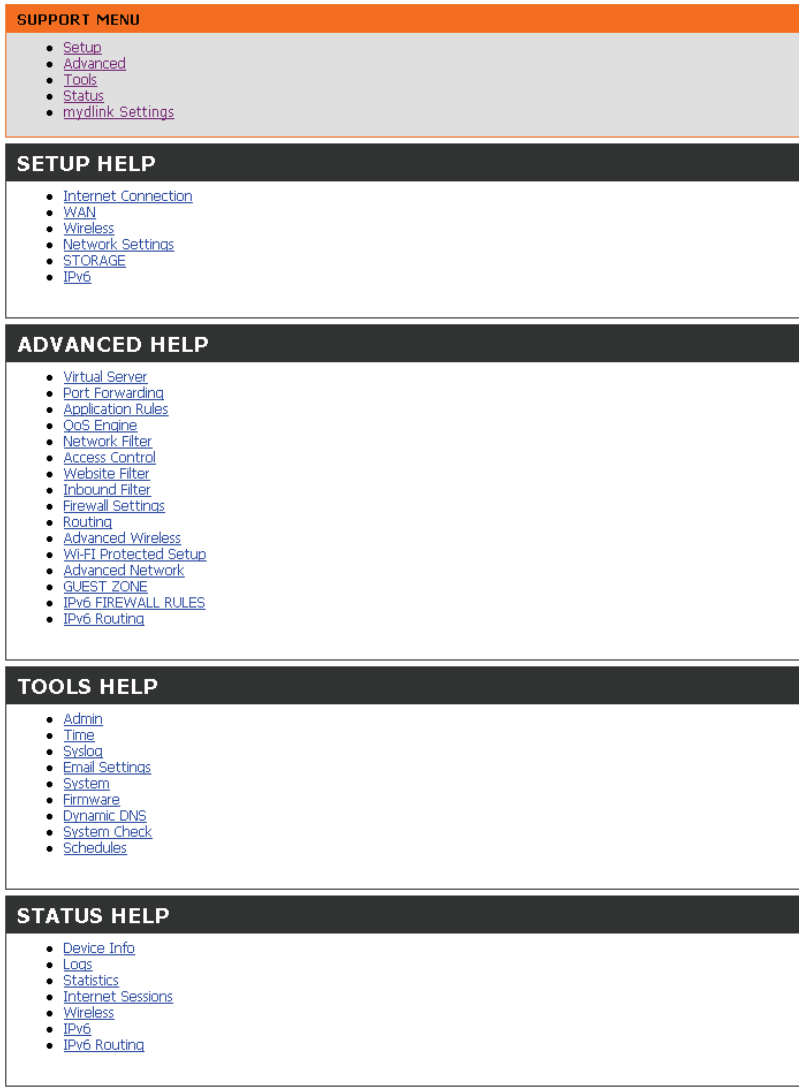


IPV6 Routing

This page displays the IPV6 routing details configured for your router.



Support


SUPPORT MENU
Setup
Advanced
Tools
Status
mydlink Settings
SETUP HELP
Internet Connection
WAN
Wireless
Network Settings
STORAGE
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
IPv6 FIREWALL RULES
IPv6 Routing
TOOLS HELP
Admin
Time
Syslog
Email Settings
System
Firmware
Dynamic DNS
System Check
Schedules
STATUS HELP
Device Info
Logs
Statistics
Internet Sessions
Wireless
IPv6
IPv6 Routing

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-808L router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the DIR-808L for about 1 second. The power LED on the front will start to blink.

Step 2 - Within 120 seconds, press the WPS button on your wireless client (or launch the software utility and start the WPS process).

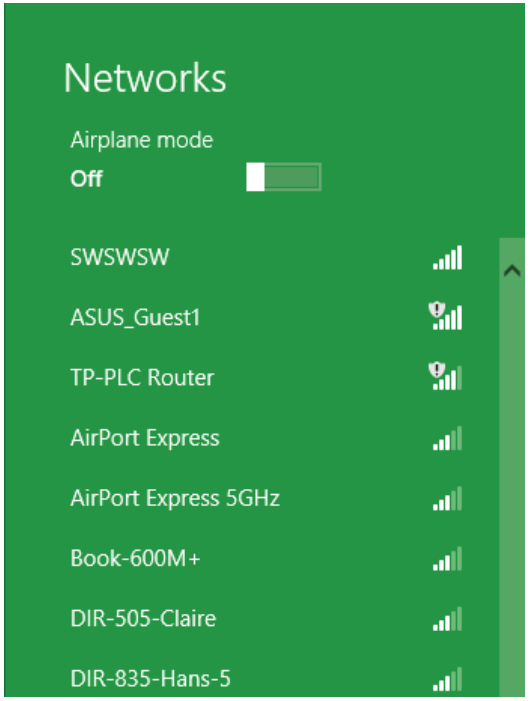
Step 3 - Allow up to 1 minute for the configuration process to complete. Once the power light stops blinking, you will be connected and your wireless connection will be secured with WPA2.

Windows® 8
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 (Wi-Fi password) being used.

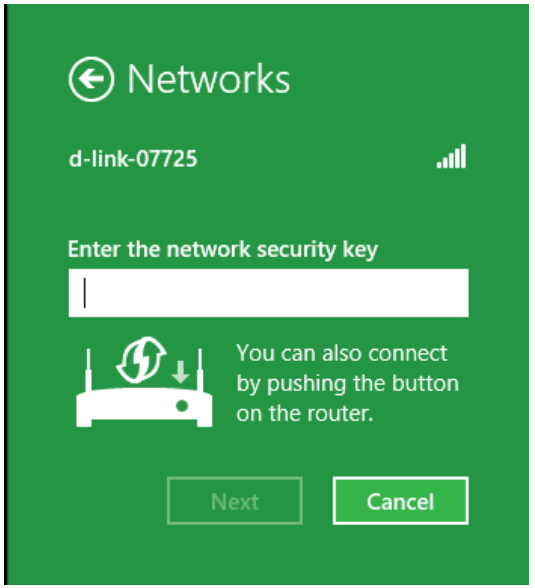
To join an existing network, locate the wireless network icon in the taskbar, next to the time display.

Clicking on this icon will display a list of wireless networks which are within connecting proximity of your computer. Select the desired network by clicking on the network name.

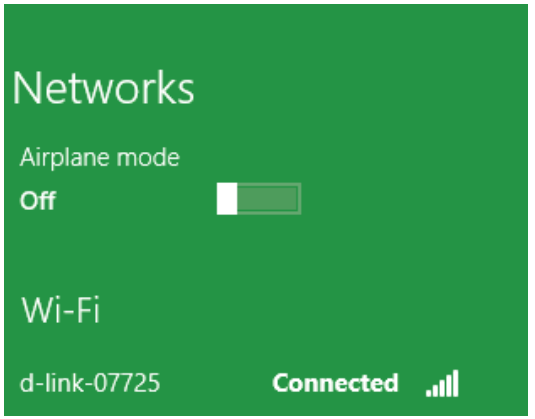


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

If you wish to use Wi-Fi Protected Setup (WPS) to connect to the router, you can also press the WPS button on your router at this point to enable the WPS function.



When you have established a successful connection to a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



Windows® 7
WPA/WPA2

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

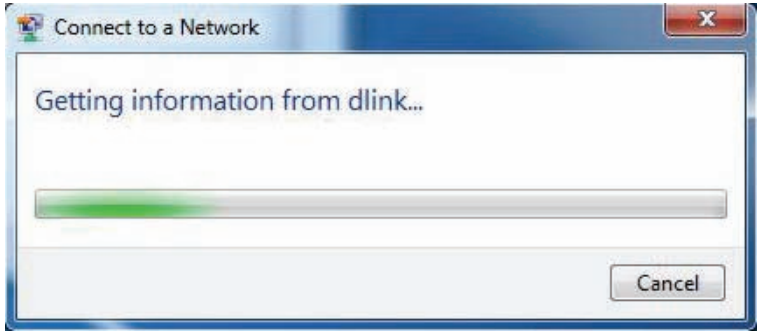
1. Click on the wireless icon in your system tray (lower-right corner).

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

3. Highlight the wireless connection with the Wi-Fi name (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.



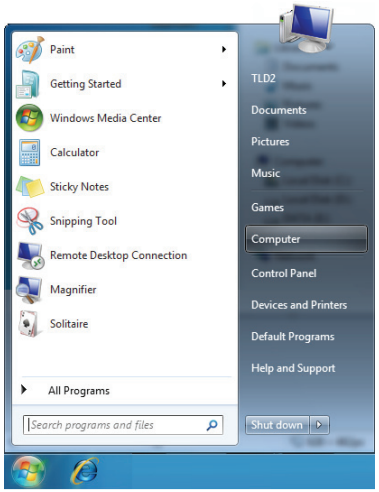
5. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**. You can also connect by pushing the WPS button on the router.

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.

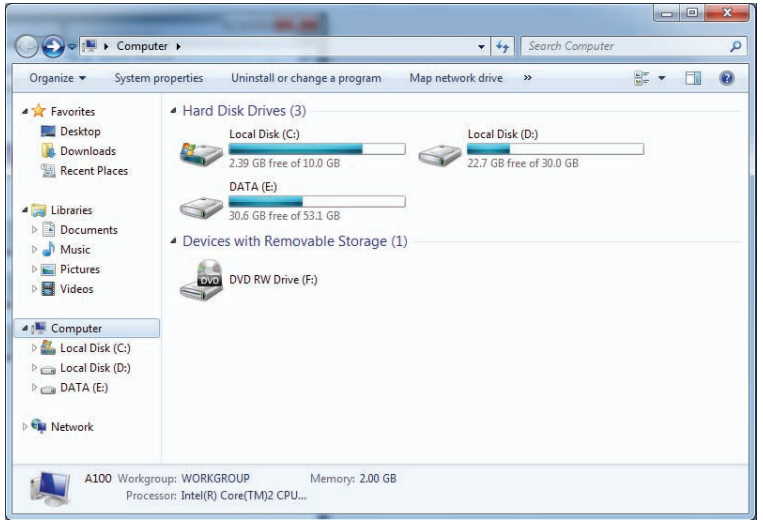
WPS

The WPS feature of the DIR-808L can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

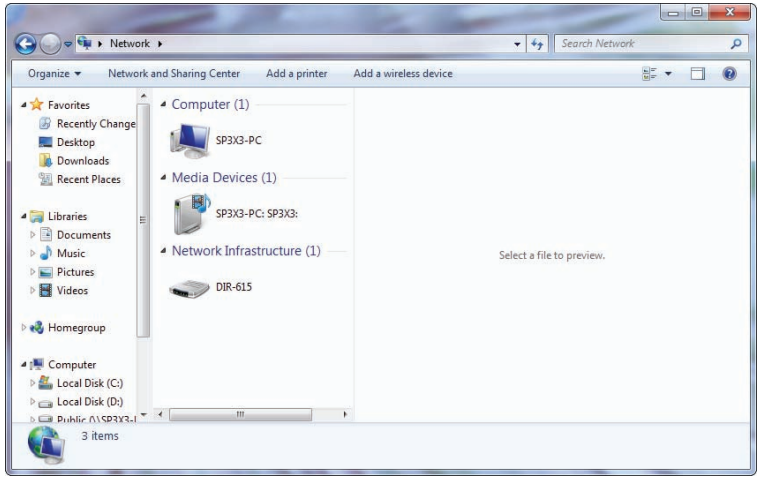
1. Click the **Start** button and select **Computer** from the Start menu.



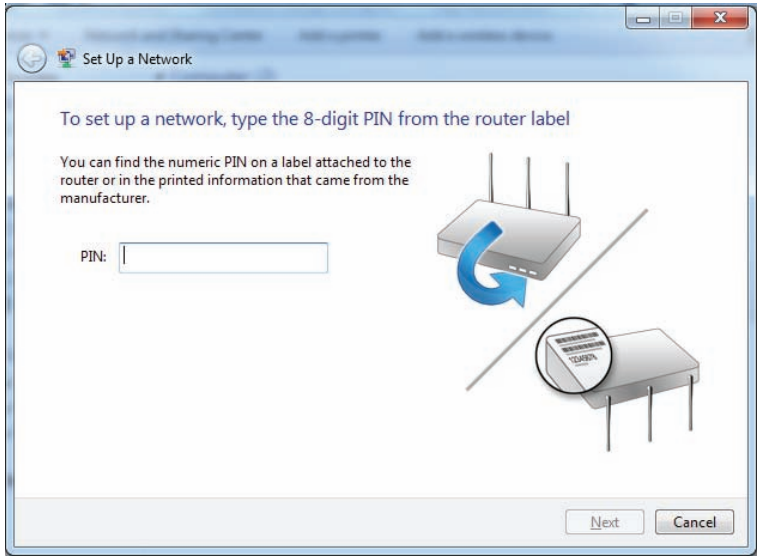
2. Click **Network** on the left side.



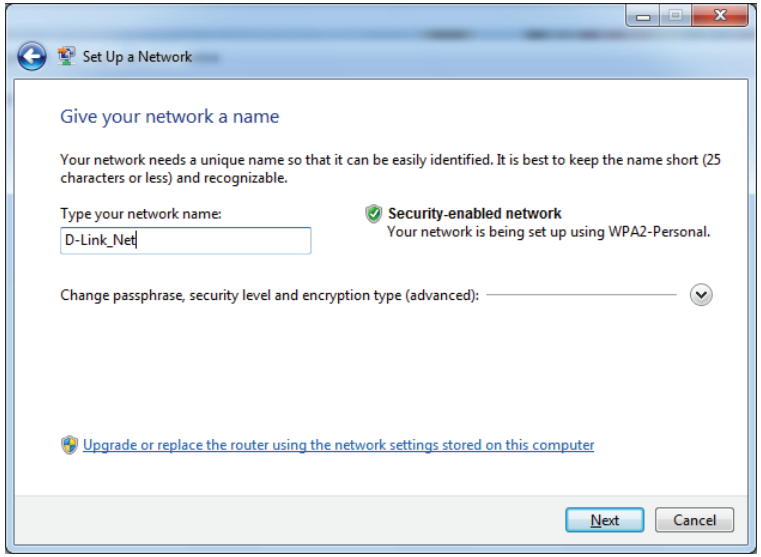
3. Double-click the DIR-808L.



4. Input the WPS PIN number (displayed in the WPS box on the router's label, or in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.

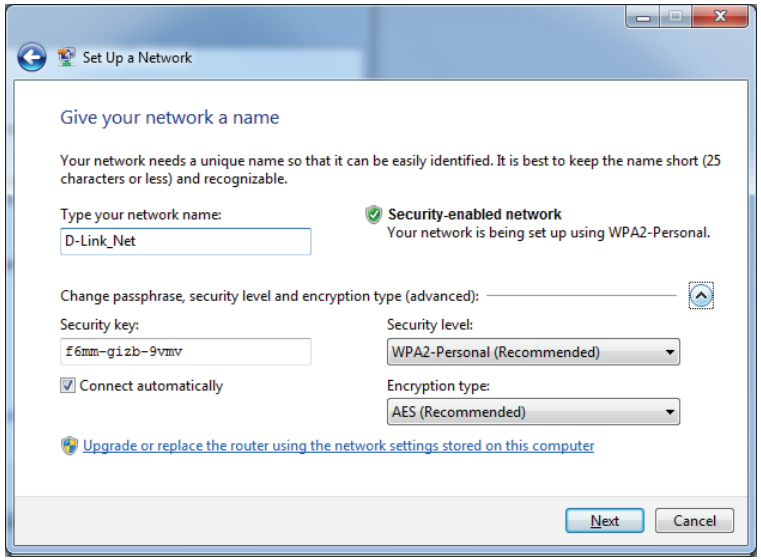


5. Type a name to identify the network.



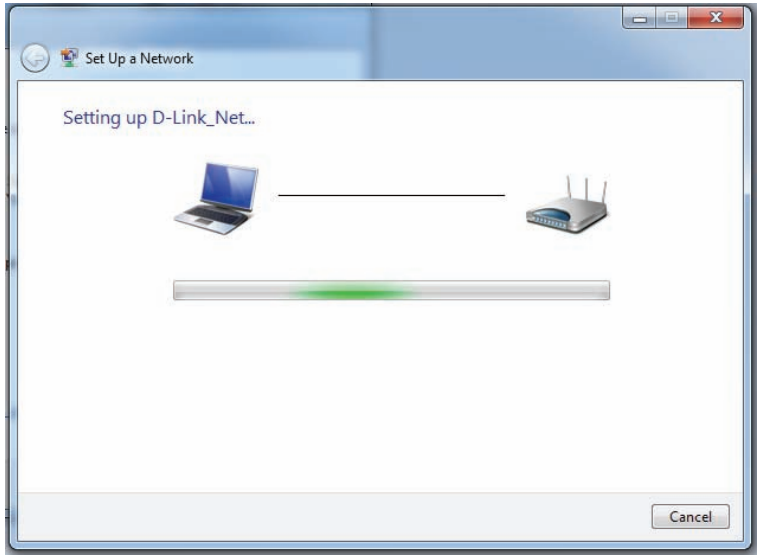
6. To configure advanced settings, click the icon.

Click **Next** to continue.



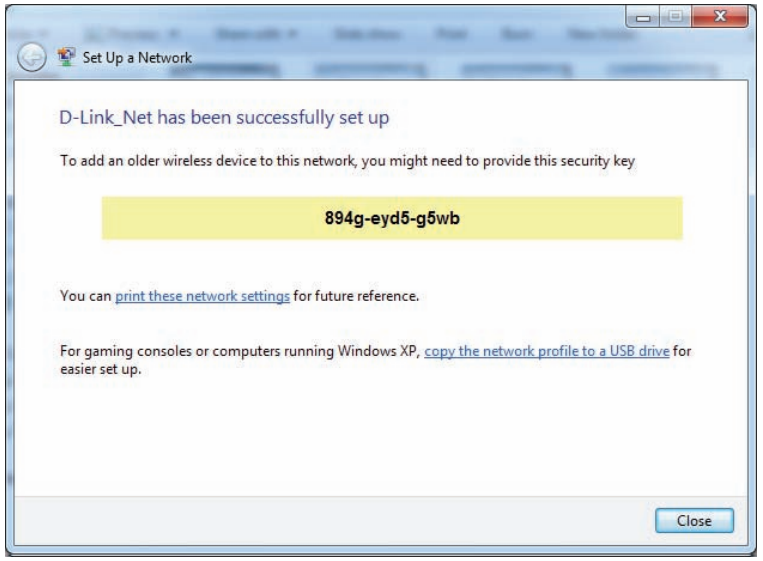
7. The following window appears while the router is being configured.

   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.

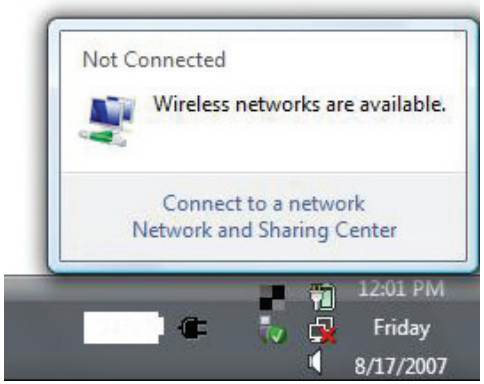
Windows Vista®

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.

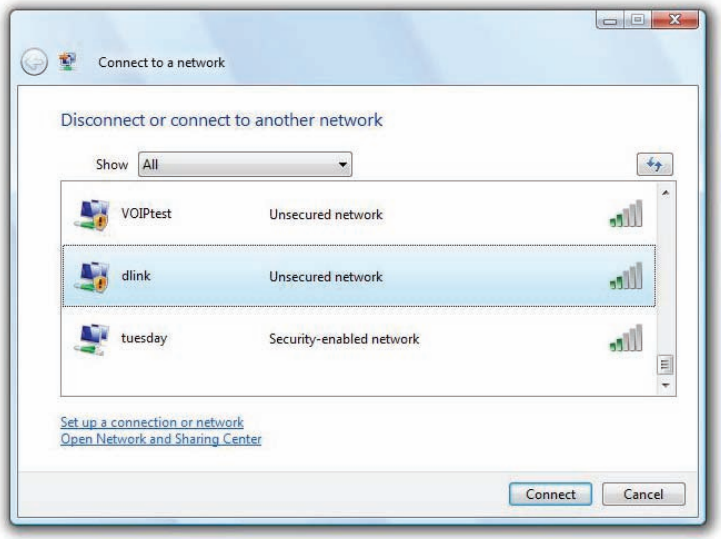
or

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.

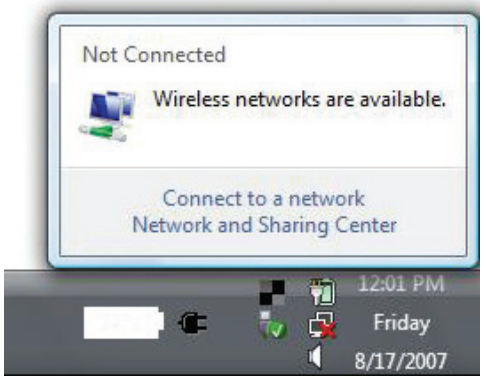
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



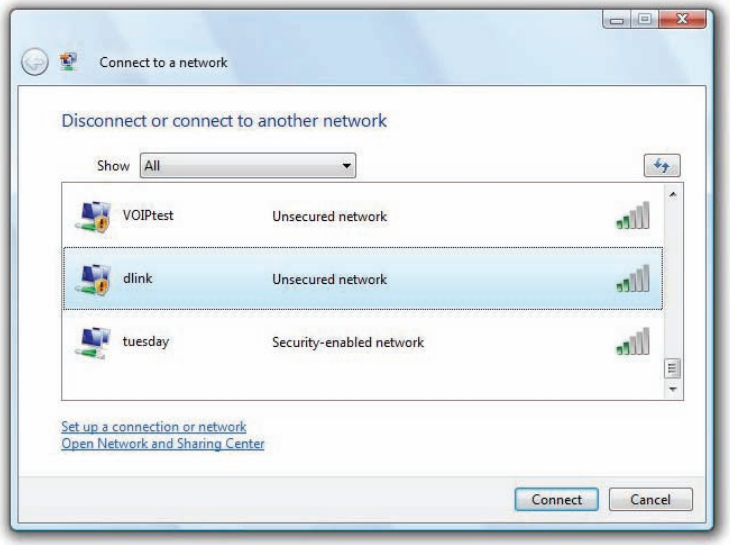
WPA/WPA2

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 Wi-Fi name (SSID) you would like to connect to and click **Connect**.



3. Enter the same security key or passphrase (Wi-Fi password) that is on your router and click **Connect**.

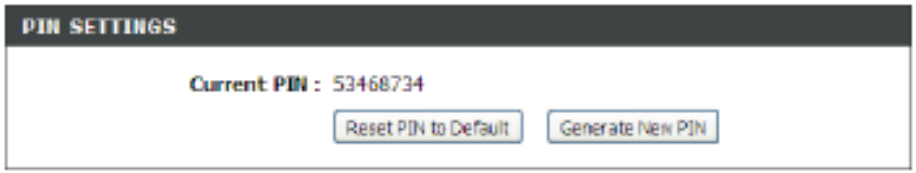
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

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 any 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 configure manually.

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

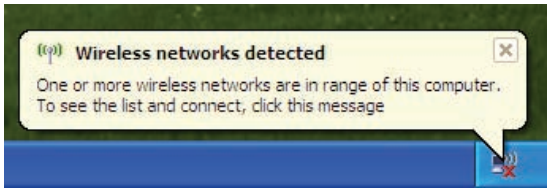


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Windows® XP

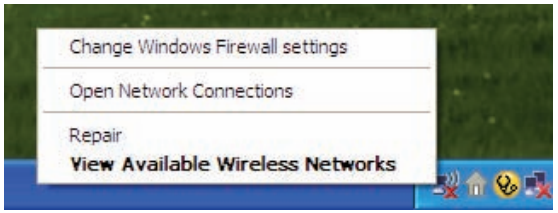
Windows XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using a third party utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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



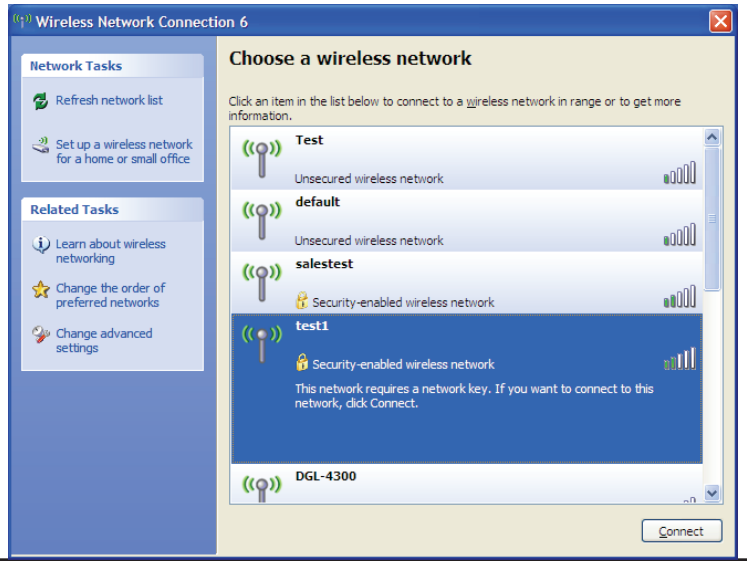
or

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

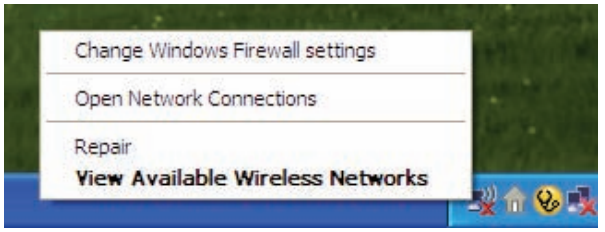
If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



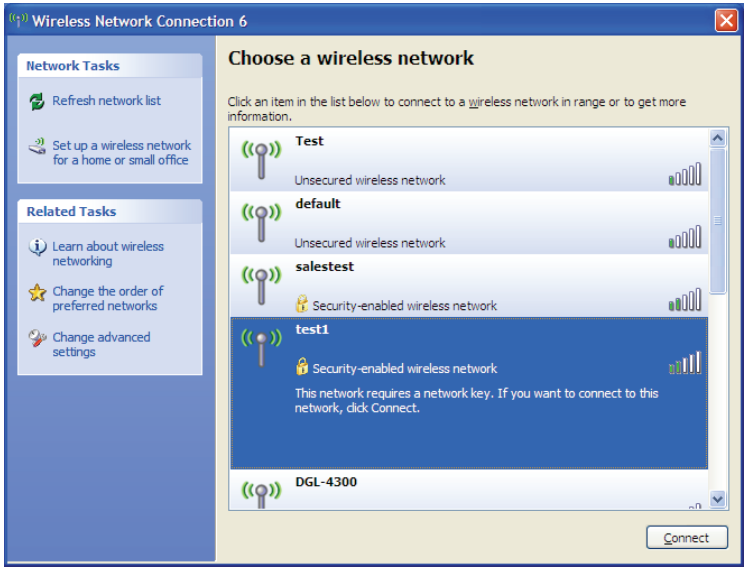
WPA/WPA2

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.

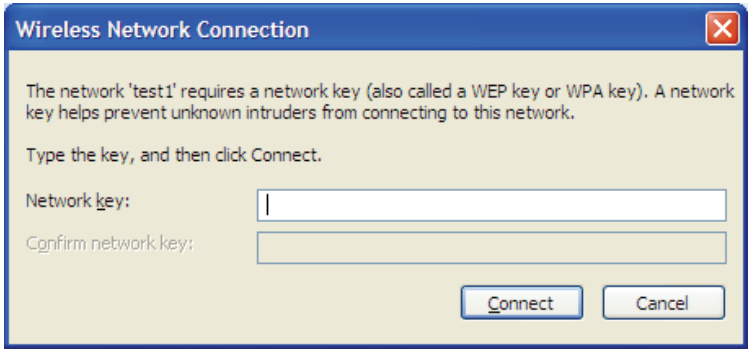
1. Open the Windows XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.



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



3. The **Wireless Network Connection** box will appear. Enter the WPA-PSK Wi-Fi password 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 Wi-Fi password 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-808L. Read the following descriptions if you are having problems. The examples below are illustrated in Windows XP. If you have a different operating system, any screenshots on your computer may appear different 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 on 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 3.5 and higher
  - Google™ Chrome 8 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 ZoneAlarm, BlackICE, 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 re-open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

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

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

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

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

- Click on **Start** and then click **Run**.
- Windows NT, 2000, XP, Vista, 7, and 8 users type in **cmd** and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

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

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

```
C:\>ping yahoo.com -f -l 1482

Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:

Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

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

C:\>ping yahoo.com -f -l 1472

Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:

Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52

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

C:\>
```

You should start at 1472 and work your way down by 10 each time. Once you

get a reply, go up by 2 until you get a fragmented packet. Take that value and add 28 to the value to account for the various TCP/IP headers. For example, lets say that 1452 was the proper value, the actual MTU size would be 1480, which is the optimum for the network we're working with (1452+28=1480).

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

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

- Open your browser, enter the IP address of your router (**192.168.0.1**) and click **OK**.
- Enter your username (**admin**) and password (blank if you have not changed the default setting). 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 the site that you were trying to visit. If changing the MTU has not resolved the problem, continue changing the MTU in increments of ten.

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 wireless network Cardbus adapters.

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

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

Networking Basics

Check your IP address

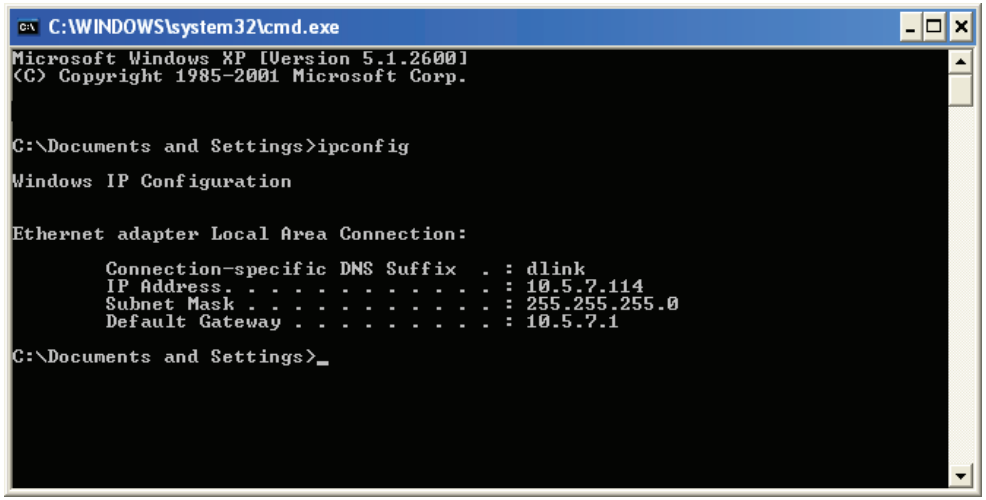
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



Assign a Static IP address

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

Step 1

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

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

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

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

Step 2

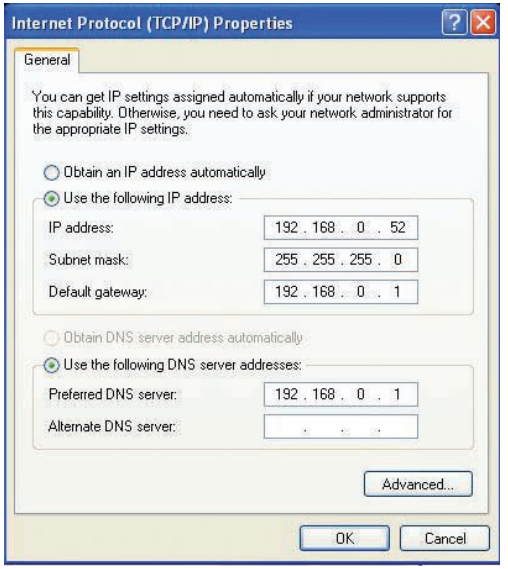
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

Step 3

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

Step 4

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



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

Set the primary DNS the same as the LAN IP address of your router (**192.168.0.1**). The secondary DNS is not required, however you may be required to enter a DNS server by your ISP.

Step 5

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

Technical Specifications

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

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

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

Wireless Frequency Range*
- 2.412 GHz ~ 2.483.5 GHz (802.11b/g/n)
- 5.15 GHz ~ 5.825 GHz (802.11a/n/ac)

Wireless Bandwidth Rate
- IEEE 802.11n: 6.5 to 150 Mbps
- IEEE 802.11ac: 6.5 to 433 Mbps

Antenna Type
- Internal Antenna

Wireless Security
- 64/128-bit WEP, WPA/WPA2-Personal, WPA/WPA2-Enterprise, WPS (PIN & PBC)

Certifications
- FCC, CE, C-Tick.
- Wi-Fi Certified
- IPv6 Certified
- CCC

Dimensions & Weight
- 156.5 x 113.2 x 53.6 mm (6.16 x 4.46 x 2.11 inches)
- 184.7 grams (0.41 lbs)

* Wireless frequency range may vary depending on region

Federal Communication Commission Interference 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.

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

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

Important Note:

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.

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

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

Caution :
(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
(ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

Avertissement:
(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

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

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