D-Link®

Version 3.0 | 05/09/2013

User Manual

Wireless N Gigabit Router

DIR-655

Preface

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

Manual Revisions

Revision	Date	Description
2.0	May 25, 2010	• New Revision
2.1	July 6, 2012	• Added IPv6 Routing and Firewall • Added QRS Mobile app • Added Quick Setup Wizard
3.0	May 9, 2013	• Removed WISH • Removed QRS Mobile app

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 © 2008-2013 by D-Link Corporation.

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

Table of Contents

Preface i
Manual Revisions i
Trademarks i

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

Installation 7
Before you Begin 7
Wireless Installation Considerations 8

Getting Started 9
Quick Setup Wizard 10

Configuration 16
Internet Connection Setup 17
Manual Configuration 18
Static IP 18
Dynamic IP (DHCP) 19
PPPoE (DSL) 20
PPTP 22
L2TP 24
DS-Lite 26
Wireless Settings 27
Manual Wireless Connection Setup 28
Wireless Security 29
What is WPA? 29
Wireless Security Setup Wizard 30
WPA-Personal (PSK) 32
WPA-Enterprise (RADIUS) 33
Network Settings 35
Router Settings 35
DHCP Server Settings 36
DHCP Reservation 37
Media Server 38
IPv6 39
IPv6 Internet Connection Setup Wizard 40
IPv6 over PPPoE 42
Static IPv6 Address Connection 43
Tunneling Connection (6rd) 44
IPv6 Manual Setup 45
Auto Detection 45
Static IPv6 46
Autoconfiguration 47
PPPoE 48
IPv6 in IPv4 Tunneling 50
6to4 Tunneling 51
6rd 52
Local Connectivity Only 53
Advanced Settings 54
Virtual Server 54
Port Forwarding 55

Application Rules 56
QoS Engine 57
Network Filter 59
Access Control 60
Access Control Wizard 60
Website Filter 63
Inbound Filter 64
Firewall Settings 65
Routing 67
Advanced Wireless 68
Wi-Fi Protected Setup (WPS) 69
Advanced Network Settings 71
Guest Zone 72
IPv6 Firewall 73
IPv6 Routing 74
Tools 75
Admin 75
Time 76
SysLog 77
E-mail Settings 78
System 79
Firmware 80
Dynamic DNS 81
System Check 82
Schedules 83
Status 84
Device Info 84
Logs 85
Statistics 86
Internet Sessions 87
Routing 88
Wireless 89
IPv6 90
IPv6 Routing 91
Support 92

Connect a Wireless Client to your Router 93
WPS Button 93
Windows® 8 94
WPA/WPA2 94
Windows® 7 96
WPA/WPA2 96
WPS 99
Windows Vista® 103
WPA/WPA2 104
WPS/WCN 2.0 106
Windows® XP 107
WPA/WPA2 108

Troubleshooting 110

Wireless Basics 114
Tips 116
Wireless Modes 117

Networking Basics 118
Check your IP address 118

Technical Specifications 120

Package Contents

D-Link DIR-655 Wireless N Gigabit Router with 3 Detachable Antennas	
Power Adapter	
CAT 5 Ethernet Cable	
CD-ROM	

Note: *Using a power supply with a different voltage rating than the one included with the DIR-655 will cause damage and void the warranty.*

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n or 802.11g wireless clients • 10/100/1000 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Mozilla 1.7.12 or higher • Firefox 1.5 or higher • Safari 1.0 or higher (with Java 1.3.1 or higher) **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	**Computer with the following:** • Windows 7, Vista®, or XP with Service Pack 2 • An installed Ethernet adapter • CD-ROM drive

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 excellent coverage throughout the whole home.

ULTIMATE PERFORMANCE
The D-Link Wireless N Gigabit Router (DIR-655) 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 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 Wireless N technology, this high performance router provides superior home coverage while reducing dead spots. The Wireless N Gigabit Router is designed for use in bigger homes and for users who demand higher performance networking. Add a 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 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 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 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-655 provides up to 300 Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio. 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-655 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.

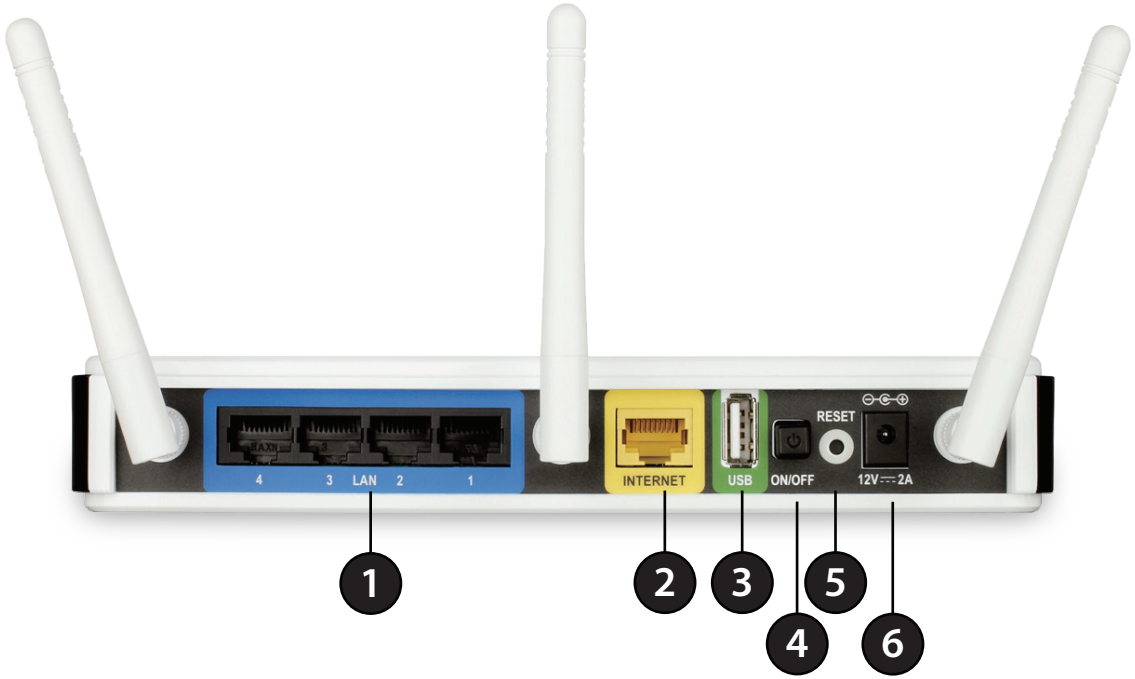
    - **Filter Scheduling** - These filters can be scheduled to be active on certain days or for a duration of hours or minutes.

    - **Secure Multiple/Concurrent Sessions** - The DIR-655 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-655 can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use web-based user interface, the DIR-655 lets you control what information is accessible to those on the wireless network, whether from the Internet or from your company's server. Configure your router to your specific settings within minutes.

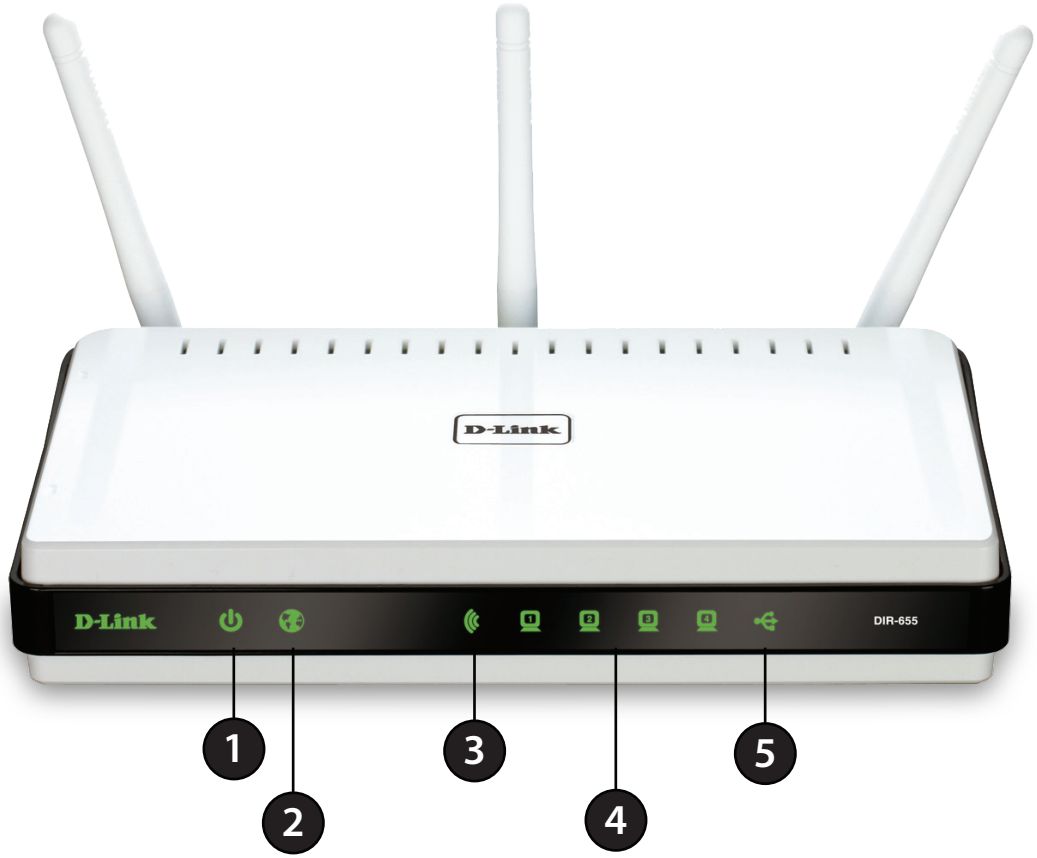
* Maximum wireless signal rate derived from IEEE Standard 802.11g and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.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

Hardware Overview
Connections



1	LAN Ports (1-4)	Connect Ethernet devices such as computers, switches, and hubs.
2	Internet Port	The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.
3	USB	Connect a USB flash drive or printer.
4	On/Off Button	Pressing the on/off button toggles power to the router.
5	Reset	Pressing the Reset button restores the router to its original factory default settings.
6	Power Receptor	Receptor for the supplied power adapter.

LEDs



1	Power LED	A solid light indicates a proper connection to the power supply.
2	Internet LED	A solid light indicates connection on the Internet port. This LED blinks during data transmission. A solid blue light indicates that there is an Internet connection, an orange light indicates that there is none.
3	WLAN LED	A solid light indicates that the wireless segment is ready. This LED blinks during wireless data transmission.
4	Local Network's LED	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.
5	USB LED	A solid light indicates a USB drive or a printer is plugged in.

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 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 2.4 GHz 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 2.4 GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

Getting Started

The DIR-655 includes a Quick Router Setup Wizard CD. Follow the simple steps below to run the wizard to guide you quickly through the installation process.

Insert the **Wizard CD** in the CD-ROM drive.

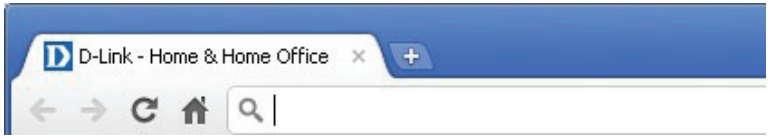
If the CD autorun function does not automatically start on your computer, go to **Start** > **Run**. In the run box type "**D:\WIZARD.exe**" (where ***D:*** represents the drive letter of your CD-ROM drive).

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

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

Quick Setup Wizard

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

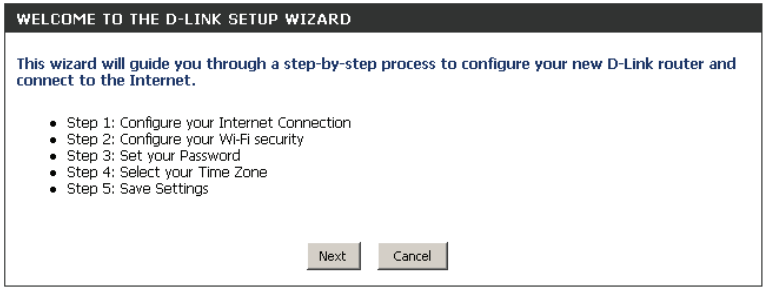


If you have already configured your settings and you would like to access the configuration utility, please refer to page 16.

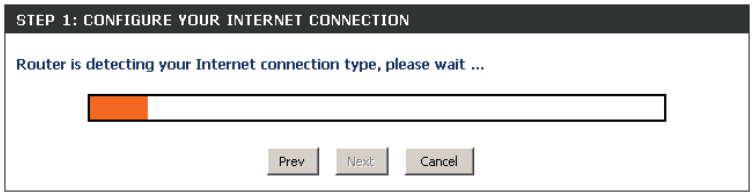
If you did not run the setup wizard from the CD and this is the first time logging into the router, this wizard will start automatically.

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

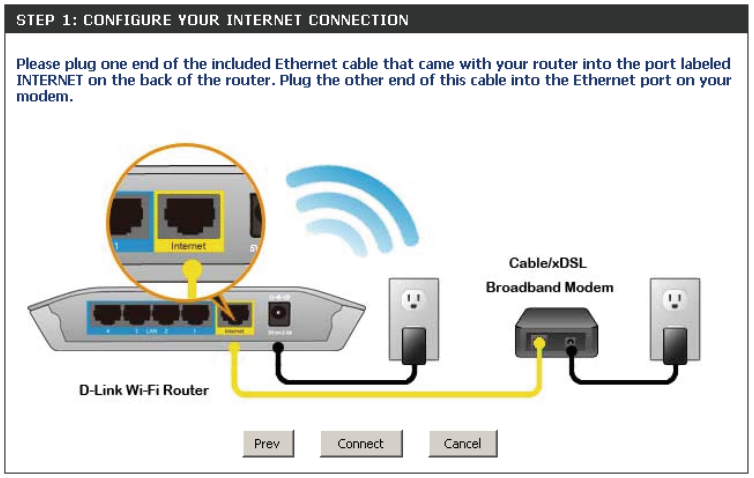
Click **Next** to continue.



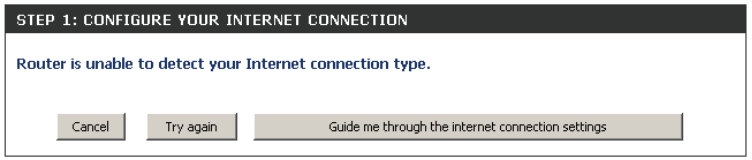
Please wait while your router detects your internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password.



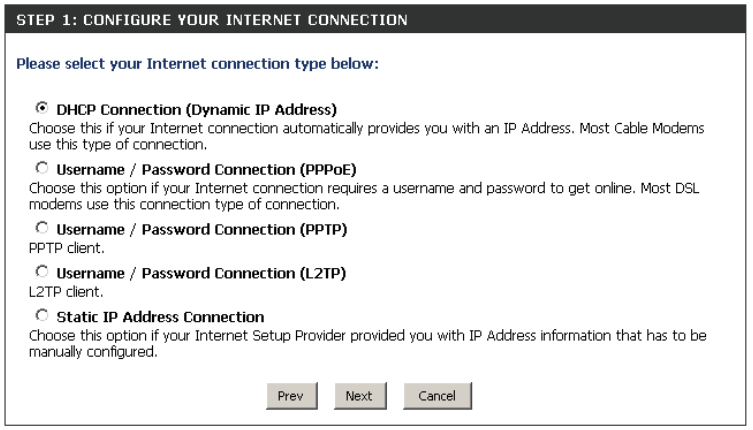
If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Connect your broadband modem to the Internet port and then click **Try Again**.



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

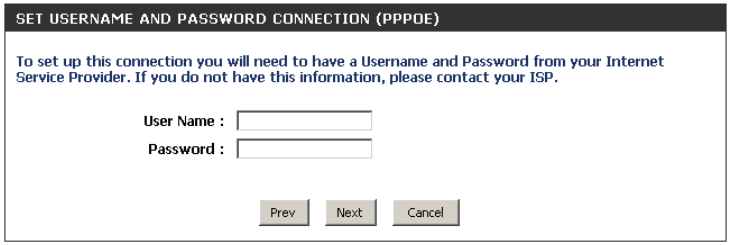


Select your Internet connection type and click **Next** to continue.

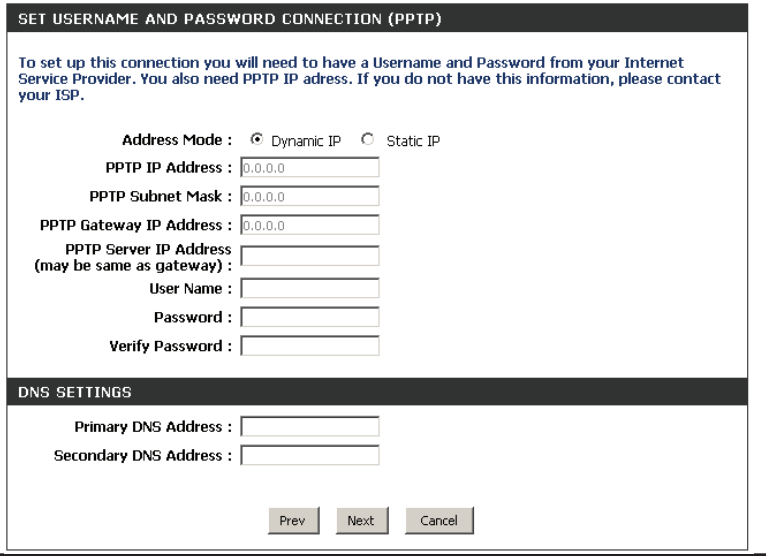


If the router detected or you selected **PPPoE**, enter your PPPoE username and password and click **Next** to continue.

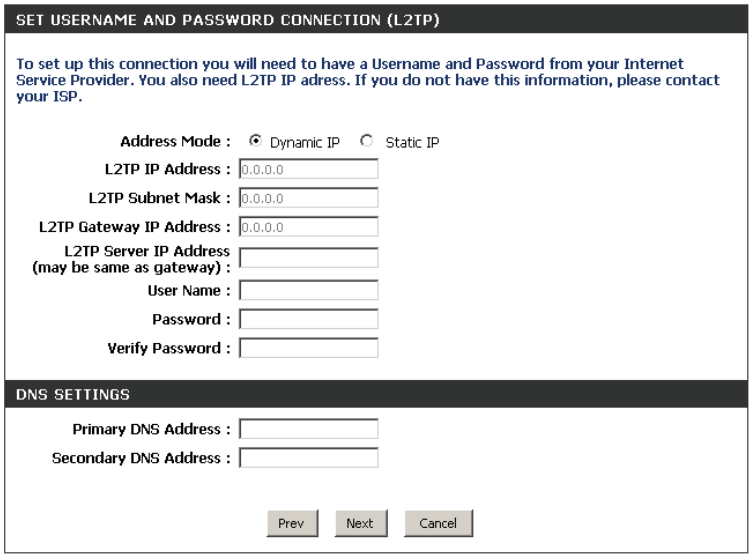
Note: *Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through a router.*



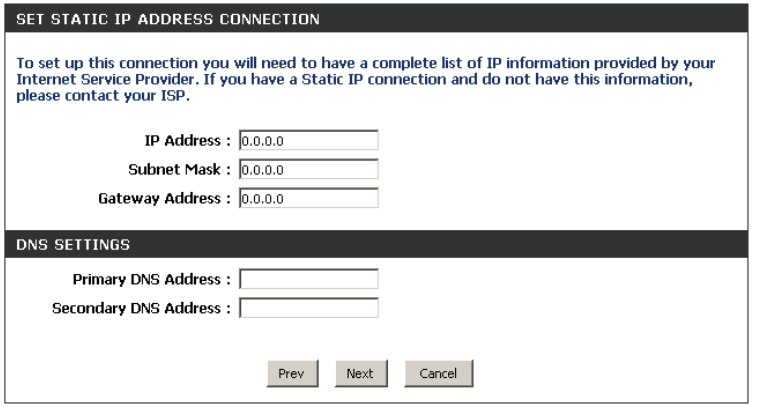
If the router detected or you selected **PPTP**, enter your PPTP username, password, and other information supplied by your ISP. Click **Next** to continue.



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



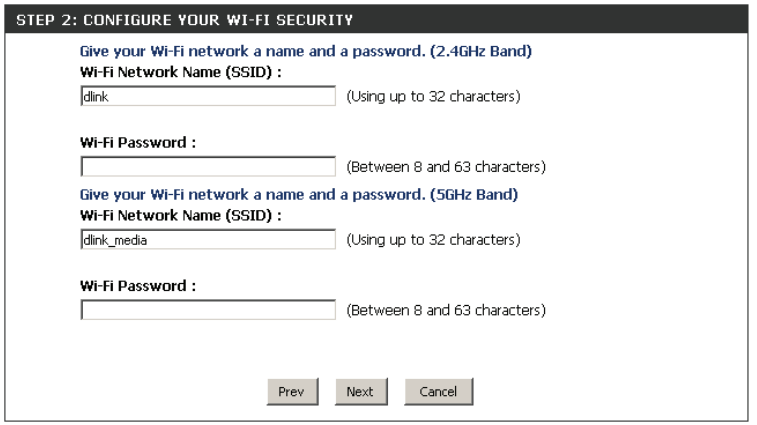
If the router detected or you selected **Static**, enter the IP and DNS settings supplied by your ISP. Click **Next** to continue.



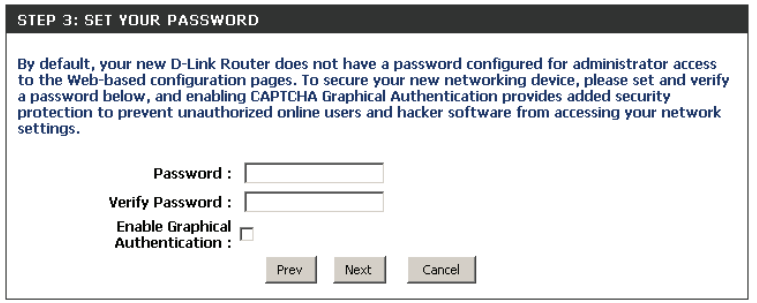
For both the 2.4 GHz and 5 GHz segments, create a wireless network a name (SSID) using up to 32 characters.

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

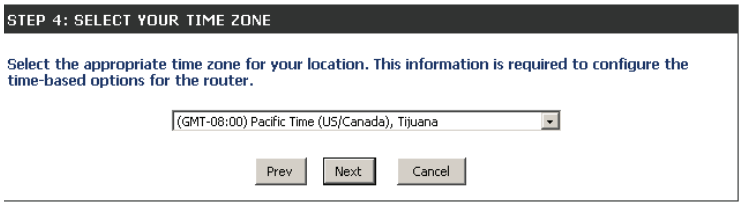
Click **Next** to continue.



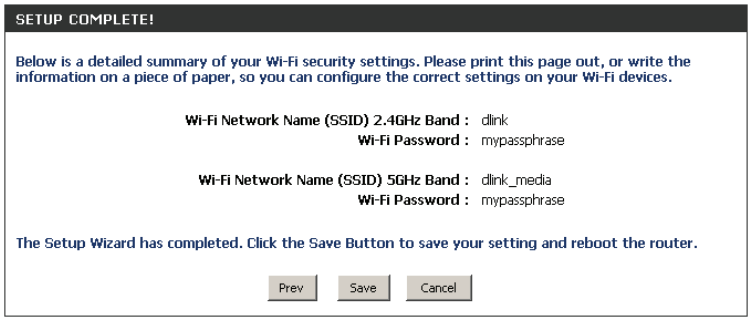
In order to secure your router, please enter a new password. Check the Enable Graphical Authentication box to enable CAPTCHA authentication for added security. Click **Next** to continue.



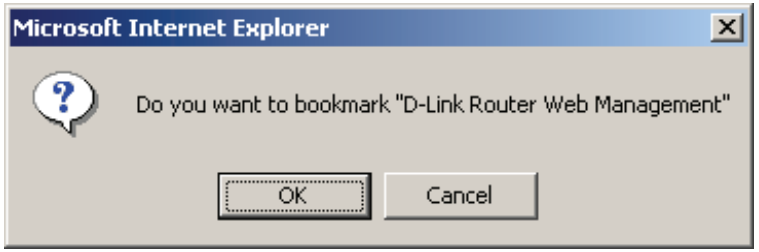
Select your time zone from the drop-down menu and click **Next** to continue.



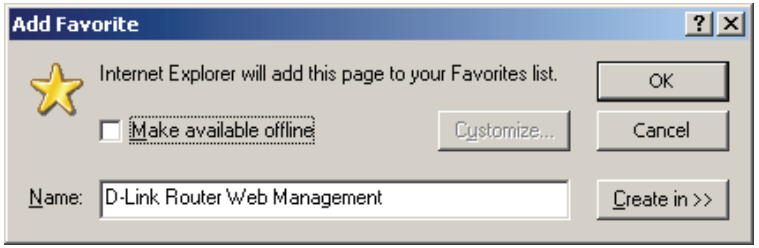
The Setup Complete window will display your wireless settings. Click **Save and Connect** to continue.



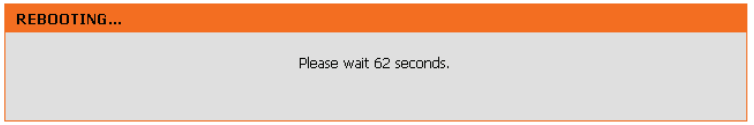
If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.



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



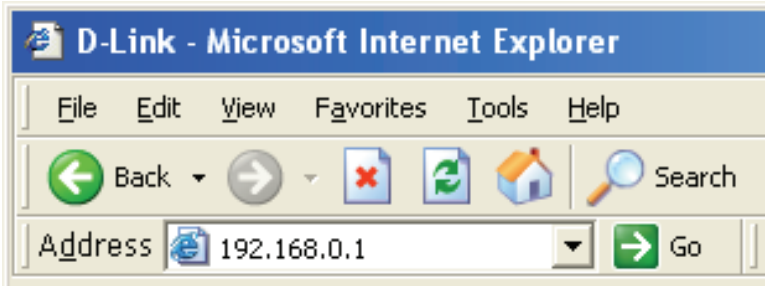
The router will now reboot. Please allow a minute or two. Click the **Continue** button once it is active.



Configuration

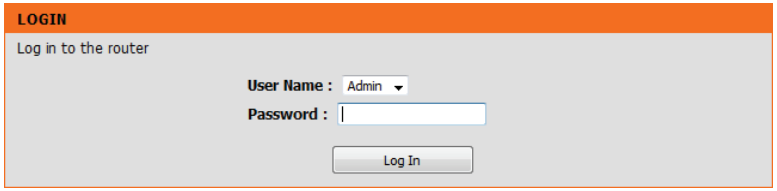
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (**192.168.0.1**).

You can also enter **http://dlinkrouter** to connect.



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

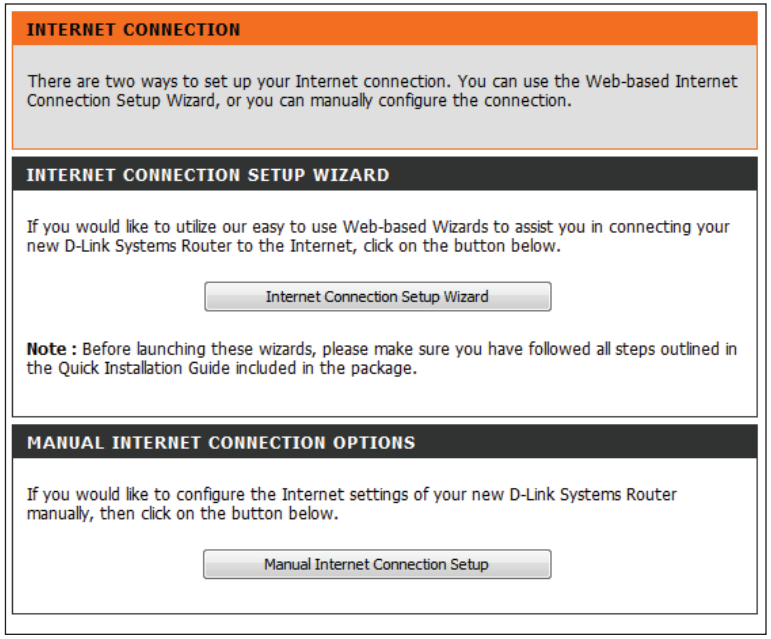
If you get a **Page Cannot be Displayed** error, please refer to the **Troubleshooting** section for assistance.



Internet Connection Setup

You may click **Internet Connection Setup Wizard** to quickly configure your router. Refer to page 10 for details.

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



Manual Configuration

Static IP

Select **Static IP** if your 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.

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.*

True Gigabit Routing Connectivity Setting: Check to enable true Gigabit routing. This will increase the throughput of the WAN-LAN connectivity of the router.

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

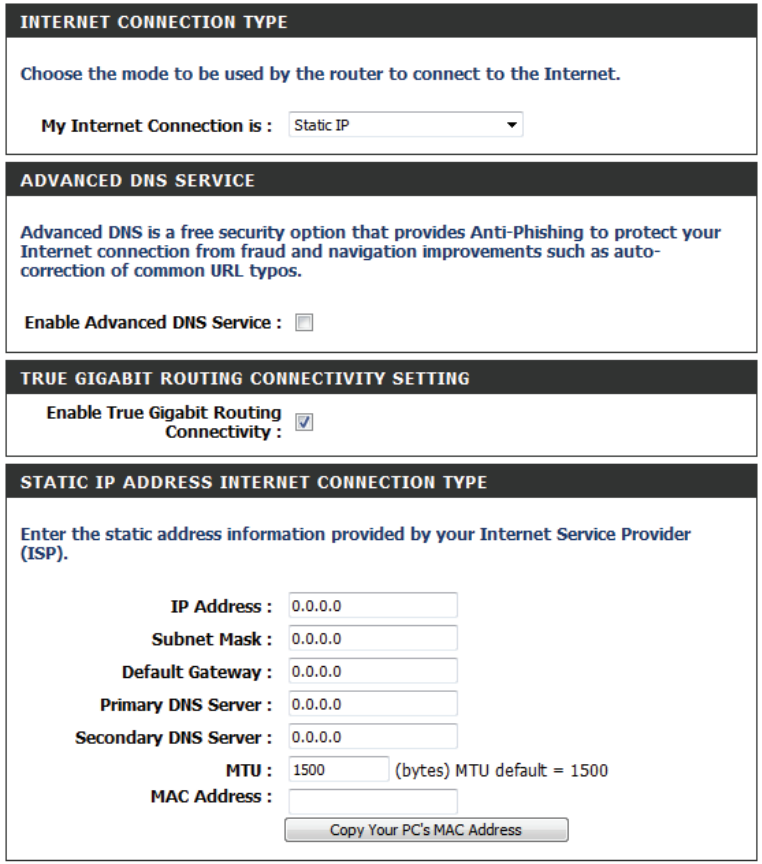
Subnet Mask: Enter the subnet mask assigned by your ISP.

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.



Dynamic IP (DHCP)

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.*

True Gigabit Routing Connectivity Setting: Check to enable true Gigabit routing. This will increase the throughput of the WAN-LAN connectivity of the router.

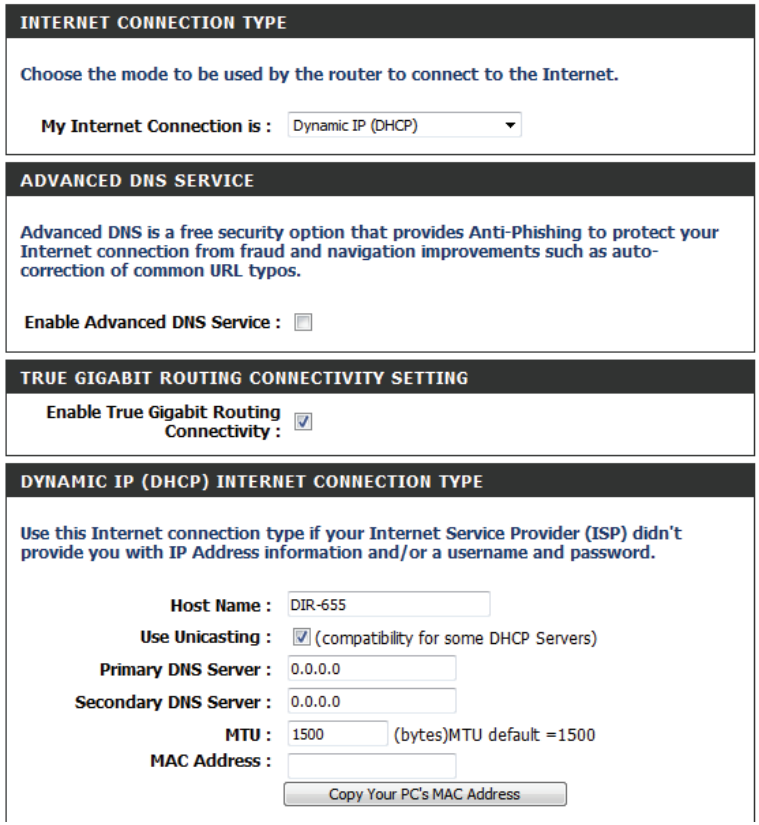
Host Name: The host name is optional but may be required by some ISPs. Leave blank if you are not sure.

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.



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.

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.*

True Gigabit Routing Connectivity Setting: Check to enable true Gigabit routing. This will increase the throughput of the WAN-LAN connectivity of the router.

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).

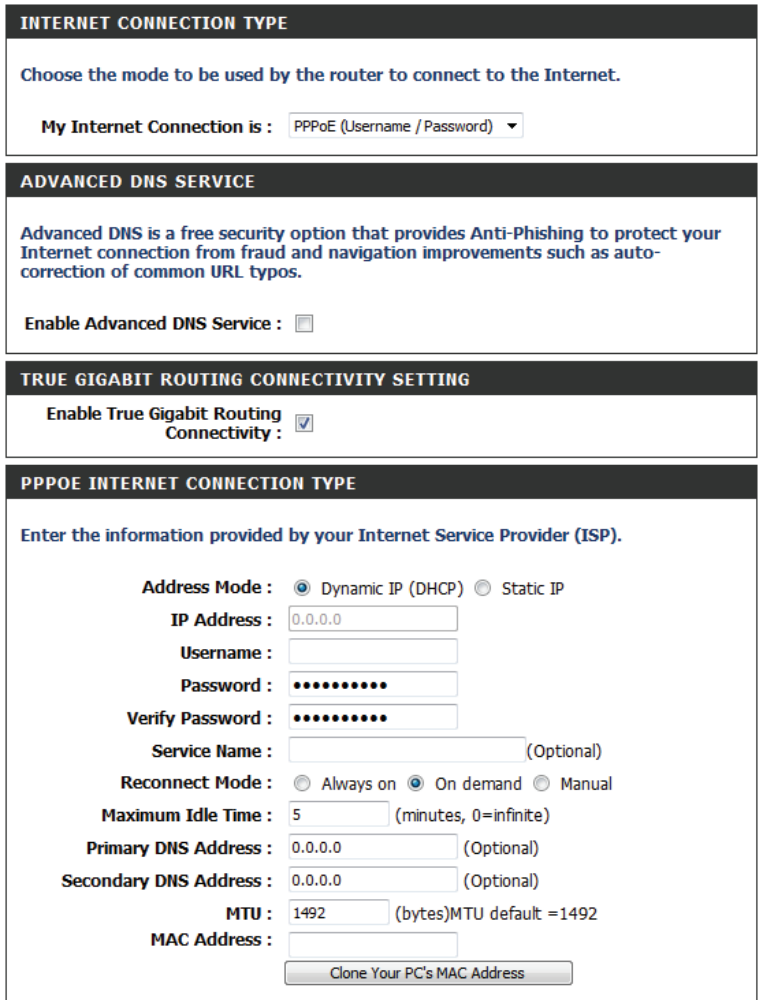
User Name: Enter your PPPoE user name.

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**.

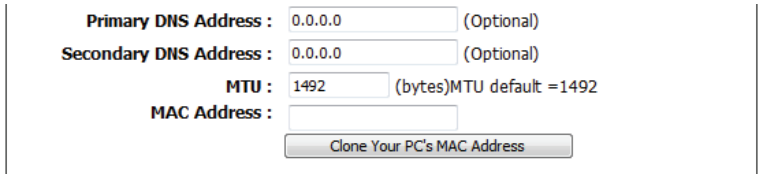
Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.



DNS Addresses: Enter the primary and secondary DNS server addresses (Static PPPoE only).

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

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



PPTP

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

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.*

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).

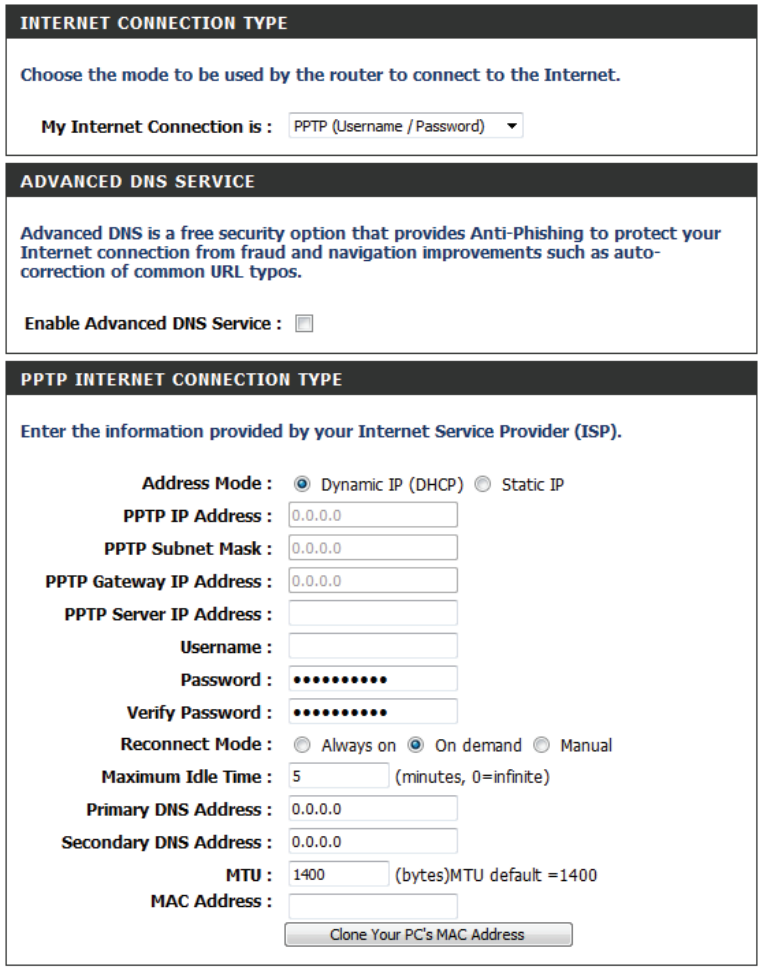
Username: Enter your PPTP username.

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

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

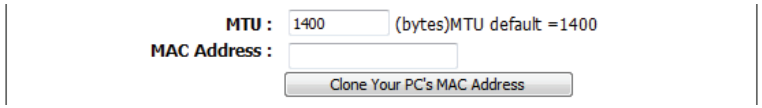
Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

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



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

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



L2TP

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

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.*

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).

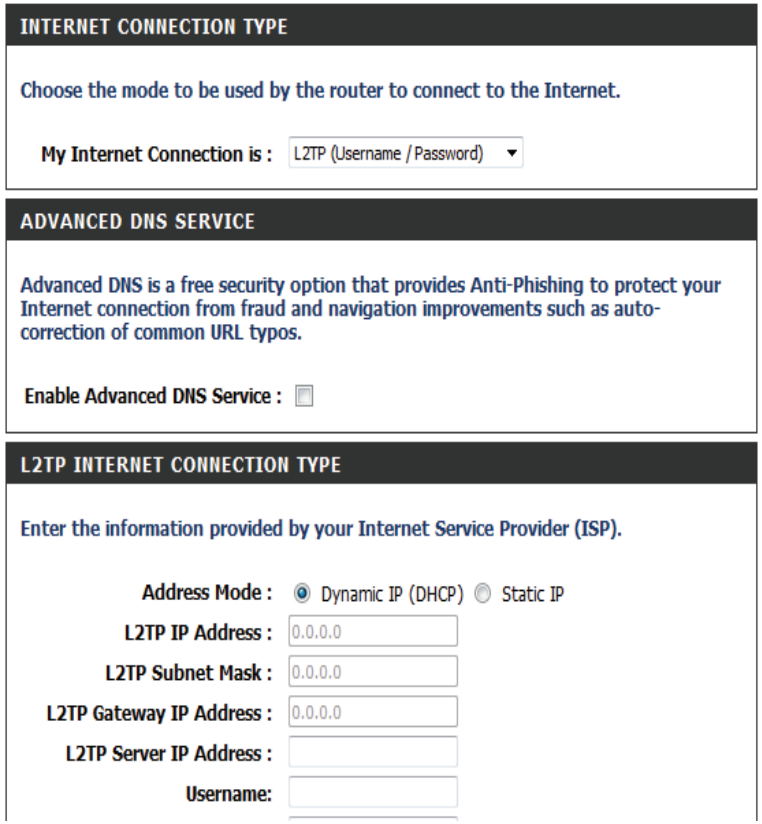
Username: Enter your L2TP username.

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

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

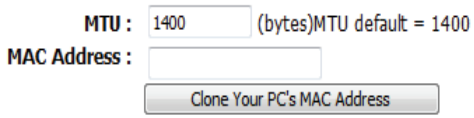
Maximum Idle Time: Enter a maximum idle time during which the Internet connection is maintained during inactivity. To disable this feature, enable Auto-reconnect.

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.



DS-Lite

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

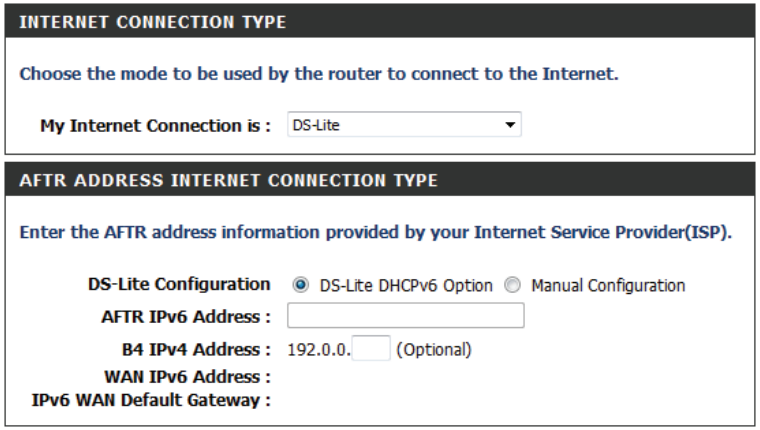
DS-Lite Configuration: Select **DS-Lite DHCPv6 Option** to let the router allocate the AFTR IPv6 address automatically. Select **Manual Configuration** to enter the AFTR IPv6 address in manually.

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

B4 IPv6 Address: Enter the B4 IPv4 address value used here.

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

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

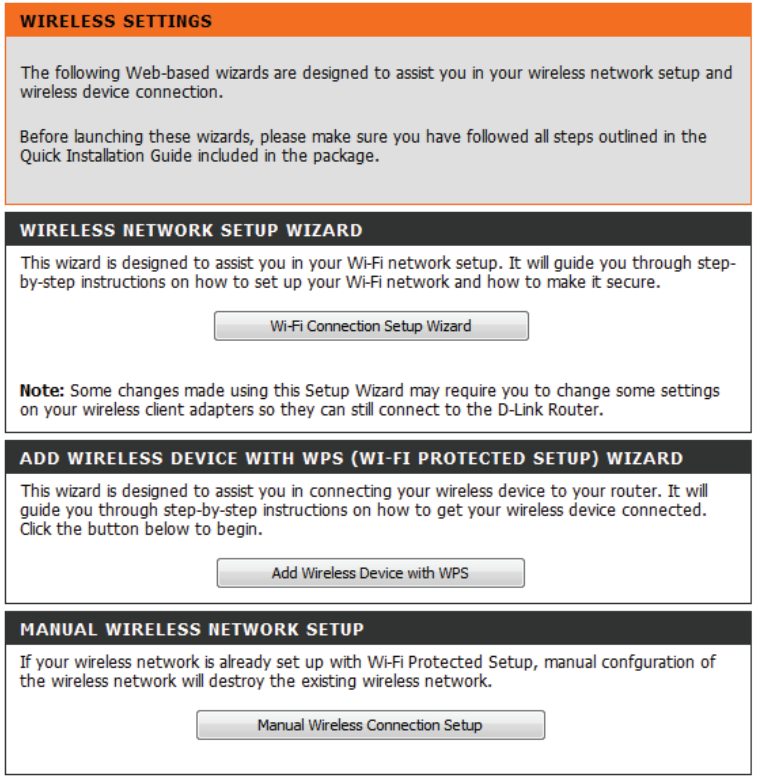


Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Security Setup Wizard** and refer to page 37.

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 93.

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



Manual Wireless Connection Setup

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 **Auto Channel Scan** setting can be selected to allow the DIR-655 to choose the channel with the least amount of interference.

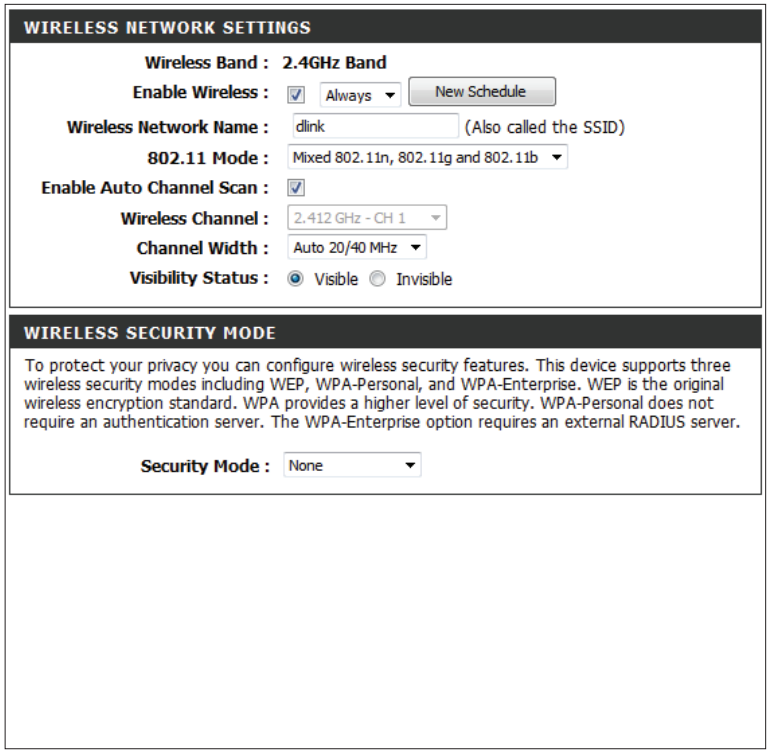
Wireless Channel: Indicates the channel setting for the DIR-655. By default the channel is set to 6. The channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

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-655. If Invisible is selected, the SSID of the DIR-655 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-655



Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-655 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.

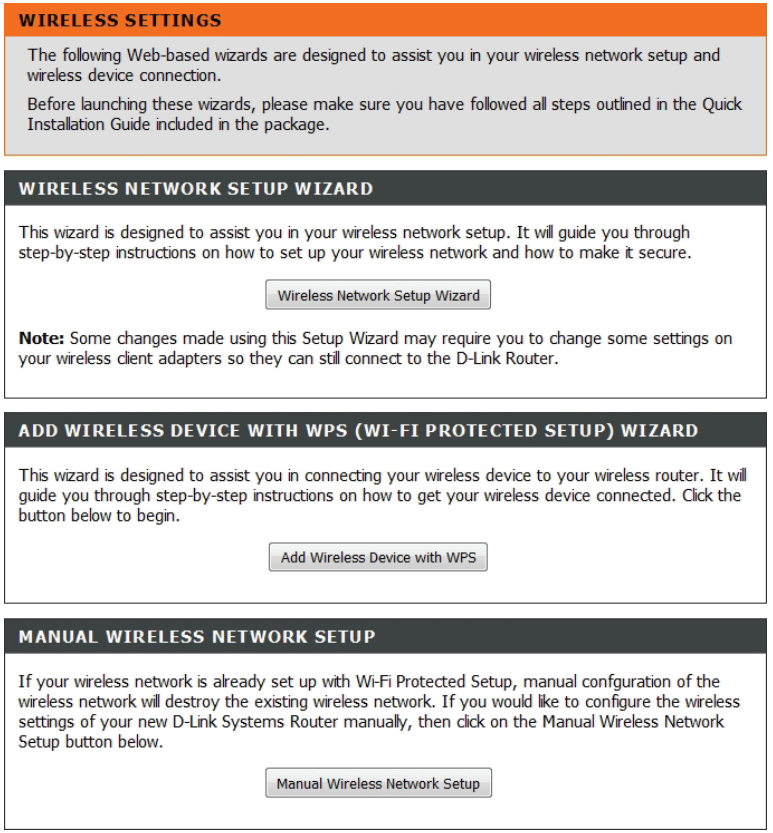
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key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

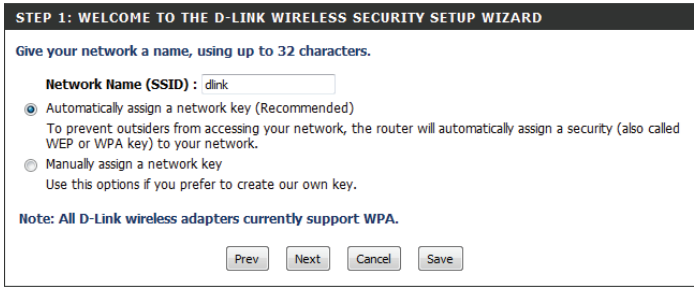
WPA/WPA2 incorporates user authentication through the Extensible Authentication Protocol (EAP). EAP is built on a more secure public key encryption system to ensure that only authorized network users can access the network.

Wireless Security Setup Wizard

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

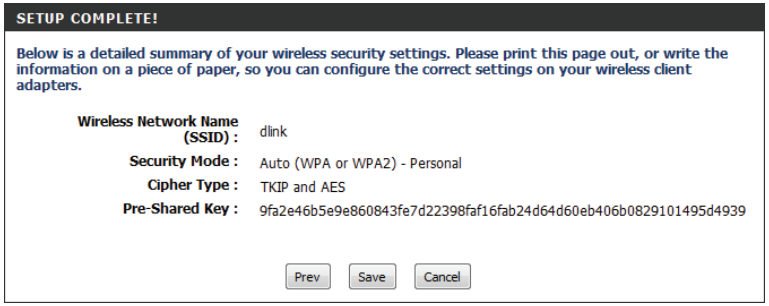


Click **Next** to continue.



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.

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.

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.

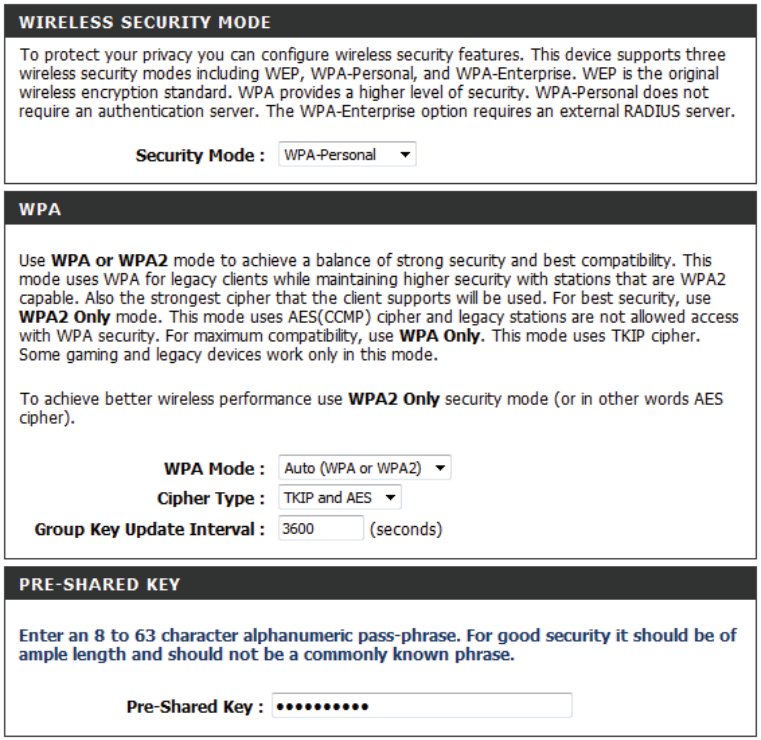
2. Next to *Security Mode*, select **WPA-Personal**.

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.



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.

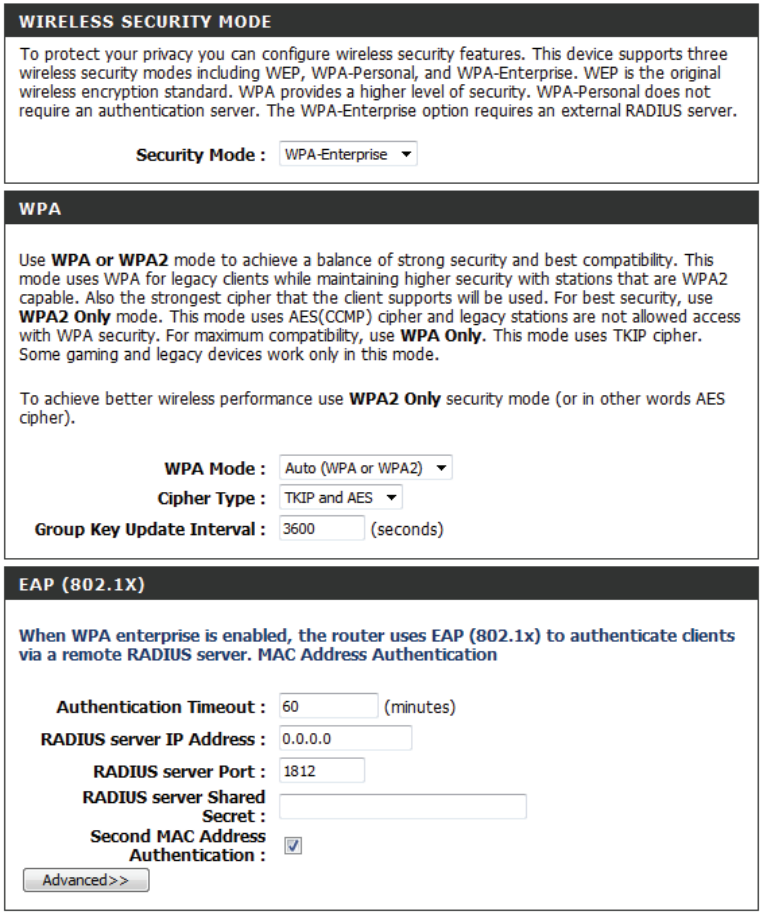
4. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

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.

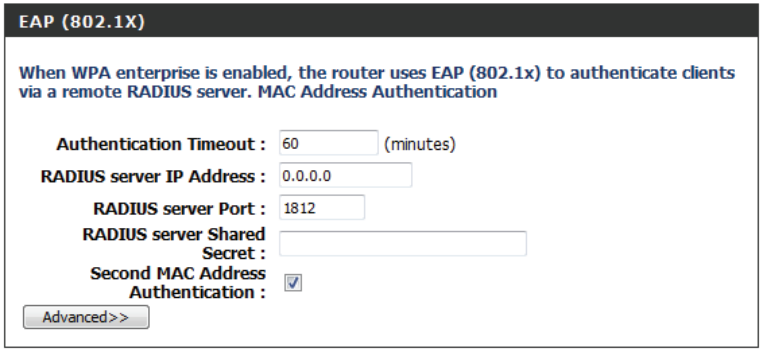
8. Next to *RADIUS Server Shared Secret*, enter the security key.



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 **Save Settings** to save your settings.



Network Settings
Router Settings

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

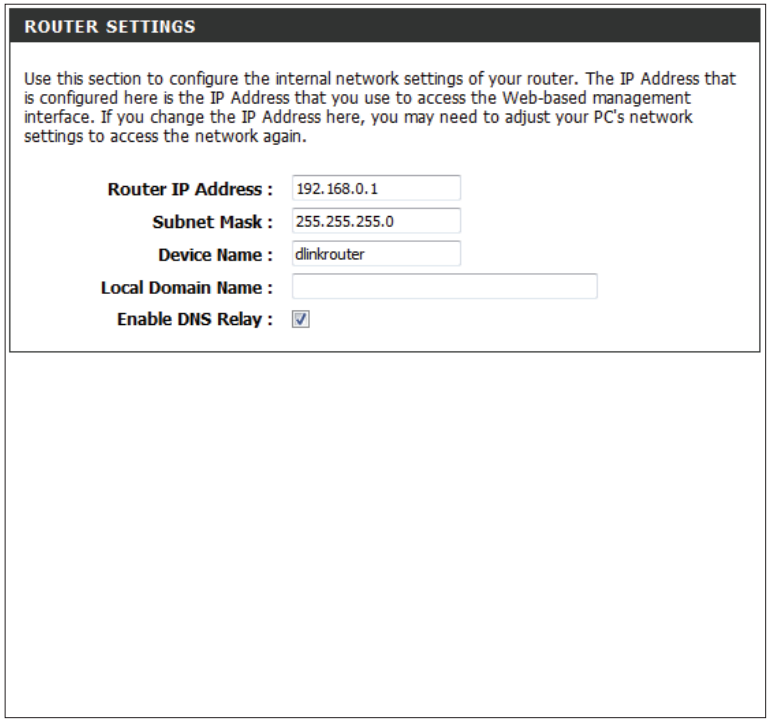
IP Address: Enter the IP address of the router. The default IP address is **192.168.0.1**.

If you change the IP address, once you click **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-655 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-655. 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.

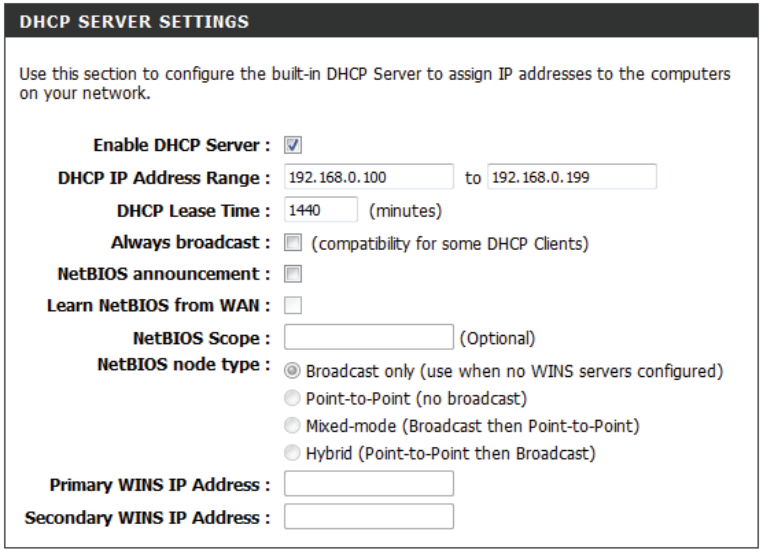
NetBIOS Announcement: NetBIOS allows LAN hosts to discover all other computers within the network, enable this feature to allow the DHCP Server to offer NetBIOS configuration settings.

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 operate. 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.

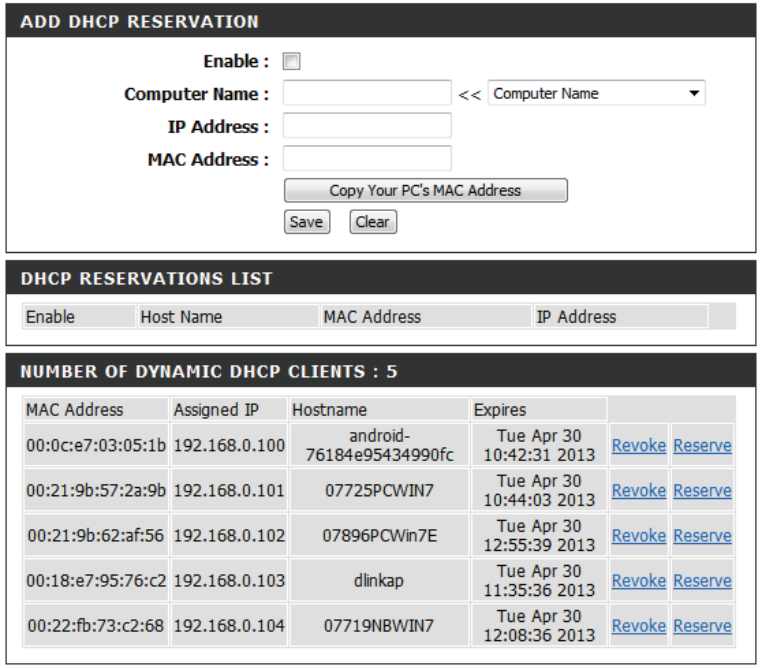
Save: Click **Save** to save your entry. You must click **Save Settings** at the top to activate your reservations.

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.



Media Server

This feature allows you to share music, pictures and videos from a USB external drive/thumb drive and/or SD card with any device connected to your network.

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

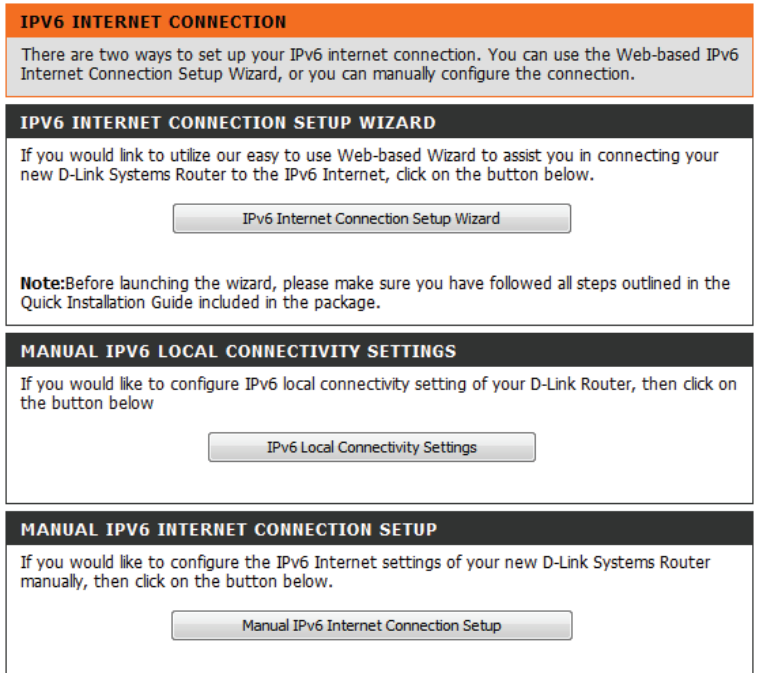
Media Server Name: Enter the media server's name.

IPv6

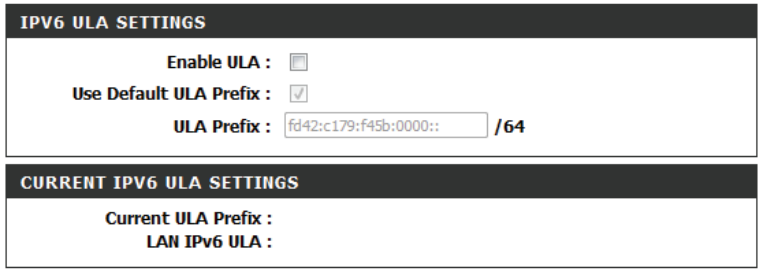
On this page, the user can configure the IPv6 connection type. There are two ways to set up the IPv6 Internet connection. You can use the web-based *IPv6 Internet Connection Setup Wizard* or you can manually configure the connection.

For the beginner user that has not configured a router before, click on the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running. Skip to the next page for details.

For the advanced user that has configured a router before, click on the **Manual IPv6 Internet Connection Setup** button to input all the settings manually. Refer to page 45 for details.



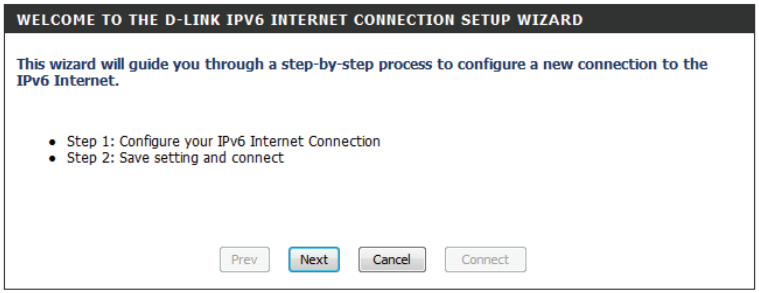
To configure the IPv6 local settings, click on the **IPv6 Local Connectivity Setup** button.



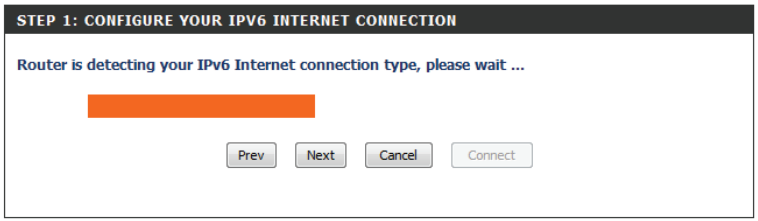
IPv6 Internet Connection Setup Wizard

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

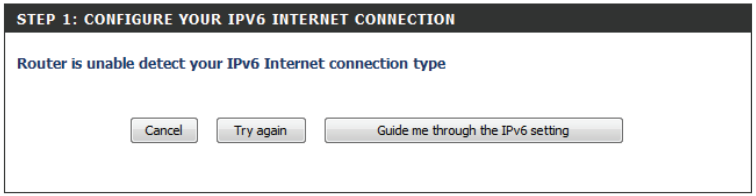
Click the **IPv6 Internet Connection Setup Wizard** button and the router will guide you through a few simple steps to get your network up and running. Click **Next** to continue to the next page. Click **Cancel** to discard the changes made and return to the main page.



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



However, if the automatic detection fails, the user will be prompted to either **Try again** or to click on the **Guide me through the IPv6 settings** button to set up IPv6 manually, with the wizard's guidance.



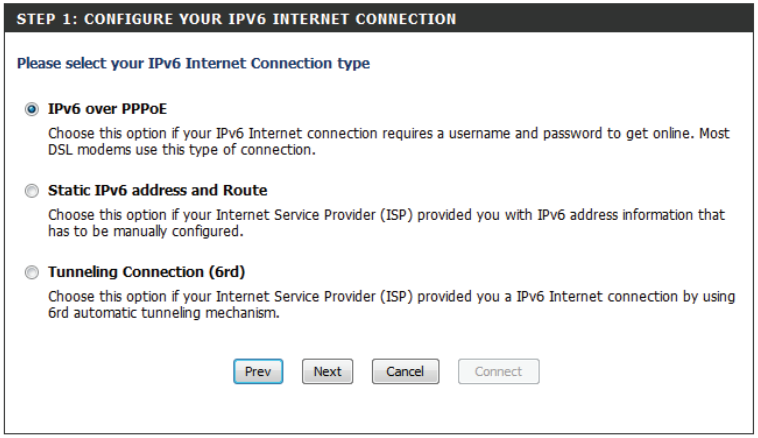
There are several connection types to choose from. If you are unsure of your connection method, please contact your IPv6 Internet service provider.

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

Choose the required *IPv6 Internet Connection* type and click on the **Next** button to continue.

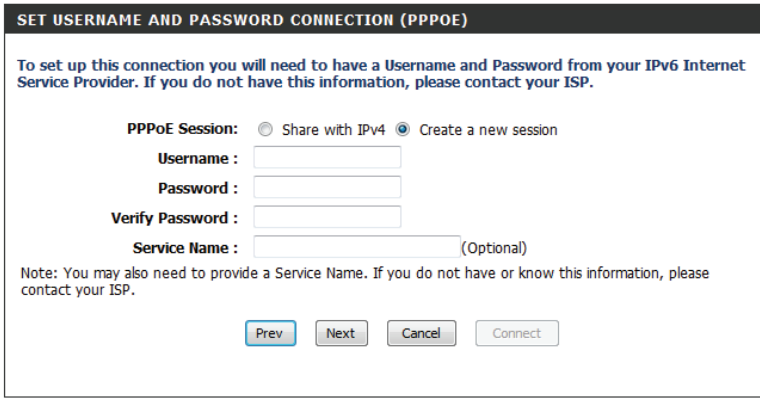
Click on the **Prev** button to return to the previous page.

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



IPv6 over PPPoE

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



The following parameters will be available for configuration:

PPPoE Session: Select the PPPoE Session type. This option will state that this connection shares its information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.

Username: Enter the PPPoE username. If you do not know your username, please contact your ISP.

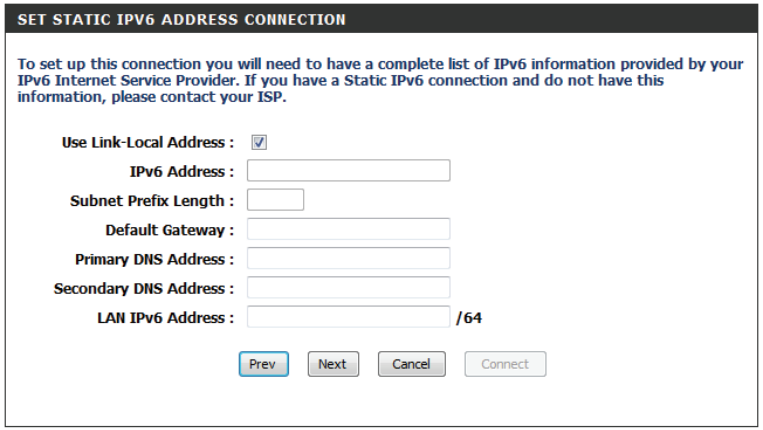
Password: Enter the PPPoE password. If you do not know your password, please contact your ISP.

Verify Password: Re-enter the PPPoE password.

Service Name: Enter the service name for this connection. (This is optional.)

Static IPv6 Address Connection

Choose **Static IPv6 Address Connection** when your ISP provides you with a set IPv6 addresses that does not change. The IPv6 information is manually entered in your IPv6 configuration settings. You must enter the IPv6 address, Subnet Prefix Length, Default Gateway, Primary DNS Server and Secondary DNS Server. Your ISP provides you with all of this information.



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

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

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

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

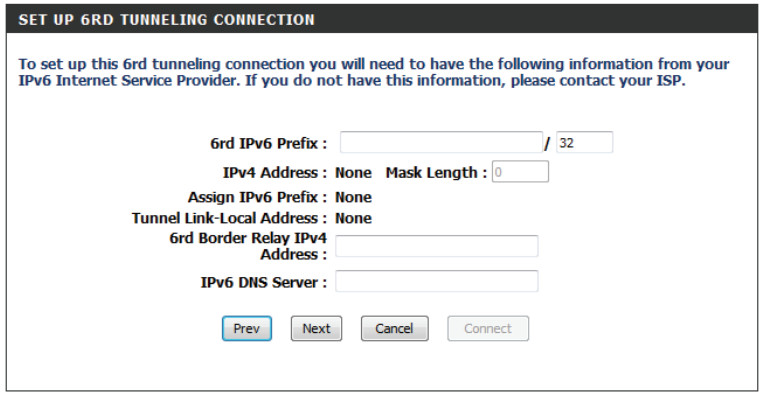
Primary DNS Address: Enter the WAN primary DNS Server address used here.

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

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

Tunneling Connection (6rd)

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



The following parameters will be available for configuration:

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

IPv4 Address: Enter the IPv4 address used here.

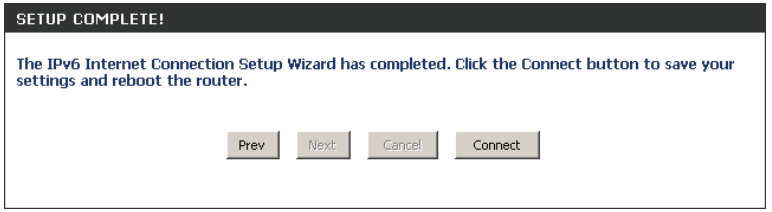
Mask Length: Enter the IPv4 mask length used here.

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

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

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

When the setup wizard is complete, click on the **Connect** button to continue. Click on the **Prev** button to return to the previous page. Click on the **Cancel** button to discard all the changes made and return to the main page.



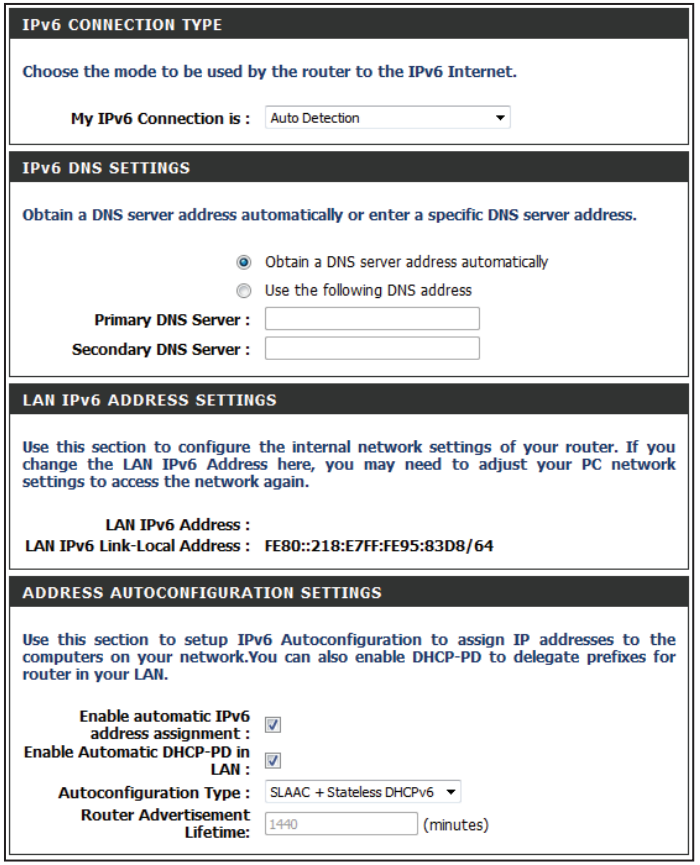
IPv6 Manual Setup

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

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

Auto Detection

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



Static IPv6

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

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.

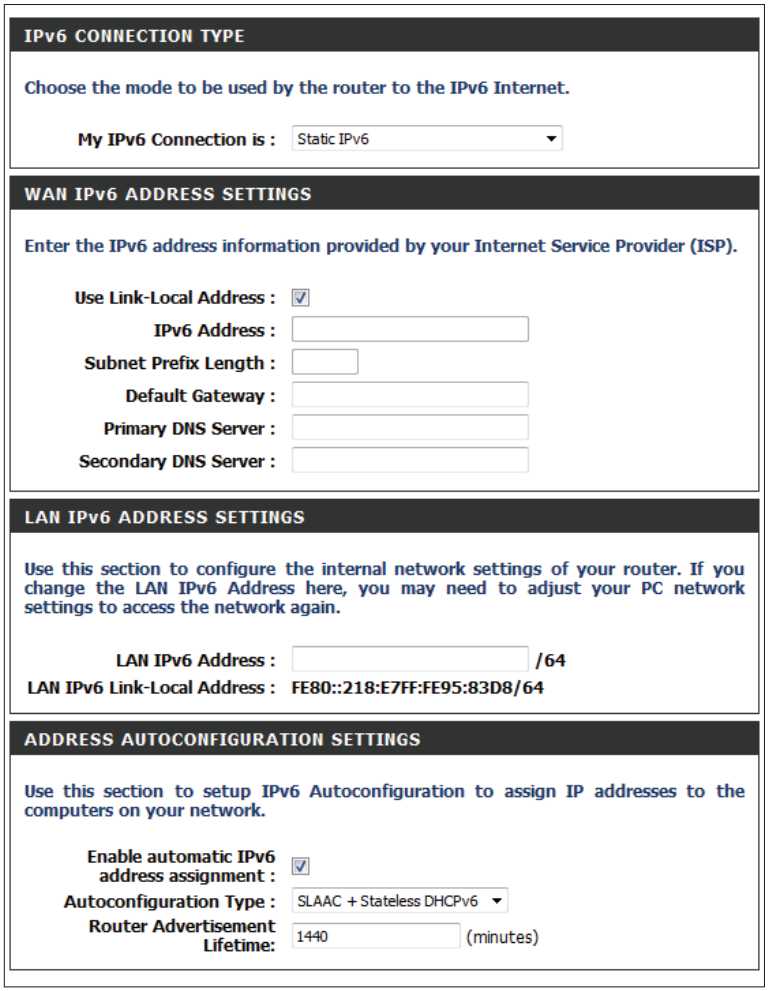
Enable Automatic IPv6 Address Assignment: Check to enable the autoconfiguration feature.

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

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).



Autoconfiguration

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

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

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

Enable DHCP-PD: Check to enable the DHCP-PD feature.

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

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

Enable Automatic IPv6 Address Assignment: Check to enable the autoconfiguration feature.

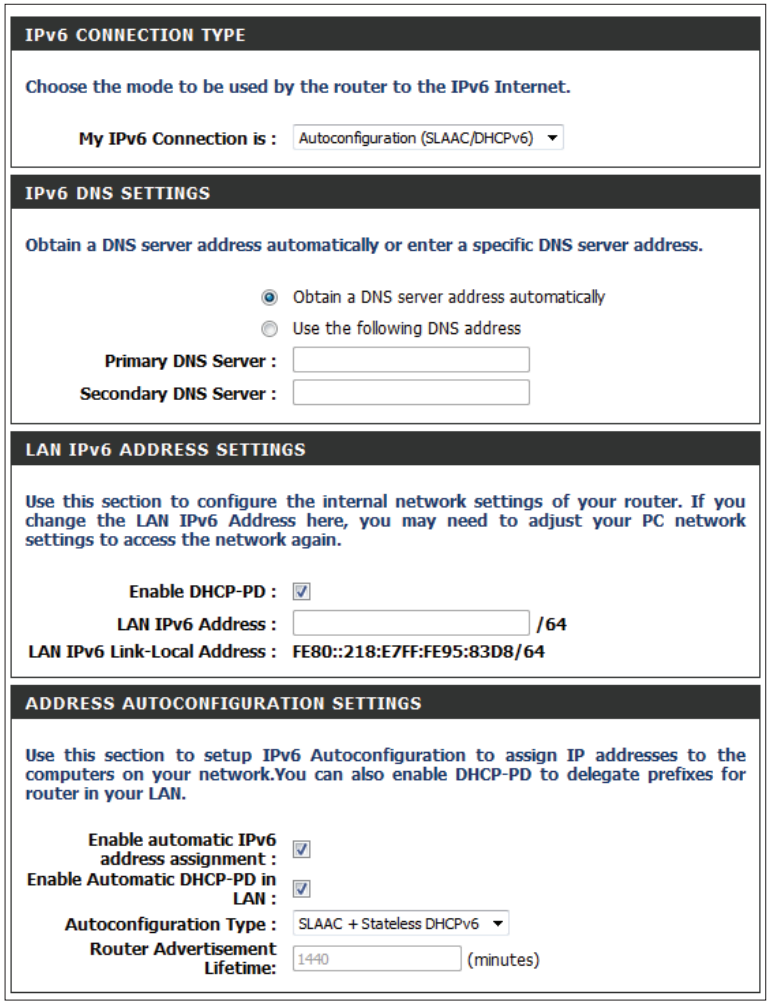
Enable Automatic DHCP-PD in LAN: Check to enable automatic DHCP-PD in LAN.

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

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).



PPPoE

My IPv6 Connection: 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**.

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

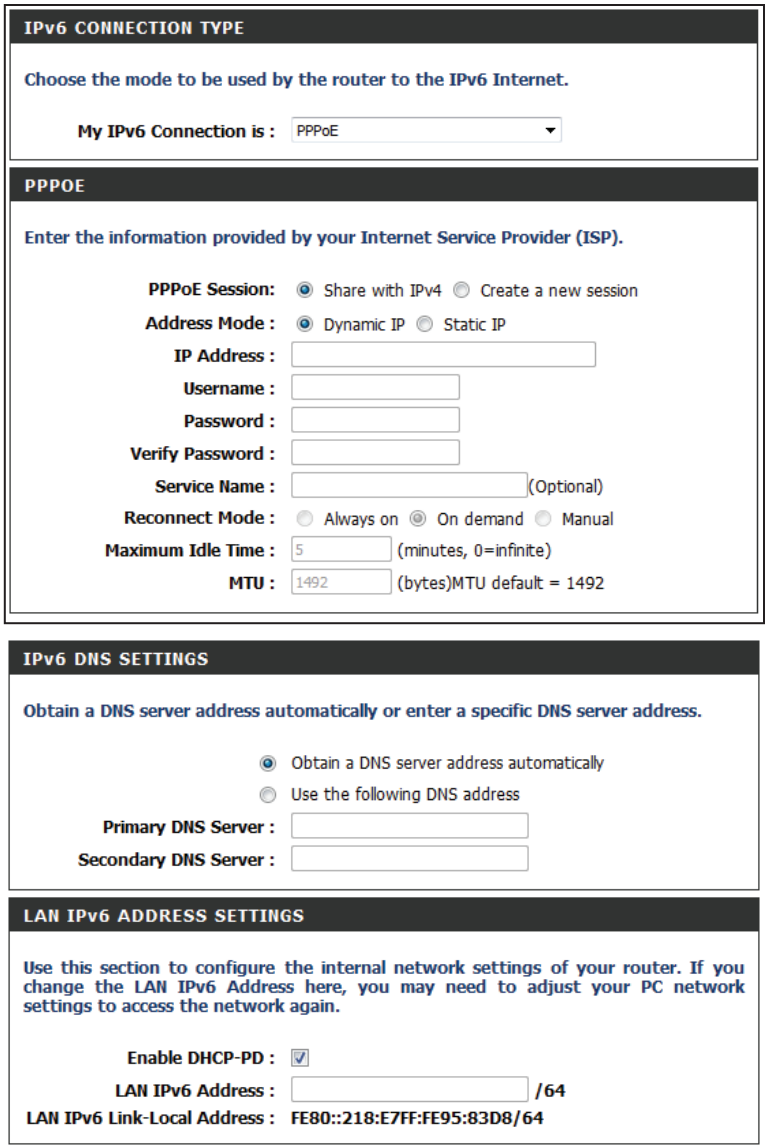
IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

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

Enable DHCP-PD: Check to enable the DHCP-PD feature.

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

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



Enable Automatic IPv6 Address Assignment: Check to enable the autoconfiguration feature.

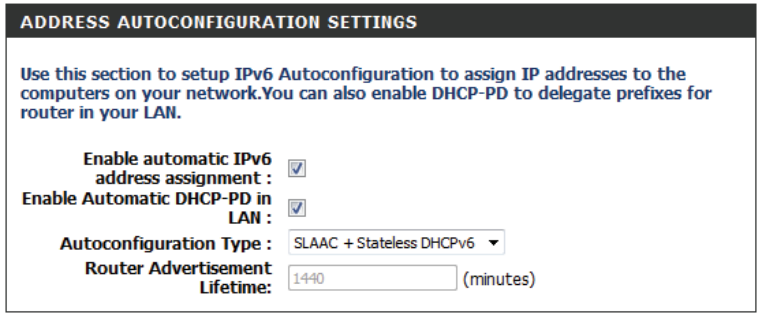
Enable Automatic DHCP-PD in LAN: Check to enable automatic DHCP-PD in LAN.

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

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 in IPv4 Tunneling

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).

IPv6 DNS Settings: Automatically obtain a DNS server address or enter a specific DNS address.

Enable DHCP-PD: Check to enable the DHCP-PD feature.

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

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

Enable Automatic IPv6 Address Assignment: Check to enable automatic IPv6 address assignment.

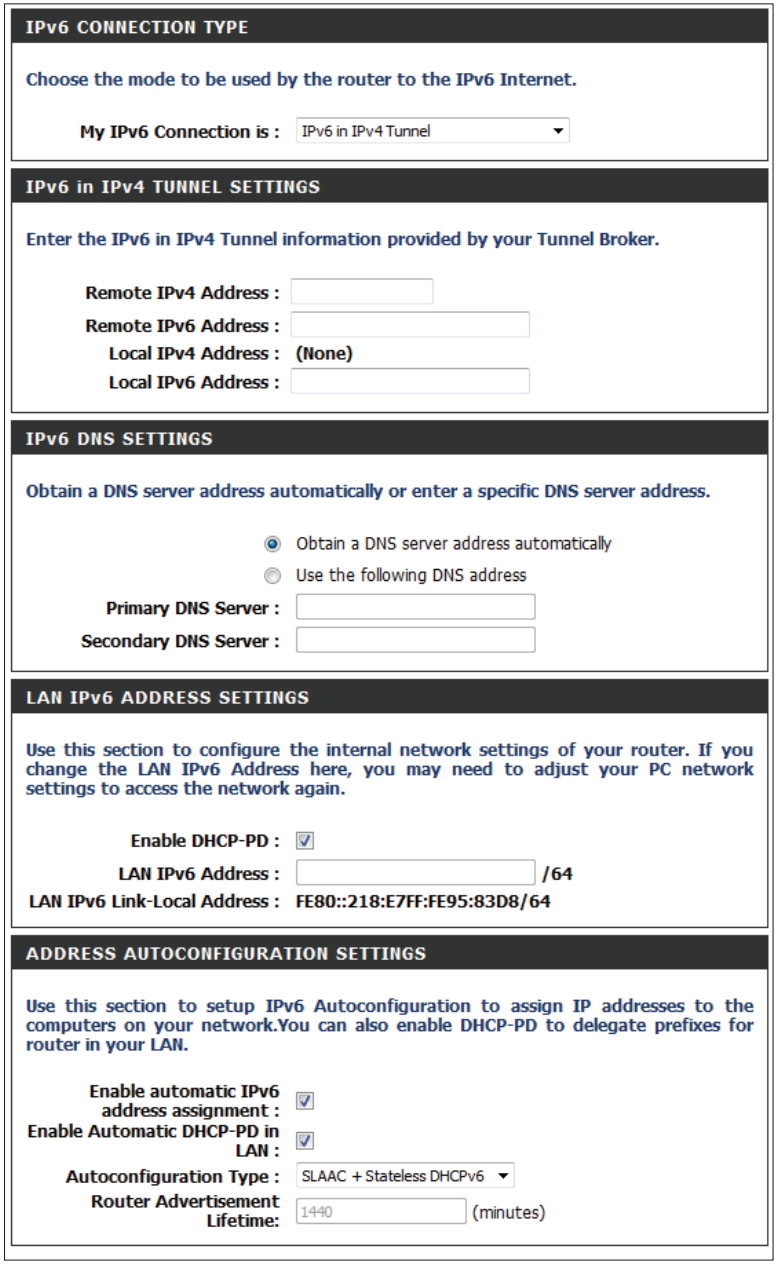
Enable Automatic DHCP-PD in LAN: Check to enable automatic DHCP-PD in LAN.

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

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).



6to4 Tunneling

My IPv6 Connection: Select **6to4** from the drop-down menu.

6to4 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.

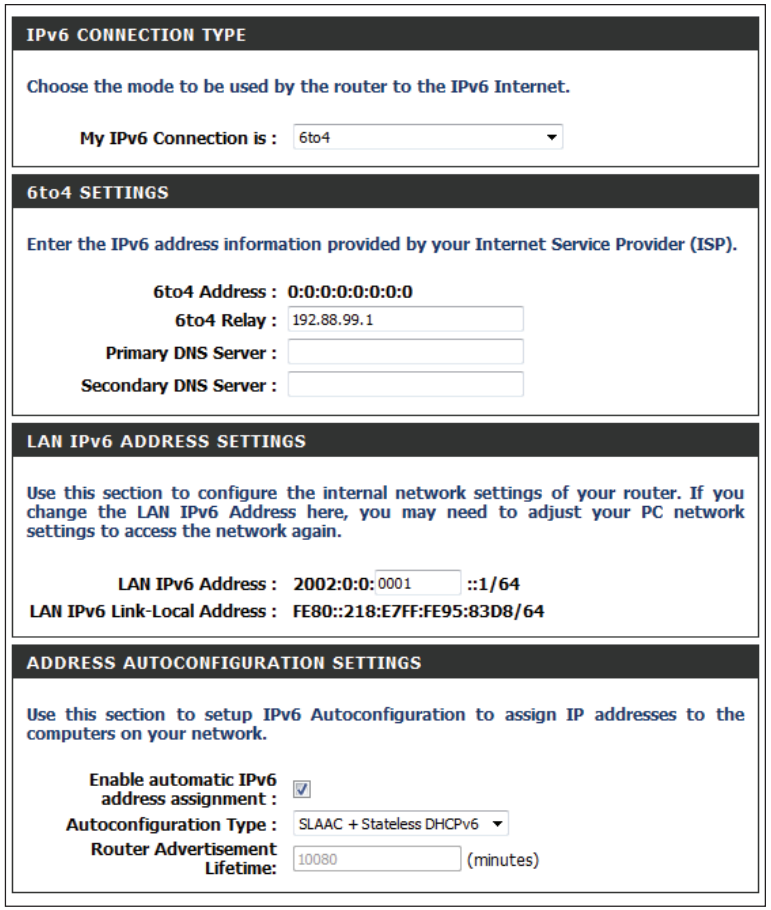
Enable Automatic DHCP-PD in LAN: Check to enable the autoconfiguration feature.

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

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).



6rd

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

6rd 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.

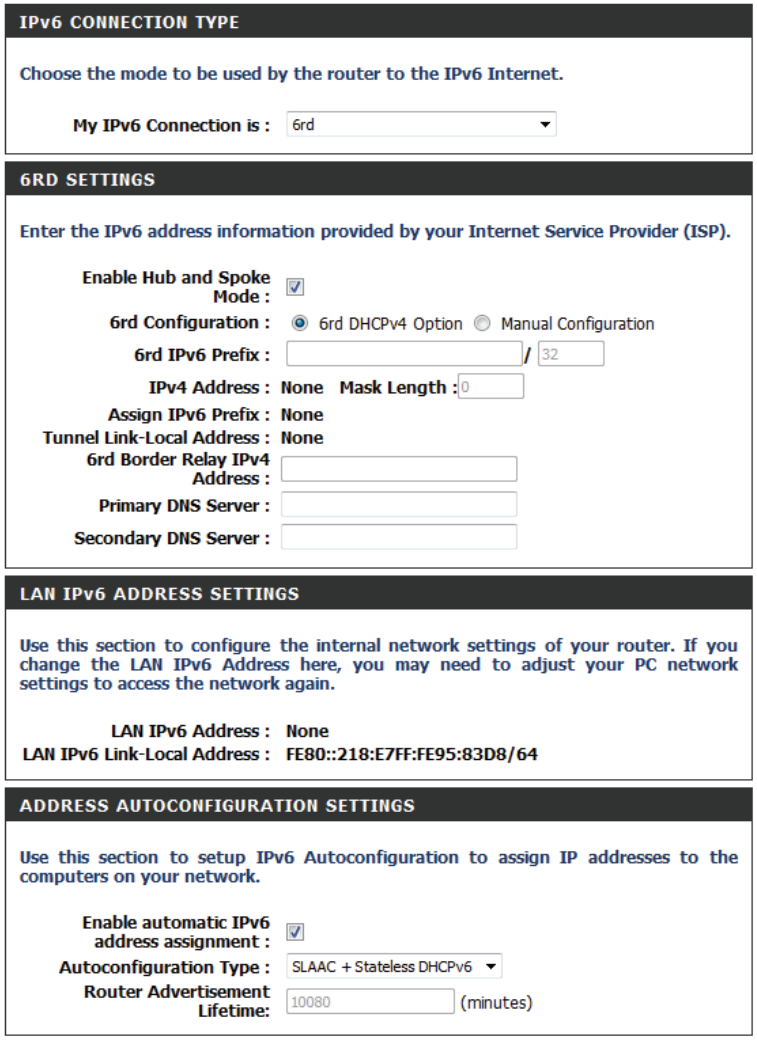
Enable Automatic DHCP-PD in LAN: Check to enable the autoconfiguration feature.

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

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.

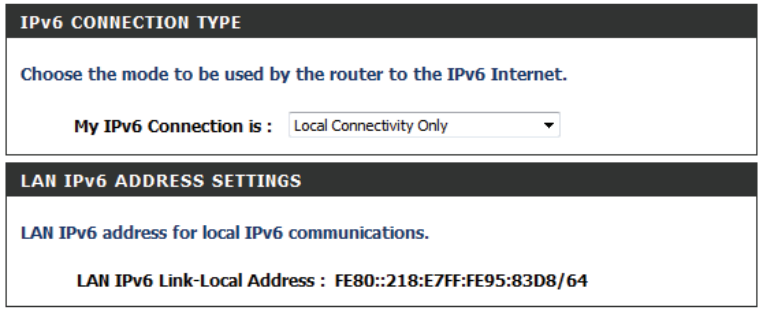
Router Advertisement Lifetime: Enter the router advertisement lifetime (in minutes).



Local Connectivity Only

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

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



Advanced Settings
Virtual Server

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

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

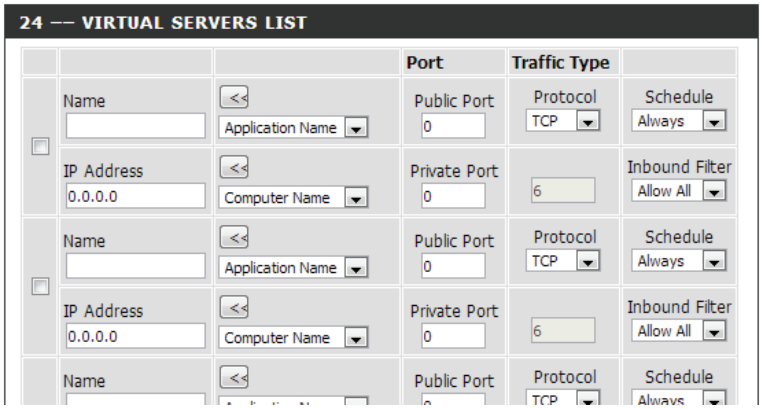
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the *Computer Name* drop-down menu. Select your computer and click **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

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

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

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

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



Port Forwarding

This will allow you to open a single port or a range of ports.

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.

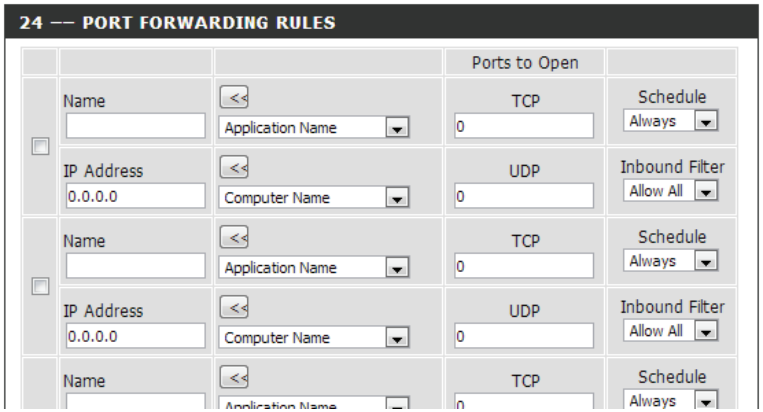
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the **Computer Name** drop-down menu. Select your computer and click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

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. Separate ports with a comma.

Example: 24,1009,3000-4000

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

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



Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). *Application Rules* makes some of these applications work with the DIR-655. 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-655 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 **<<**.

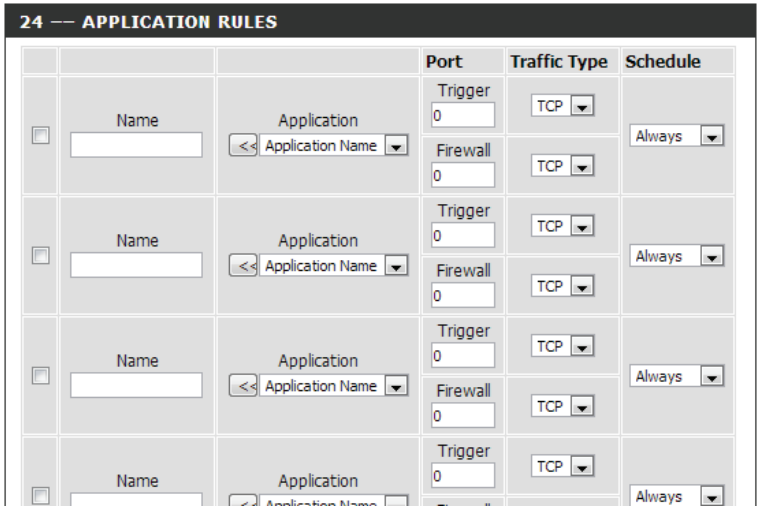
Trigger: This is the port used to trigger the application. It can be either a single port or a range of ports.

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* 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 note 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 *speedtest.net*.

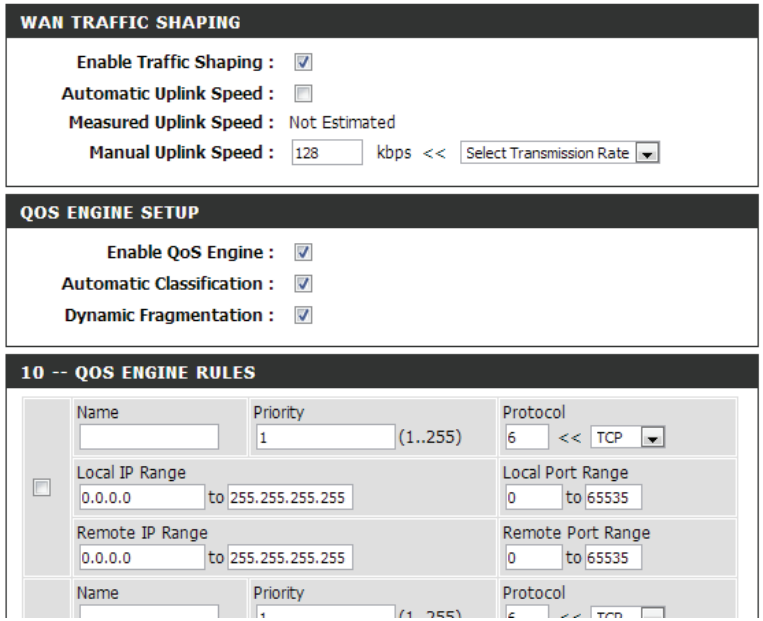
Enable QoS Engine: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Classification: This option is enabled by default so that your router will automatically determine which programs should have network priority. For best performance, use the Automatic Classification option to automatically set the priority for your applications.

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.

QoS Engine Rules: A QoS Engine rule identifies a specific message flow and assigns a priority to that flow. For most applications, automatic classification will be adequate and specific QoS Engine rules will not be required.

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



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

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

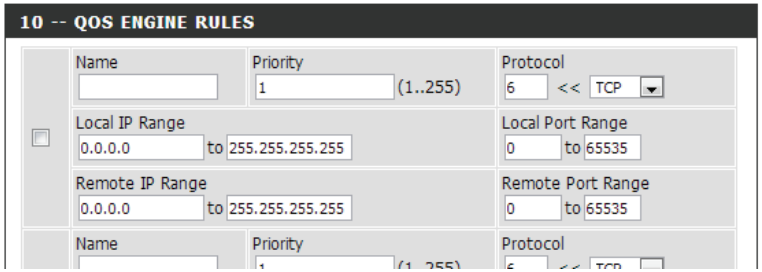
Protocol: The protocol used by the messages.

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

Local Port Range: The rule applies to a flow of messages whose LAN-side port number is within the range set here.

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

Remote Port Range: The rule applies to a flow of messages whose WAN-side port number is within the range set here.



Network Filter

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 router.

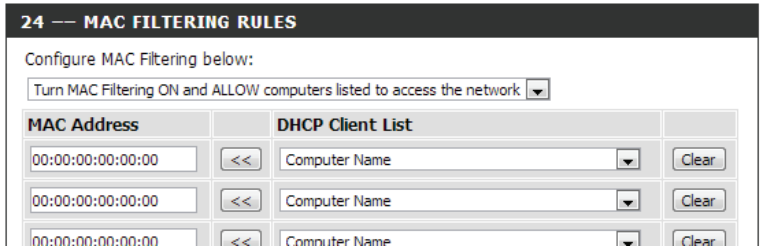
Configure MAC Filtering: Select **Turn MAC Filtering Off**, **Allow MAC addresses listed below**, or **Deny MAC addresses listed below** from the drop-down menu.

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

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

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

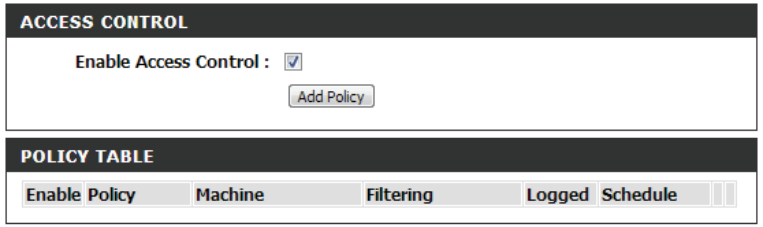
Clear: Click to remove the MAC address.



Access Control

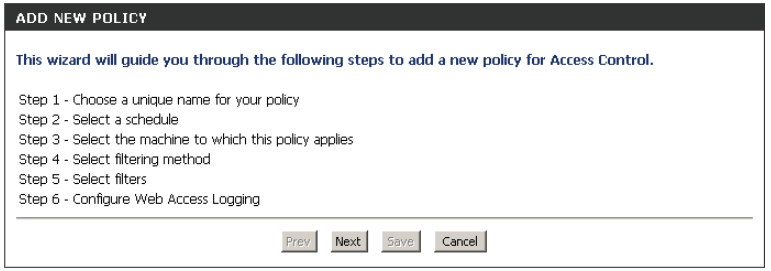
The *Access Control* section allows you to control access in and out of your network. Use this feature as "Parental Controls" to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

Add Policy: First, click the **Enable Access Control** box. Next, click the **Add Policy** button to start the *Access Control Wizard*.



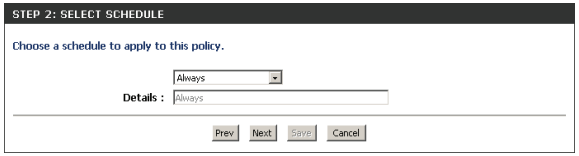
Access Control Wizard

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



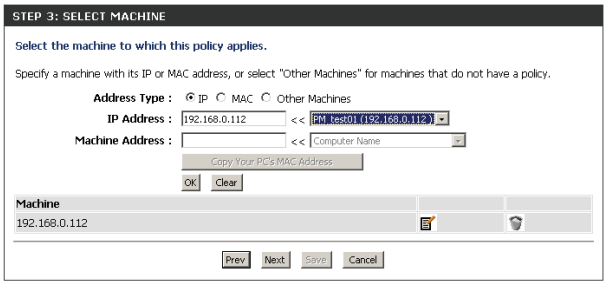
Enter a name for the policy and then click **Next** to continue.

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



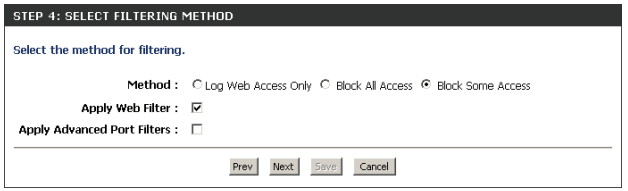
Enter the following information and then click **Next** to continue:

- **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.
- **Machine Address** - Enter the PC MAC address (i.e., 00:00.00.00.00).



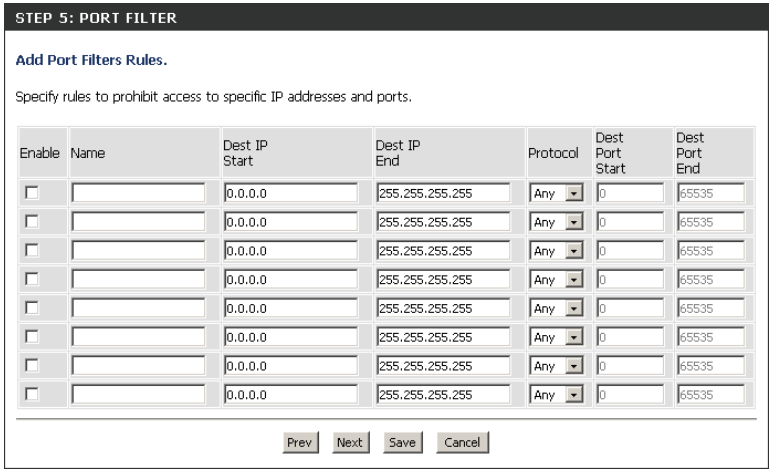
Select the filtering method and then click **Next** to continue.

Note: *If you select the* ***Apply Advanced Port Filters*** *option you will be forwarded to the* ***Add Port Filters Rules*** *window. Otherwise, you will be advanced to the* ***Configure Web Access Logging*** *window (see next page).*



Enter the rule:

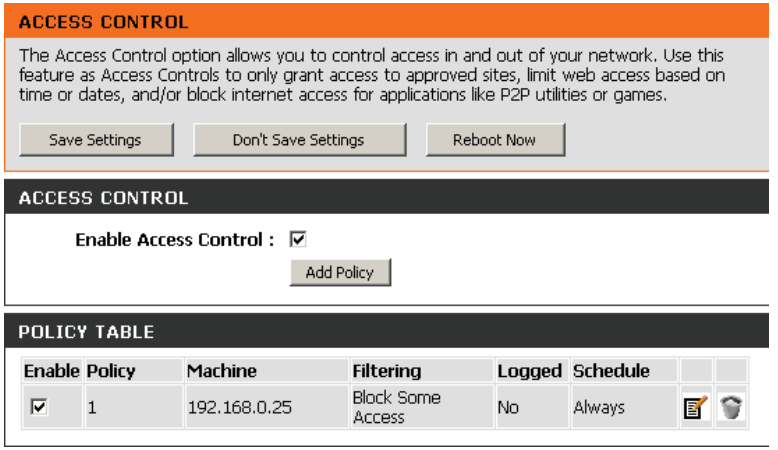
Enable - Check to enable the rule.
Name - Enter a name for your rule.
Dest IP Start - Enter the starting IP address.
Dest IP End - Enter the ending IP address.
Protocol - Select the protocol.
Dest Port Start - Enter the starting port number.
Dest Port End - Enter the ending port number.



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

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

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

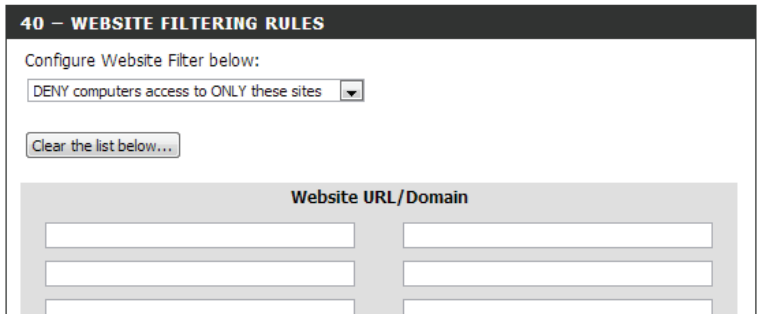


Website Filter

Website Filters are used to allow you to set up a list of websites that can be viewed by multiple users through the network. To use this feature, select to **Allow** or **Deny**, enter the domain or website and click **Save Settings**. You must also select **Apply Web Filter** under the *Access Control* section (page 60).

Add Website Filtering Rule: Select either **DENY computers access to ONLY these sites** or **ALLOW computers access to ONLY these sites**.

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



Inbound Filter

The *Inbound Filter* feature provides 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**.

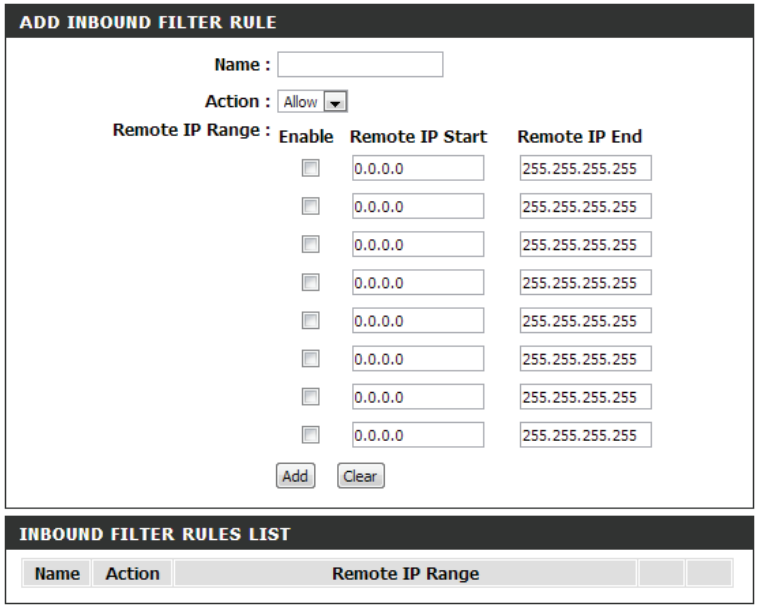
Enable: Check to enable the rule.

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

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

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

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



Firewall Settings

A firewall protects your network from the outside world. The DIR-655 offers a firewall type functionality. The *Stateful Packet Inpection* (*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 can 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.

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

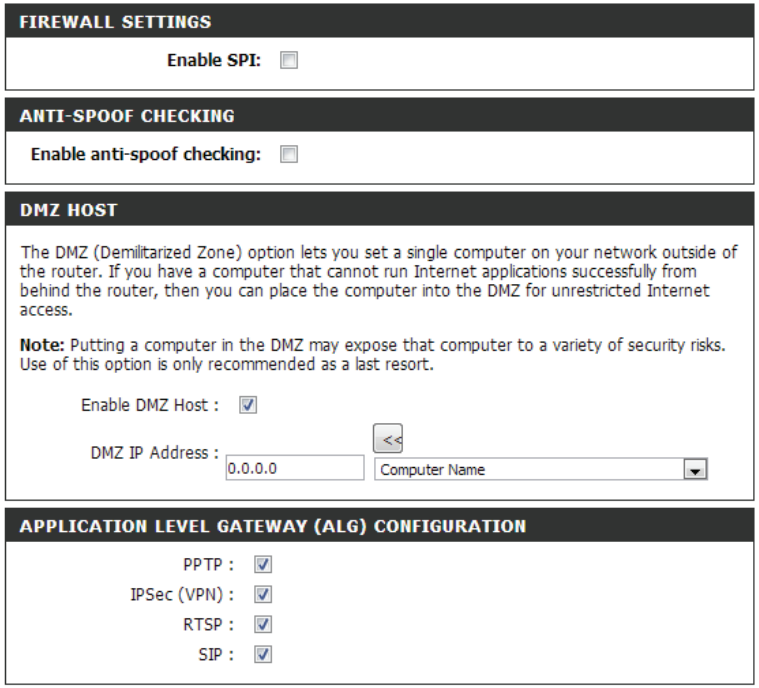
Enable DMZ: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

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.*

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

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

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



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

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

Routing

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

Name: Enter a name for your route.

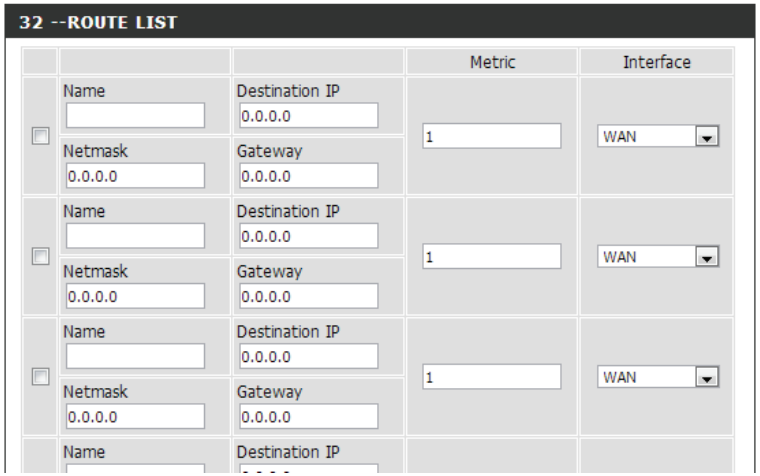
Destination IP: Enter the IP address of packets that will take this route.

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

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

Metric: The route metric is a value from 1 to 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

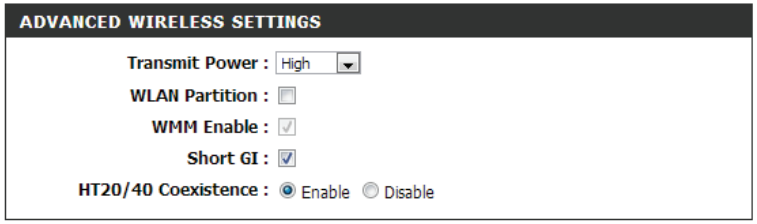
Transmit Power: Set the transmit power of the antennas.

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

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

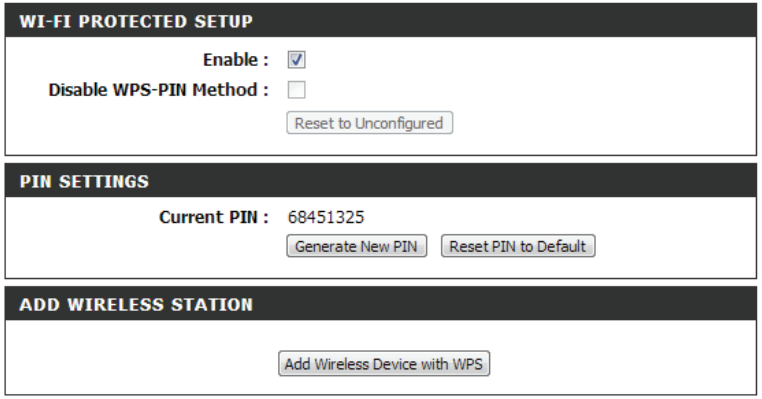
Short GI: Check this box to reduce the guard interval time therefore increasing the data capacity. However, it's less reliable and may create higher data loss.

HT20/40 Coexistence: Enable this option to reduce interference from other wireless networks in your area. If the channel width is operating at 40MHz and there is another wireless network's channel over-lapping and causing interference, the router will automatically change to 20MHz.



Wi-Fi Protected Setup (WPS)

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



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

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

Disable WPS-PIN Method: Disabling 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 PIN.

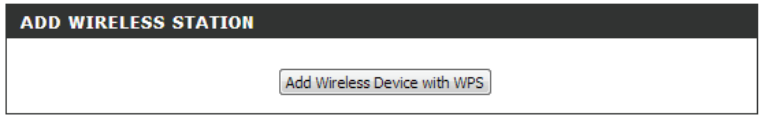
Generate New PIN: Create a random number that is a valid PIN. This becomes the router's PIN. You can then copy this PIN to the user interface of the registrar.
This wizard helps you add wireless devices to the wireless network.

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

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



Advanced Network Settings

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

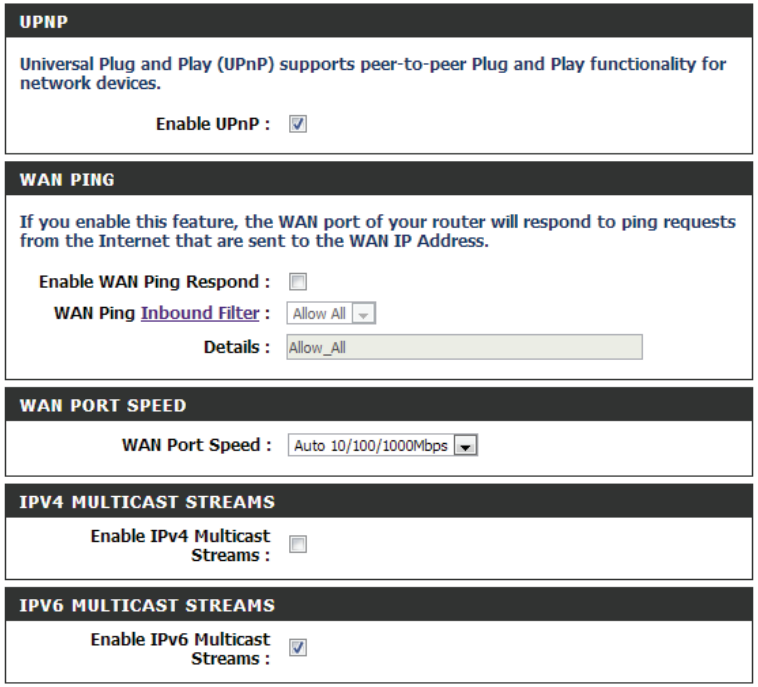
WAN Ping: Checking the box will allow the DIR-655 to respond to pings. Unchecking the box may provide some extra security from hackers.

WAN Ping Inbound Filter: Select from the drop-down menu if you would like to apply the *Inbound Filter* to the WAN ping. Refer to the *Inbound Filters* section for more information.

WAN Port Speed: You may set the port speed of the Internet port to **10Mbps**, **100Mbps**, **1000Mbps** or **Auto** (recommended).

Enable IPV4 Multicast Streams: Check the box to allow multicast traffic to pass through the router from the Internet (IPv4).

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



Guest Zone

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

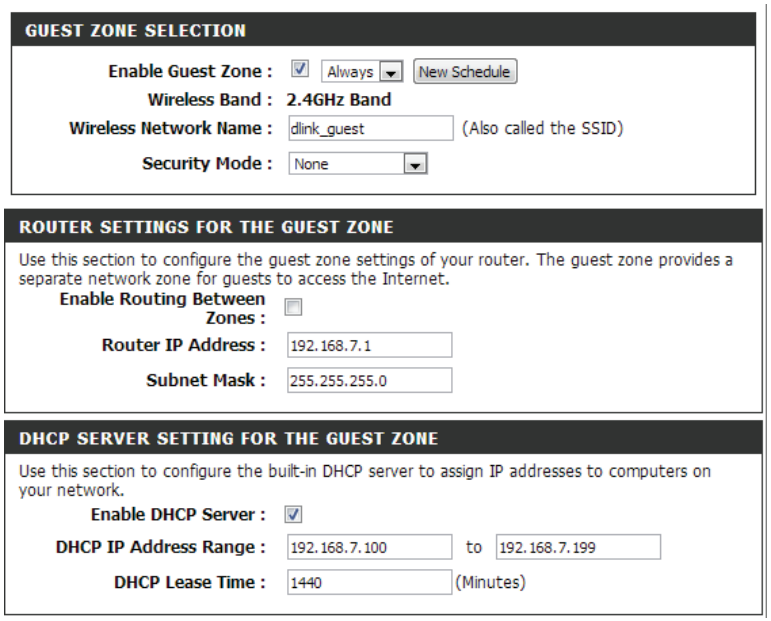
Enable Guest Zone: Check to enable the *Guest Zone* feature.

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

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

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

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



IPv6 Firewall

The DIR-655's *IPv6 Firewall* feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-655's *IPv6 Firewall* functions in a similar way to the *Inbound Filters* feature.

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

Enable IPv6 Ingress Filtering: Check to enable IPv6 ingress filter.

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

Name: Enter a name to identify the *IPv6 Firewall Rule*.

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

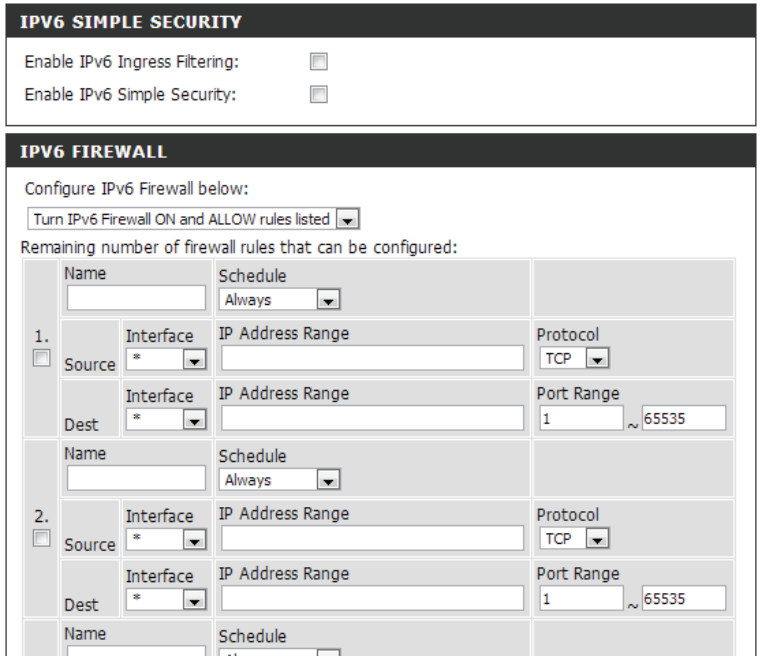
Source: Use the *Source* drop-down menu to specify the interface that connects to the source IPv6 addresses of the firewall rule.

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

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

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

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



IPv6 Routing

The *IPv6 Routing* section allows you to specify custom routes that determine how data is moved around your network.

Route List: Check the box next to the route you wish to enable.

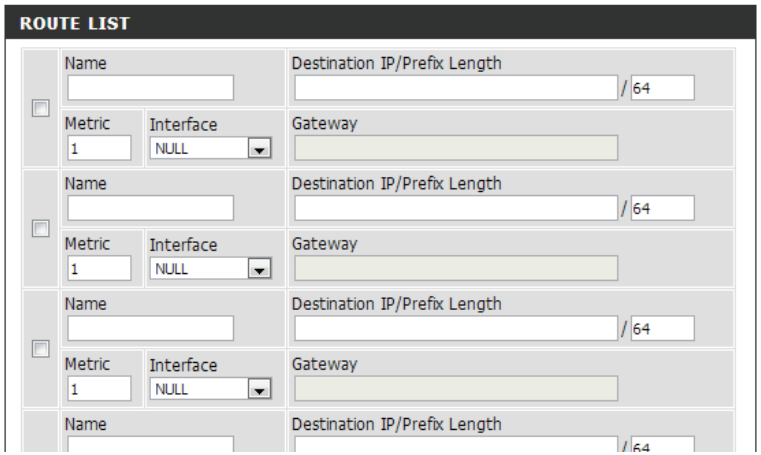
Name: Enter a specific name to identify this route.

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

Metric: Enter the metric value for this rule here.

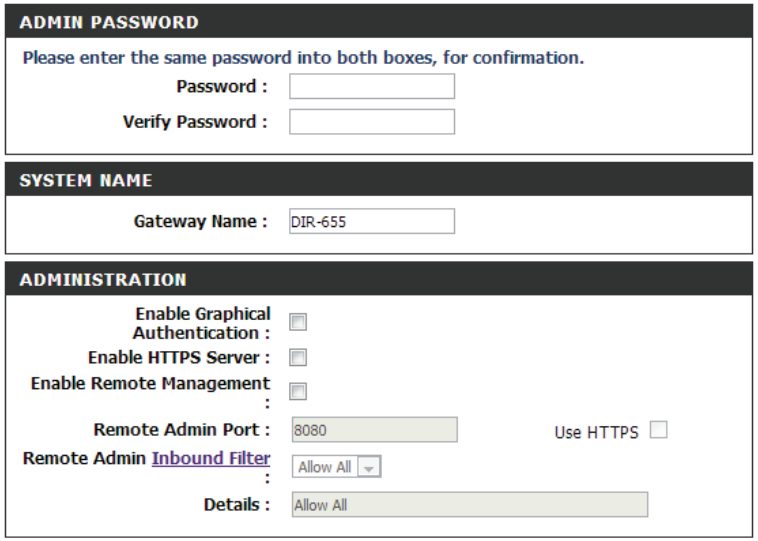
Interface: Use the drop-down menu to specify if the IP packet must use the WAN or LAN interface to transit out of the router.

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



Tools
Admin

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



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

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).

System Name: Enter a name for your router.

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

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

Enable Remote Management: R*emote Management* allows the DIR-655 to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

Remote Admin Port: The port number used to access the DIR-655 is used in the URL. Example: **http://x.x.x.x:8080** whereas x.x.x.x is the Internet IP address of the DIR-655 and 8080 is the port used for the Web Management interface.

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

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

Time

The *Time Configuration* section 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: Displays the current date and time of the router.

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

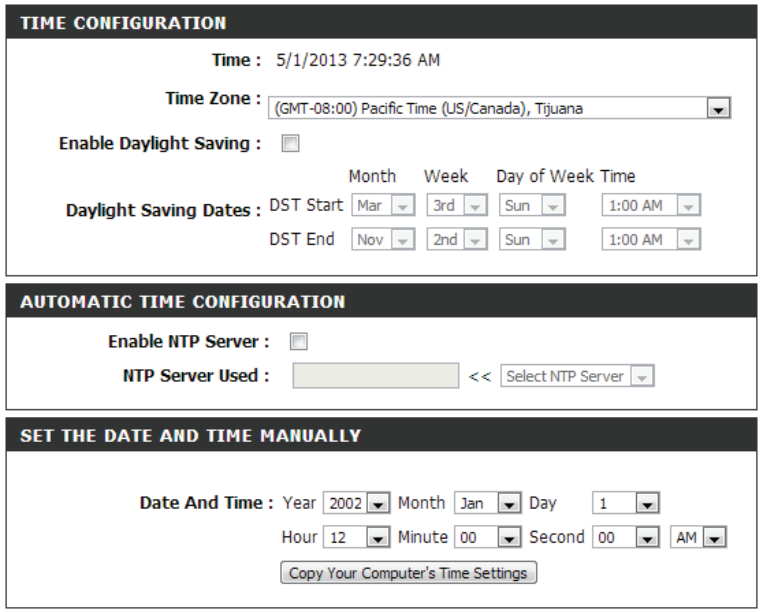
Enable Daylight Saving: To enable Daylight Saving time manually, check the box and enter a start date and an end date for daylight saving time.

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

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

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** to synch the date and time with the computer you are currently on.



SysLog

The DIR-655 keeps a running log of events and activities occurring. 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).

E-mail Settings

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

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

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

To E-mail 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.

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

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

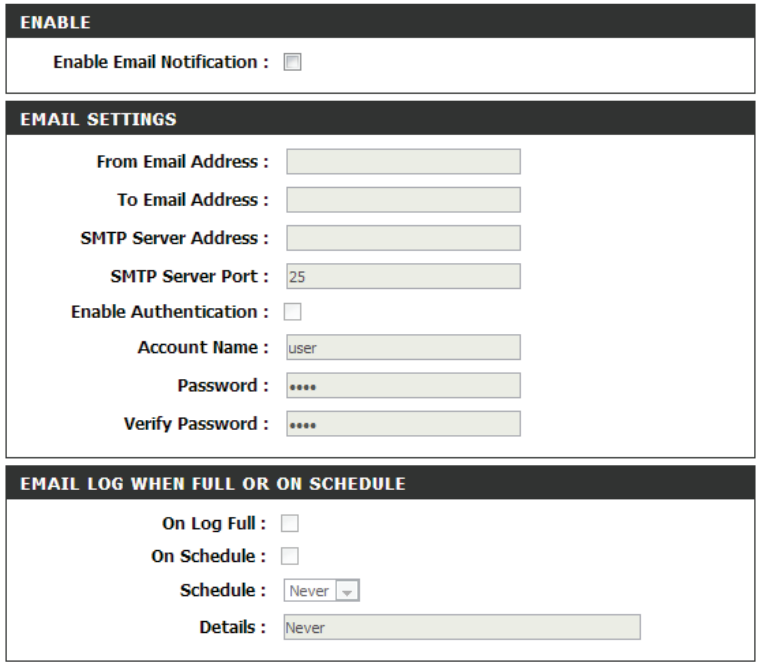
Account Name: Enter your account for sending e-mail.

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

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

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

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



System

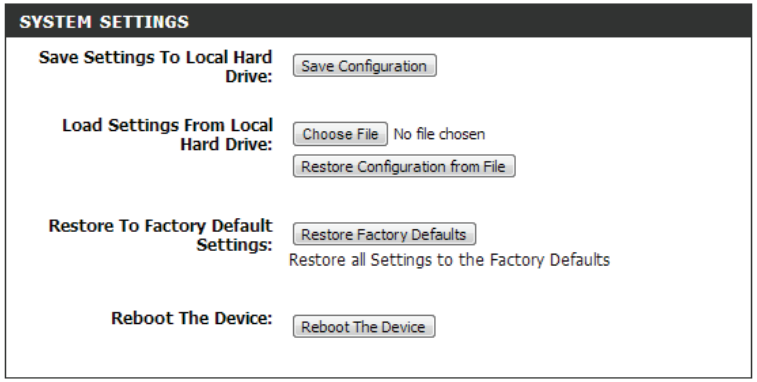
The *System Settings* section allows you to manage the router's configuration settings, reboot the router, and restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings, including any rules that you've created.

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

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

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

Reboot Device: Click to reboot the router.



Firmware

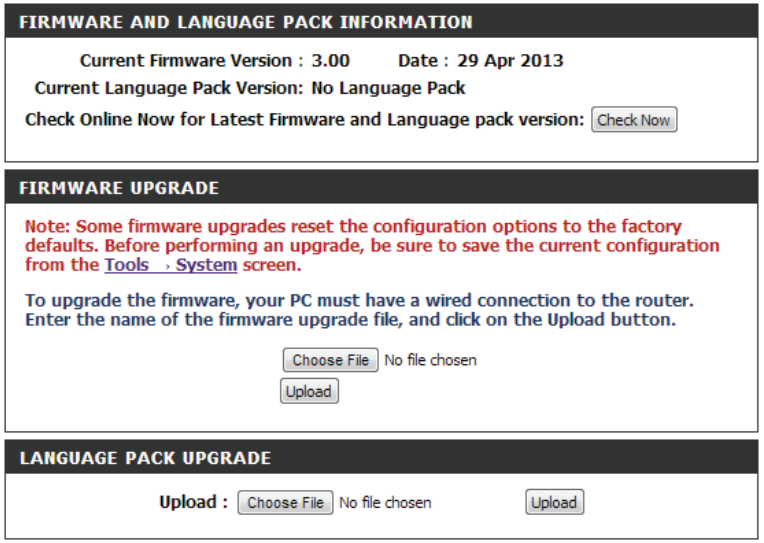
The *Firmware Update* section allows you to upgrade the firmware of the DIR-655. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to locate the firmware file to be used for the update. Please check the D-Link support website for firmware updates at **http://support.dlink.com**. You can download firmware upgrades to your hard drive from this site.

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

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

Language Pack Upgrade: You can change the language of the web UI by uploading available language packs.

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



Dynamic DNS

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

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

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

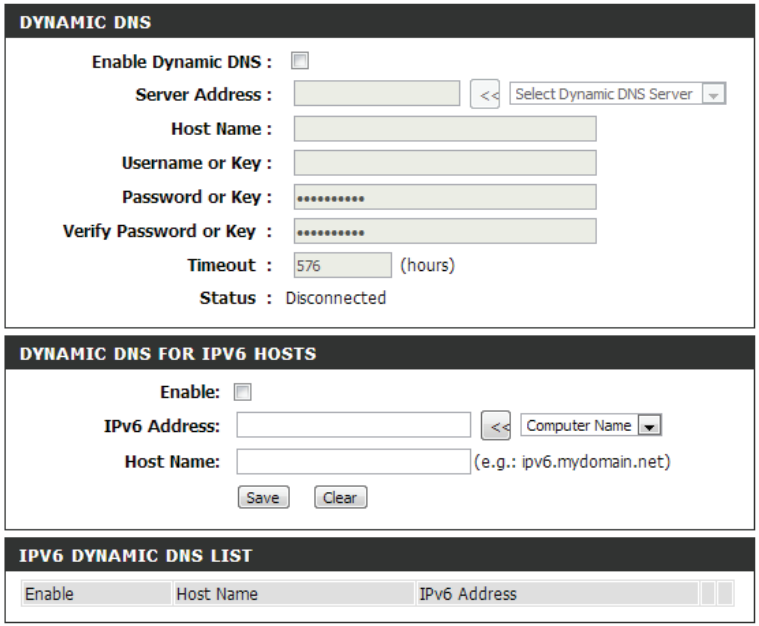
Host Name: Enter the host name that you registered with your DDNS service provider.

Username or Key: Enter the username or key for your DDNS account.

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

Timeout: Enter a timeout time (in hours).

Status: Displays the current connection status.

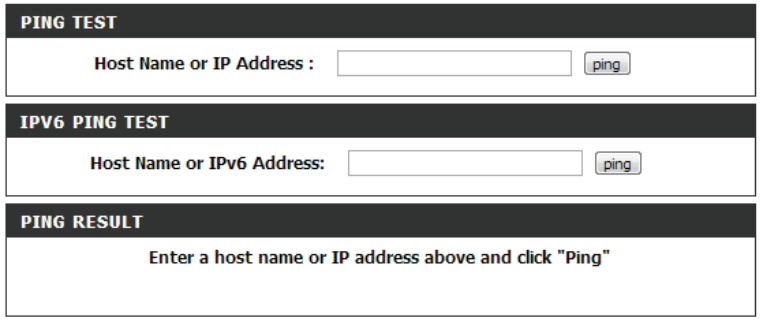


System Check

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

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

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



Schedules

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

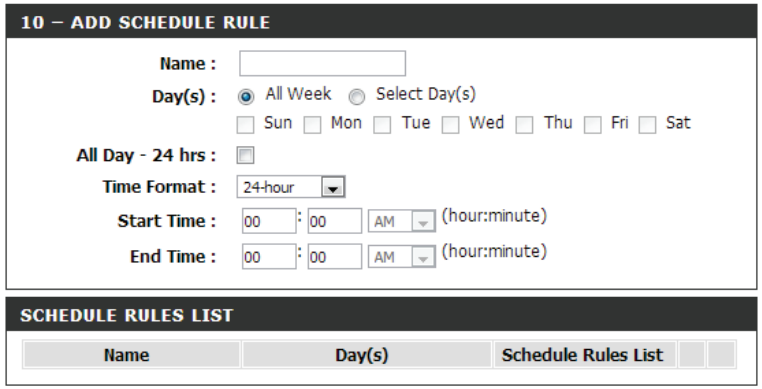
Name: Enter a name for your new schedule.

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

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

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

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



Status
Device Info

The *Device Info* page displays the current information for the DIR-655. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

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

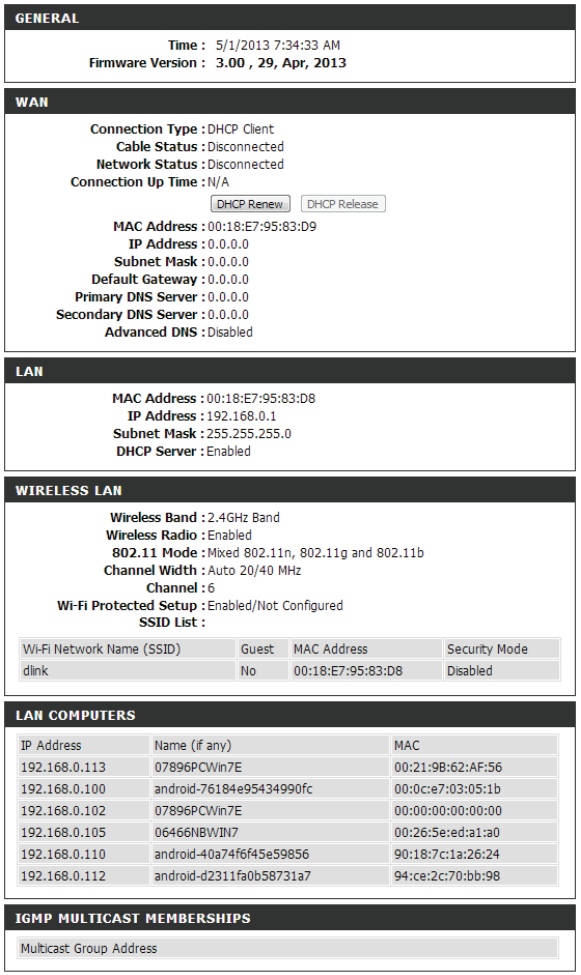
General: Displays the router's time and firmware version.

WAN: Displays the MAC address and the public IP settings

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

Wireless LAN1: Displays the 2.4GHz 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).



GENERAL

Time : 5/1/2013 7:34:33 AM
Firmware Version : 3.00 , 29, Apr, 2013

WAN

Connection Type : DHCP Client
Cable Status : Disconnected
Network Status : Disconnected
Connection Up Time : N/A
DHCP Renew | DHCP Release
MAC Address : 00:18:E7:95:83:D9
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0
Advanced DNS : Disabled

LAN

MAC Address : 00:18:E7:95:83:D8
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

Wireless Band : 2.4GHz Band
Wireless Radio : Enabled
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Channel Width : Auto 20/40 MHz
Channel : 6
Wi-Fi Protected Setup : Enabled/Not Configured
SSID List :

Wi-Fi Network Name (SSID)	Guest	MAC Address	Security Mode
dlink	No	00:18:E7:95:83:D8	Disabled

LAN COMPUTERS

IP Address	Name (if any)	MAC
192.168.0.113	07896PCWin7E	00:21:9B:62:AF:56
192.168.0.100	android-76184e95434990fc	00:0c:e7:03:05:1b
192.168.0.102	07896PCWin7E	00:00:00:00:00:00
192.168.0.105	06466NBWIN7	00:26:5e:ed:a1:a0
192.168.0.110	android-40a74f6f45e59856	90:18:7c:1a:26:24
192.168.0.112	android-d2311fa0b58731a7	94:ce:2c:70:bb:98

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address

Logs

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

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

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

First Page: Click to go to the first page.

Last Page: Click to go to the last page.

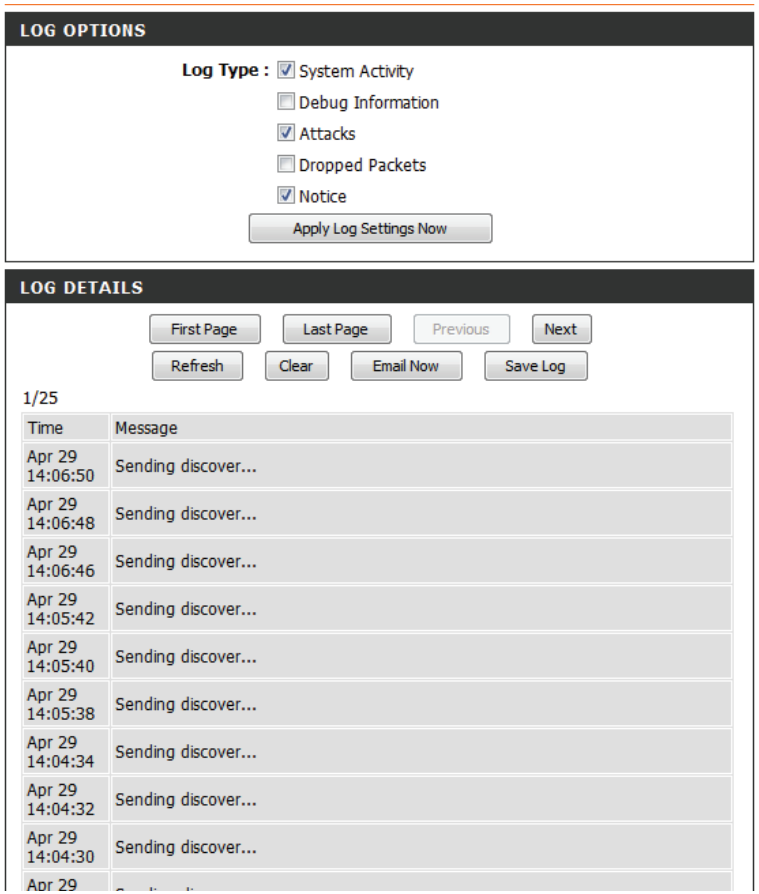
Previous: Click to go back one page.

Next: Click to go to the next page.

Clear: Clears all of the log contents.

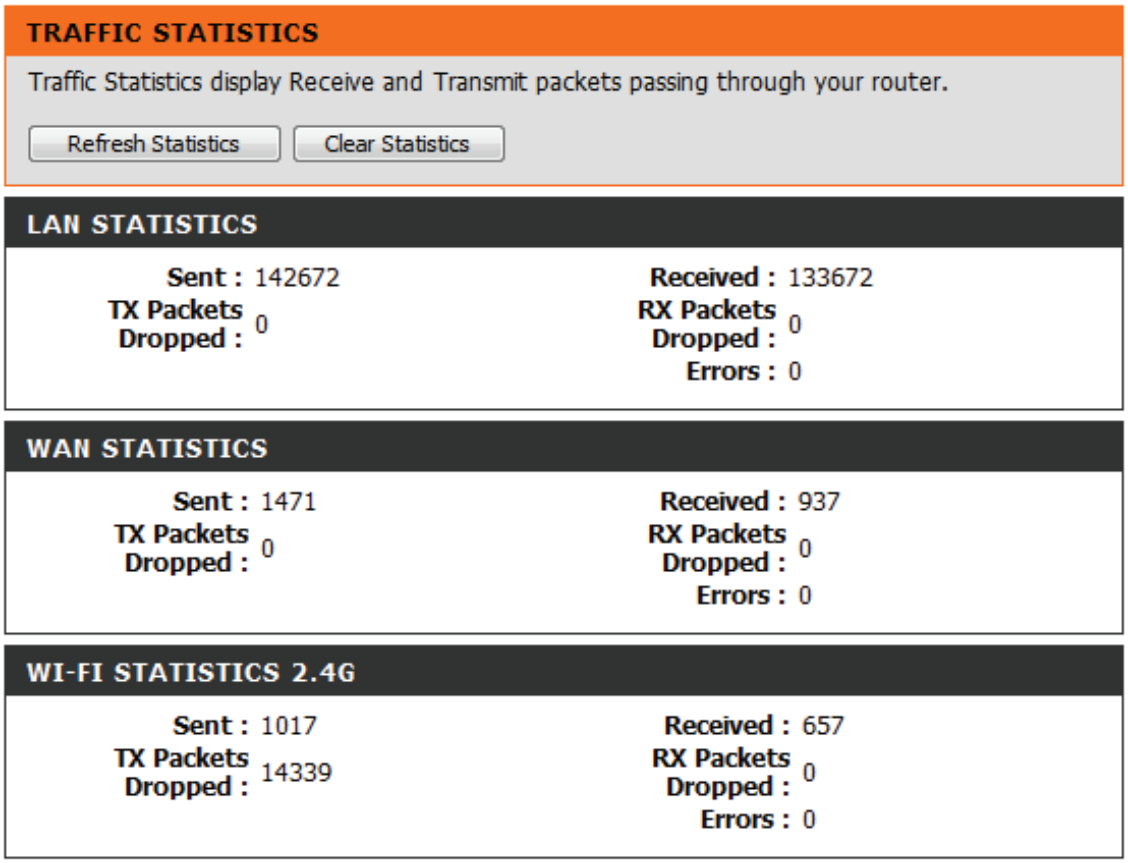
E-mail Now: This option will send a copy of the router log to your e-mail address configured in the **Tools** > **E-mail Settings** screen.

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



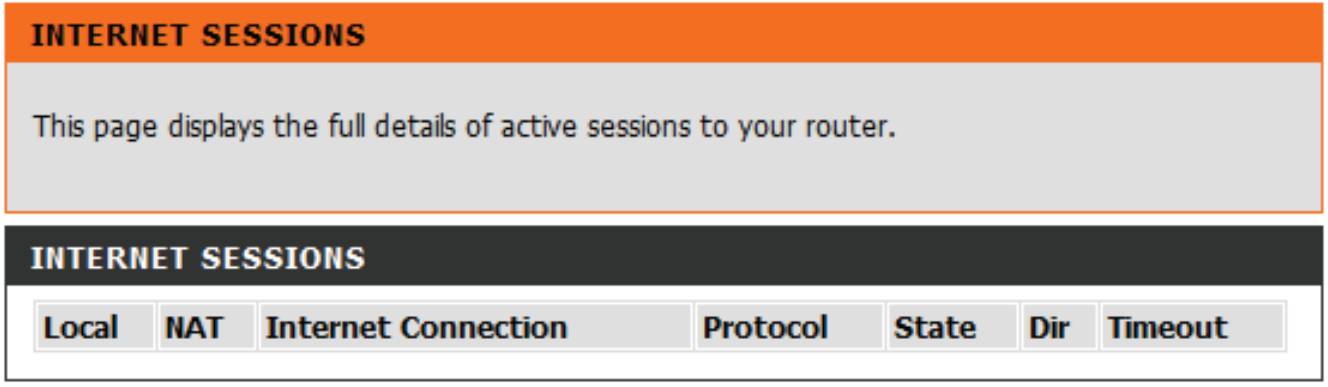
Statistics

The screen below displays the *Traffic Statistics*. Here you can view the amount of packets that pass through the DIR-655 on both the WAN, LAN ports and the wireless segments. The traffic counter will reset if the device is rebooted.



Internet Sessions

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



Routing

This page will display your current routing table.

ROUTING

Routing Table

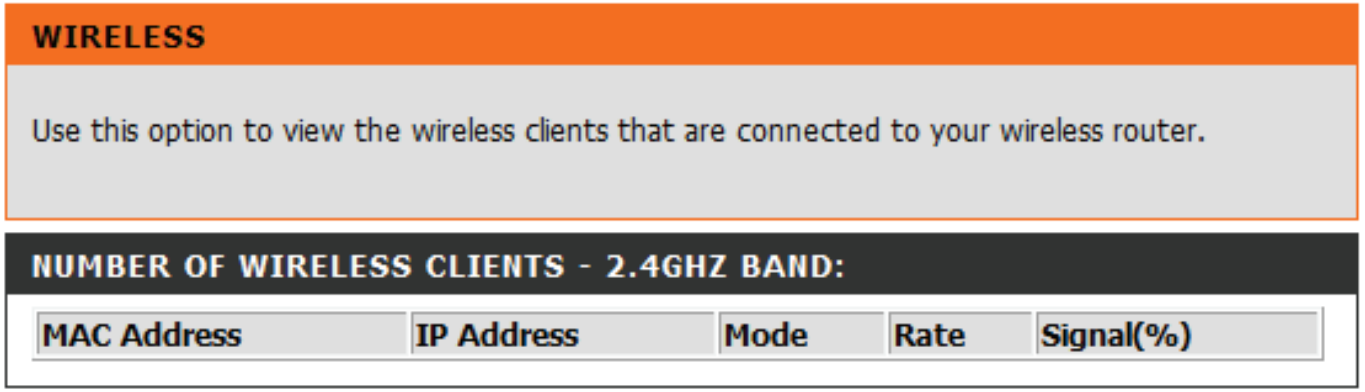
This page displays the routing details configured for your router.

ROUTING TABLE

Destination IP	Netmask	Gateway	Metric	Interface	Type	Creator
192.168.0.0	255.255.255.0	0.0.0.0	0	LAN	Internal	System
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN	Internal	System
127.0.0.0	255.0.0.0	0.0.0.0	0	Local Loopback	LOCAL	System

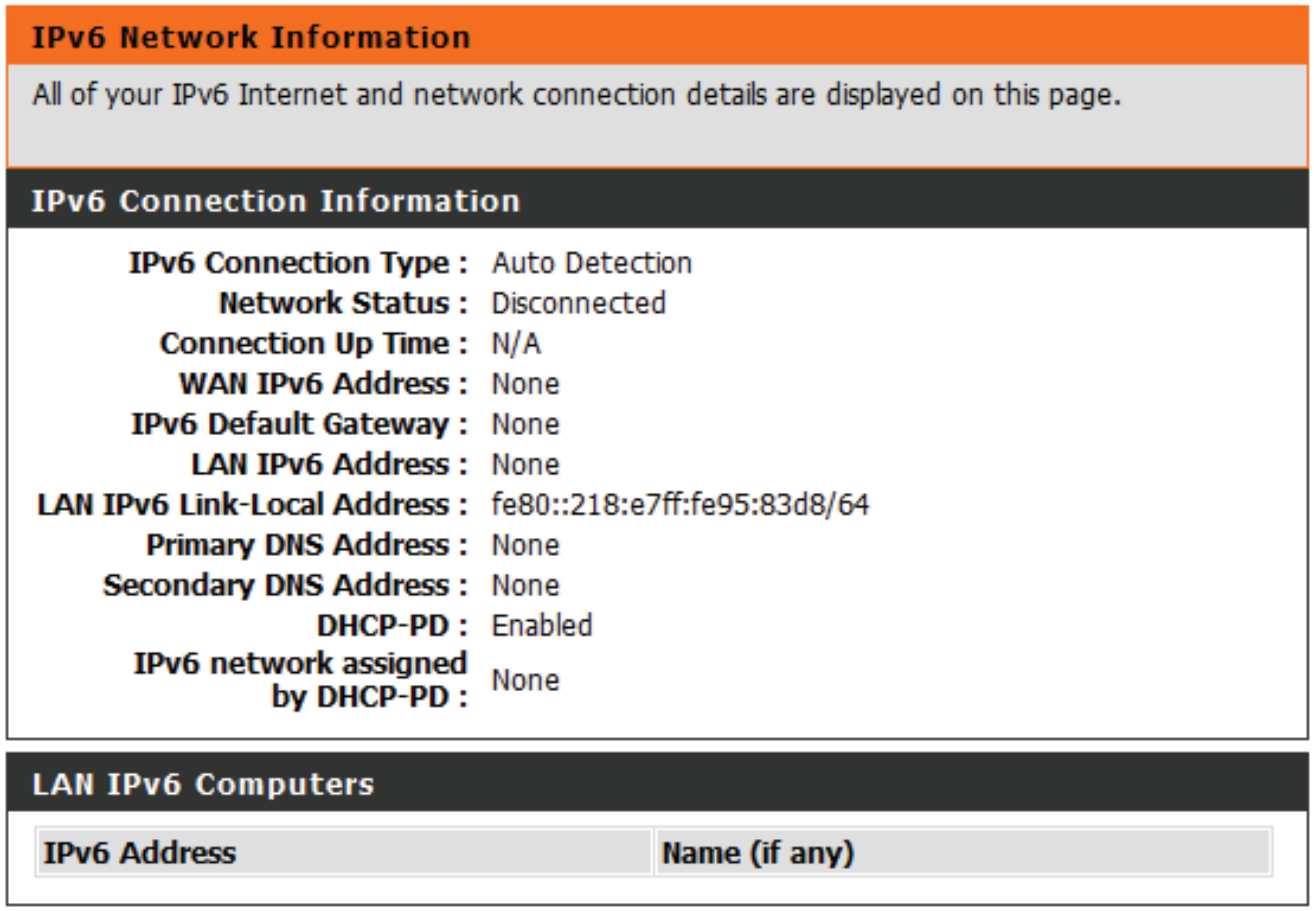
Wireless

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



IPv6 Routing

This page displays the *IPv6 Routing* details configured for your router.

Support

SETUP HELP

- Internet Connection
- WAN
- Wireless Settings
- Network Settings
- IPV6

ADVANCED HELP

- Virtual Server
- Port Forwarding
- Application Rules
- QoS Engine
- Network Filter
- Access Control
- Website Filter
- Inbound Filter
- Firewall Settings
- Routing
- Advanced Wireless
- Wi-Fi Protected Setup
- Advanced Network
- GUEST ZONE
- IPV6Firewall
- IPv6 Routing

TOOLS HELP

- Admin
- Time
- Syslog
- Email Settings
- System
- Firmware
- Dynamic DNS
- System Check
- Schedules

STATUS

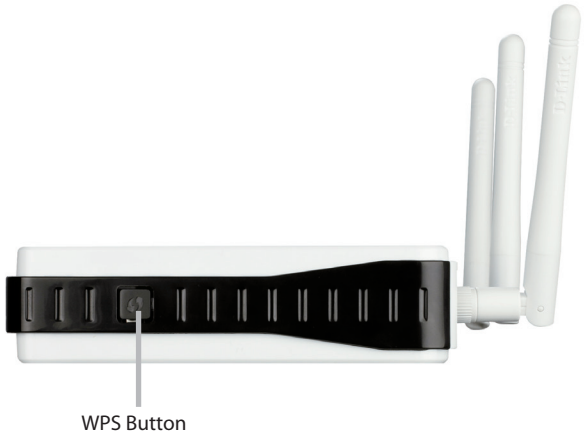
- Device Info
- Logs
- Statistics
- Internet Sessions
- Routing
- Wireless
- IPV6
- IPv6 Routing

Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DIR-655 router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the DIR-655 for about 1 second. The Internet LED on the front will start to blink.



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

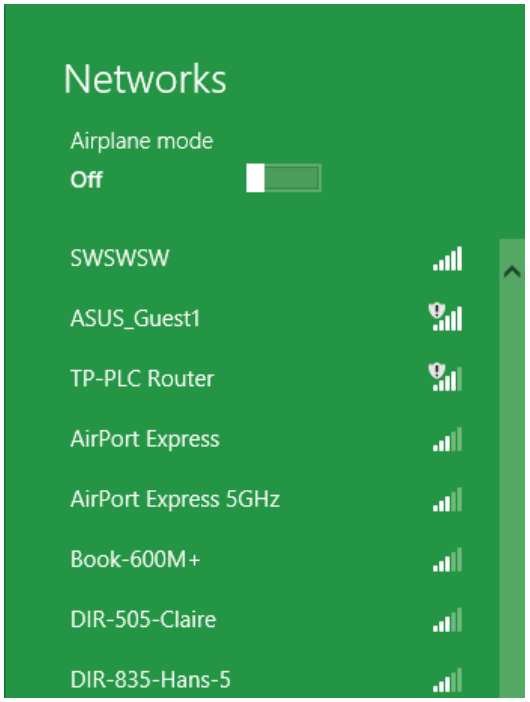
Step 3 - Allow up to 1 minute to configure. Once the Internet light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

Windows® 8
WPA/WPA2

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

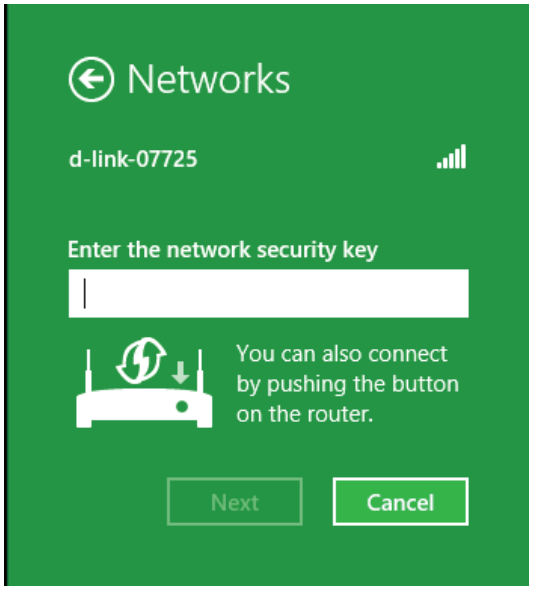
To join an existing network, locate the wireless network icon in the taskbar, next to the time display.

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

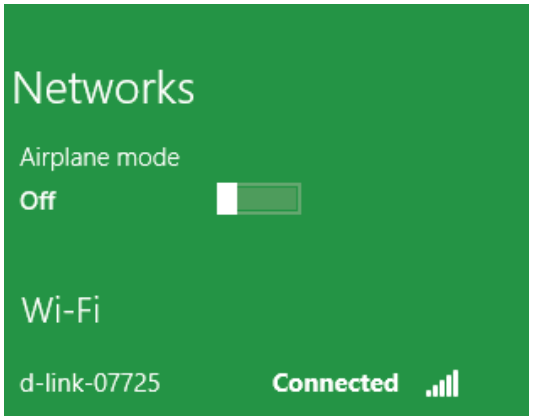


You will then be prompted to enter the network security key (Wi-Fi password) for the wireless network. Enter the password into the box and click **Next**.

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



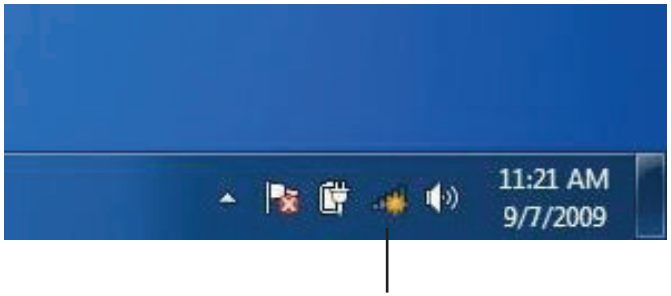
When you have established a successful connection a wireless network, the word **Connected** will appear next to the name of the network to which you are connected.



Windows® 7
WPA/WPA2

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

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

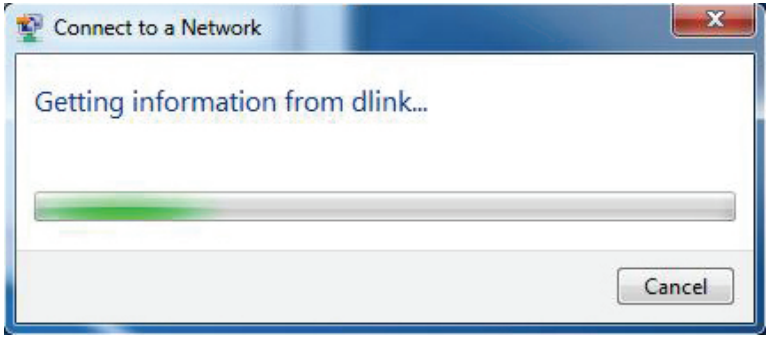


2. The utility will display any available wireless networks in your area.

3. Highlight the wireless connection with Wi-Fi name (SSID) you would like to connect to and click the **Connect** button.

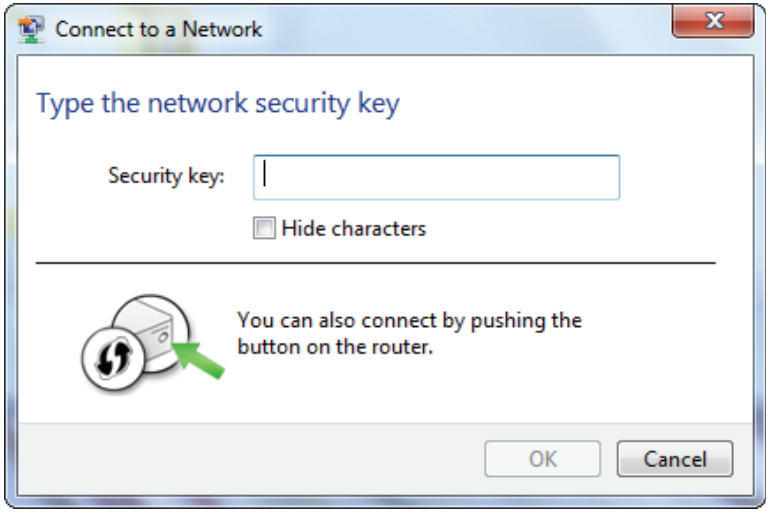
   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.

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



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

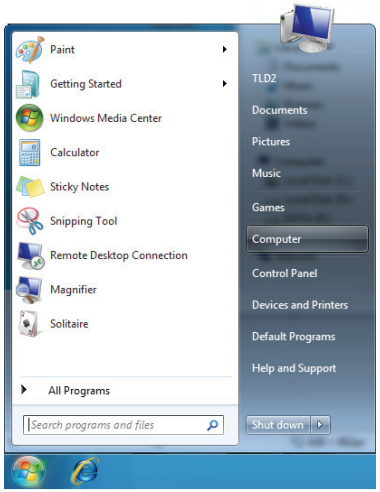
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



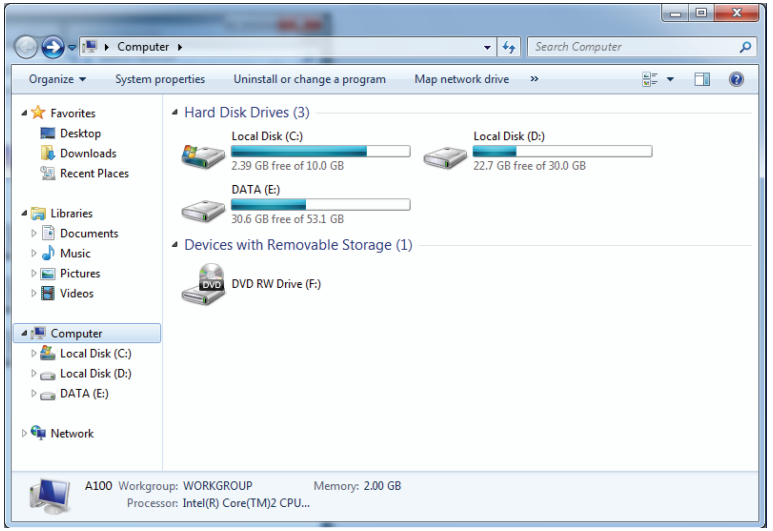
WPS

The WPS feature of the DIR-655 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

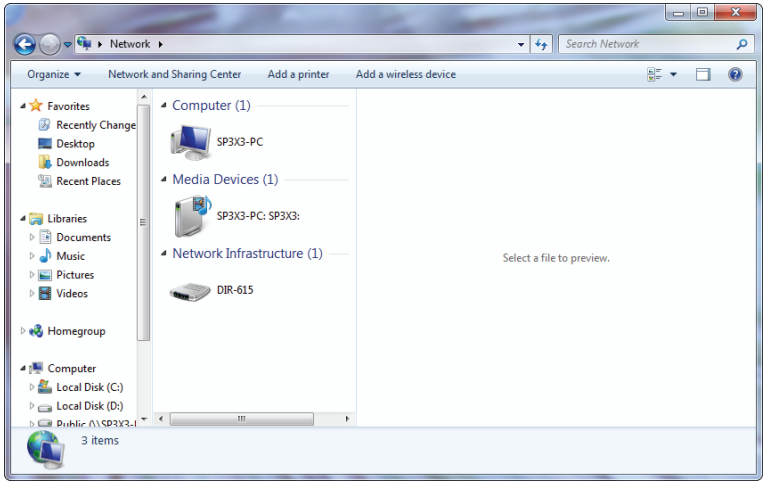
1. Click the **Start** button and select **Computer** from the Start menu.



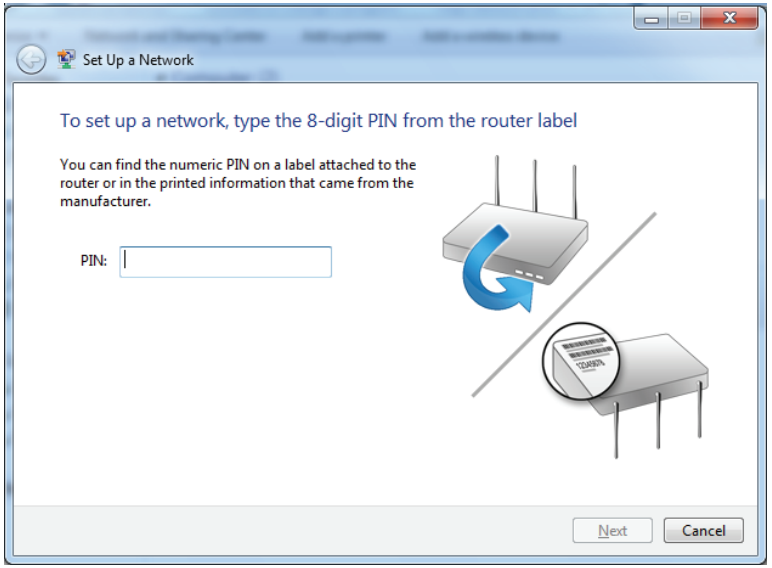
2. Click **Network** on the left side.



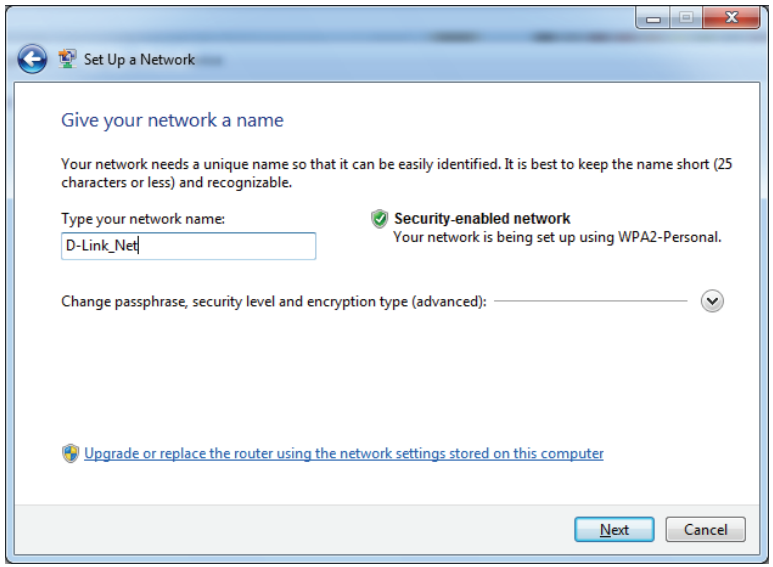
3. Double-click the DIR-655.



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

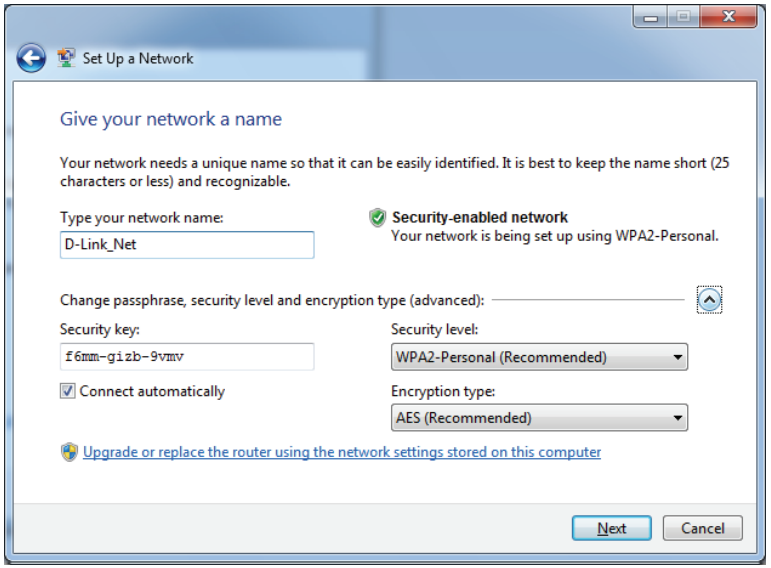


5. Type a name to identify the network.



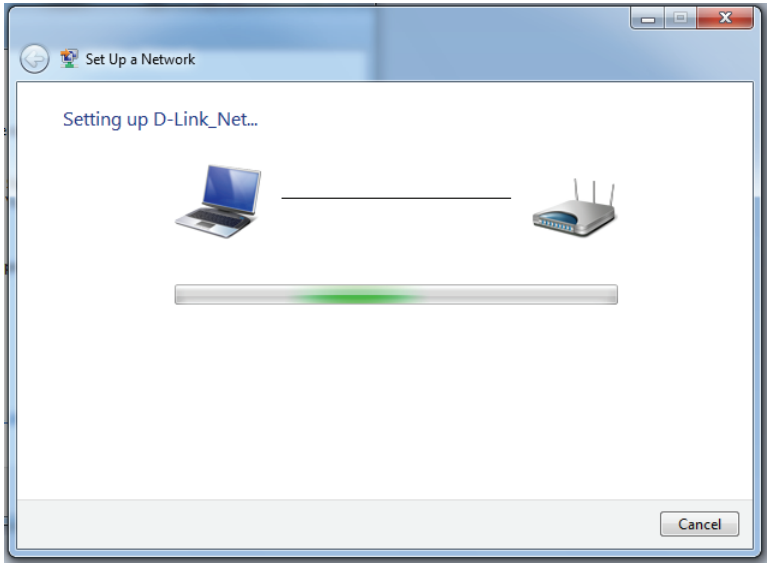
6. To configure advanced settings, click the icon.

Click **Next** to continue.



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

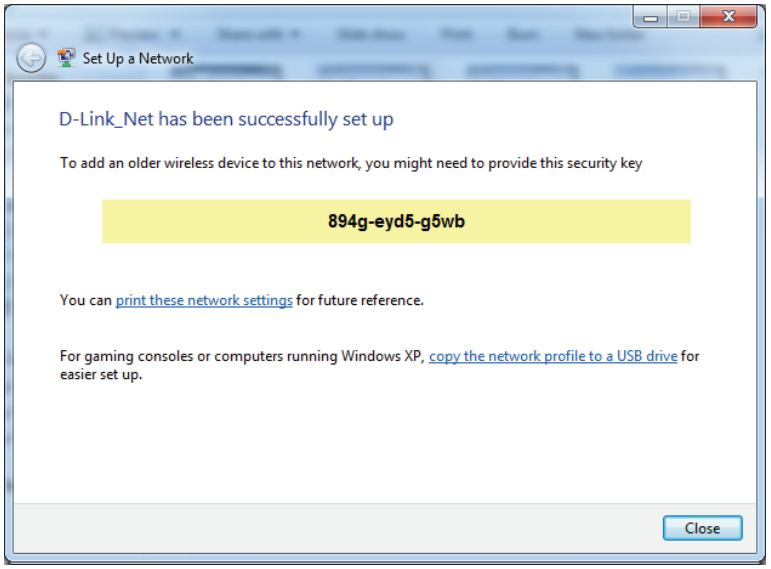
   Wait for the configuration to complete.



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

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

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



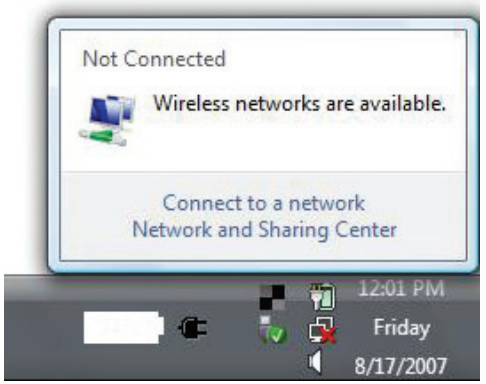
Windows Vista®

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

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

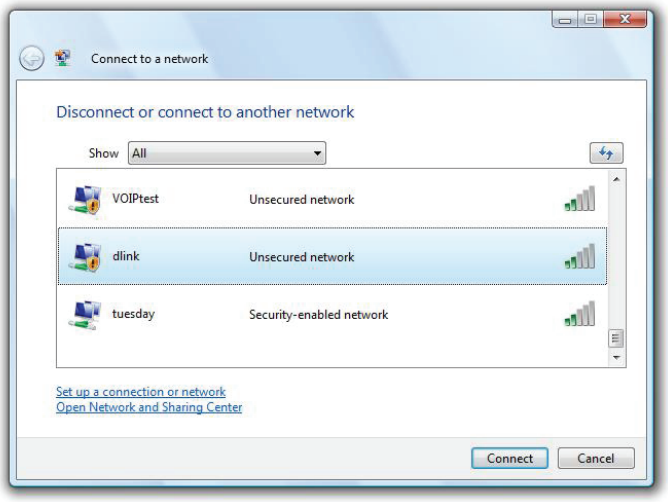
or

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



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

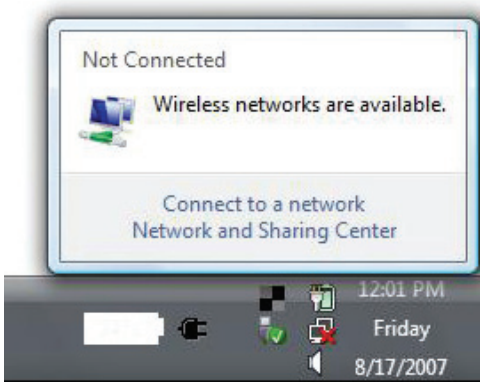
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



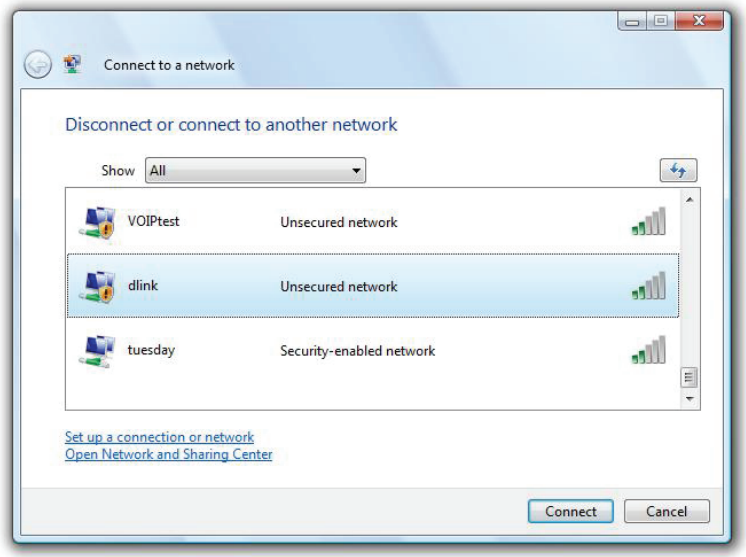
WPA/WPA2

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

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



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



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

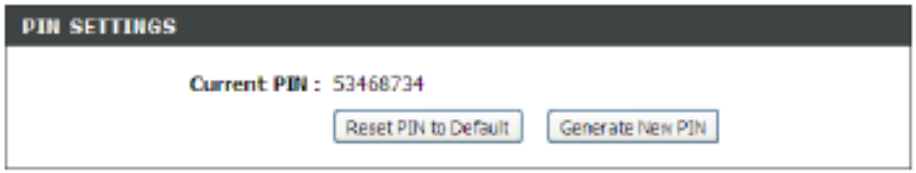
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.

WPS/WCN 2.0

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

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

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

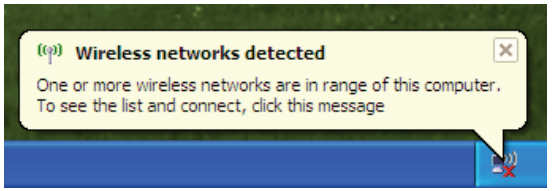


If you are using third party software to set up Wi-Fi Protection, carefully follow the directions. When you are finished, proceed to the next section to set up the newly-configured router.

Windows® XP

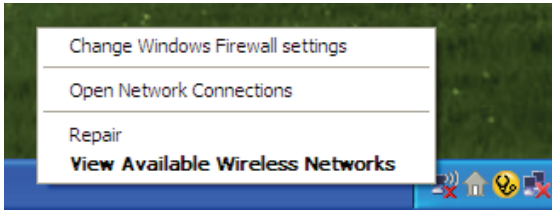
Windows XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities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

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



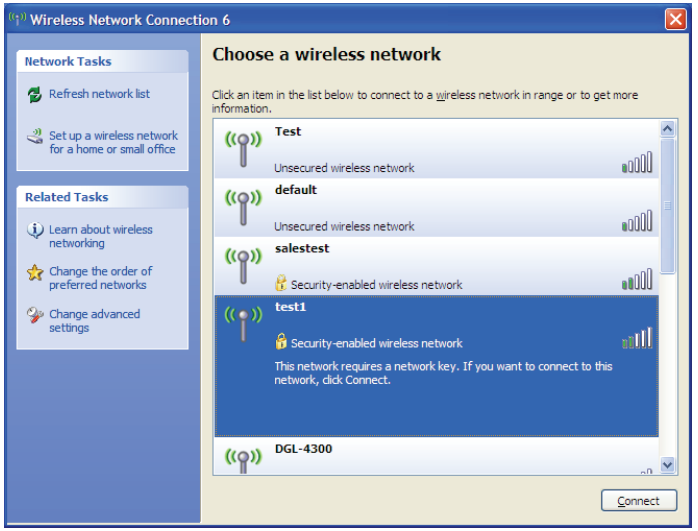
or

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



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

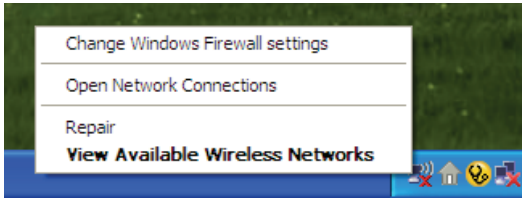
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



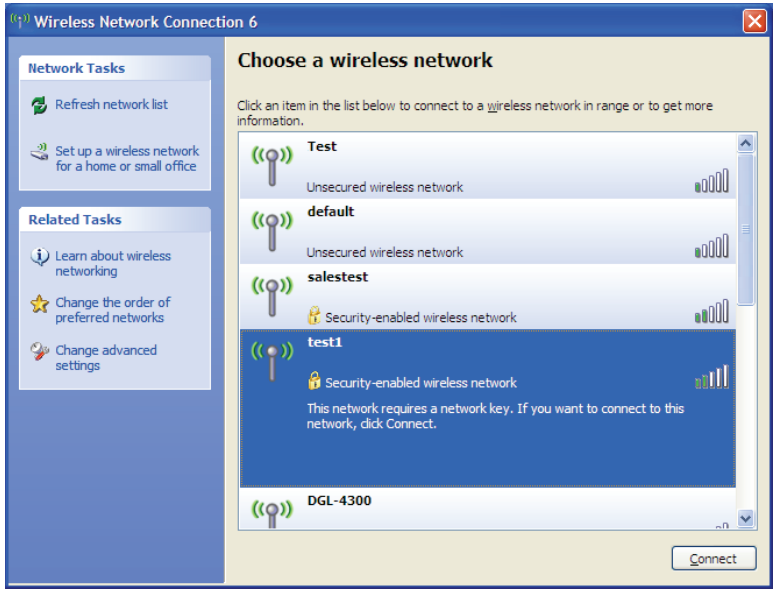
WPA/WPA2

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

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

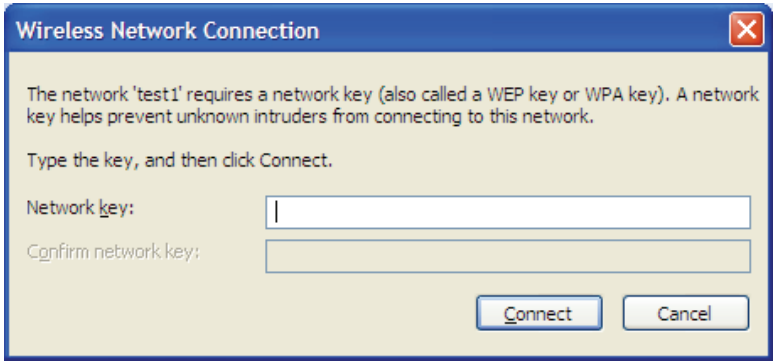


2. Highlight the Wi-Fi network (SSID) you would like to connect to and click **Connect**.



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

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



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-655. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link router (**192.168.0.1** for example), you are not connecting to a website 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 ZoneAlarm, BlackICE, Sygate, Norton Personal Firewall, and Windows XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

• Configure your Internet settings:

  • Go to **Start** > **Settings** > **Control Panel**. Double-click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.

  • Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.

  • Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.

  • Close your web browser (if open) and 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, Vista® and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

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

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

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

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

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

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

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

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

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

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

C:\>
```

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

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

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

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

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

Bluetooth is the industry standard wireless technology used for WPAN. Bluetooth devices in WPAN operate in a range up to 30 feet away. Compared to WLAN the speed and wireless operation range are both less than WLAN, but in return it doesn't use nearly as much power which makes it ideal for personal devices, such as mobile phones, PDAs, headphones, laptops, speakers, and other devices that operate on batteries.

Who uses wireless?

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

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, 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 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-655 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.

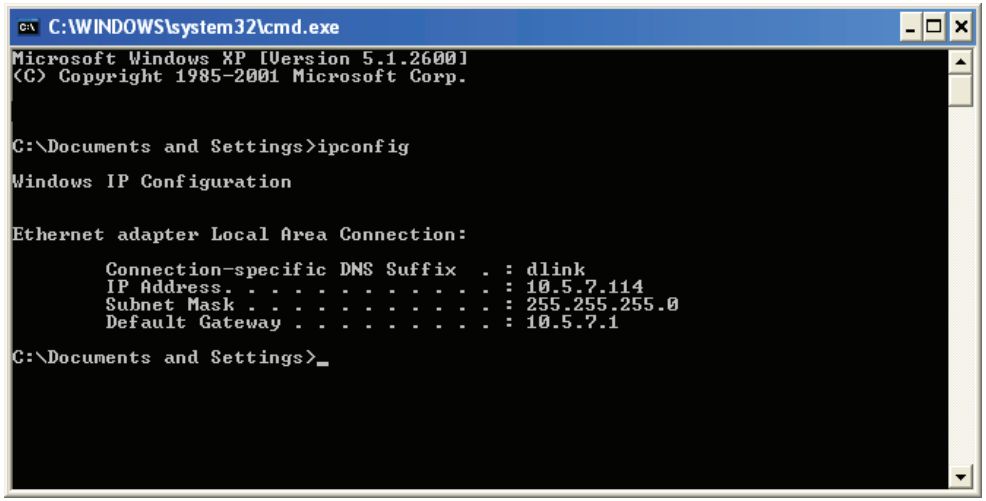
Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK.** (Windows Vista® users type *cmd* in the **Start Search** box.)

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® 7 - Click on **Start > Control Panel > Network and Internet > Network and Sharing Center**.
Windows Vista® - Click on **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center** > **Manage Network Connections.**
Windows XP - Click on **Start** > **Control Panel** > **Network Connections**.
Windows 2000 - From the desktop, right-click **My Network Places** > **Properties**.

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

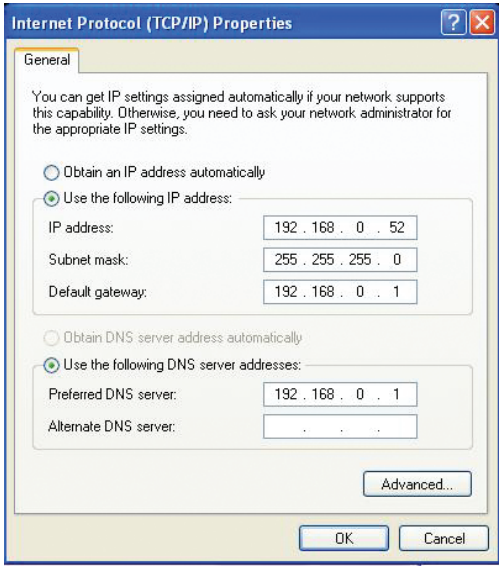
Step 3
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

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[1]

- 6.5 Mbps ~ 300 Mbps

Frequency Range

- 2.4 GHz to 2.483 GHz[2]

External Antenna Type

- Three (3) detachable reverse SMA Antennas

Operating Temperature

- 32°F to 131°F (0°C to 55°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- CE
- IC

Dimensions

- L = 7.6 inches
- W = 4.6 inches
- H = 1.2 inches

Warranty

- 2 years

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

[2] Wireless frequency range may vary depending on region

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.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Industry Canada Notice:

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

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

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

This device has been designed to operate with an antenna having a maximum gain of 2dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

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

This radio transmitter(IC: 4216A-IR655C1) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Cet émetteur radio (IC: 4216A-IR655C1) a été approuvé par Industrie Canada pour fonctionner avec les types d'antennes énumérés ci-dessous avec le gain maximal admissible et nécessaire impédance d'antenne pour chaque type d'antenne indiqué. Types d'antennes ne figurent pas dans cette liste, ayant un gain supérieur au gain maximum indiqué pour ce type, sont strictement interdites pour une utilisation avec cet appareil.

"To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication"

"This device has been designed to operate with an antenna having a maximum gain of [2] dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms."

«Pour réduire le risque d'interférence avec d'autres utilisateurs, le type d'antenne et son gain doivent être choisis afin que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie"
«Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de [2] dBi. Antenne ayant un gain supérieur sont strictement interdites par la réglementation d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms."