# USER MANUAL

## DIR-652

VERSION 1.1

D-Link®

WIRELESS

# 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

| | | |
|---|---|---|
| 1.0 | January 20, 2010 | • Initial version |
| 1.1 | May 12, 2011 | • Revisions |

## 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 © 2008-2010 by D-Link Systems, Inc.

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

# Table of Contents

**Preface** ..... **i**
Manual Revisions ..... i
Trademarks ..... i

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

**Installation** ..... **6**
Before you Begin ..... 6
Wireless Installation Considerations ..... 7
Getting Started ..... 8

**Configuration** ..... **9**
Web-based Configuration Utility ..... 9
Setup Wizard ..... 10
Manual Configuration ..... 14
Dynamic (Cable) ..... 14
PPPoE (DSL) ..... 15
PPTP ..... 16
L2TP ..... 18
Static (assigned by ISP) ..... 20
Wireless Settings ..... 21
Network Settings ..... 22
DHCP Server Settings ..... 23
DHCP Reservation ..... 25
Virtual Server ..... 27
Port Forwarding ..... 29
Application Rules ..... 30
QoS Engine ..... 31
Network Filters ..... 33
Access Control ..... 34
Access Control Wizard ..... 34
Website Filters ..... 37
Inbound Filters ..... 38
Firewall Settings ..... 39
SPI ..... 39
NAT Endpoint Filtering ..... 39
DMZ ..... 39
SPI ..... 40
NAT Endpoint Filtering ..... 40
DMZ ..... 40
Routing ..... 41
Advanced Wireless Settings ..... 42
Transmit Power ..... 42
Mode ..... 42
WISH Settings ..... 43

Wi-Fi Protected Setup (WPS) ..... 45
Advanced Network Settings ..... 47
UPnP ..... 47
Internet Ping Block ..... 47
Internet Port Speed ..... 47
Multicast Streams ..... 47
Guest Zone ..... 48
IPV6 ..... 49
Link-Local Connectivity ..... 49
Static IPv6 (Stateful) ..... 50
Static IPv6 (Stateless) ..... 51
DHCPv6 (Stateful) ..... 52
DHCPv6 (Stateless) ..... 53
IPv6 over PPPoE (Stateful) ..... 54
IPv6 over PPPoE (Stateless) ..... 56
6 to 4 Tunneling (Stateful) ..... 58
6 to 4 Tunneling (Stateless) ..... 59
IPv6 in IPv4 Tunneling (Stateful) ..... 60
IPv6 in IPv4 Tunneling (Stateless) ..... 61
Administrator Settings ..... 62
Time Settings ..... 64
SysLog ..... 65
Email Settings ..... 66
System Settings ..... 68
Update Firmware ..... 69
DDNS ..... 70
System Check ..... 71
Schedules ..... 72
Device Information ..... 73
Logs ..... 74
Statistics ..... 75
Internet Sessions ..... 75
Wireless ..... 76
IPv6 ..... 76
Support ..... 77

**Wireless Security ..... 78**
What is WPA? ..... 78
Wireless Security Setup Wizard ..... 79
Configure WPA-Personal (PSK) ..... 82
Configure WPA-Enterprise (RADIUS) ..... 83
Using Windows® 7 and WPS for Wireless Configuration ..... 85
Connecting to a Wireless Network Using Windows® 7 ..... 89
Connecting to a Wireless Network Using Windows Vista® ..... 92
Connecting to a Wireless Network ..... 94
Using Windows® XP ..... 94

**Troubleshooting ..... 96**

**Wireless Basics ..... 100**
What is Wireless? ..... 101
Tips ..... 103
Wireless Modes ..... 104

**Networking Basics ..... 105**
Check your IP address ..... 105
Statically Assign an IP address ..... 106

**Technical Specifications..... 107**

**Certifications..... 108**

# Package Contents

- D-Link DIR-652 Wireless N Gigabit Home Router
- 2 Fixed Reverse SMA External Antennas
- Power Adapter
- Ethernet Cable - CAT5
- CD-ROM with Manual

***Note:*** *Using a power supply with a different voltage rating than the one included with the DIR-652 will cause damage and void the warranty.*

# System Requirements

- Ethernet-based Cable or DSL modem
- Windows®, Macintosh, or Linux-based operating system with an installed Ethernet adapter, or an 802.11n, 802.11g, or 802.11b wireless adapter
- Internet Explorer 6.0, Mozilla 1.7.12, Firefox 1.5, or Safari 1.0 (with Java 1.3.1 or higher) or higher (for configuration)
- Installation Wizard requires Windows® XP with Service Pack 2

# Introduction

## TOTAL PERFORMANCE
Combines award winning router features and 802.11n wireless technology to provide the best wireless performance.

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

## TOTAL COVERAGE
Provides greater wireless signal rates even at farther distances for best-in-class Whole Home Coverage.

## ULTIMATE PERFORMANCE
The D-Link Wireless N Gigabit Home Router (DIR-652) is a 802.11n compliant device that delivers real world performance of up to 650% faster than an 802.11g wireless connection (also faster than a 100Mbps wired Ethernet connection). Create a secure wireless network to share photos, files, music, video, printers, and network storage throughout your home. Connect the Wireless N Gigabit Home Router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this Router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

## EXTENDED WHOLE HOME COVERAGE
Powered by 802.11n technology, this high performance router provides superior coverage throughout your entire home while reducing dead spots. The Wireless N Gigabit Home Router is designed for use in bigger homes and for users who demand higher performance networking. Add a D-Link Wireless N notebook or desktop adapter and stay connected to your network from virtually anywhere in your home.

## TOTAL NETWORK SECURITY
The Wireless N Gigabit Home Router supports all of the latest wireless security features to prevent unauthorized access, be it from over the wireless network or from the Internet. Support for WPA and WEP standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this Wireless N Gigabit Home Router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

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

# Features

- **Faster Wireless Networking** - The DIR-652 provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. The performance of this 802.11n wireless router gives you the freedom of wireless networking at speeds 650% faster than 802.11g.

- **Compatible with 802.11g Devices** - The DIR-652 is still fully compatible with the IEEE 802.11g standard, so it can connect with existing 802.11g PCI, USB and Cardbus adapters.

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

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

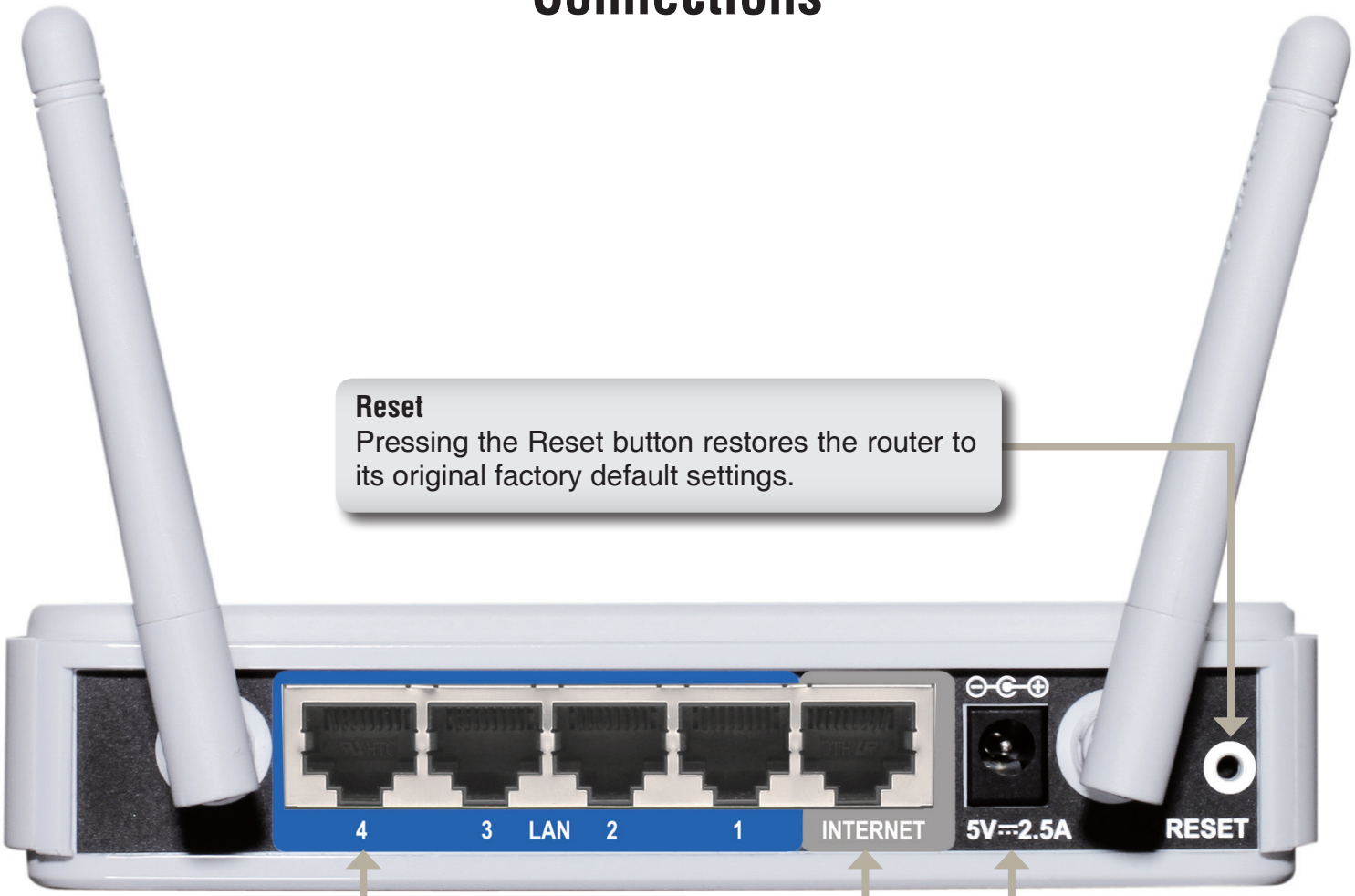
    - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.

    - **Secure Multiple/Concurrent Sessions** - The DIR-652 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-652 can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-652 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

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

# Hardware Overview
## Connections




**Reset**
Pressing the Reset button restores the router to its original factory default settings.

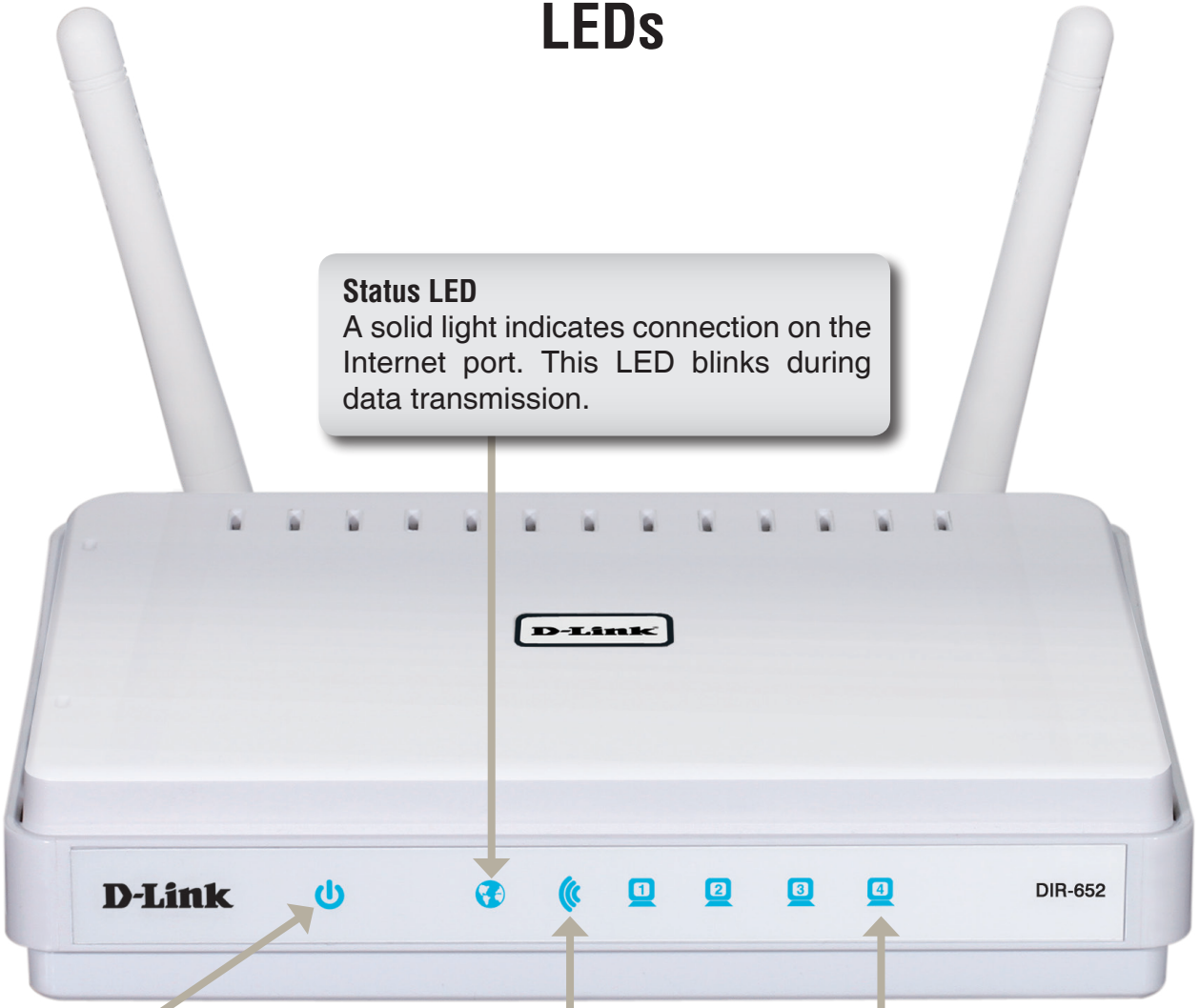
**LAN Ports (1-4)**
Connect Ethernet devices such as computers, switches, and hubs.

**Internet Port**
The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.

**Power Receptor**
Receptor for the supplied power adapter.

# Hardware Overview

## LEDs




**Status LED**
A solid light indicates connection on the Internet port. This LED blinks during data transmission.

**Power LED**
A solid light indicates a proper connection to the power supply.

**WLAN LED**
A solid light indicates that the wireless segment is ready. This LED blinks during wireless data transmission.

**Local Network LEDs**
A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

# Installation

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

# Before you Begin

Please configure the router with the computer that was last connected directly to your modem. Also, you can only use the Ethernet port on your modem. If you were using the USB connection before using the 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 D-Link wireless router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

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

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

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

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

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

# Getting Started

The DIR-652 includes a Quick Router Setup Wizard CD. Follow the simple steps below to run the Setup Wizard to guide you quickly through the installation process.

Insert the included CD-ROM into your CD-ROM drive. The step-by-step instructions that follow are shown in Windows® XP. The steps and screens are similar for the other Windows operating systems.

If the CD Autorun function does not automatically start on your computer, go to **Start > Run...**. In the run box type "**D:\D-Link.exe**" (where ***D:*** represents the drive letter of your CD-ROM drive).

When the autorun screen appears, click on the **Start** button.

***Note:*** *It is recommended to write down the SSID and Security Key, followed by the login password on the provided CD holder.*

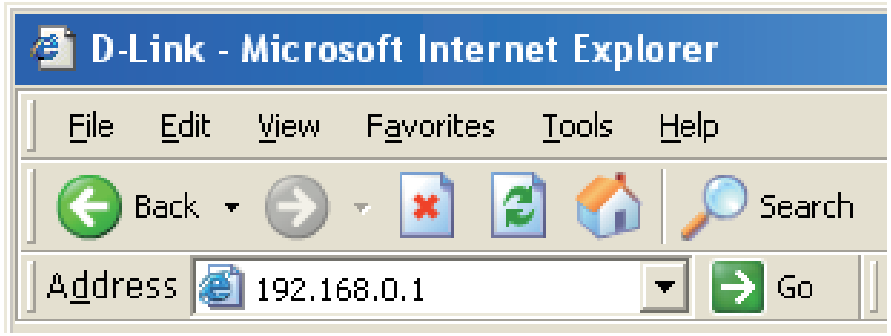
# Configuration

This section will show you how to configure your new D-Link wireless router using the web-based configuration utility.

## Web-based Configuration Utility

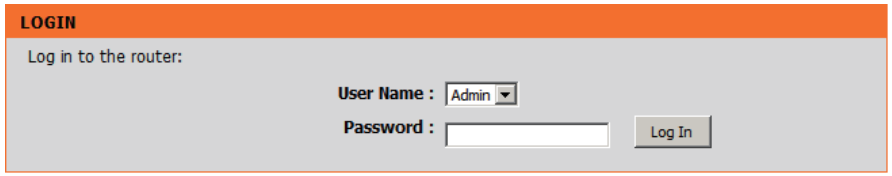
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (192.168.0.1).

You may also connect using the NetBIOS name in the address bar (**http://dlinkrouter**).




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

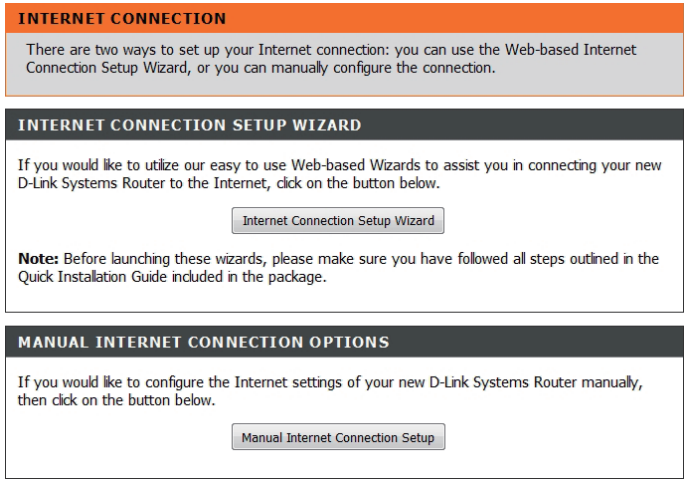
If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



# Setup Wizard

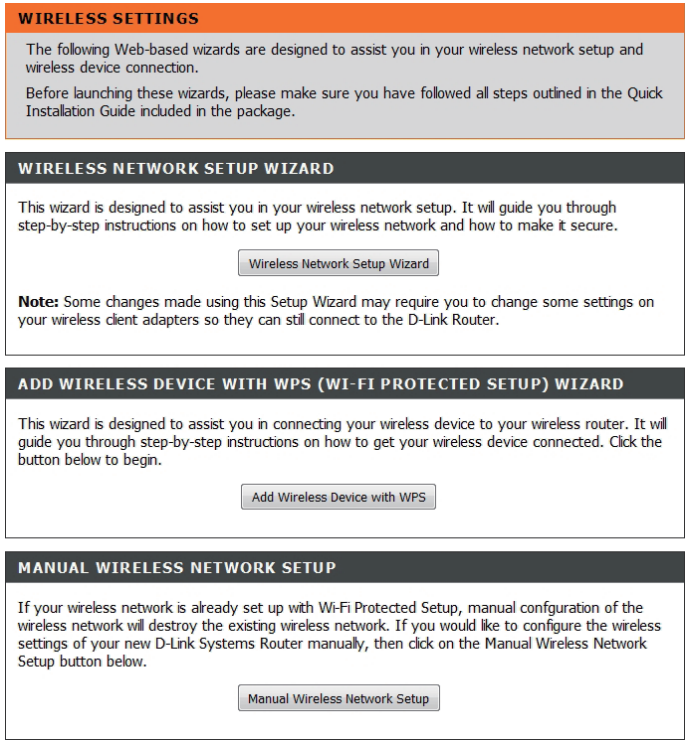
You may click **Setup Wizard** to quickly configure your router.

If you want to enter your settings without running the wizard, click **Manual Configuration** and skip to page 14.

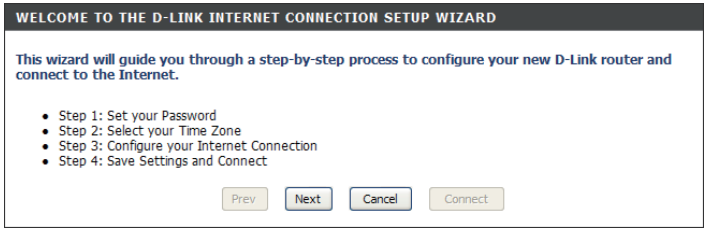



Click **Launch Internet Connection Setup Wizard** to begin.

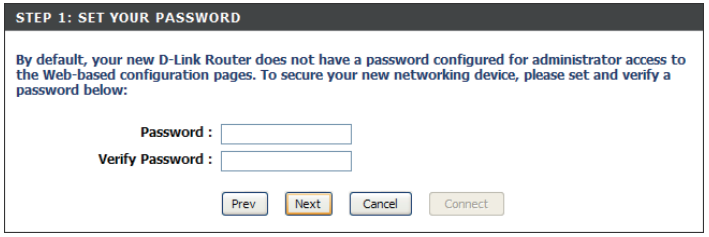
If you want to configure your wireless settings, click **Launch Wireless Security Setup Wizard** and skip to page 63.



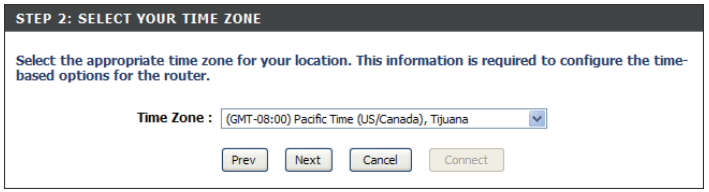
Click **Next** to continue.



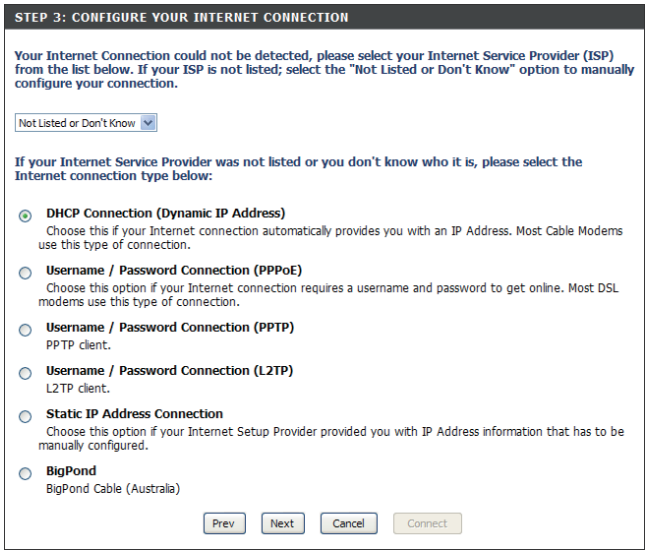

Create a new password and then click **Next** to continue.




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

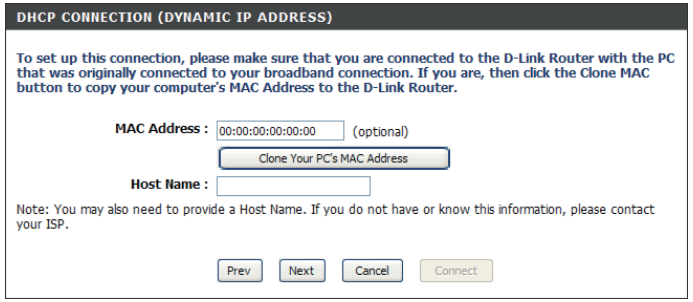



Select the type of Internet connection you use and then click **Next** to continue.



If you selected Dynamic, you may need to enter the MAC address of the computer that was last connected directly to your modem. If you are currently using that computer, click **Clone Your PC's MAC Addres** and then click **Next** to continue.

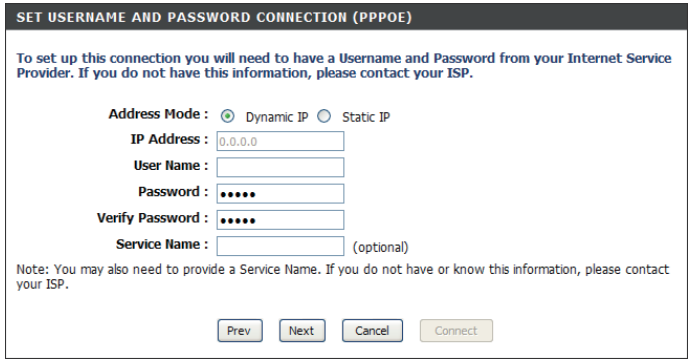
The Host Name is optional but may be required by some ISPs. The default host name is the device name of the Router and may be changed.



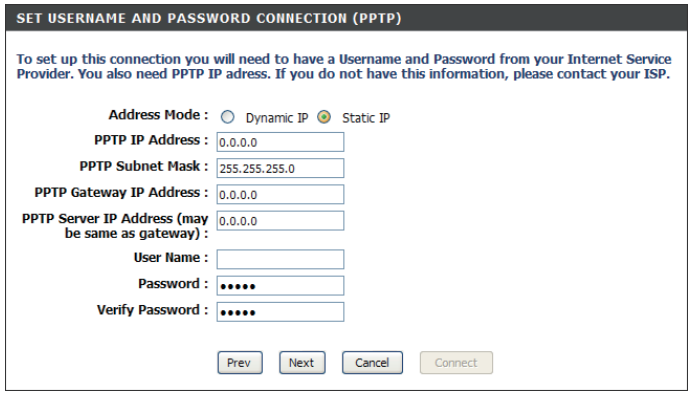

If you selected PPPoE, enter your PPPoE username and password. Click **Next** to continue.

Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses.

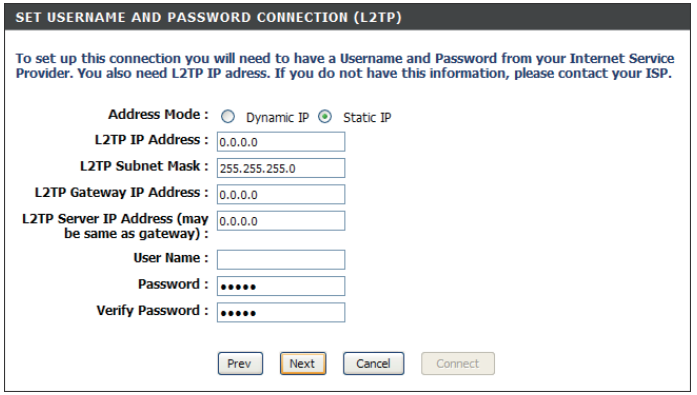
***Note:*** *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*



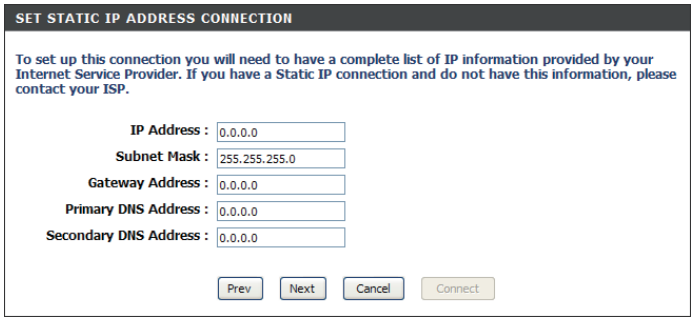

If you selected PPTP, enter your PPTP username and password. Click **Next** to continue.



If you selected L2TP, enter your L2TP username and password. Click **Next** to continue.

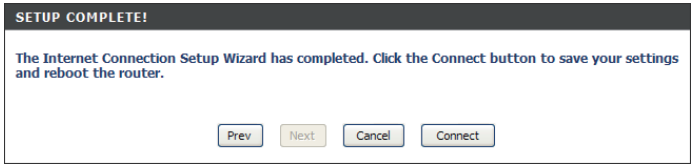



If you selected Static, enter your network settings supplied by your Internet provider. Click **Next** to continue.

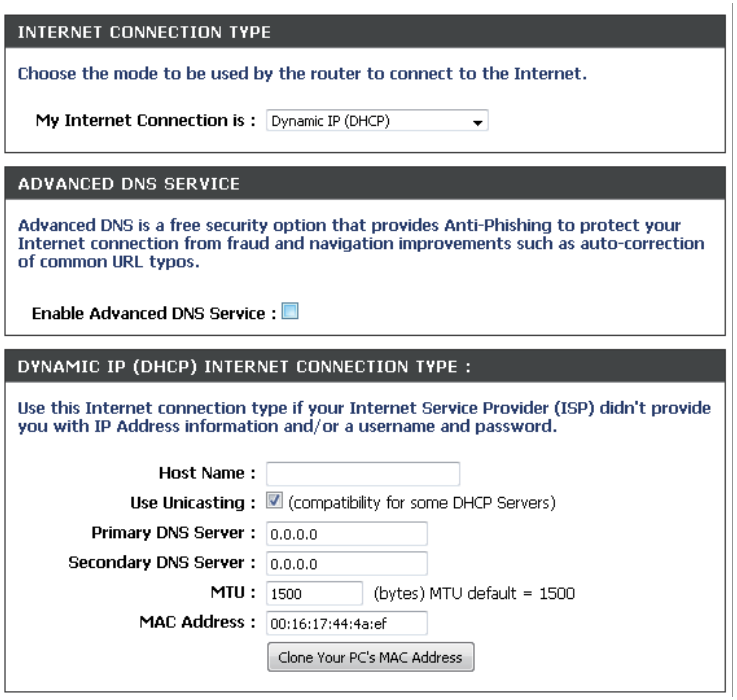



Click **Connect** to save your settings. Once the router is finished rebooting, click **Continue**. Please allow 1-2 minutes to connect.

Close your browser window and reopen it to test your Internet connection. It may take a few tries to initially connect to the Internet.



# Manual Configuration
## Dynamic (Cable)




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

**Enable Advanced DNS Service:** Advanced Domain Name System (DNS) services enhances your Internet performance by getting you the information and web pages you are looking for faster and more reliably. In addition, it improves your overall Internet experience by correcting many common typo mistakes automatically, taking you where you intended to go and saving you valuable time.

***Disclaimer:*** *D-Link makes no warranty as to the availability, reliability, functionality and operation of the Advanced DNS service or its features.*

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

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

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

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

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

# Internet Setup
## PPPoE (DSL)

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

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

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

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

**User Name:** Enter your PPPoE user name.

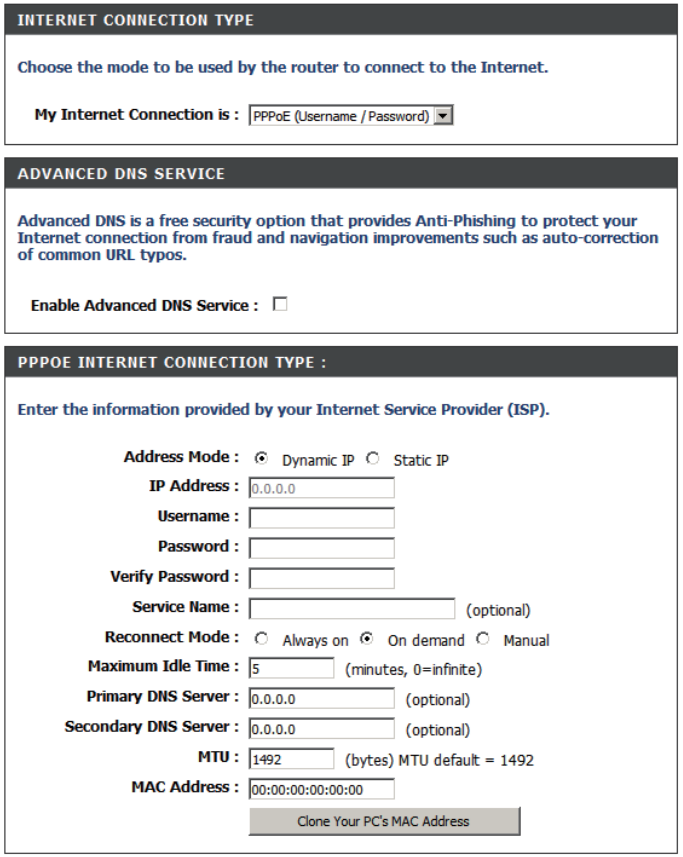
**Password:** Enter your PPPoE password and then retype the password in the next box.

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

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

**Maximum Idle Time:** Enter the Primary and Secondary DNS Server Addresses (Static PPPoE only).

**DNS Addresses:** 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.

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

# Internet Setup
## PPTP

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

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

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

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

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

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

**Username:** Enter your PPTP username.

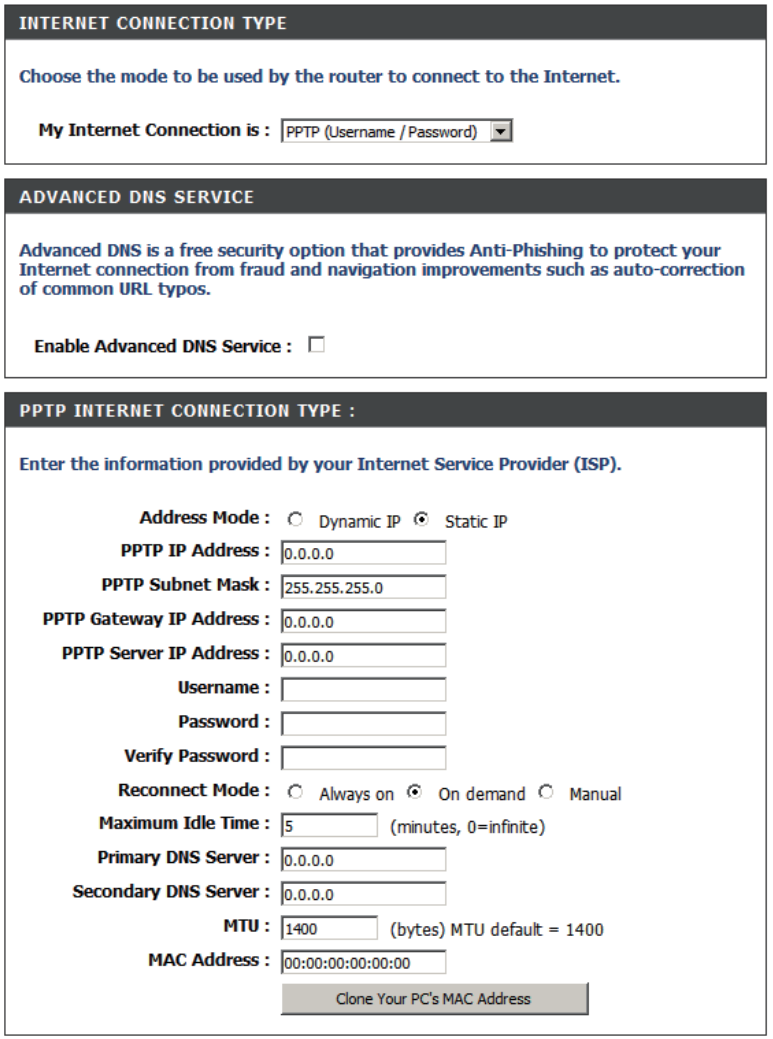
**Password:** Enter your PPTP password and then retype the password in the next box.

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

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

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

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



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

# 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.

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

**L2TP IP Address:** Enter the L2TP IP address supplied by your ISP (Static only).

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

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

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

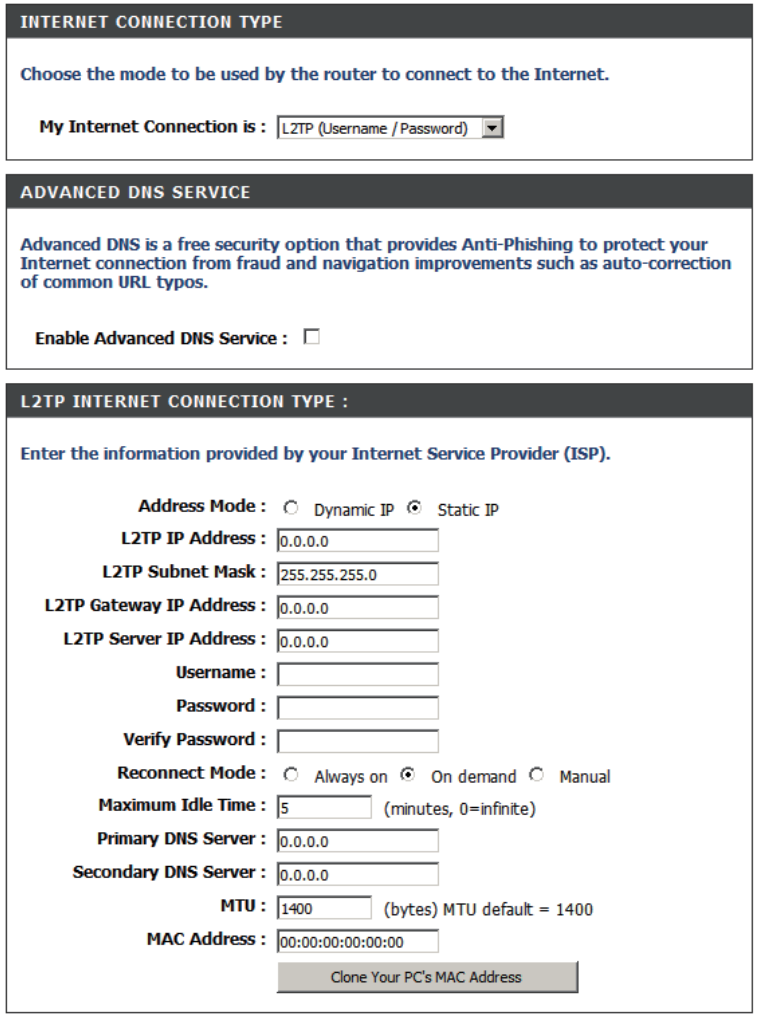
**Username:** Enter your L2TP username.

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

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

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

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



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

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

# Internet Setup
## Static (assigned by ISP)

Select Static IP Address if all the Internet port's IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.

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

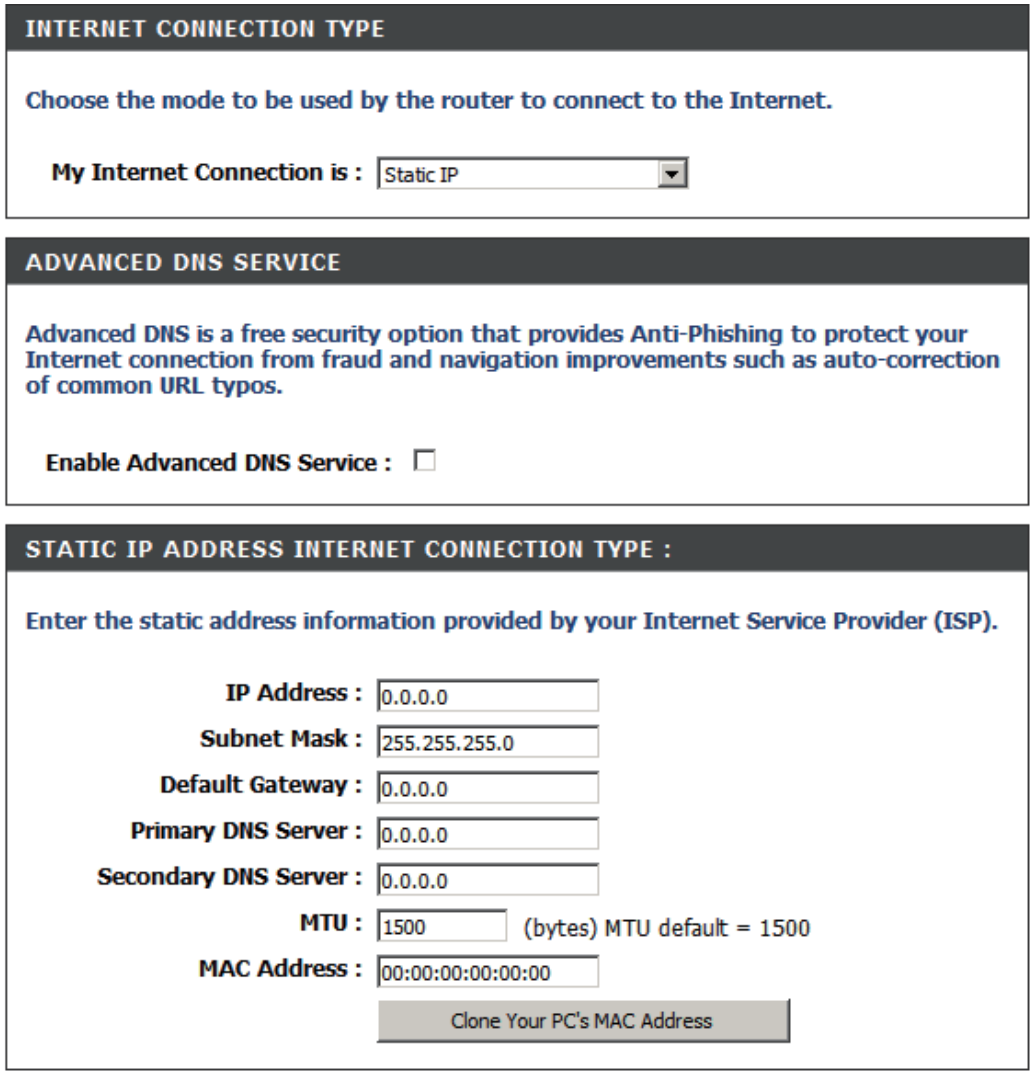
**Subnet Mask:** Enter the Subnet Mask assigned by your ISP.

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

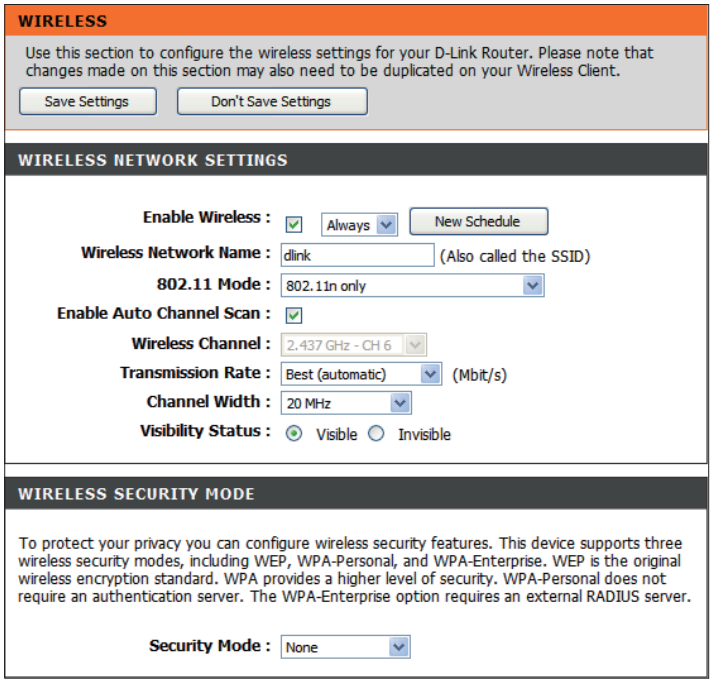
**DNS Servers:** The DNS server information will be supplied by your ISP (Internet Service Provider.)

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

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



# Wireless Settings




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

**Schedule:** The schedule of time when the wireless settings rules 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.

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

**Enable Auto Channel Scan:** The  setting can be selected to allow the DIR-652 to choose the channel with the least amount of interference.

**Wireless Channel:** Indicates the channel setting for the DIR-652. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

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

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

**Transmission Rate:** Select the transmit rate. It is strongly suggested to select **Best (Auto)** for best performance.

**Visibility Status:** Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-652. If Invisible is selected, the SSID of the DIR-652 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-652

# Network Settings

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

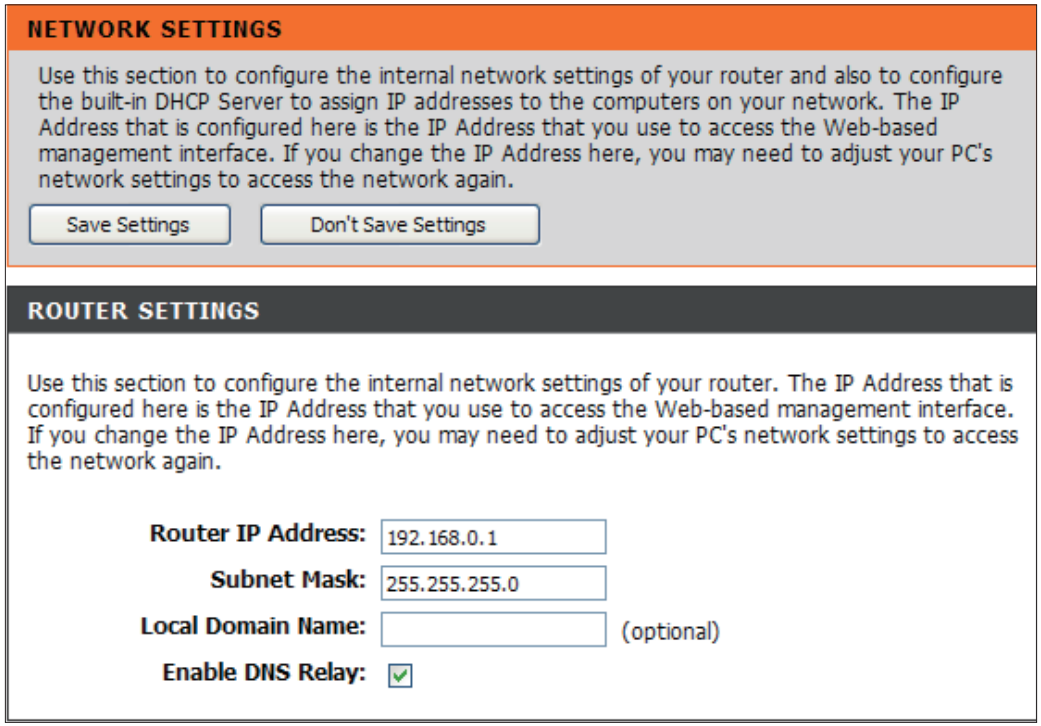
**IP Address:** Enter the IP address of the router. The default IP address is 192.168.0.1.

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

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

**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 Control Protocol. The DIR-652 has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DIR-652. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

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

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

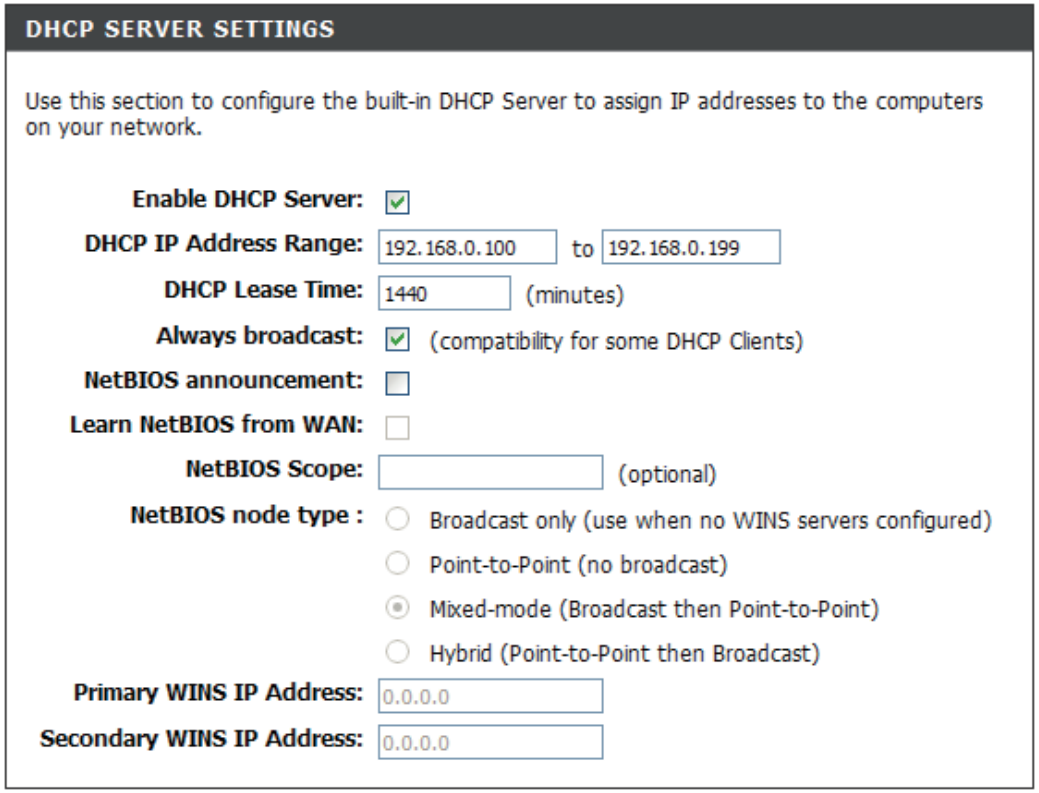
***Note:*** *If you statically (manually) assign IP addresses to your computers or devices, make sure the IP addresses are outside of this range or you may have an IP conflict.*

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

**Always Broadcast:** Enable this feature to broadcast your networks DHCP server to LAN/WLAN clients.

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

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



**NetBIOS Scope:** This feature allows the configuration of a NetBIOS ‘domain’ name under which network hosts operates. This setting has no effect if the ‘Learn NetBIOS information from WAN’ is activated.”

**NetBIOS Mode Type:** Select the different type of NetBIOS node: **Broadcast only**, **Point-to-Point**, **Mixed-mode**, and **Hybrid**.

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

# DHCP Reservation

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

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

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

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

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

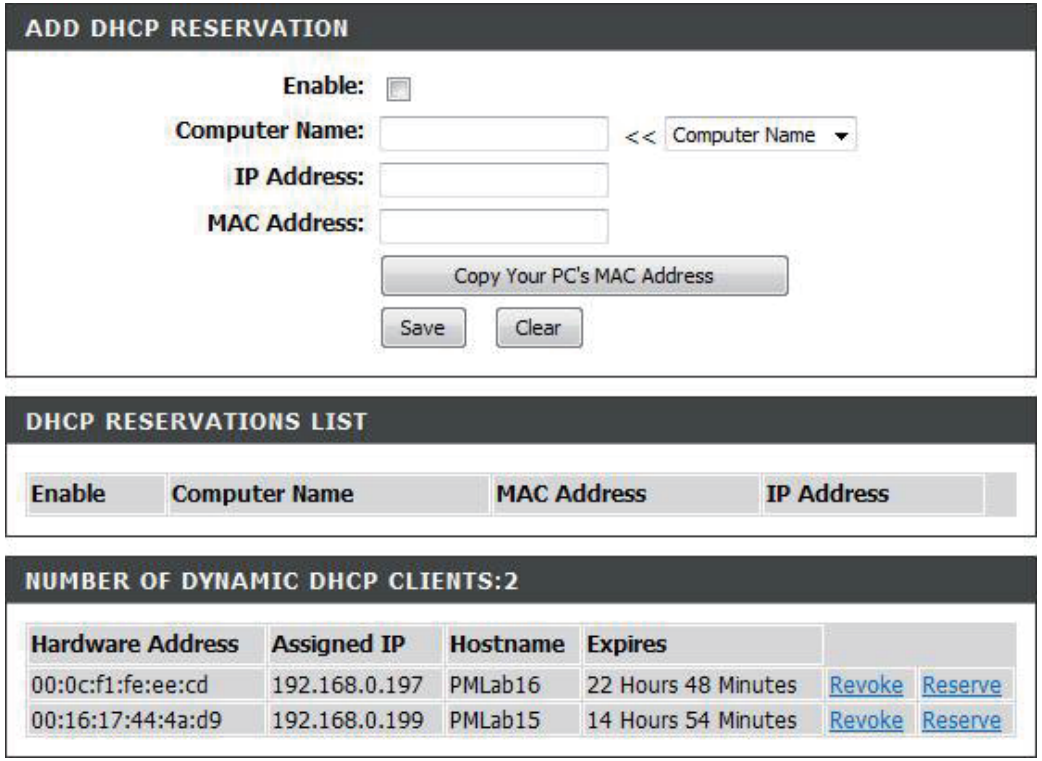
**MAC Address:** Enter the MAC address of the computer or device.

**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.

**Number of Dynamic DHCP Clients:** In this section you can see what LAN devices are currently leasing IP addresses.

**Revoke:** Click **Revoke** to cancel the lease for a specific LAN device and free an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.



***Note:*** *The Revoke option will not disconnect a PC with a current network session from the network; you would need to use MAC Address Filter to do that. Revoke will only free up a DHCP Address for the very next requester. If the previous owner is still available, those two devices may both receive an IP Address Conflict error, or the second device may still not receive an IP Address; in that case, you may still need to extend the "DHCP IP Address Range" to address the issue, it is located in the DHCP Server section.*

**Reserve:** The Reserve option converts this dynamic IP allocation into a DHCP Reservation and adds the corresponding entry to the DHCP Reservations List.

# Virtual Server

The DIR-652 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DIR-652 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-652 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-652 redirects the external service request to the appropriate server within the LAN network.

The DIR-652 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

For a list of ports for common applications, please visit **http://support.dlink.com/faq/view.asp?prod_id=1191**.

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

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

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), 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 open next to Private Port and Public Port. The private and public ports are usually the same. The public port is the port seen from the Internet side, and the private port is the port being used by the application on the computer within your local network.

**Protocol Type:** Select **TCP**, **UDP**, or **Both** or 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.

**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.

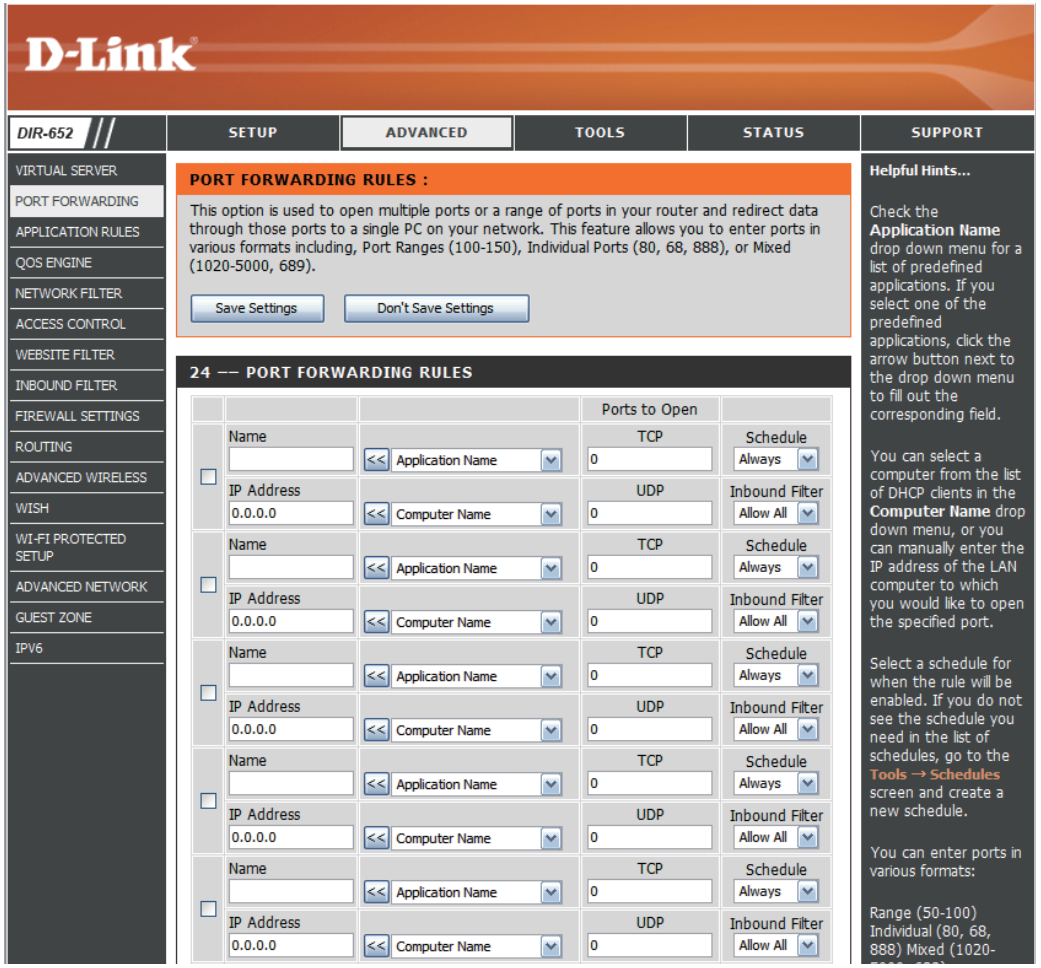
**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click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

**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. Seperate ports with a common.

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 Applications makes some of these applications work with the DIR-652. 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-652 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 **<<**.

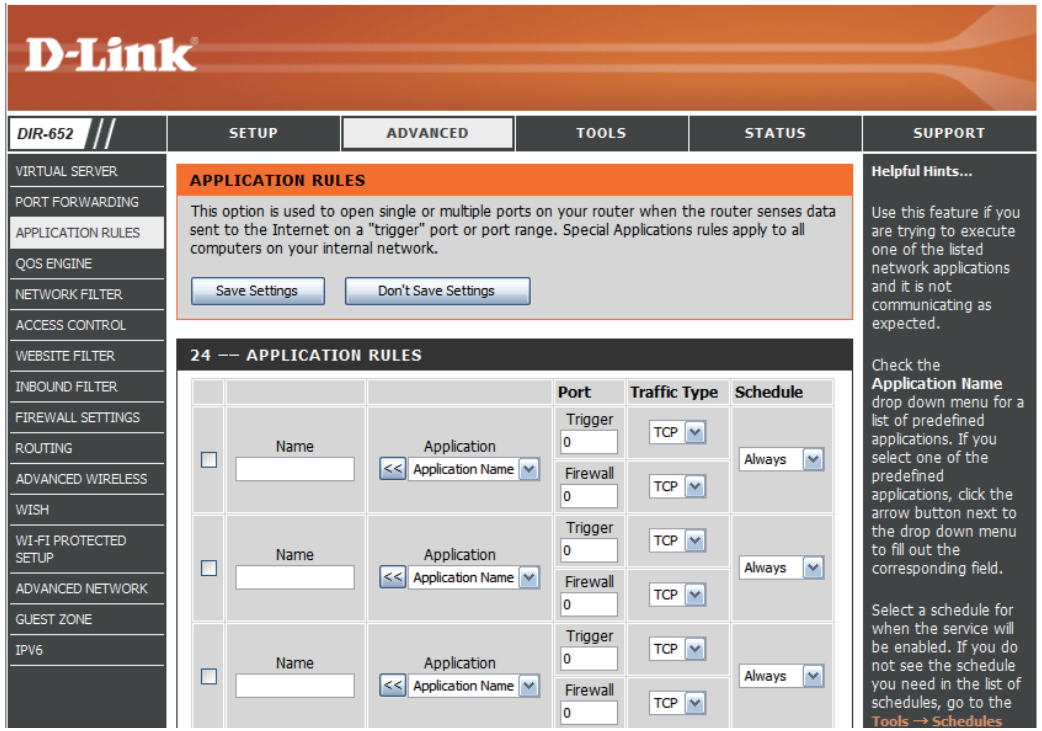
**Trigger:** This is the port used to trigger the application. It can be either a single port or a range of ports.

**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 gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.

**Enable Traffic Shaping:** 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:** This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

**Measured Uplink Speed:** This displays the detected uplink speed.

**Manual Uplink Speed:** The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.

**Enable QoS Engine:** 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 Classification:** This option is enabled by default. This will allow your router to automatically determine the network priority of running programs.

**Dynamic Fragmentation:** This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones.

# 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.

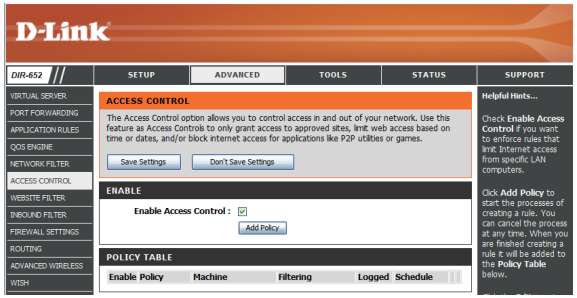
**MAC Address:** Enter the MAC address you would like to filter. To find the MAC address on a computer, please refer to the Networking Basics section in this manual.

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

# Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls 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.

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

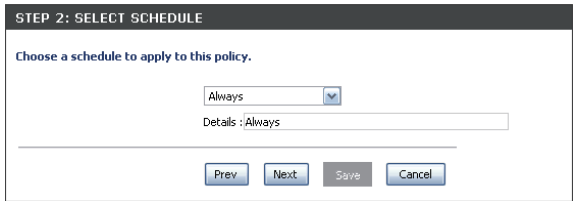



# Access Control Wizard

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

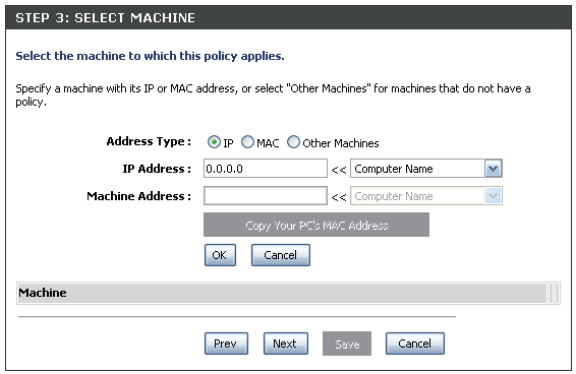
Enter a name for the policy and then click **Next** to continue.

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

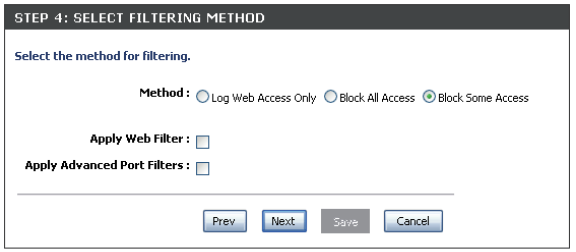



Enter the following information and then click **Next** to continue.

- **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.

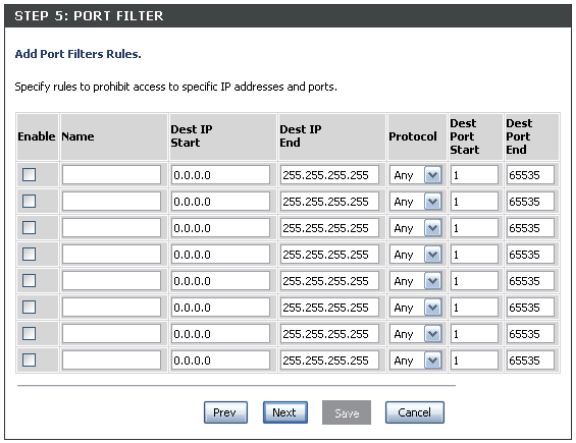


Select the filtering method and then click **Next** to continue.



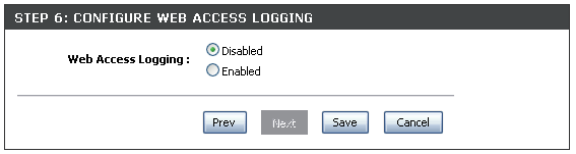

Enter the rule:

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




To enable web logging, select **Enabled**.

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



# Website Filters

Website Filters are used to deny LAN computers from accessing specific web sites by the URL or domain. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display. To use this feature, enter the text string to be blocked  and click . The text to be blocked will appear in the list. To delete the text, click **Clear the List Below**.

**Website URL/ Domain:** Enter the keywords or URLs that you want to block (or allow). Any URL with the keyword in it will be blocked.

# 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**.

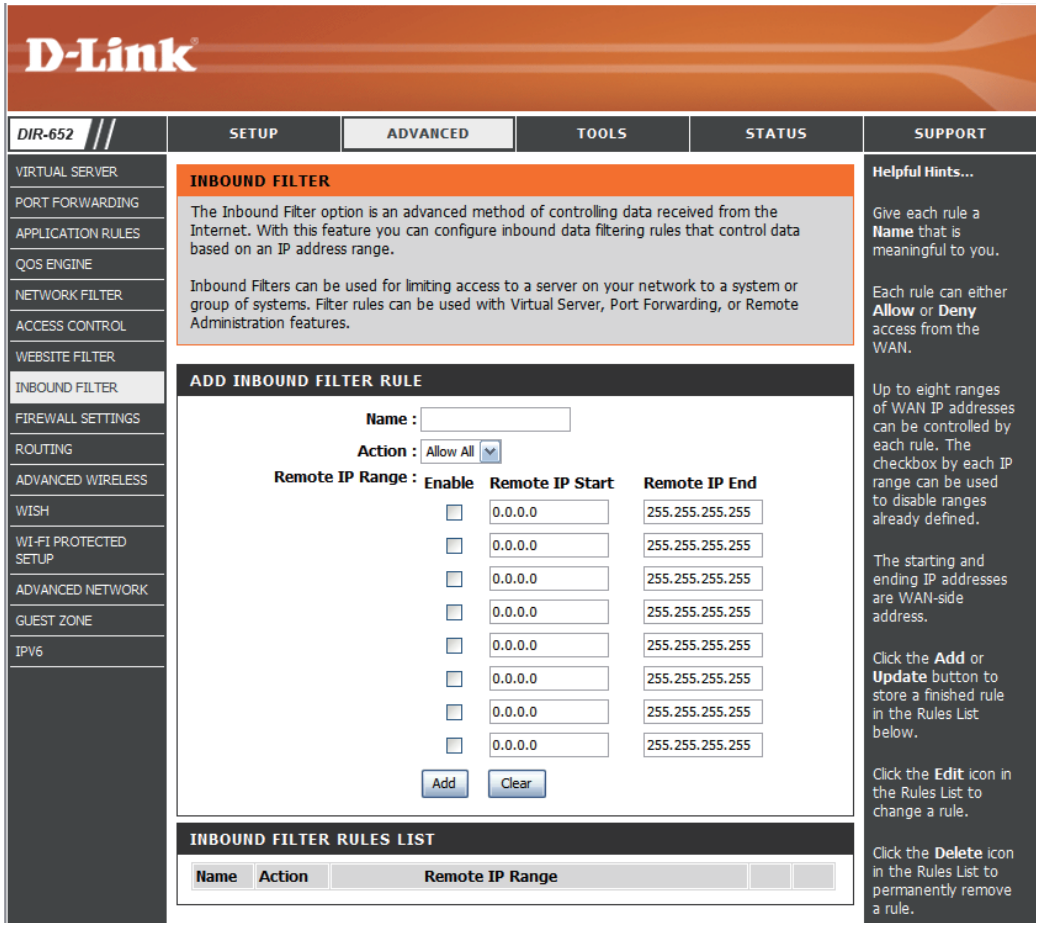
**Enable:** Check to enable rule.

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

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

**Save:** Click the **Save** 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

A firewall protects your network from the outside world. The D-Link DIR-652 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you cam enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

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

**NAT Endpoint Filtering:** Select one of the following for TCP and UDP ports:

**Endpoint Independent** - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

**Address Restricted** - Incoming traffic must match the IP address of the outgoing connection.

**Address + Port Restriction** - Incoming traffic must match the IP address and port of the outgoing connection.

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

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

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

# Routing

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

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

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

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

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

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

# Advanced Wireless Settings

**Transmit Power:** Set the transmit power of the antennas.

**Beacon Period:** Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

**RTS Threshold:** This value should remain at its default setting of 2432. If inconsistent data flow is a problem, only a minor modification should be made.

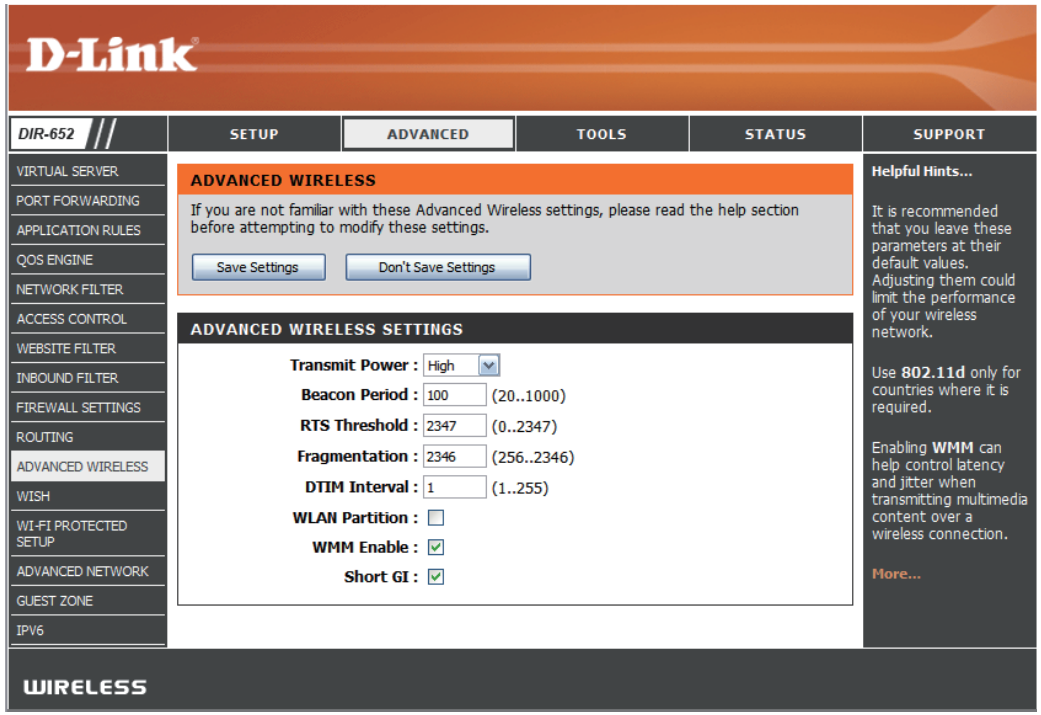
**Fragmentation:** The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

**DTIM Interval:** (Delivery Traffic Indication Message) 3 is the default setting. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages.

**WLAN Partition:** Enable this option to prevent associated wireless clients from communicating with each other.

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

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



# WISH Settings

WISH is short for Wireless Intelligent Stream Handling, a technology developed to enhance your experience of using a wireless network by prioritizing the traffic of different applications.

**Enable WISH:** Enable this option if you want to allow WISH to prioritize your traffic.

**HTTP:** Allows the router to recognize HTTP transfers for many common audio and video streams and prioritize them above other traffic. Such streams are frequently used by digital media players.

**Windows Media Center:** Enables the router to recognize certain audio and video streams generated by a Windows Media Center PC and to prioritize these above other traffic. Such streams are used by systems known as Windows Media Extenders, such as the Xbox 360.

**Automatic:** When enabled, this option causes the router to automatically attempt to prioritize traffic streams that it doesn't otherwise recognize, based on the behaviour that the streams exhibit. This acts to deprioritize streams that exhibit bulk transfer characteristics, such as file transfers, while leaving interactive traffic, such as gaming or VoIP, running at a normal priority.

**WISH Rules:** A WISH Rule identifies a specific message flow and assigns a priority to that flow. For most applications, the priority classifiers ensure the right priorities and specific WISH Rules are not required.

WISH supports overlaps between rules. If more than one rule matches for a specific message flow, the rule with the highest priority will be used.

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

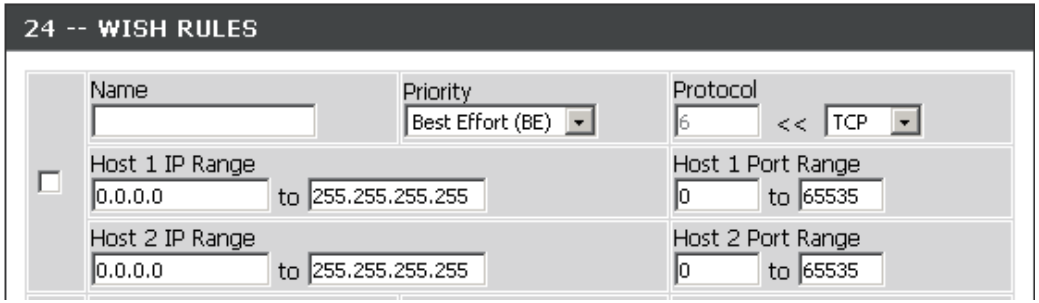
**Priority:** The priority of the message flow is entered here. The four priorities are defined as:

**BK:** Background (least urgent)
**BE:** Best Effort.
**VI:** Video
**VO:** Voice (most urgent)

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

**Host IP Range:** The rule applies to a flow of messages for which one computer's IP address falls within the range set here.

**Host Port Range:** The rule applies to a flow of messages for which host's port number is within the range set here.



# Wi-Fi Protected Setup (WPS)

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

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

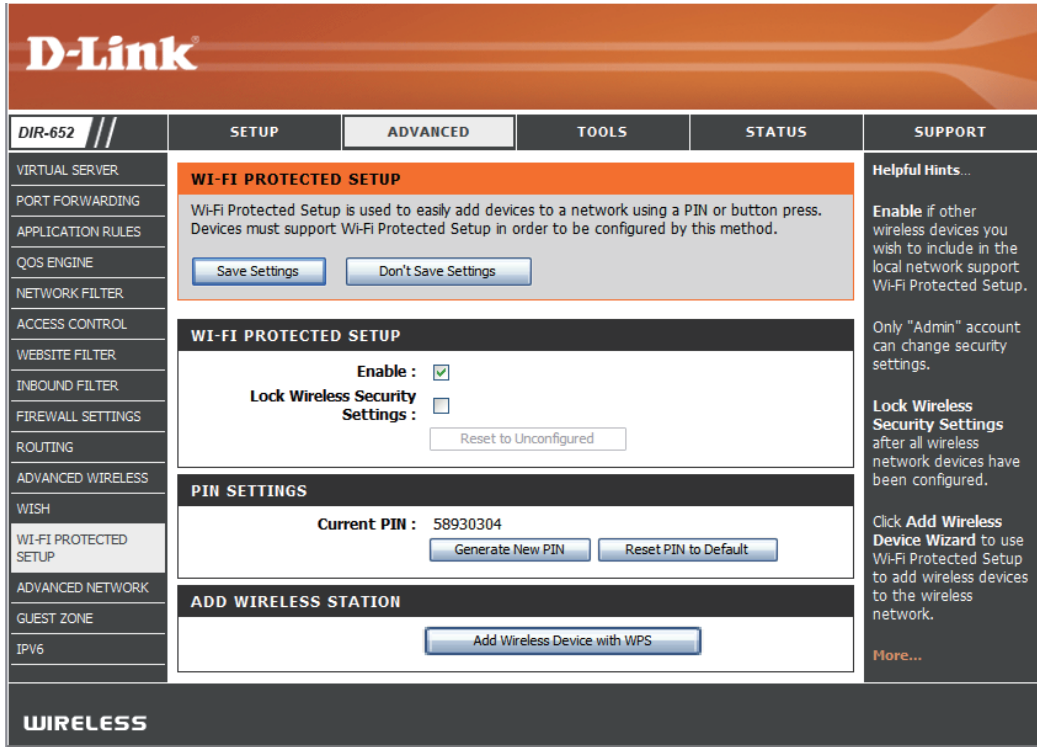
**Lock Wireless Security Settings:** Locking the wireless security settings prevents the settings from being changed by the Wi-Fi Protected Setup feature of the router. Devices can still be added to the network using Wi-Fi Protected Setup. However, the settings of the network will not change once this option is checked.

**PIN Settings:** A PIN is a unique number that can be used to add the router to an existing network or to create a new network. The default PIN may be printed on the bottom of the router. For extra security, a new PIN can be generated. You can restore the default PIN at any time. Only the Administrator (“admin” account) can change or reset the PIN.

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

**Generate New PIN:** Creates a random number that is a valid PIN. This becomes the router’s PIN. You can then use this PIN when creating a connection using the WPS-PIN method.

**Reset PIN to Default:** Restores the default PIN of the router.

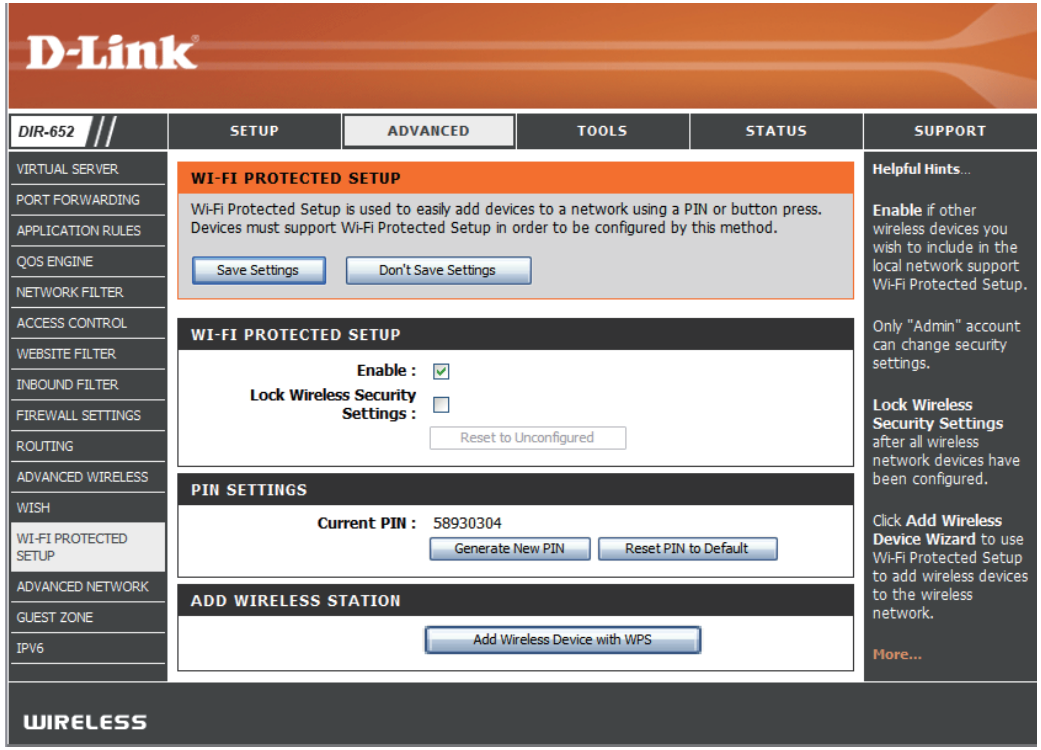


**Add Wireless Station:** This Wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the configuration button on the device. If the device supports Wi-Fi Protected Setup and has a configuration button, you can add it to the network by pressing the configuration button on the device and then the on the router within 60 seconds. The status LED on the router will flash three times if the device has been successfully added to the network.

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

**Add Wireless Device Wizard:** Start the wizard.



# Advanced Network Settings

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

**PPPoE Pass Through:** This feature enables the Router to allow a "dial-up" or separate bridged PPP connection to an individual PC. In this instance the Router will serve as a bridge.

**Internet Ping:** Unchecking the box will not allow the DIR-652 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be "pinged."

**Internet Port Speed:** You may set the port speed of the Internet port to 10Mbps, 100Mbps, 1000Mbps, or Auto 10/100/1000Mbps. Some older cable or DSL modems may require you to set the port speed to 10Mbps.

**Multicast streams:** Check the box to allow multicast traffic to pass through the router from the Internet.

# Guest Zone

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

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

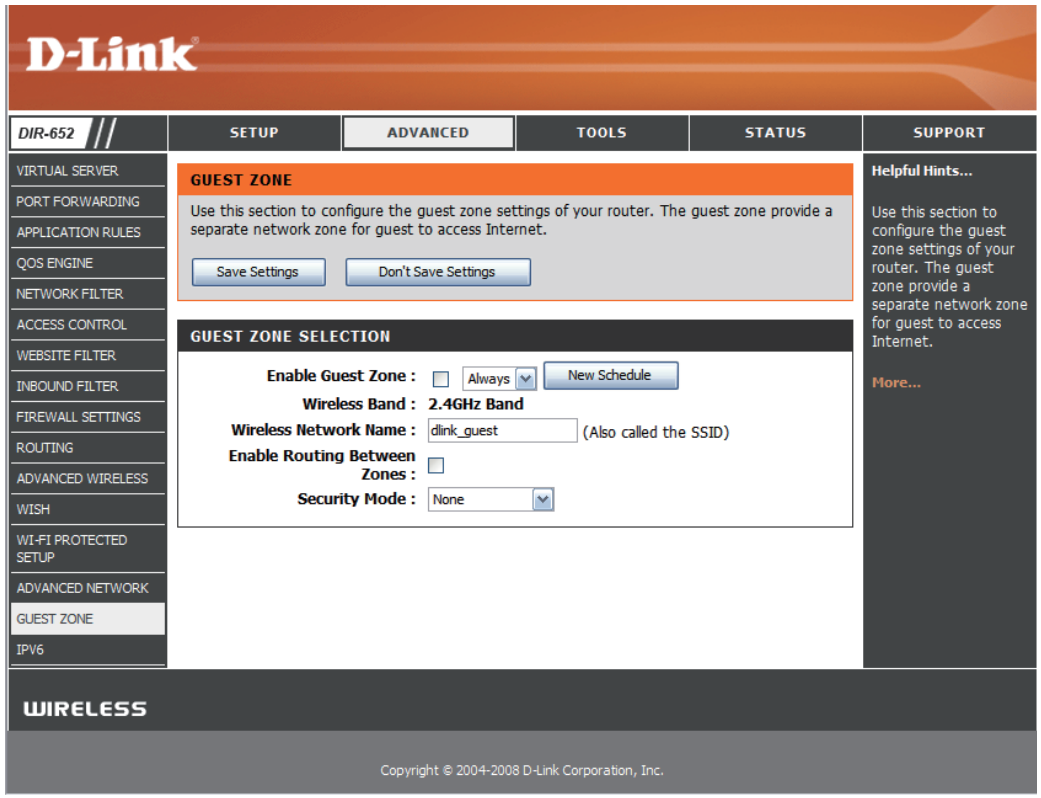
**Schedule:** The schedule of time when the Guest Zone will be active. The schedule may be set to Always, which will allow the particular service to always be enabled. You can create your own times in the section, or by clicking the **Tools** > **Schedules** button.

**Wireless Band:** This shows which wireless band will be used for the Guest Zone.

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

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

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

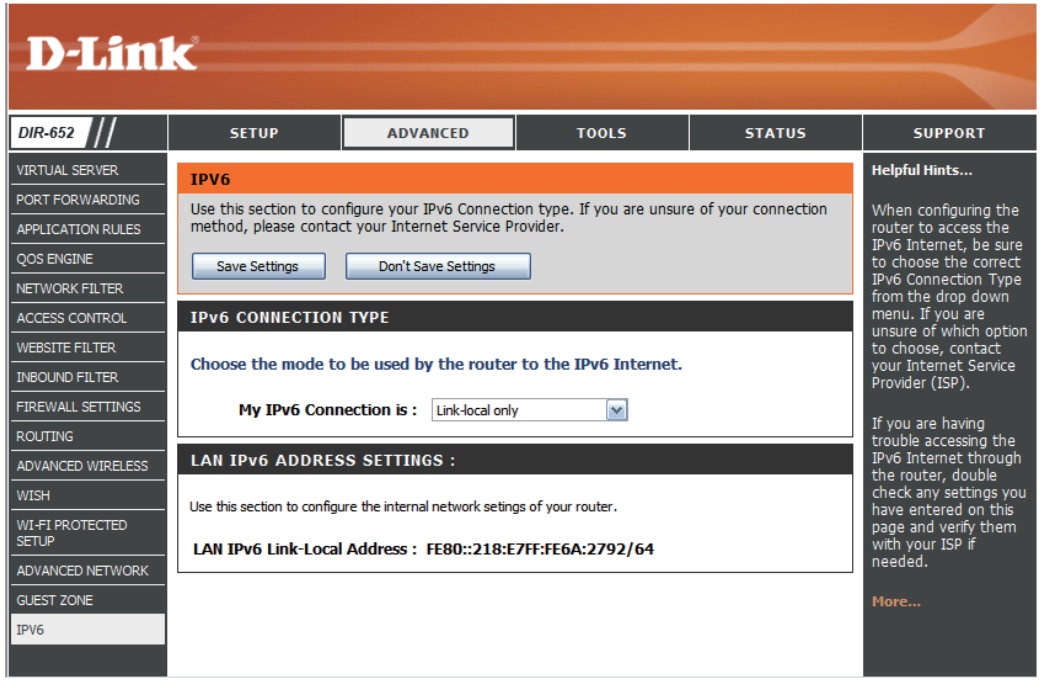


# IPV6

## 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.



# Static IPv6 (Stateful)

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

**WAN IPv6 Address Settings:** Enter the address settings supplied by your Internet provider (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.

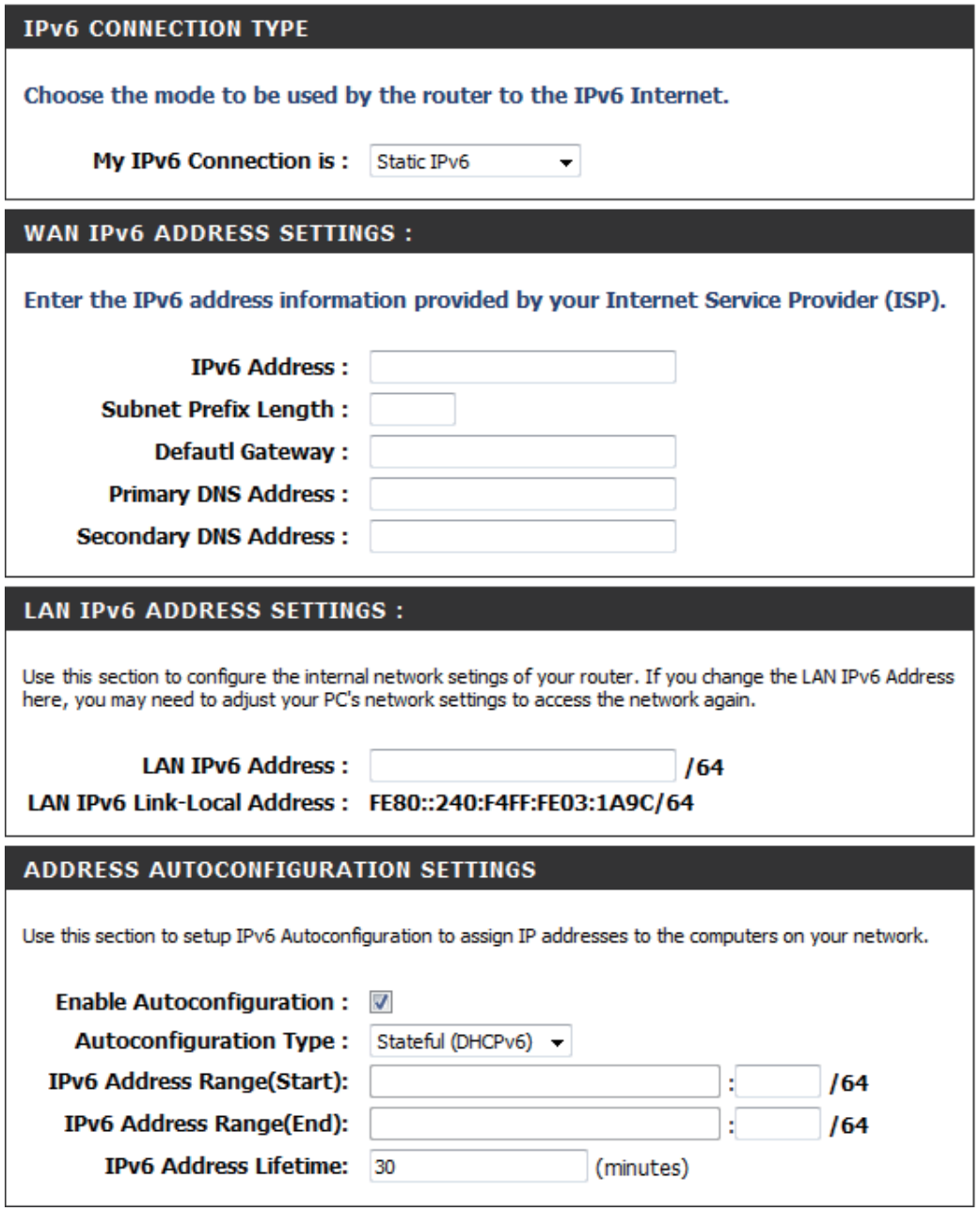
**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

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

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

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



# Static IPv6 (Stateless)

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

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

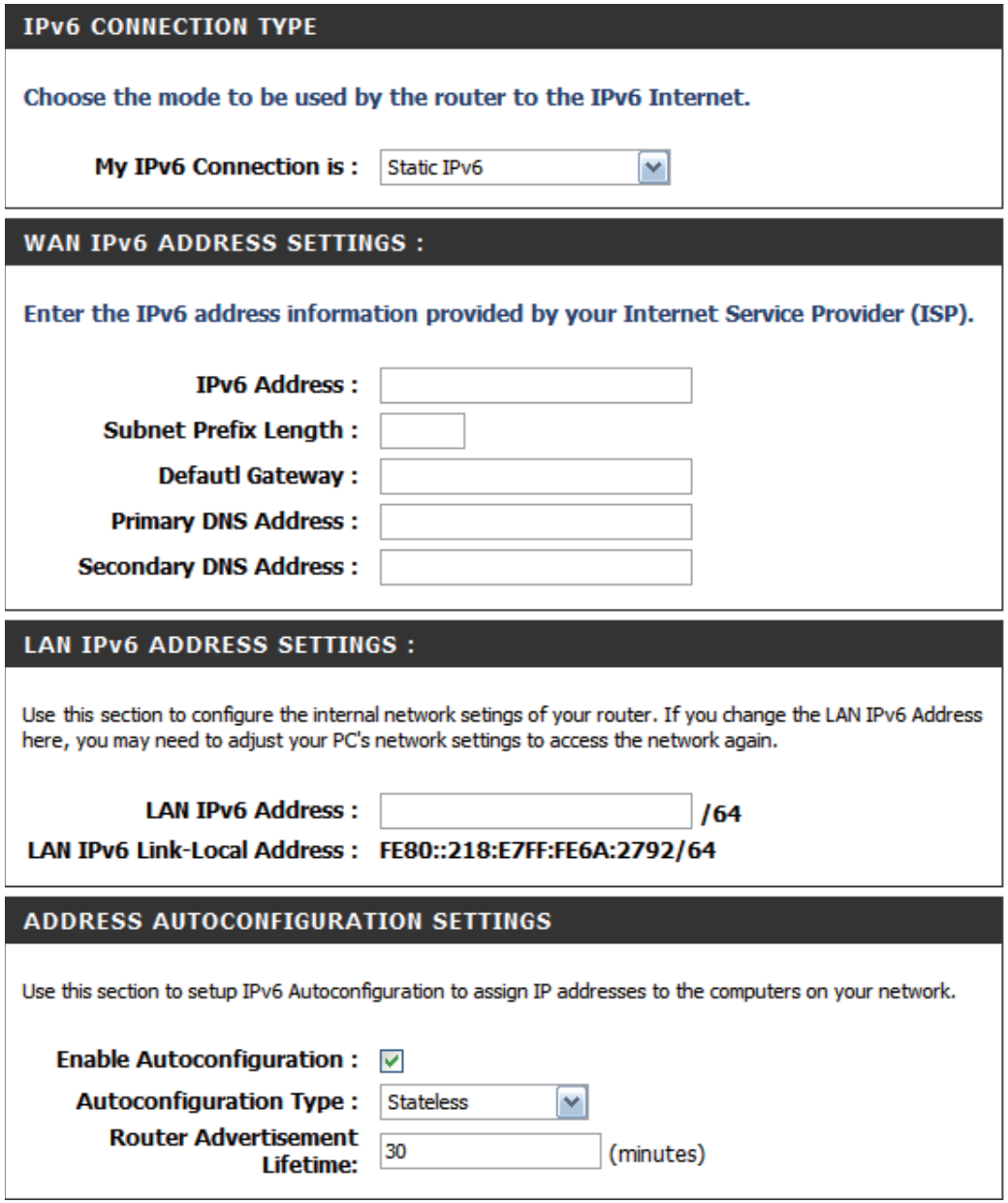
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateless**. Refer to the previous page for Stateful.

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



# DHCPv6 (Stateful)

**IPv6 Connection Type:** Select **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.

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

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

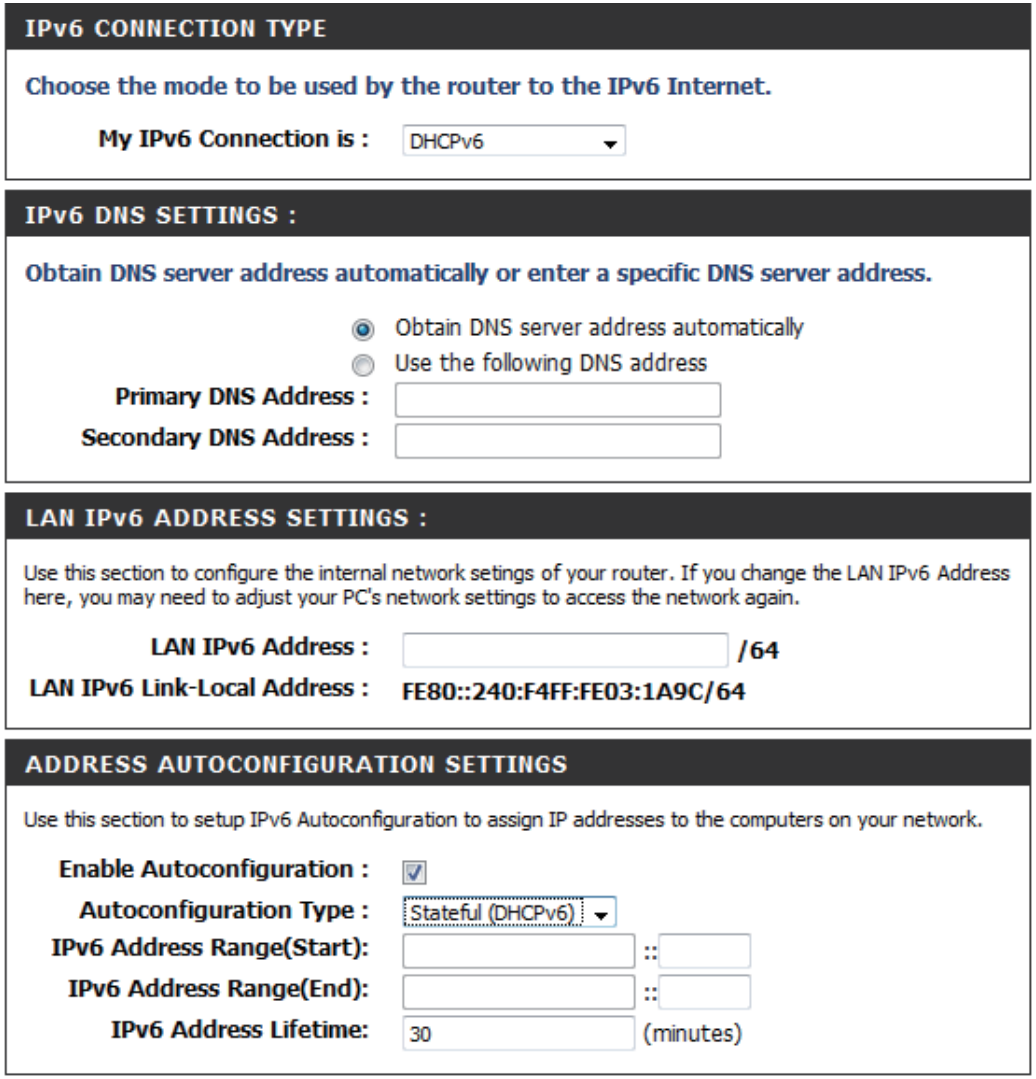
**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

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

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

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



# DHCPv6 (Stateless)

**IPv6 Connection Type:** Select **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.

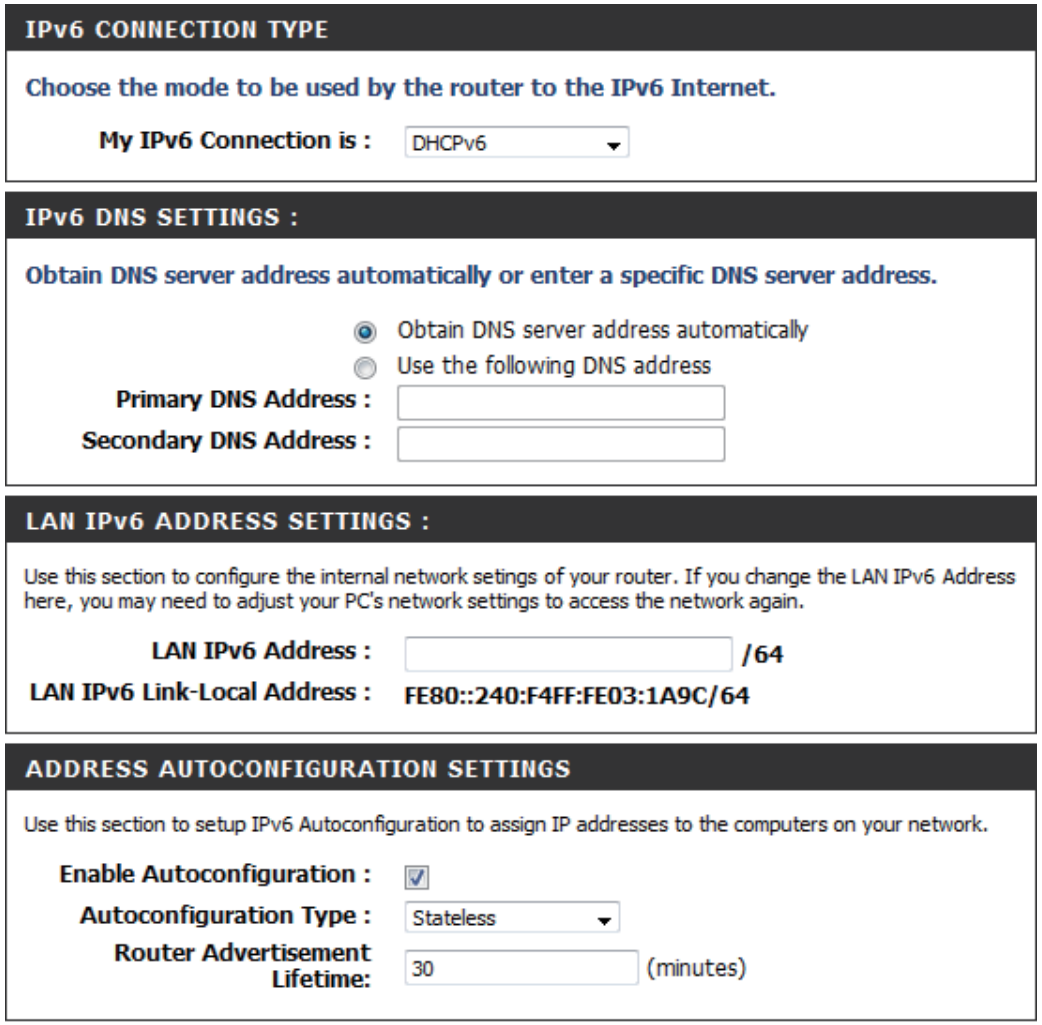
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateless**. Refer to the previous page for Stateful.

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



# IPv6 over PPPoE (Stateful)

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

**PPPoE:** 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).

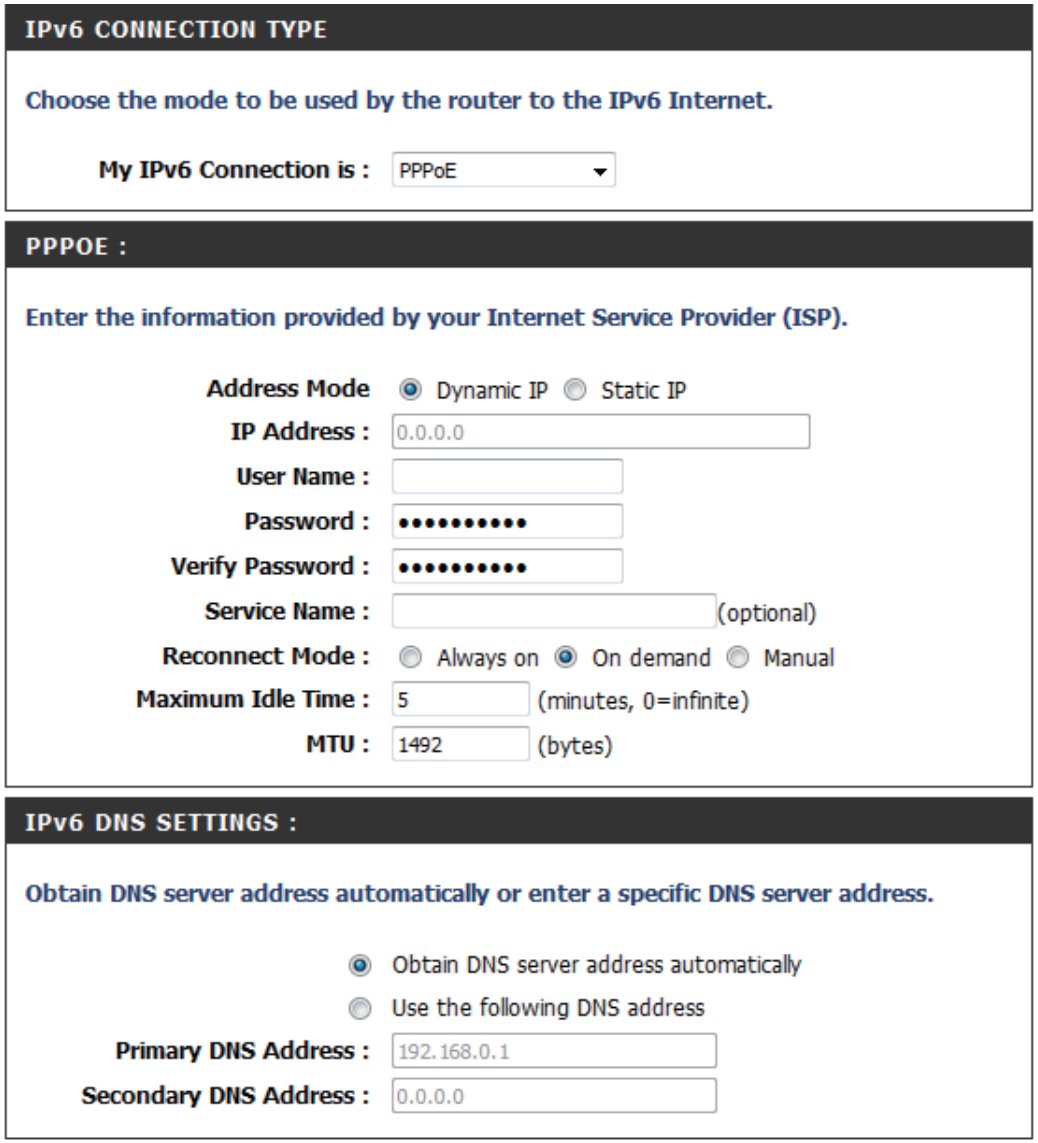
**User Name:** Enter your PPPoE user name.

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

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

**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.



**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.

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

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

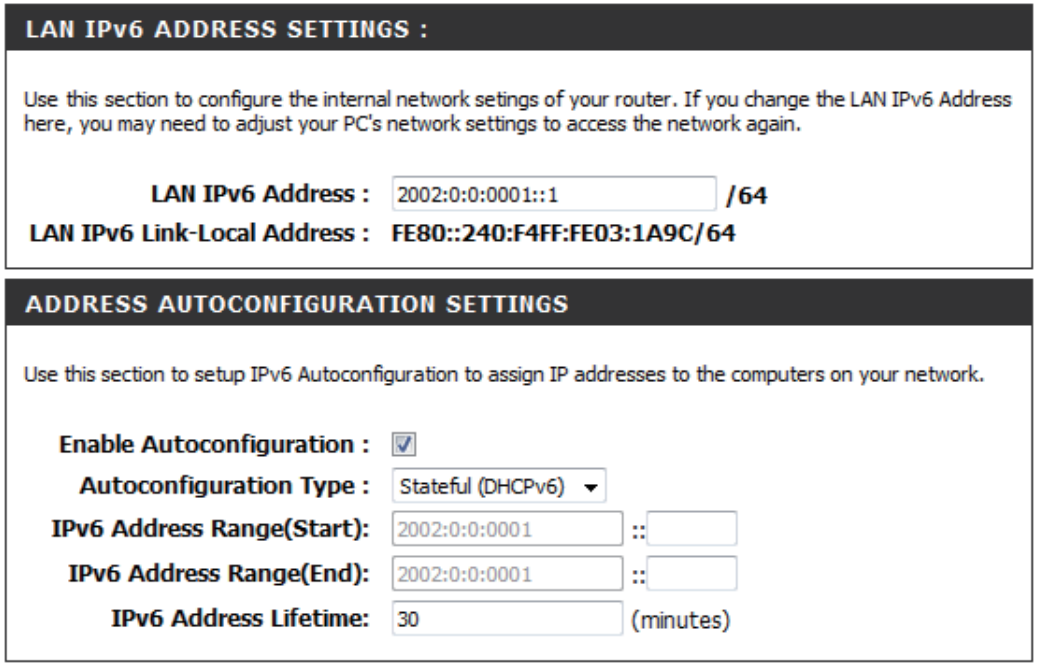
**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

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

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

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



# IPv6 over PPPoE (Stateless)

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

**PPPoE:** 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).

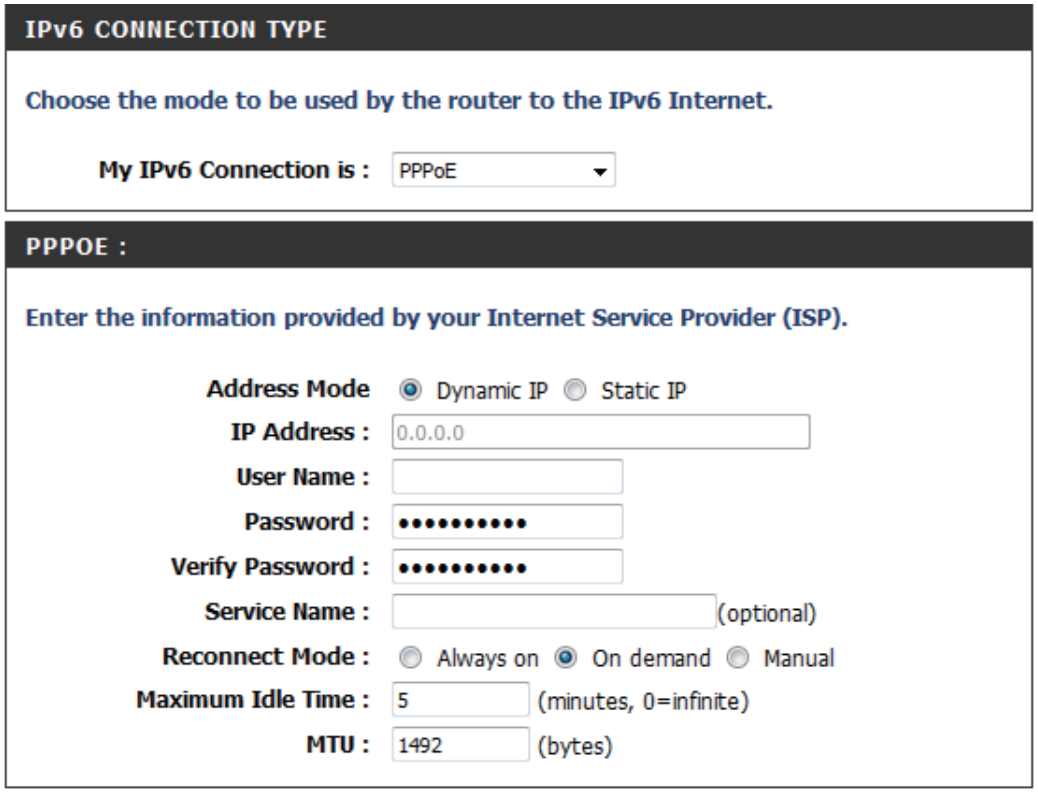
**User Name:** Enter your PPPoE user name.

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

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

**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.



**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.

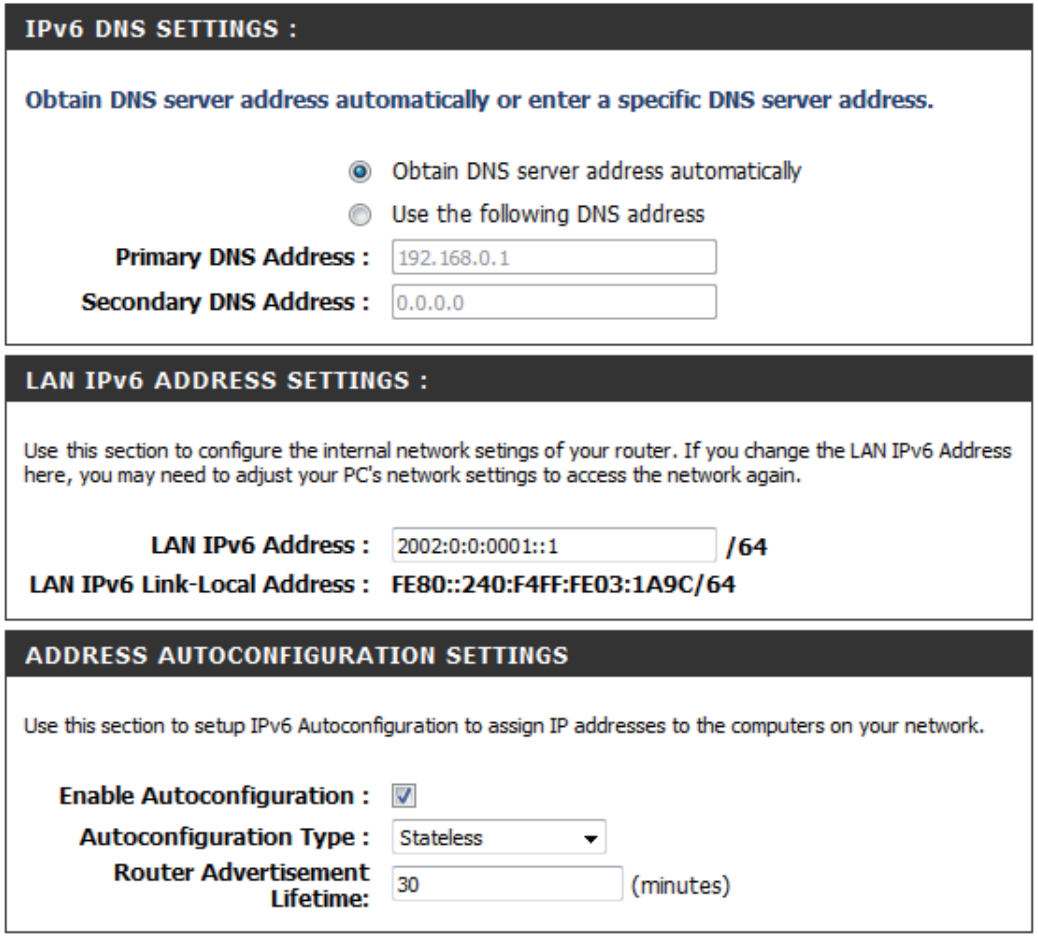
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**.

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



# 6 to 4 Tunneling (Stateful)

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

**6 to 4 Settings:** Enter the IPv6 settings supplied by your Internet provider (ISP).

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

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

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

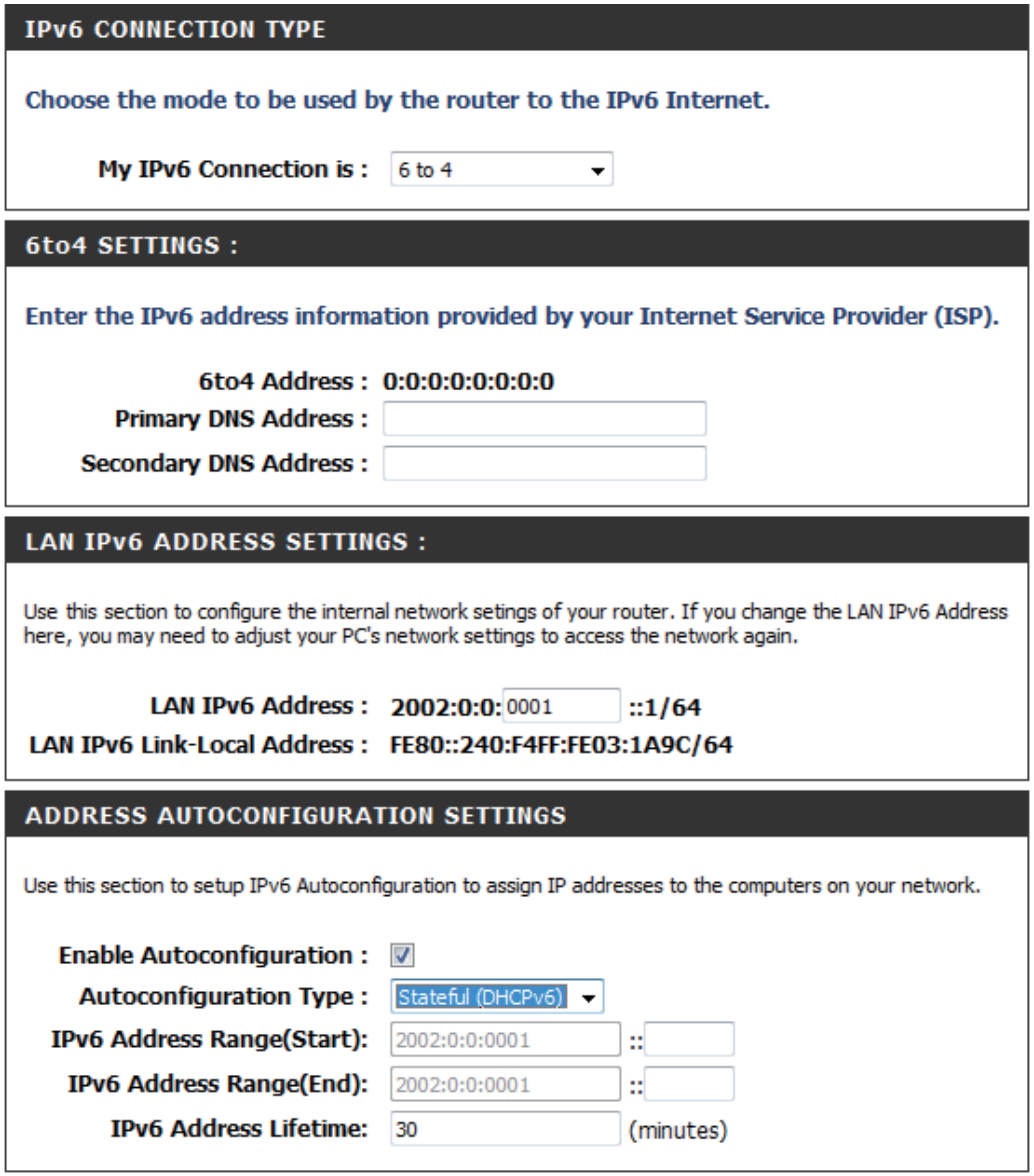
**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

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

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

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



# 6 to 4 Tunneling (Stateless)

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

**6 to 4 Settings:** Enter the IPv6 settings supplied by your Internet provider (ISP).

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

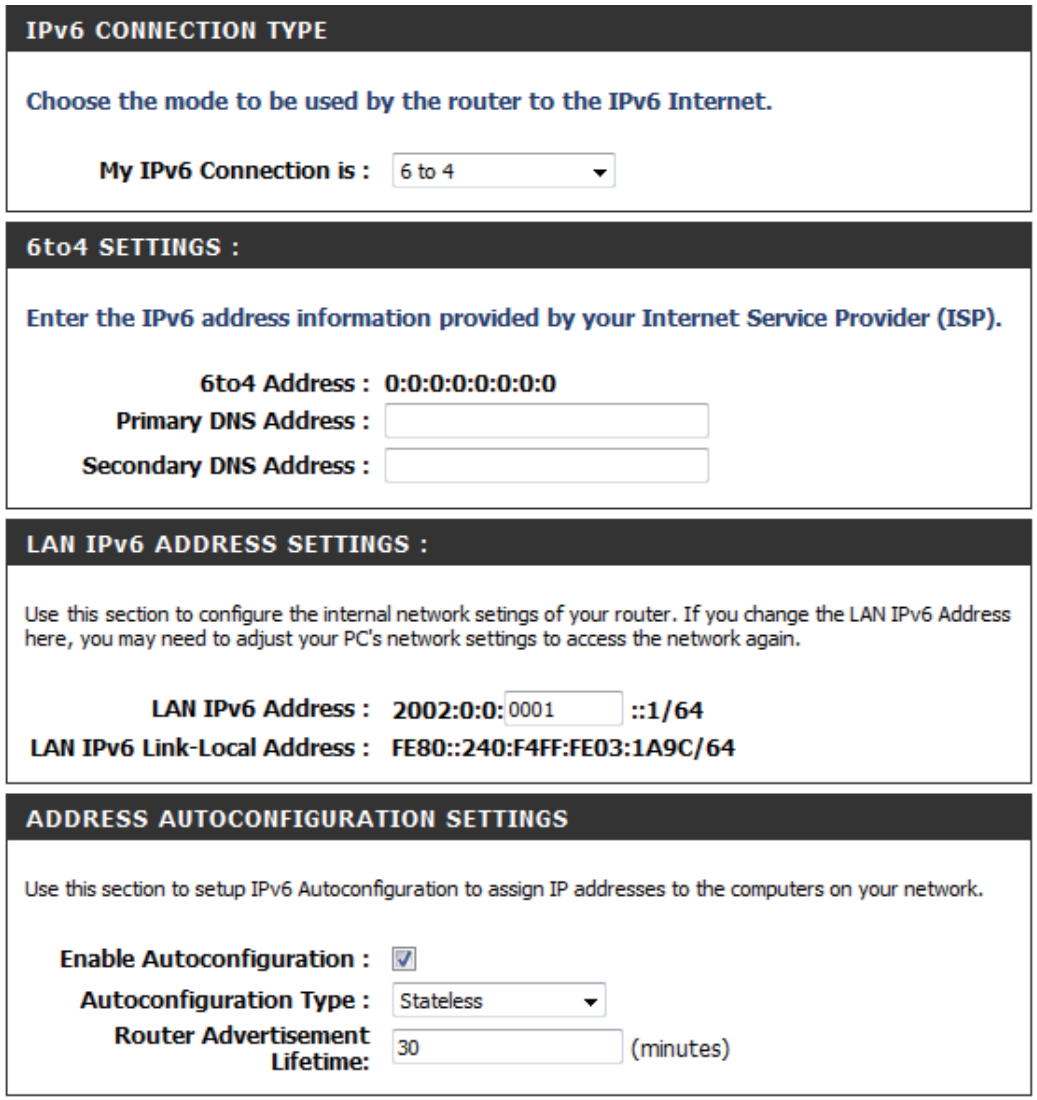
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateless**. Refer to the previous page for Stateful.

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



# IPv6 in IPv4 Tunneling (Stateful)

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

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

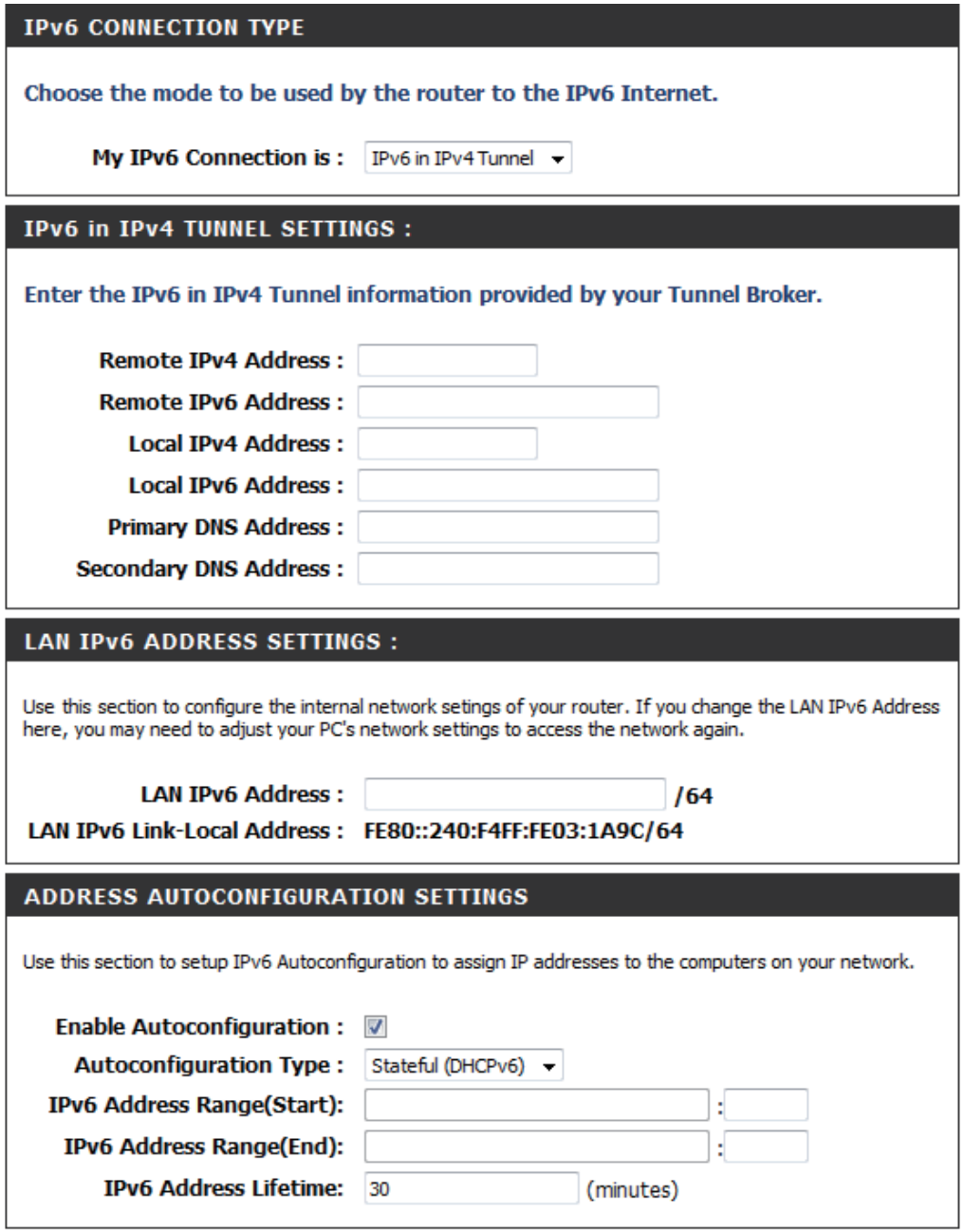
**LAN IPv6 Address:** Enter the LAN (local) IPv6 address for the router.

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

**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**. Refer to the next page for Stateless.

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



# IPv6 in IPv4 Tunneling (Stateless)

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

**IPv6 in IPv4 Tunnel Settings:** Enter the settings supplied by your Internet provider (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.

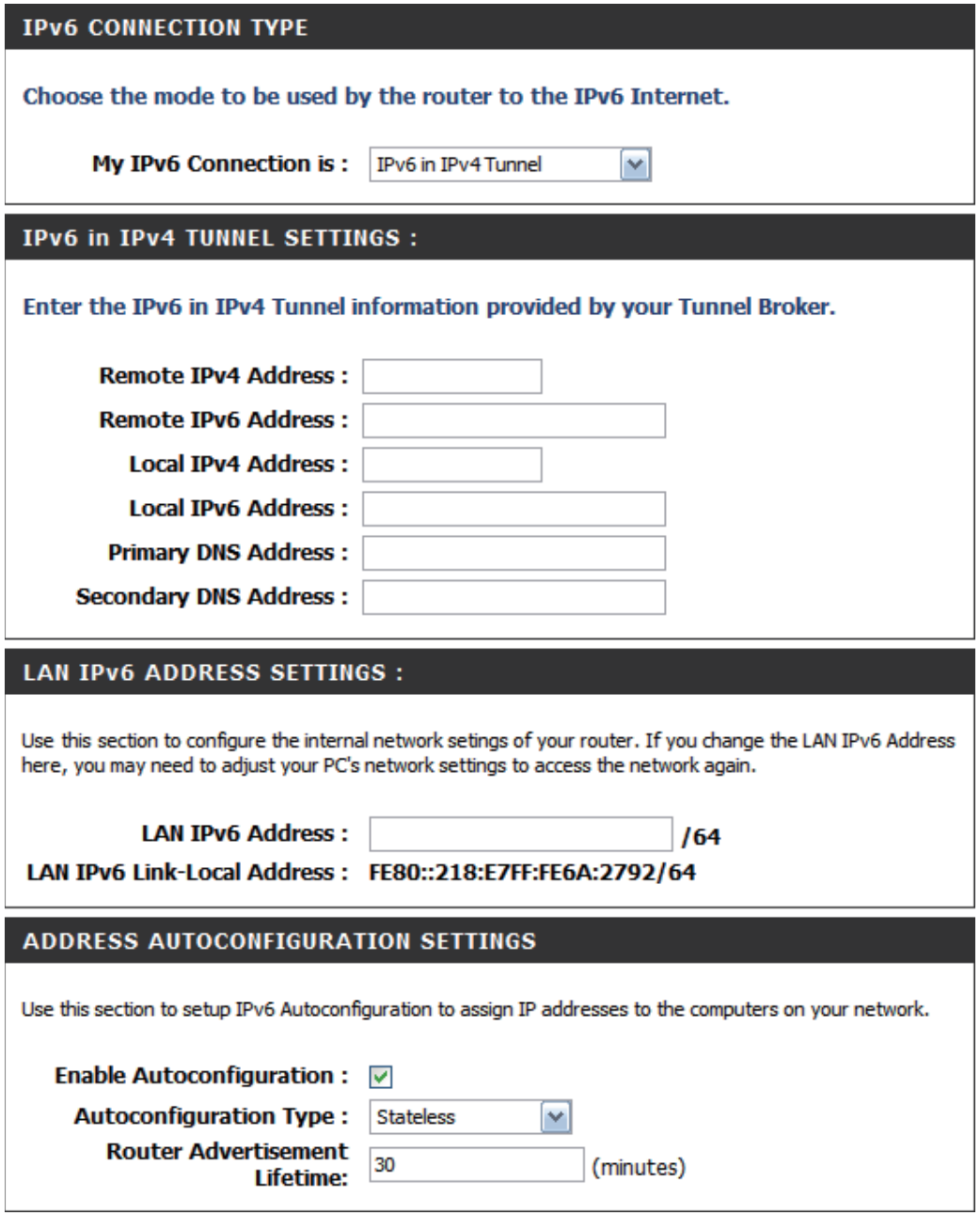
**Enable Autoconfiguration:** Check to enable the Autoconfiguration feature.

**Autoconfiguration Type:** Select **Stateful (DHCPv6)** or **Stateless**. Refer to the previous page for Stateful.

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

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

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



# Administrator Settings

This page allows you to adjust the Admin and User account settings. The Admin account can view and change settings, while the User account can only view settings and cannot make any changes. Only the admin account has the ability to change both admin and user account passwords. After making your changes, click the **Save Settings** button.

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

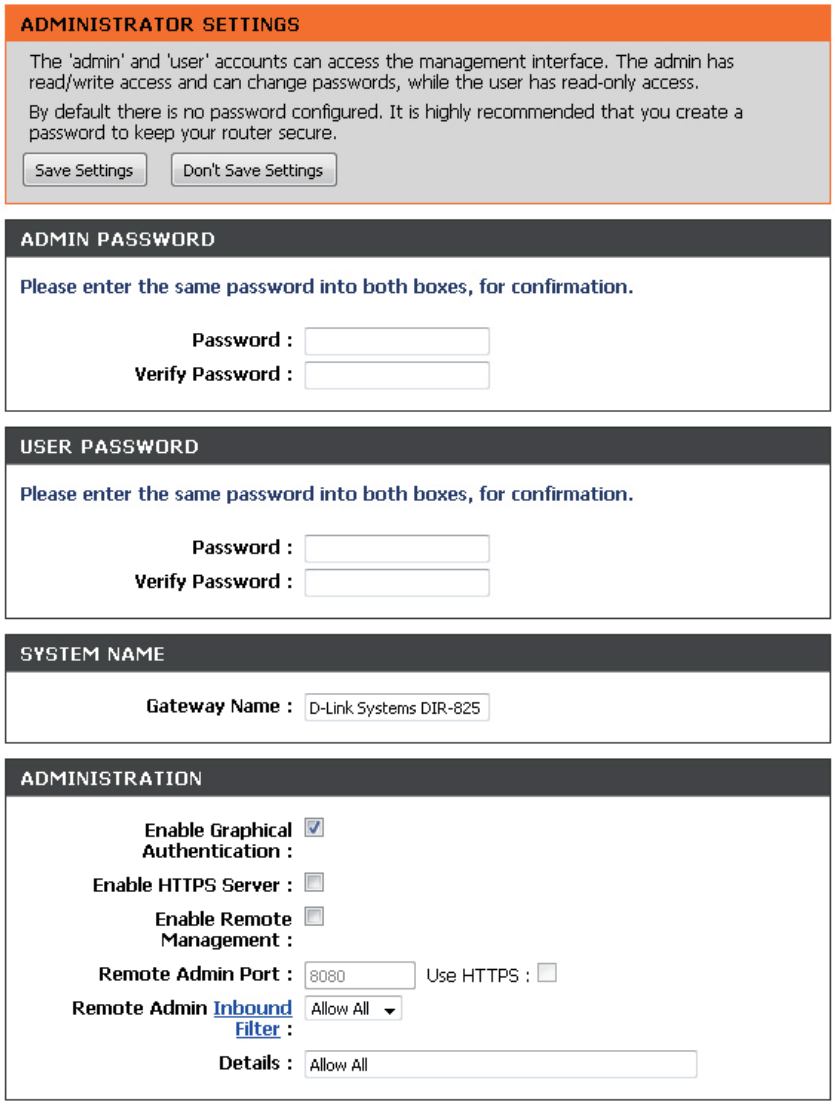
**User Password:** Enter the new password for the User login. If you login as the User, you cannot change the settings (you can only view them).

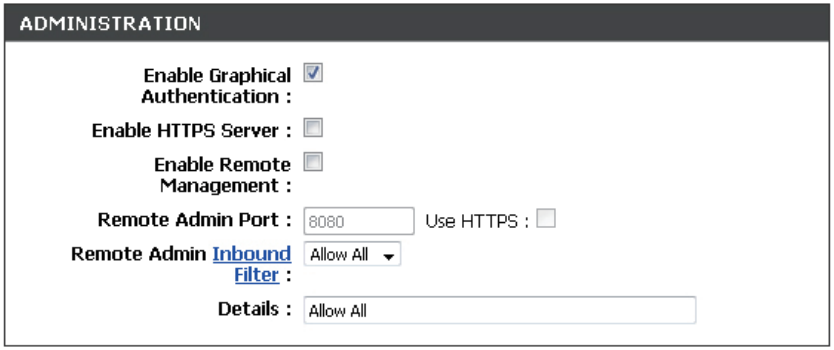
**Gateway Name:** Enter a name for the DIR-652 router.

**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.

**Enable Remote Management:** Remote management allows the DIR-652 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.






**Remote Admin Port:** The port number used to access the DIR-652.

Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DIR-652 and 8080 is the port used for the Web Management interface. If you have enabled and checked, you must enter as part of the URL to access the router remotely.

**Remote Admin Inbound Filter:** You may select “Allow All” to allow all traffic, or “Deny All” to deny all traffic. You may also specify a your own user-configured Inbound Filter. To set an Inbound Filter, simply click the Inbound Filter link and complete the instructions on that page.

**Details:** This area will display the Inbound Filter that is currently in place.

# Time Settings

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.

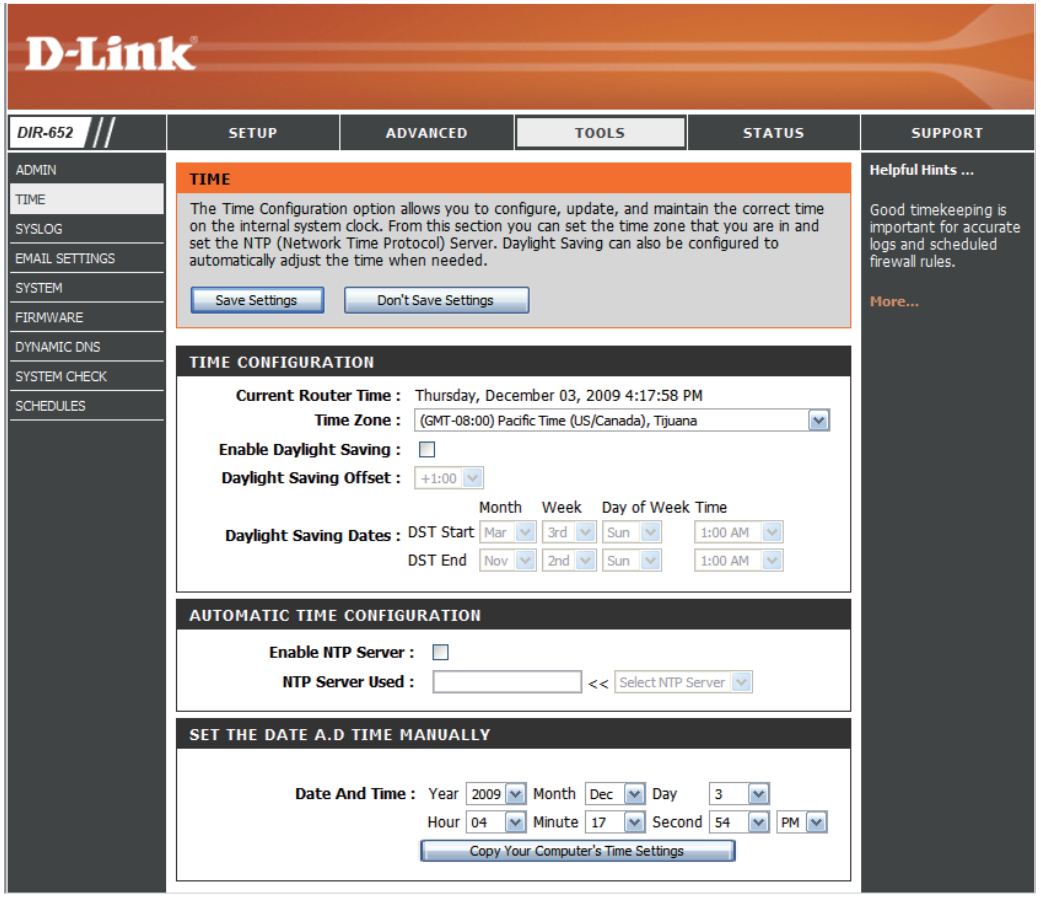
**Time Zone:** Select the Time Zone from the drop-down menu.

**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. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

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

**Manual:** To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Set Time**. You can also click **Copy Your Computer's Time Settings**.

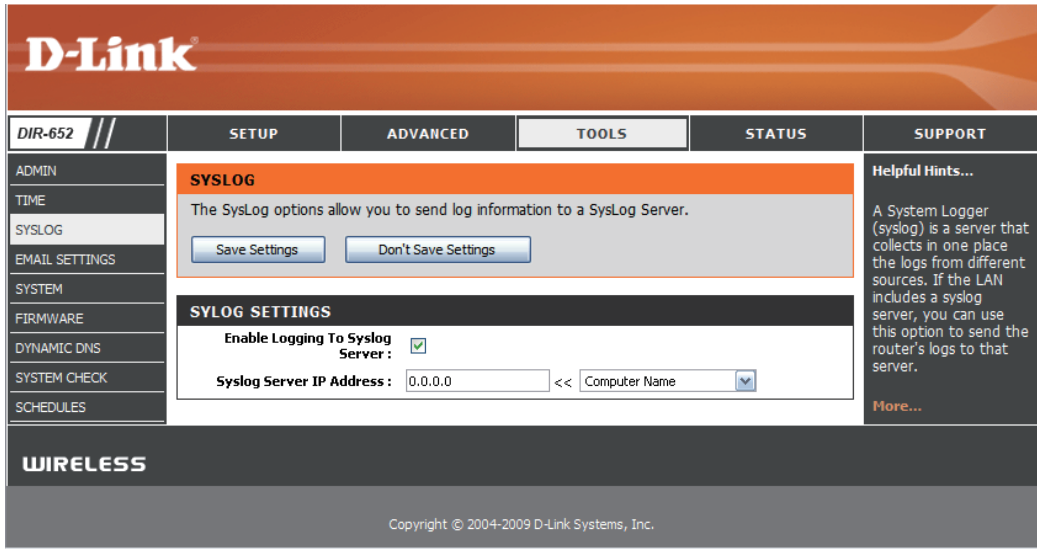


# SysLog

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

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

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



# Email Settings

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

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

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

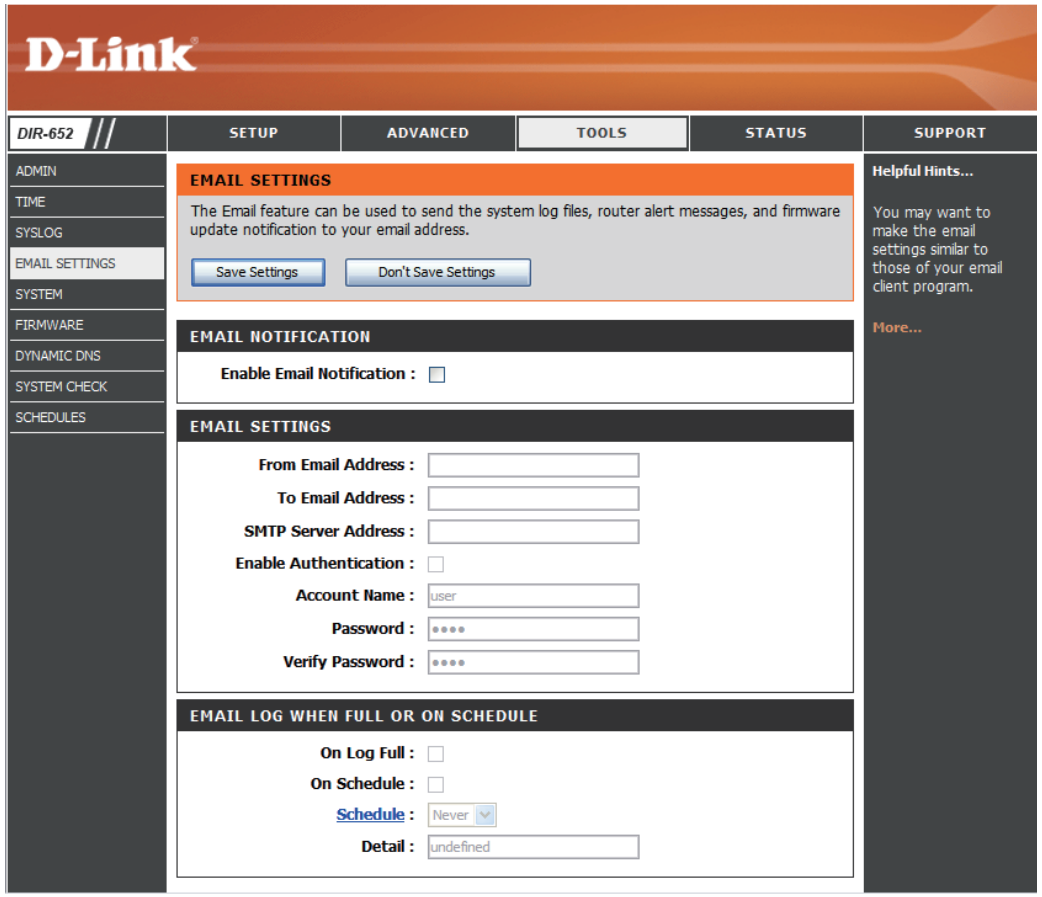
**To Email Address:** Enter the e-mail address where you want the e-mail sent.

**SMTP Server Address:** Enter the SMTP server address for sending e-mail. If your SMTP server requires authentication, select this option.

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

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

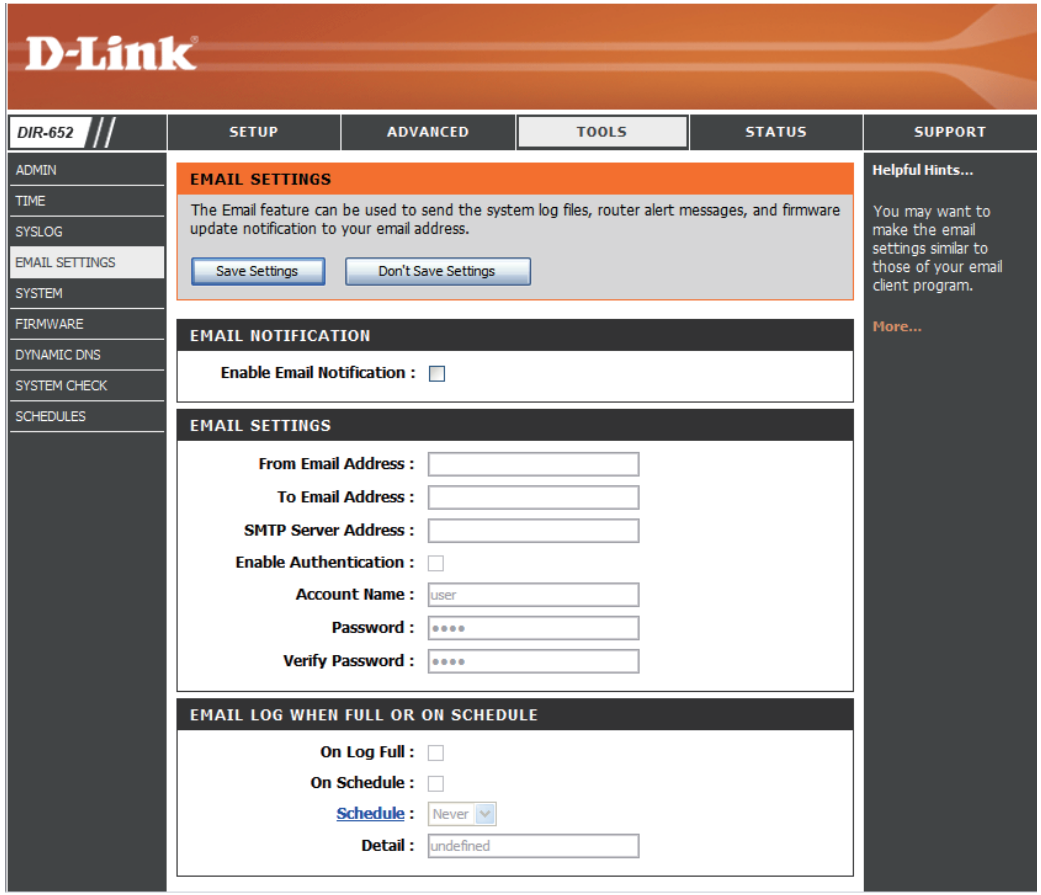
**Password:** Enter the password associated with the account. Re-type the password associated with the account.



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

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

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



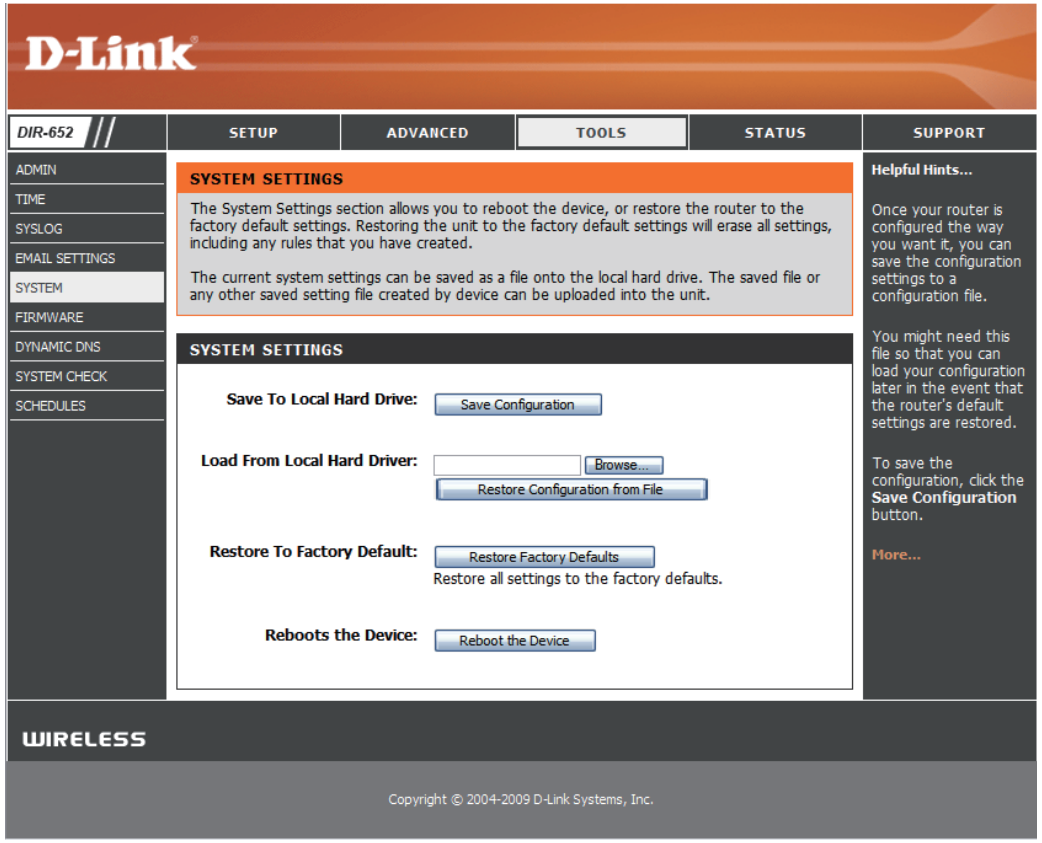
# System Settings

**Save 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. You will then see a file dialog, where you can select a location and file name for the settings.

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

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

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

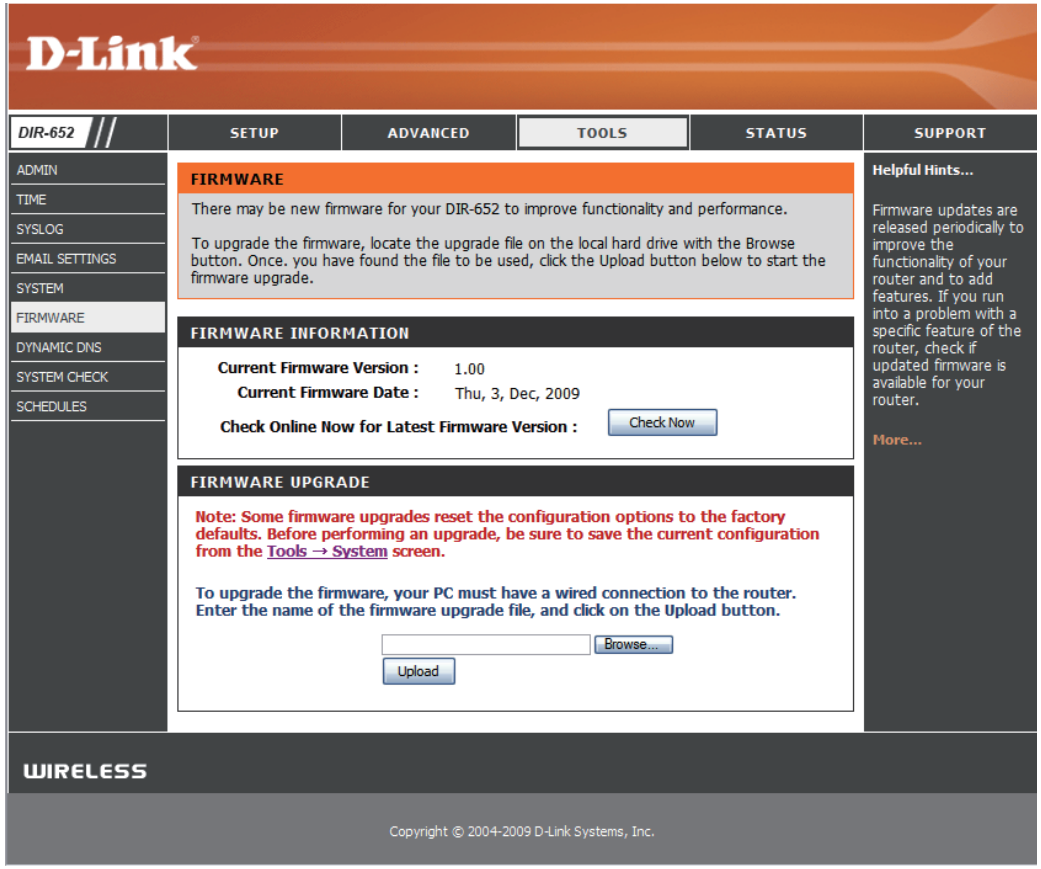


# Update Firmware

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. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

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

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



# DDNS

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

**Enable Dynamic DNS:** Check this box to enable DDNS updates.

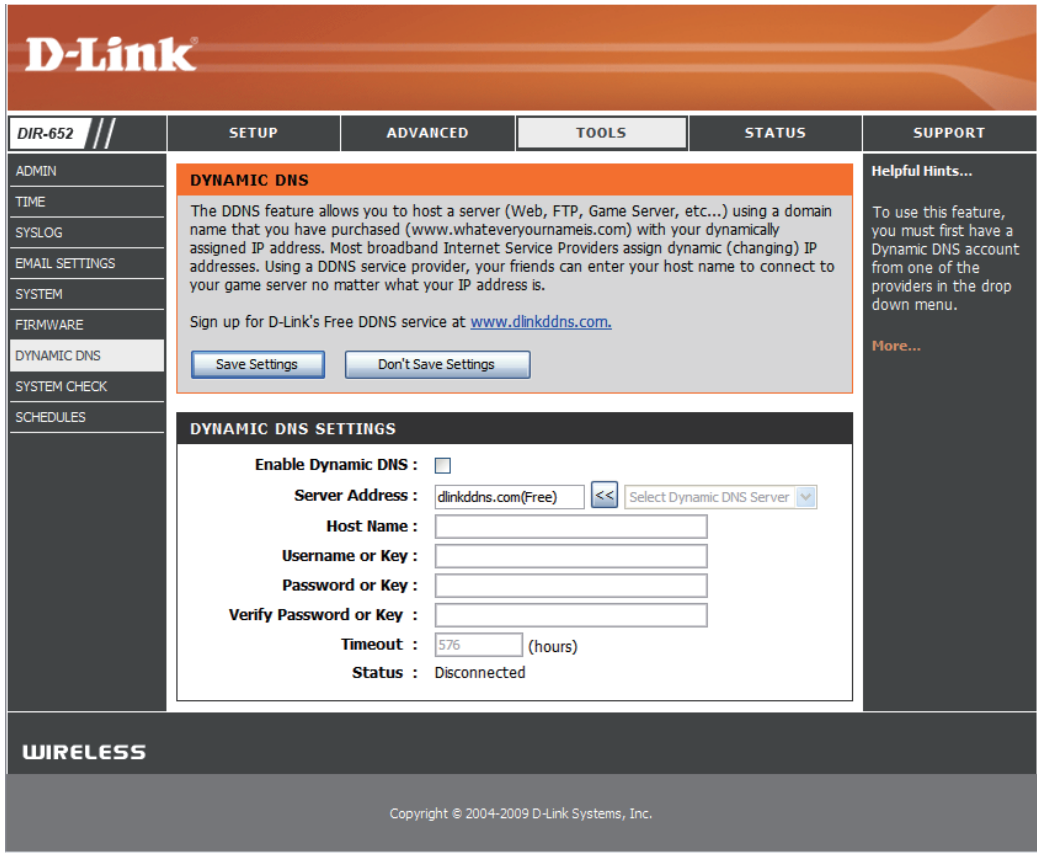
**Server Address:** Choose your DDNS provider from the drop down menu.

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

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

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

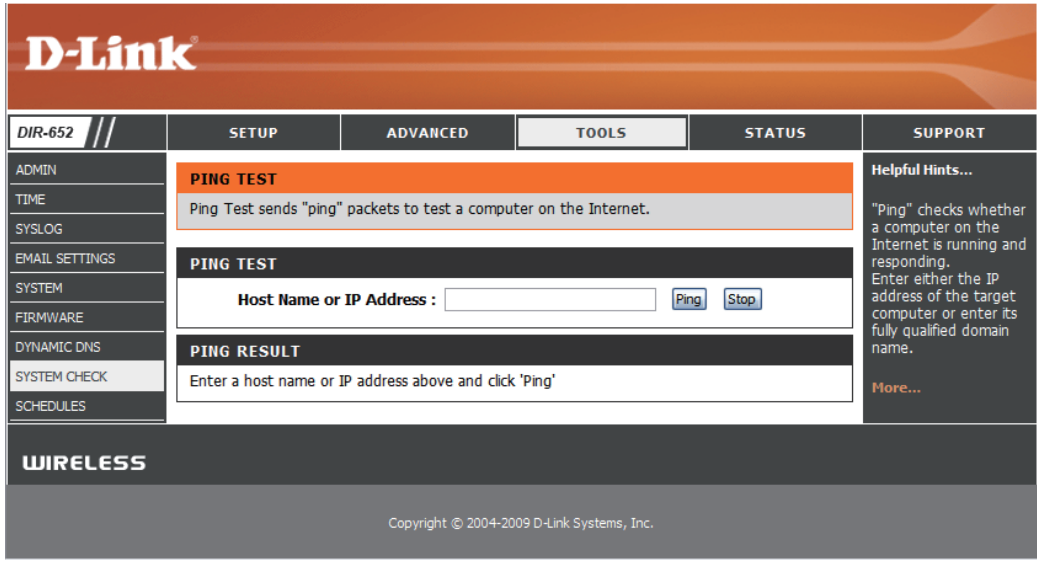
**Timeout:** Enter a time (in hours).



# System Check

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

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



# Schedules

**Name:** Enter a name for your new schedule.

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

**Time:** Enter a start and end time for your schedule, or check **All Day - 24hrs** to set the schedule to run all day (for the selected days).

**Save:** Click **Save** to save your schedule. You must click  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.

# Device Information

This page displays the current information for the DIR-652. It will display the LAN, WAN (Internet), and Wireless information.

If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

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

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

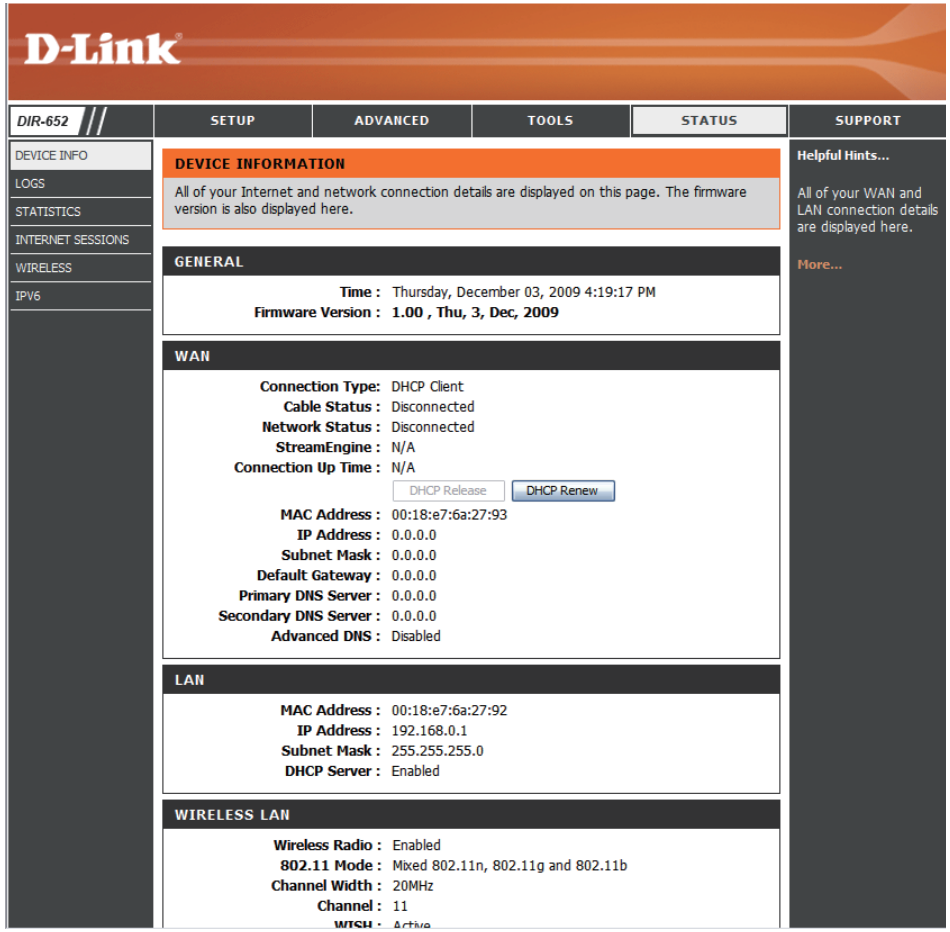
**WAN:** Displays the MAC address and the public IP settings for the router.

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

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

**LAN 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:** Displays the Multicast Group IP Address.



# Logs

The router automatically logs (records) events of 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 most recent 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 Type:** 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.

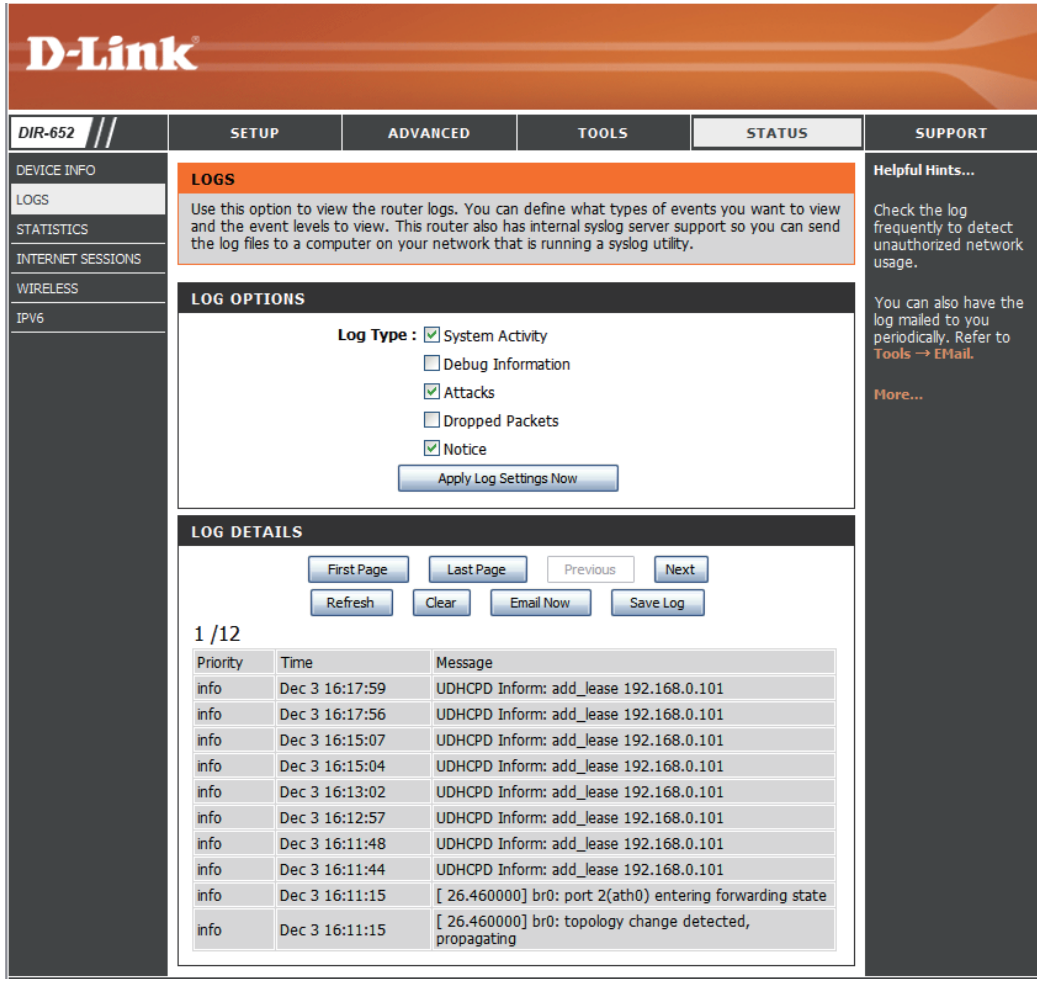
**Apply Log Settings Now:** Will filter the log results so that only the selected message types appear.

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

**Clear:** Clears all of the log contents.

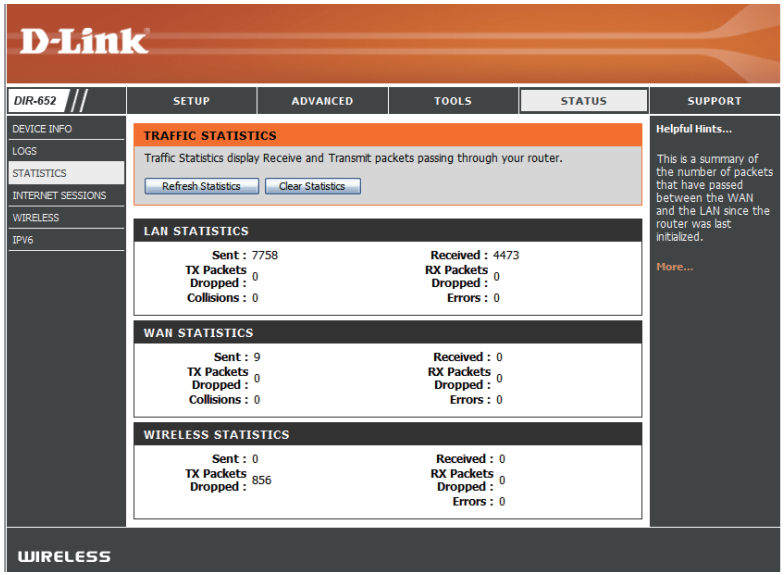
**Email Now:** This option will send a copy of the router log to the e-mail address configured in the **Tools > E-mail** screen.

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

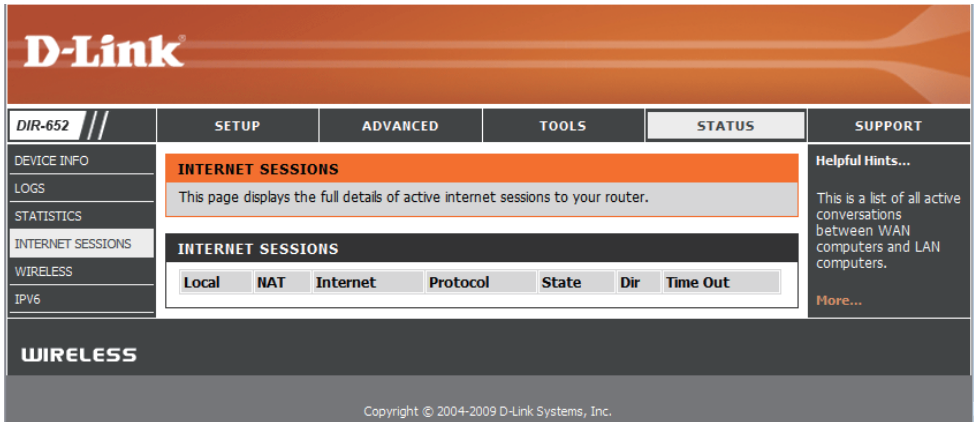


# Statistics

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-652 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.

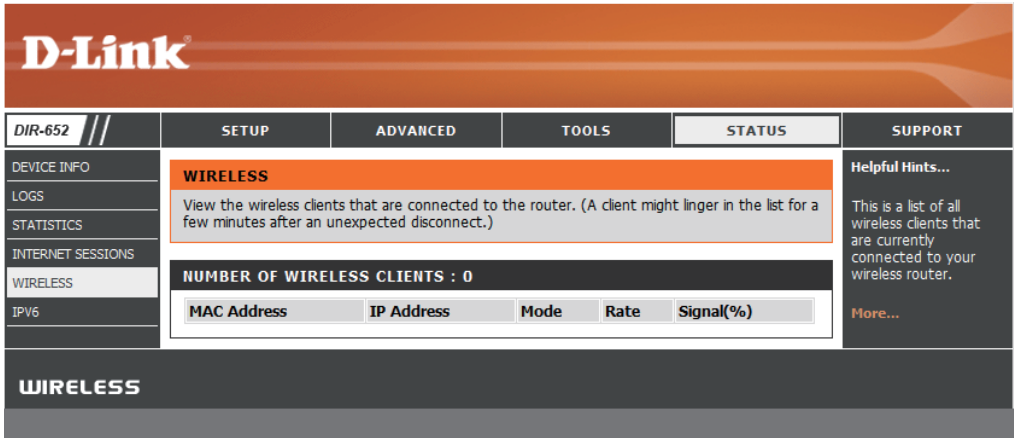



# Internet Sessions



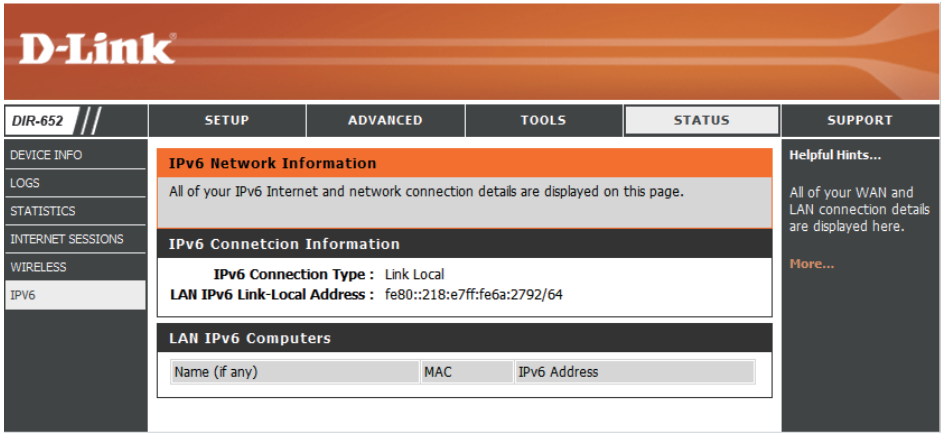
# Wireless

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

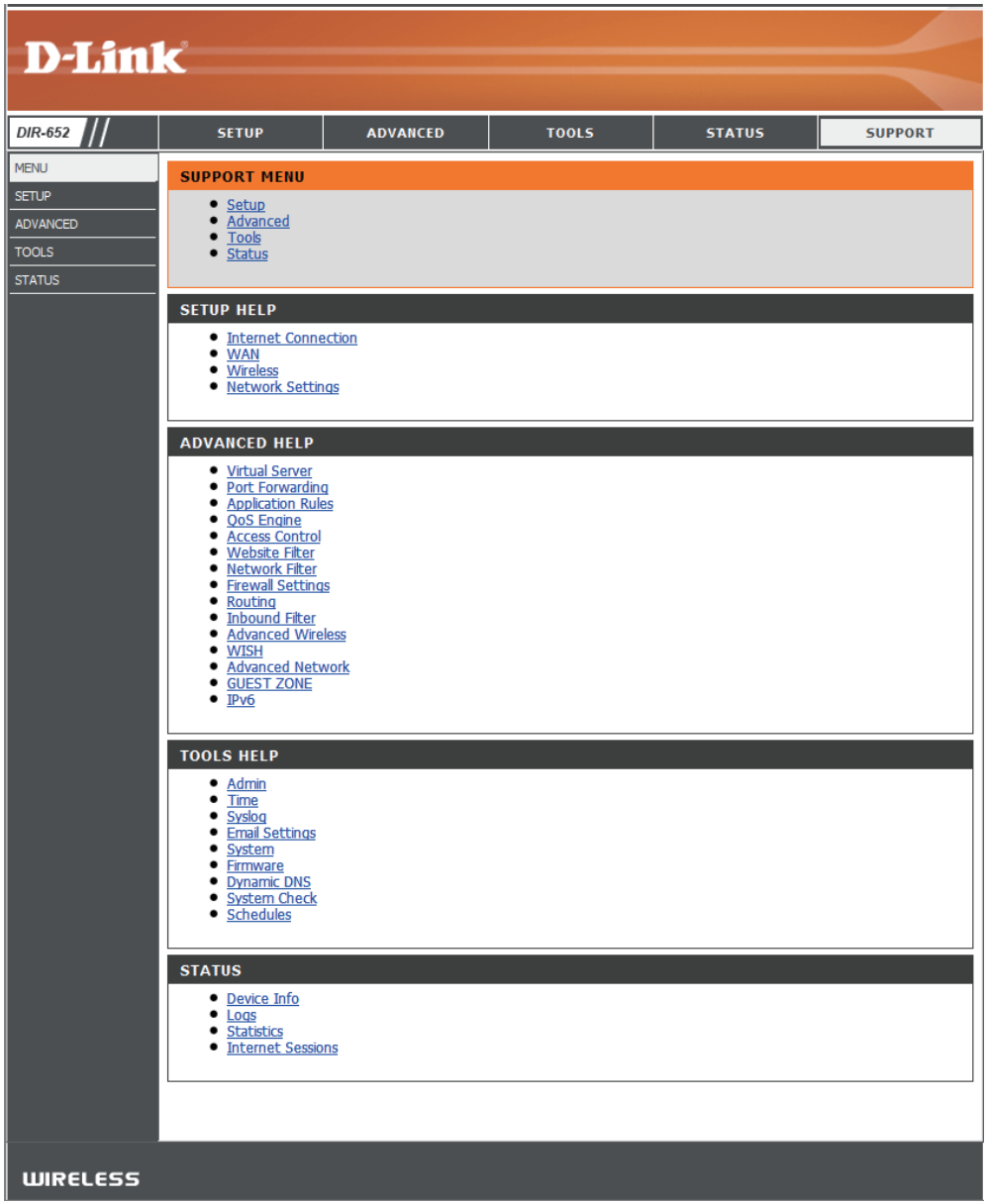



# IPv6

The IPv6 details page displays full details of IPv6 clients that are connected when IPv6 is enabled.



# Support


D-Link
DIR-652
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
MENU
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT MENU
Setup
Advanced
Tools
Status
SETUP HELP
Internet Connection
WAN
Wireless
Network Settings
ADVANCED HELP
Virtual Server
Port Forwarding
Application Rules
QoS Engine
Access Control
Website Filter
Network Filter
Firewall Settings
Routing
Inbound Filter
Advanced Wireless
WISH
Advanced Network
GUEST ZONE
IPv6
TOOLS HELP
Admin
Time
Syslog
Email Settings
System
Firmware
Dynamic DNS
System Check
Schedules
STATUS
Device Info
Logs
Statistics
Internet Sessions
WIRELESS

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-652 offers the following types of security:

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

# What is WPA?

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

The 2 major improvements over WEP:

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

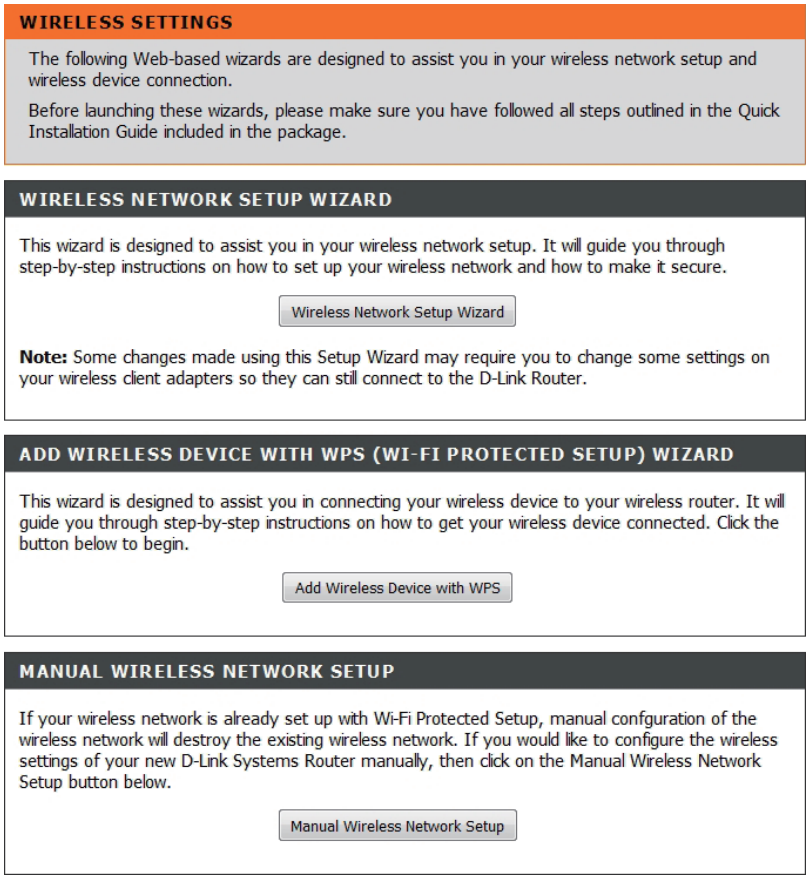
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

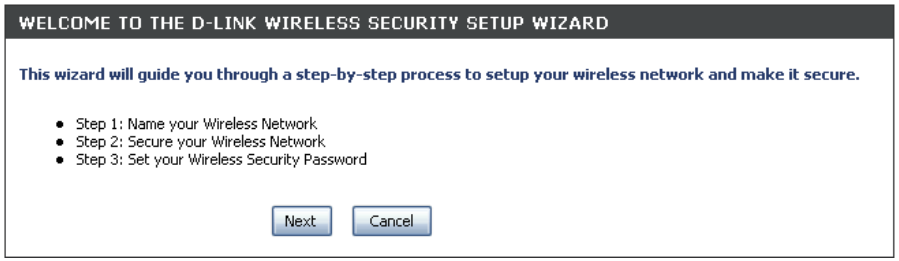
WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

# Wireless Security Setup Wizard

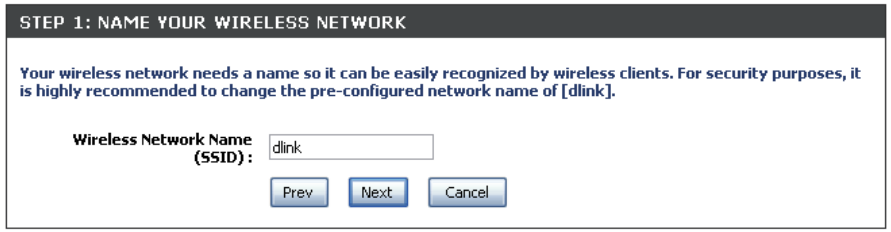
To run the security wizard, click on Setup at the top and then click **Launch Wireless Security Setup Wizard**.




Click **Next** to continue.



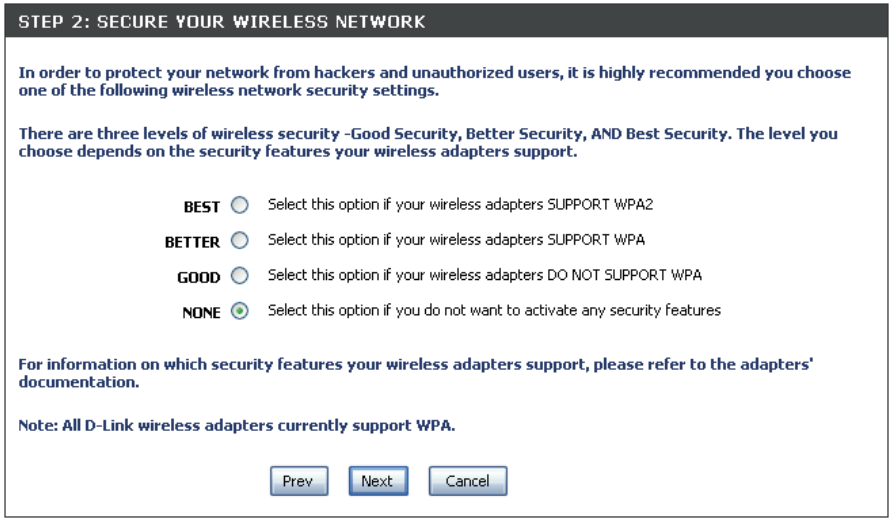
Enter the SSID (Service Set Identifier). The SSID is the name of your wireless network. Create a name using up to 32 characters. The SSID is case-sensitive.




Select the level of security for your wireless network:

- Best - WPA2 Authentication
- Better - WPA Authentication
- None - No security

Click **Next** to continue.



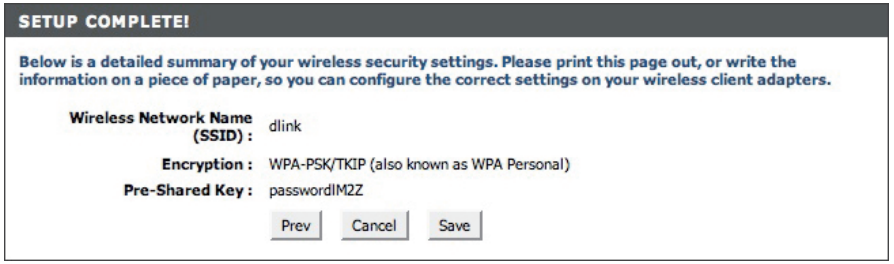

If you selected Best or Better, enter a password between 8-63 characters.

If you selected Good, enter 13 characters or 26 Hex digits.

Click **Next** to continue.

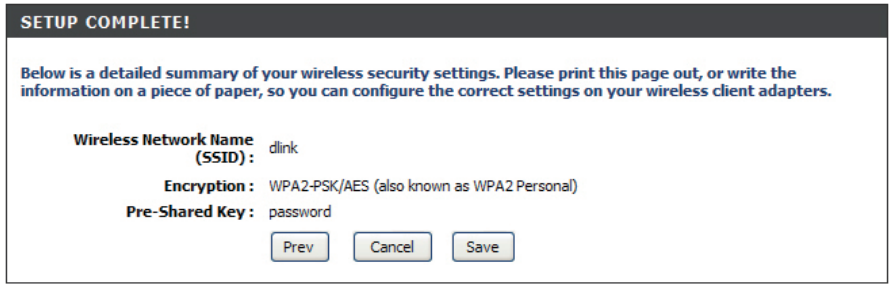
If you selected Better, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

Click **Save** to finish the Security Wizard.




If you selected Best, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

Click **Save** to finish the Security Wizard.




If you selected WPA-Enterprise, the RADIUS information will be displayed. Click **Save** to finish the Security Wizard.

# Configure WPA-Personal (PSK)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1).

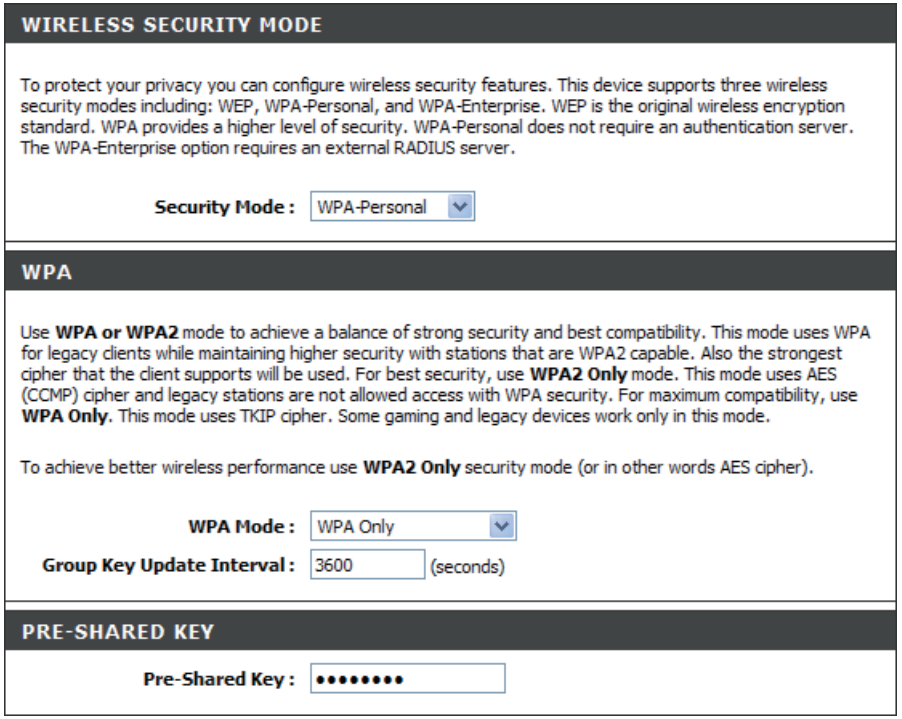
1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.

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

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

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

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

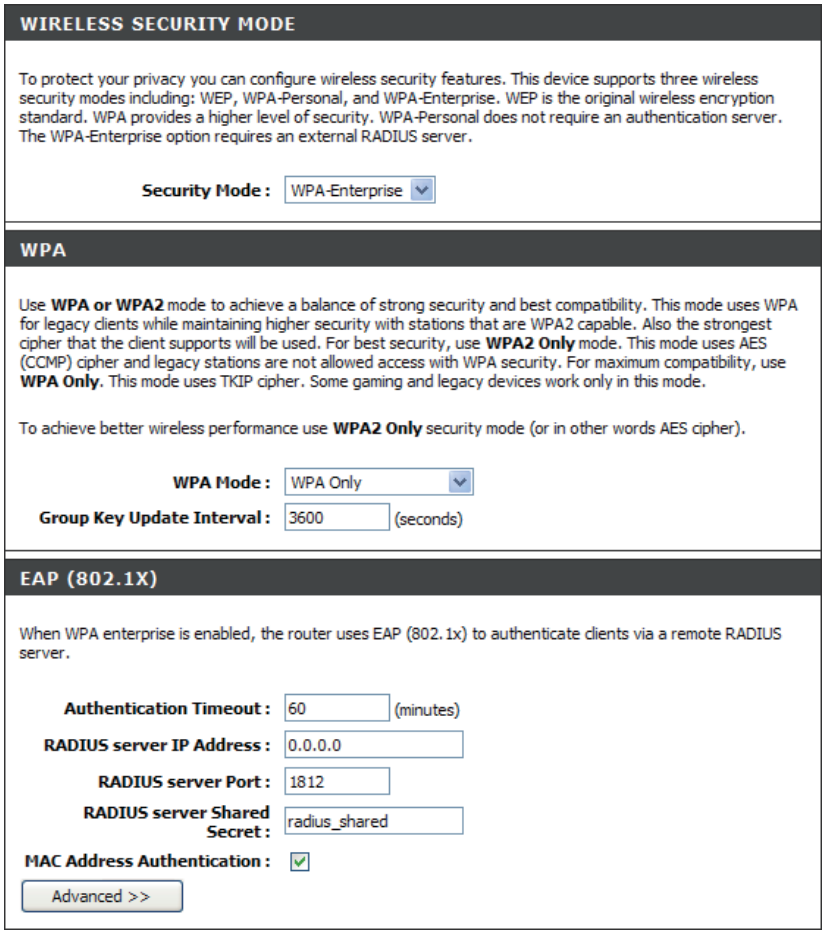



6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.

# Configure WPA-Enterprise (RADIUS)

It is recommended to enable encryption on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption. Your wireless signal may degrade when enabling encryption due to the added overhead.

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




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

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

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

5. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).

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

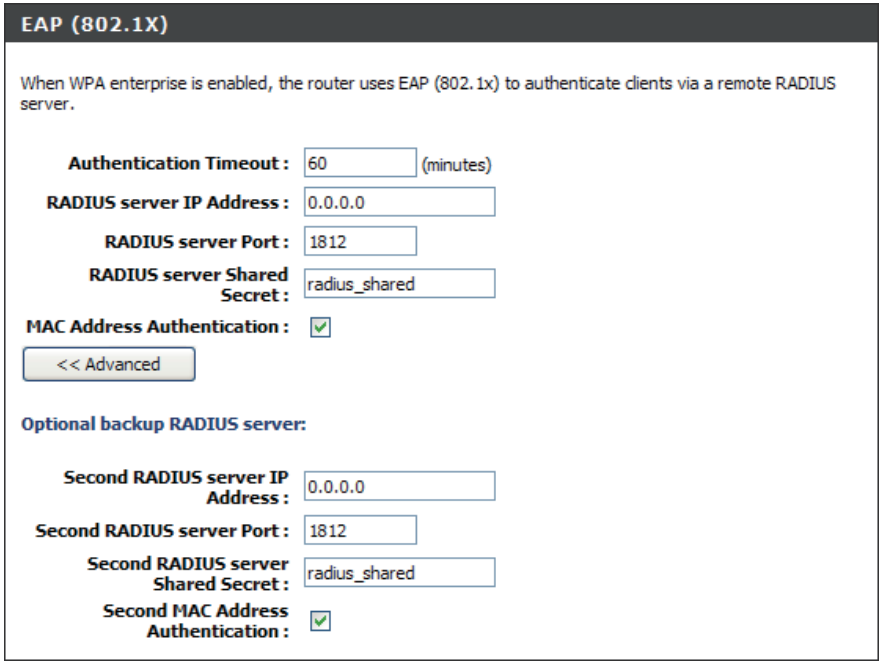
7. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.

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

9. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.

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

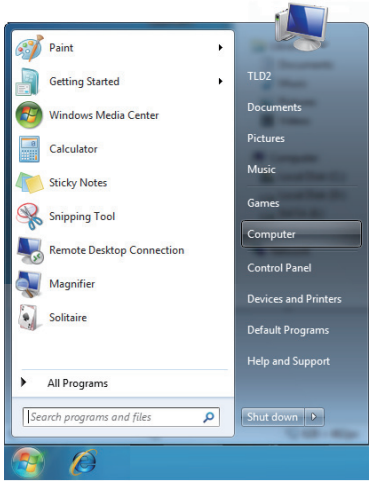
11. Click **Apply Settings** to save your settings.


EAP (802.1X)
When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.
Authentication Timeout :
60
(minutes)
RADIUS server IP Address :
0.0.0.0
RADIUS server Port :
1812
RADIUS server Shared Secret :
radius_shared
MAC Address Authentication :
<< Advanced
Optional backup RADIUS server:
Second RADIUS server IP Address :
0.0.0.0
Second RADIUS server Port :
1812
Second RADIUS server Shared Secret :
radius_shared
Second MAC Address Authentication :

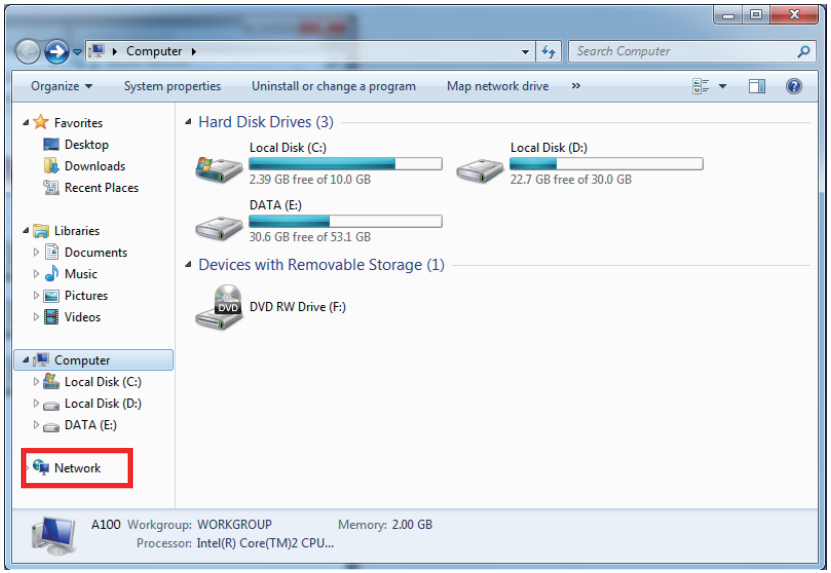
# Using Windows® 7 and WPS for Wireless Configuration

The following steps allow you to configure your DIR-652 wireless network settings using Windows® 7 through WPS.

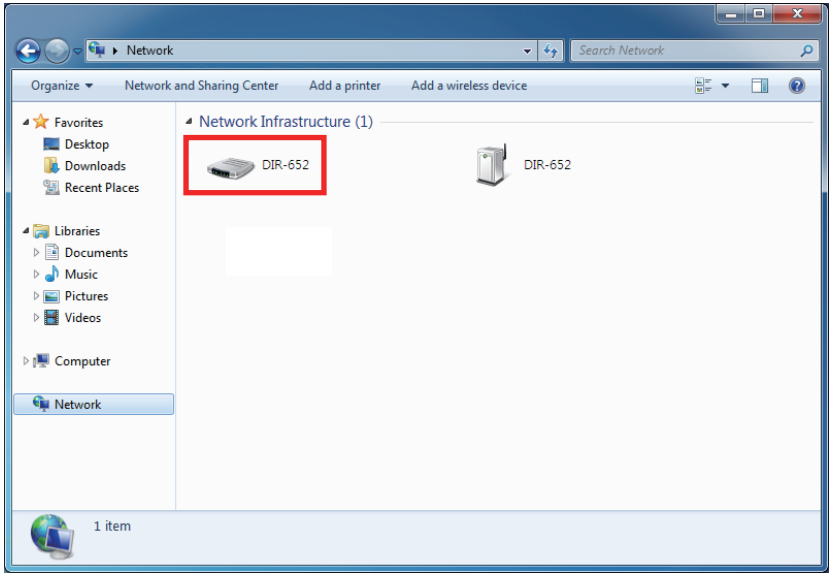
1. Click the **Start** button and select **Computer** from the Start menu.



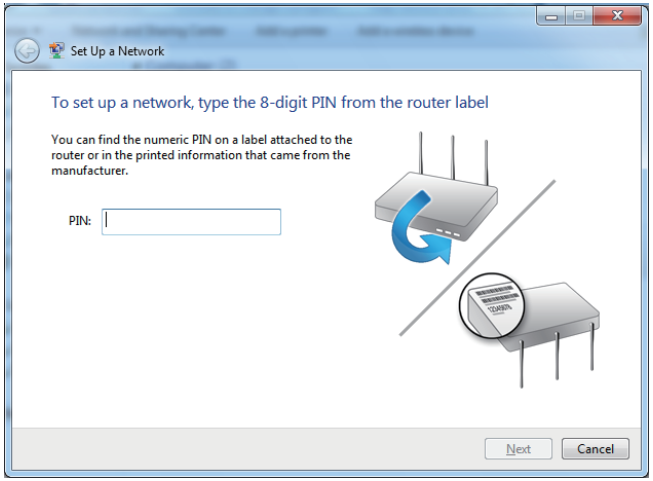

2. Click the **Network** option.



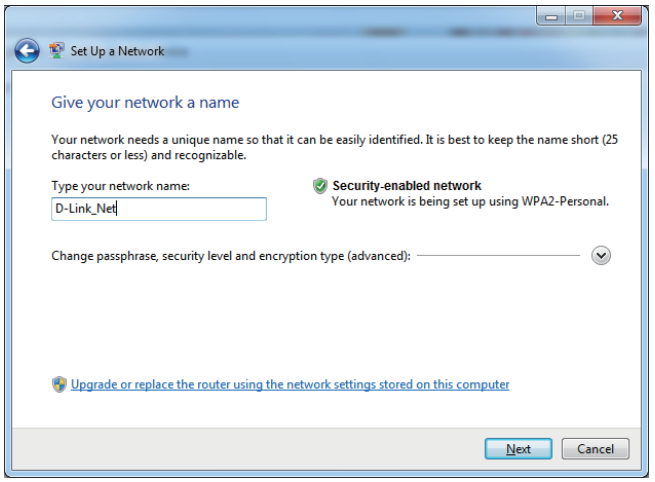
3. Double-click the DIR-652 router.




4. Input the WPS PIN number (displayed in the **Advanced > Wi-Fi Protected Setup** section in the Router's Web UI) and click **Next**.

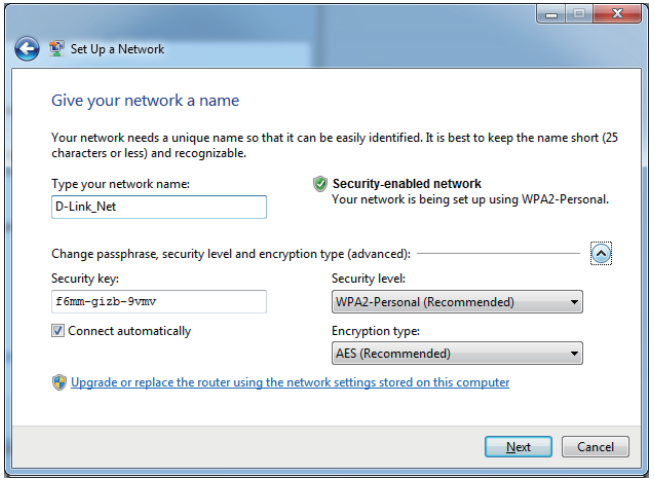


5. Type a name for your wireless network.



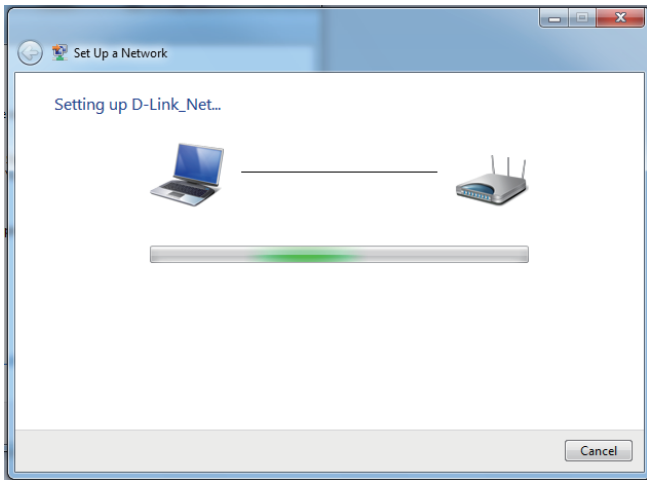

6. To configure advanced settings, click the icon.

Click **Next** to continue.



7. The following window will appear while the Router is being configured.

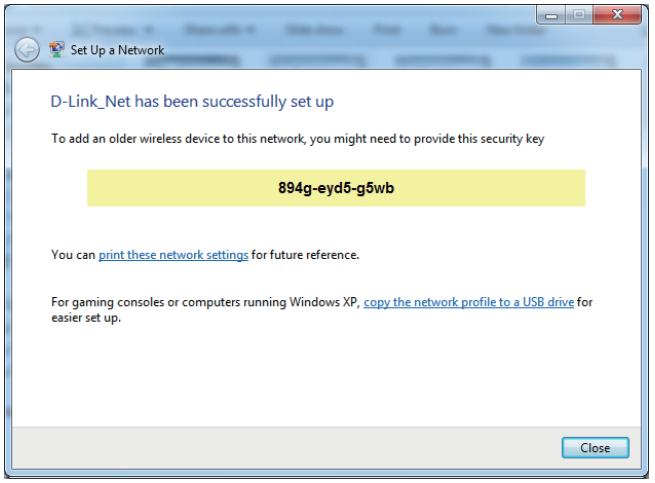
   Wait for the configuration to complete.




8. After configuration is complete, a window will appear that your wireless network has been set up successfully.

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

   Click **Close** to complete WPS setup.



# Connecting to a Wireless Network Using Windows® 7

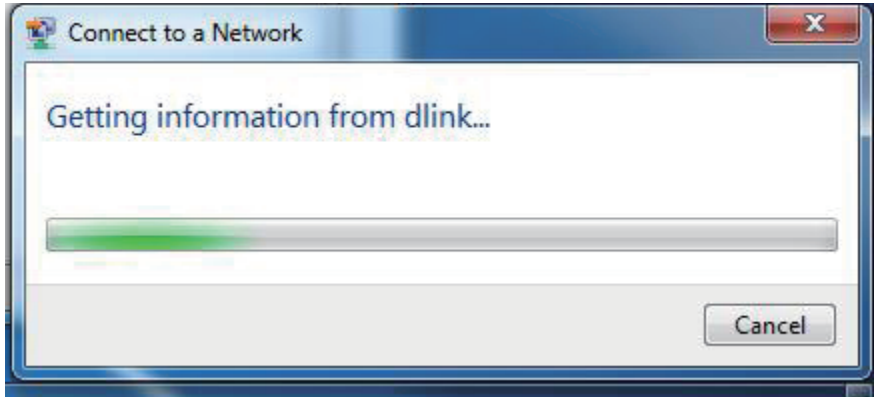
It is recommended that you enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Click on the wireless icon in the system tray in the lower-right corner of your screen.

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

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

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



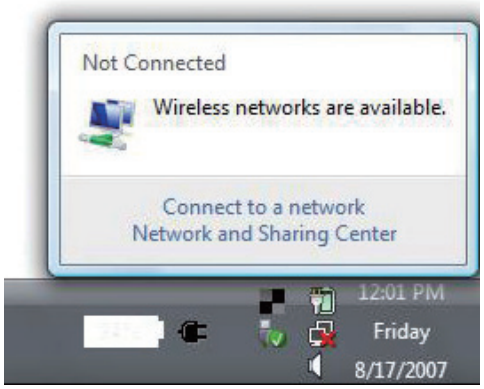
5. If your wireless network uses encryption such as WEP or WPA/WPA2, enter the encryption password/passphrase for your wireless network and click **Connect**.

   It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the key or passphrase is exactly the same as on the wireless router.

# Connecting to a Wireless Network Using Windows Vista®

It is recommended that you 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.

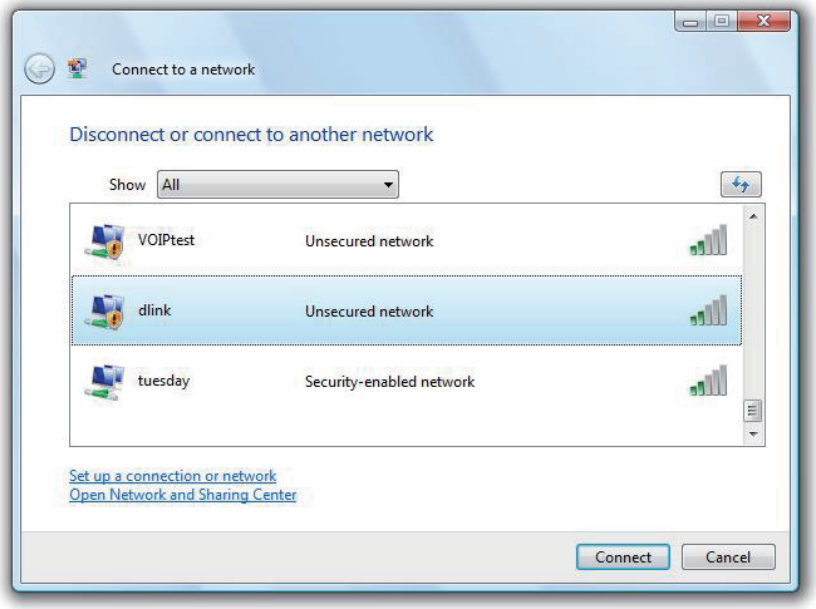
**1.** Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in the system tray in the lower right corner of the screen. Select **Connect to a network**.




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

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

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.



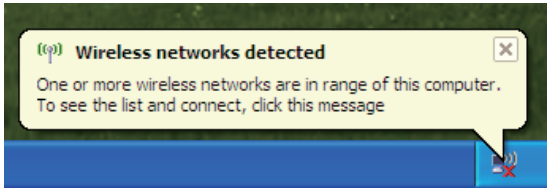
**3.** If your wireless network uses encryption such as WEP or WPA/WPA2, enter the encryption password/passphrase for your wireless network and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the key or passphrase is exactly the same as on the wireless router.

# Connecting to a Wireless Network Using Windows® XP

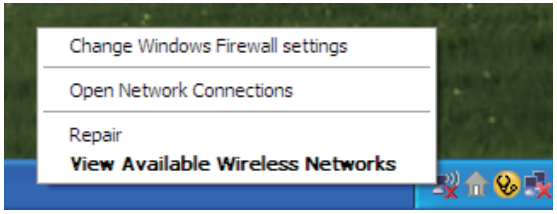
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows® XP utility as seen below.

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



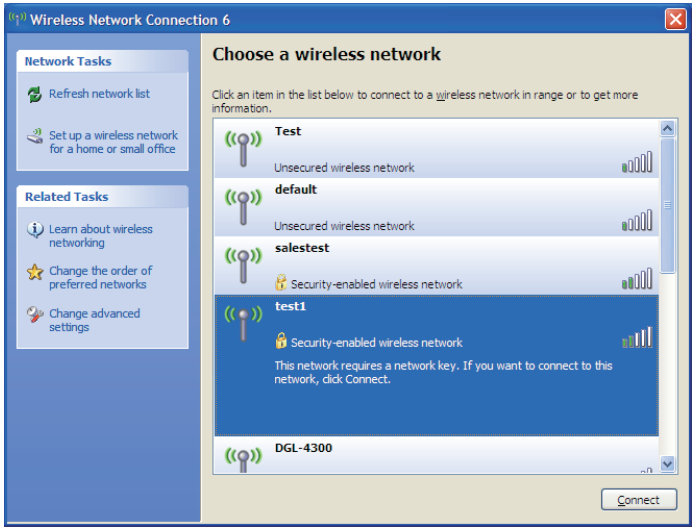

or

Right-click on the wireless computer icon in the system tray in the lower-right corner of the screen. Select **View Available Wireless Networks**.



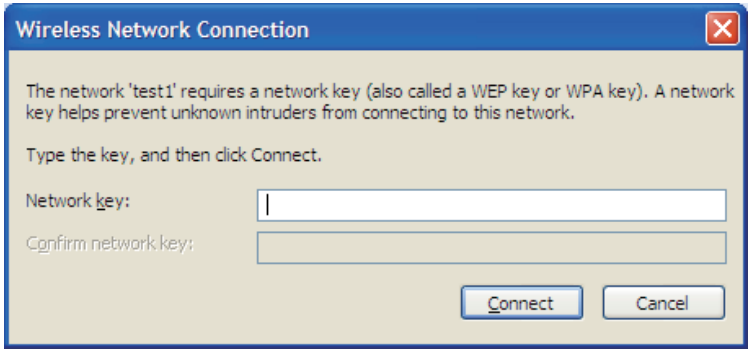

2. The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

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



**3.** If your wireless network uses encryption such as WEP or WPA/WPA2, enter the encryption password/passphrase for your wireless network and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the key or passphrase is exactly the same as on the wireless router.



# Troubleshooting

### 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 on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

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

  - Internet Explorer 6.0 or higher
  - Netscape 8 or higher
  - Mozilla 1.7.12 (5.0) or higher
  - Opera 8.5 or higher
  - Safari 1.2 or higher (with Java 1.3.1 or higher)
  - Camino 0.8.4 or higher
  - Firefox 1.5 or higher

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

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

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

***Note: AOL DSL+ users must use MTU of 1400.***

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

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

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

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

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

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

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

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

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

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

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

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

C:\>
```

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

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

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

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

# Wireless Basics

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

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

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

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

## What is Wireless?

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

## Why D-Link Wireless?

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

## How does wireless work?

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

### Wireless Local Area Network (WLAN)

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

### Wireless Personal Area Network (WPAN)

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

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

## Who uses wireless?

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

### Home

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

### Small Office and Home Office

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

## Where is wireless used?

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

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

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

## Tips

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

### Centralize your router or Access Point

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

### Eliminate Interference

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

### Security

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

# Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.

- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-652 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.

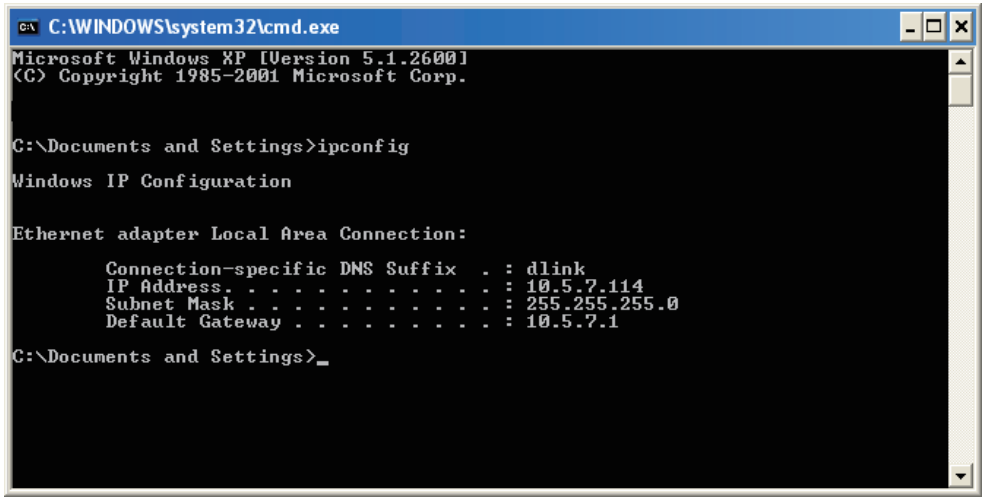
Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK.** (Windows Vista® users type *cmd* in the **Start Search** box.)

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.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



# Statically Assign an IP address

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

**Step 1**
Windows 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**.

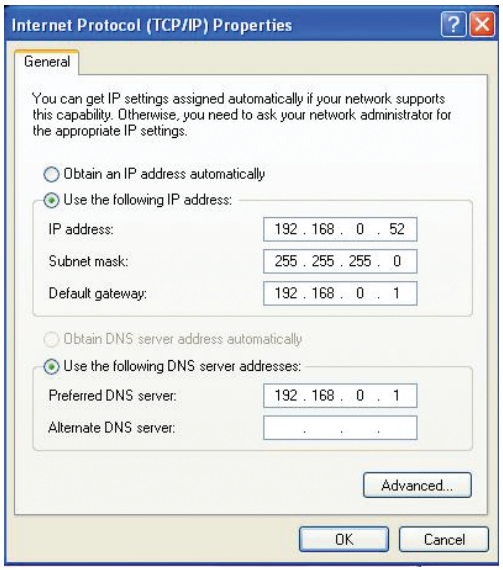
**Step 2**
Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.

**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 Default Gateway the same as the LAN IP address of your router (192.168.0.1).

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




**Step 5**
Click **OK** twice to save your settings.

# Technical Specifications

**Standards**

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

**Security**

- WPA-Personal
- WPA2-Personal
- WPA-Enterprise
- WPA2-Enterprise

**Wireless Signal Rates***

**IEEE 802.11n (HT20/40):**

- 144.4Mbps (300)
- 130Mbps (270)
- 117Mbps (243)
- 104Mbps (216)
- 78Mbps (162)
- 66Mbps (135)
- 58.5Mbps (121.5)
- 52Mbps (108)
- 39Mbps (81)
- 26Mbps (54)
- 19.5Mbps (40.5)
- 12Mbps (27)
- 6.5Mbps (13.5)

**IEEE 802.11g:**

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

**Frequency Range**

- 2.4GHz to 2.483GHz

**Transmitter Output Power**

- 15dBm ± 2dB

**External Antenna Type**

- 2 Fixed Reverse SMA External Antennas

**LEDs**

- Power/Status
- Internet
- WLAN
- LAN (10/100)

**Operating Temperature**

- 32°F to 131°F ( 0°C to 55°C)

**Humidity**

- 95% maximum (non-condensing)

**Safety & Emissions**

- FCC
- CE

**Dimensions**

- L = 5.81 inches
- W = 4.6 inches
- H = 1.2 inches

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

# Certifications

## CE Mark Warning:

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

## FCC Statement:

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

## IMPORTANT NOTICE:

### FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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