D-Link®

Version 2.0 | 03/15/2012

User Manual

Wireless N Dual Band Router

DIR-815

Preface

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

Manual Revisions

Revision	Date	Description
1.0	June 30, 2010	Initial Release
2.0	March 15, 2012	Updated for Revision B1

Trademarks

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

Table of Contents

Package Contents

DIR-815 Wireless N Dual Band Router

Ethernet Cable

Power Adapter

CD-ROM with Manual and Setup Wizard

Quick Install Guide

Note: *Using a power supply with a different voltage rating than the one included with the DIR-815 will cause damage and void the warranty for this product.*

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n or 802.11g wireless clients • IEEE 802.11a wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6 or higher • Firefox 3 or higher • Safari 4 or higher • Chrome 8 or higher **Windows® Users:** Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.
CD Installation Wizard Requirements	**Computer with the following:** • Windows® 7/ Vista® / XP with Service Pack 3 • An installed Ethernet adapter • CD-ROM drive

Introduction

TOTAL PERFORMANCE
Combines award winning router features and IEEE 802.11a/n/g wireless technology to provide the best wireless performance.

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

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

ULTIMATE PERFORMANCE
The D-Link Wireless N Dual Band router (DIR-815) is a 802.11n/802.11a compliant device that delivers real world performance of up to 13x 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 DIR-815 router to a cable or DSL modem and share your high-speed Internet access with everyone on the network. In addition, this Router includes a Quality of Service (QoS) engine that keeps digital phone calls (VoIP) and online gaming smooth and responsive, providing a better Internet experience.

TOTAL NETWORK SECURITY
The Wireless N Dual Band 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/WPA2 standards ensure that you'll be able to use the best possible encryption method, regardless of your client devices. In addition, this router utilizes dual active firewalls (SPI and NAT) to prevent potential attacks from across the Internet.

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

Features

- **Faster Wireless Networking** - The DIR-815 provides up to 600Mbps* 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 network speeds faster than 802.11g.

- **Compatible with 802.11a and 802.11g Devices** - The DIR-815 is still fully compatible with the IEEE 802.11a and 802.11g standards, so it can connect with existing 802.11a and 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.

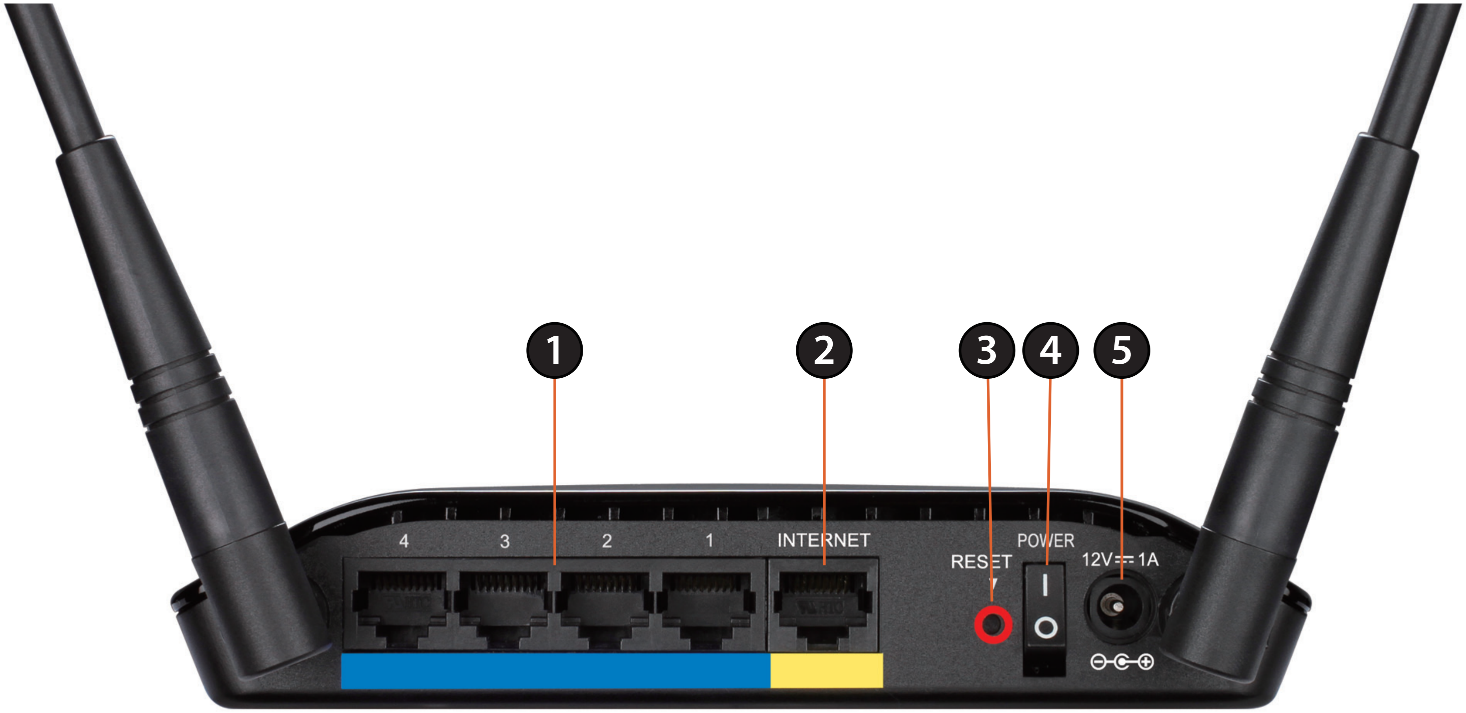
  - **Secure Multiple/Concurrent Sessions** - The DIR-815 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-815 can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, the DIR-815 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 802.11a, 802.11g, and 802.11n specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental conditions will adversely affect wireless signal range.

Hardware Overview

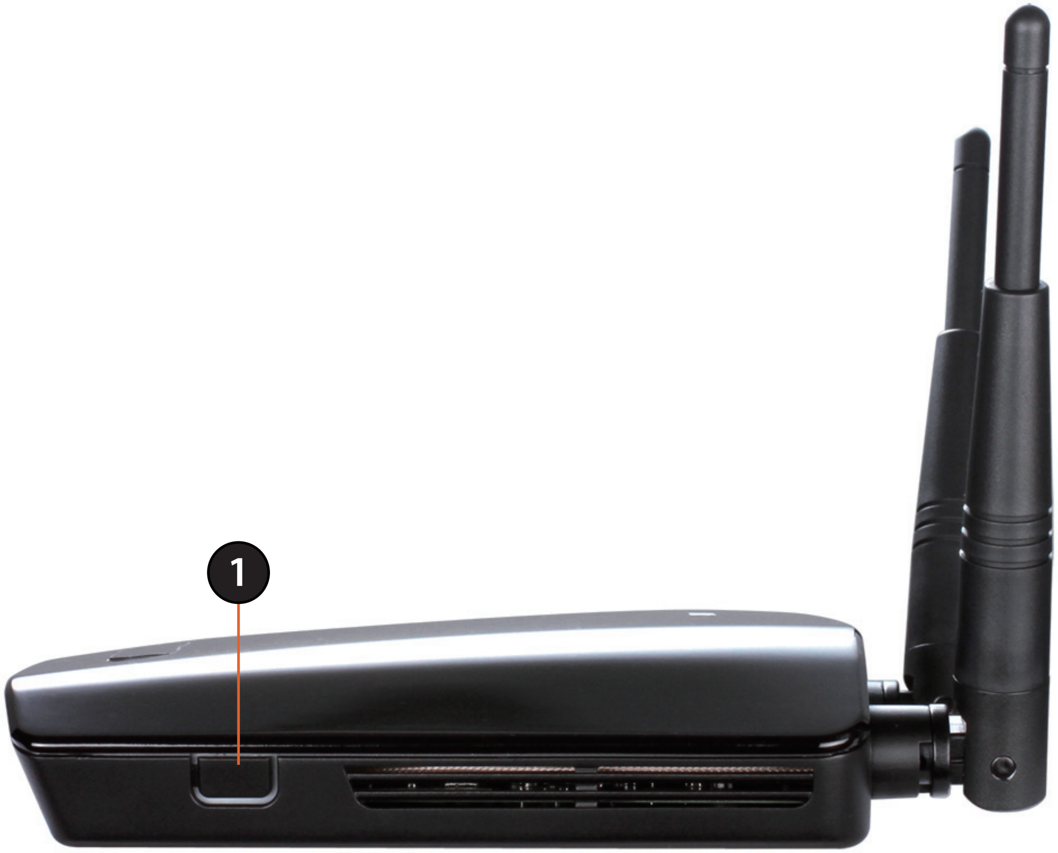
Connections



1	LAN Ports (1-4)	Connect 10/100 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	Reset Button	Pressing the Reset button restores the router to its original factory default settings.
4	Power Button	Use this switch to power on/power off the device.
5	Power Receptor	Receptor for the supplied power adapter.

Hardware Overview

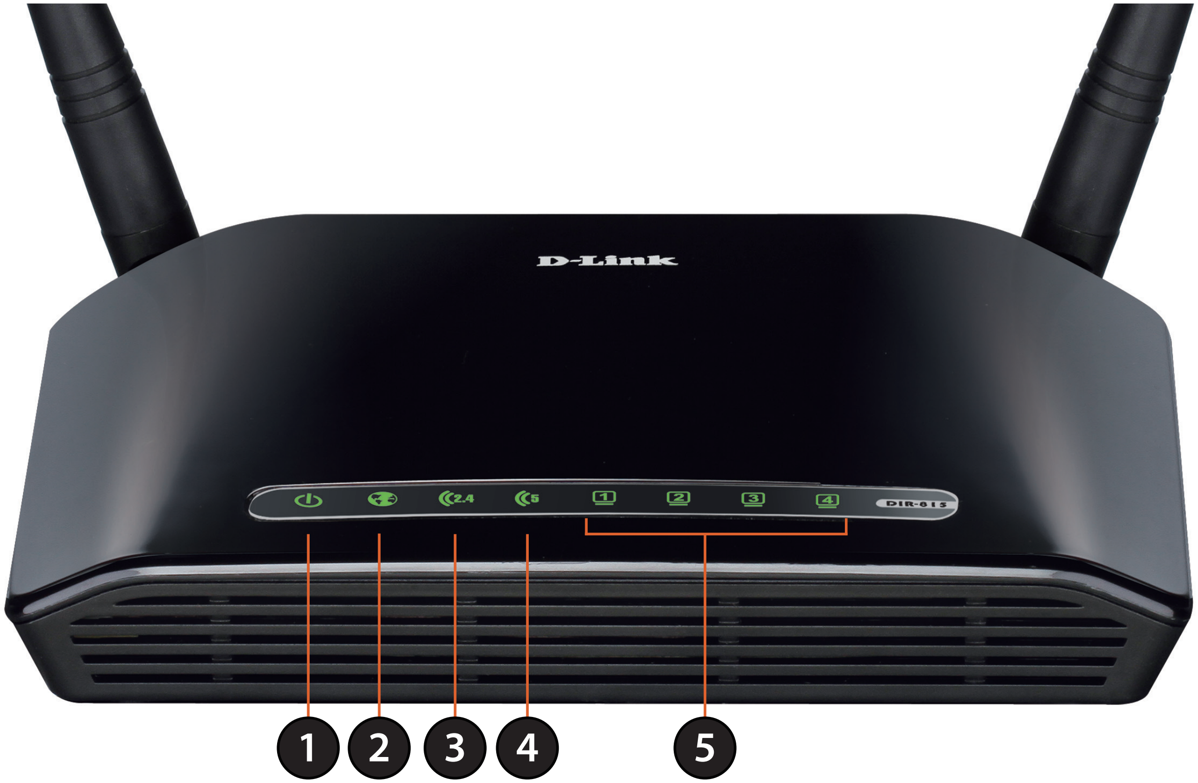
WPS Button



1	WPS Button	Press the WPS button for 1 second to initiate the WPS process. The button will flash blue while a WPS connection is being established. The button will light solid blue for 5 seconds when the device has successfully been added to the network.

Hardware Overview

LEDs



1	Power LED	A solid green light indicates a proper connection to the power supply. This LED will light orange during a factory reset or reboot. A slow blinking orange LED indicates that the Router has crashed during bootup.
2	Internet LED	A solid green light indicates the PPP negotiation has successfully completed. This LED blinks green during data transmission. A solid orange light indicates that the physical link is up, but the ISP service is down. This LED blinks orange when a session is dropped due to idle timeout.
3	WLAN LED (2.4GHz)	A solid light indicates that the 2.4GHz wireless segment is ready. This LED blinks during wireless data transmission.
4	WLAN LED (5GHz)	A solid light indicates that the 5GHz wireless segment is ready. This LED blinks during wireless data transmission.
5	LAN LEDs (1-4)	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

Installation

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

Before you Begin

- Please configure the router with the computer that was last connected directly to your modem.

- 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.

- When running the Setup Wizard from the D-Link CD, make sure the computer you are running the CD from is connected to the Internet and online or the wizard will not work. If you have disconnected any hardware, re-connect your computer back to the modem and make sure you are online.

Wireless Installation Considerations

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

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

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

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

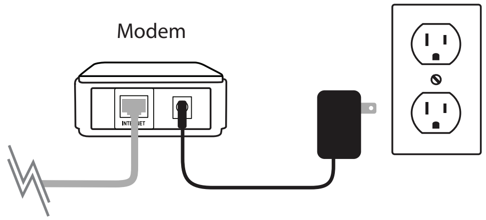
4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

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

Manual Setup

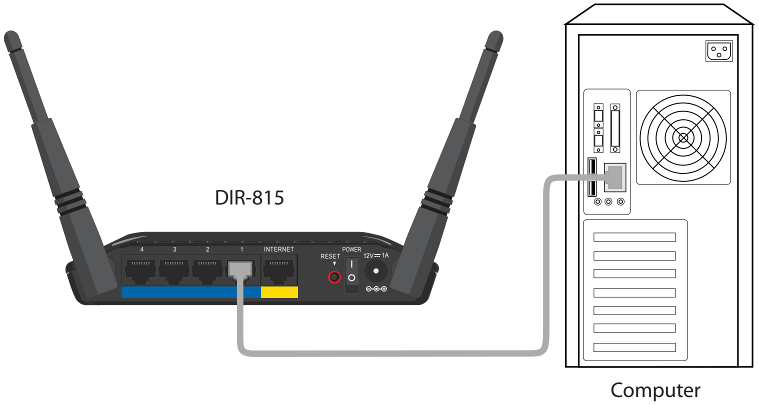
Important: for best results, insert the Installation CD and follow the on-screen instructions. If you are unable to use the CD or are using Mac or Linux, please use the following installation steps:

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

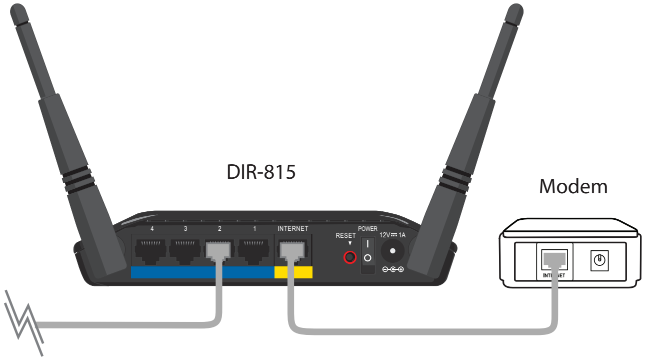


2. Position your router close to your modem and a computer. Place the router in an open area of your intended work area for better wireless coverage.

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

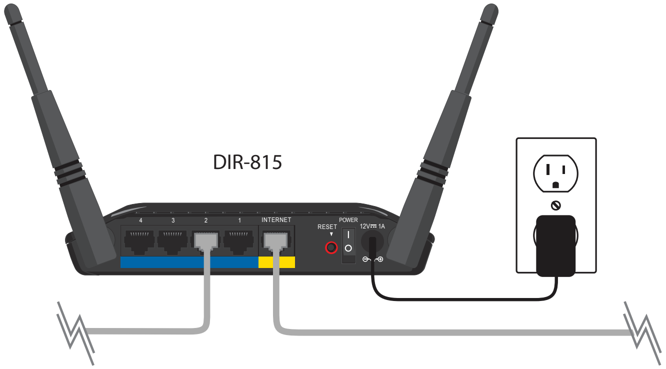


4. Plug one end of the included blue Ethernet cable that came with your router into the yellow port labeled INTERNET on the back of the router. Plug the other end of this cable into the Ethernet port on your modem.



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

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



7. If you are connecting to a Broadband service that uses a dynamic connection (not PPPoE), you may be online already. Try opening a web browser and enter a web site. If you connect, you are finished with your Internet setup. Please skip to page 14 to configure your router and use the manual setup procedure to configure your network and wireless settings. If you did not connect to the Internet, use the D-Link Setup Wizard (refer to page 15).

Connect to Another Router

Note: *It is strongly recommended to replace your existing router with the DIR-815 instead of using both. If your modem is a combo router, you may want to contact your ISP or manufacturer's user guide to put the router into Bridge mode, which will 'turn off' the router (NAT) functions.*

If you are connecting the DIR-815 router to an existing router to use as a wireless access point and/or switch, you will have to do the following to the DIR-815 before connecting it to your network:

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

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

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

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

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

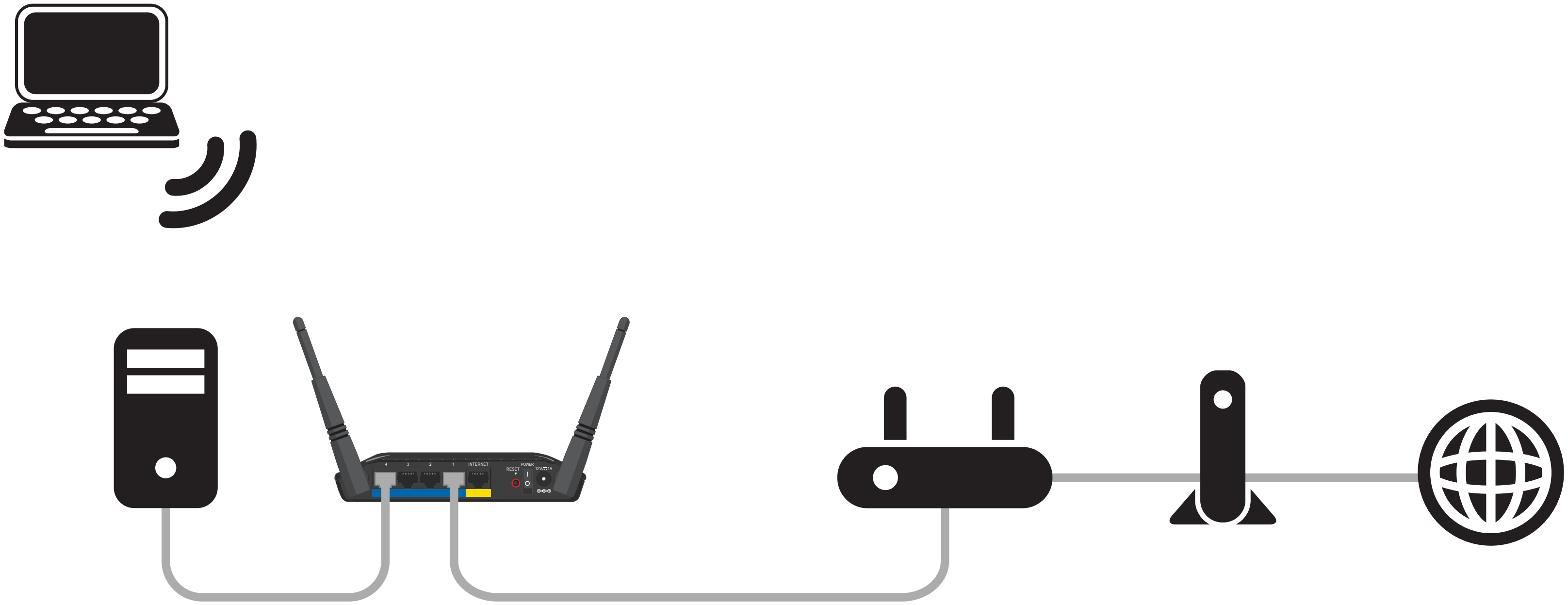
4. Click **Setup** and then click **Network Settings**. Uncheck the **Enable DHCP Server** checkbox. Click **Save Settings** to continue.

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

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

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

8. You may now use the other 3 LAN ports to connect other Ethernet devices and computers. To configure your wireless network, open a web browser and enter the IP address you assigned to the router. Refer to the **Configuration** and **Wireless Security** sections for more information on setting up your wireless network.



Configuration

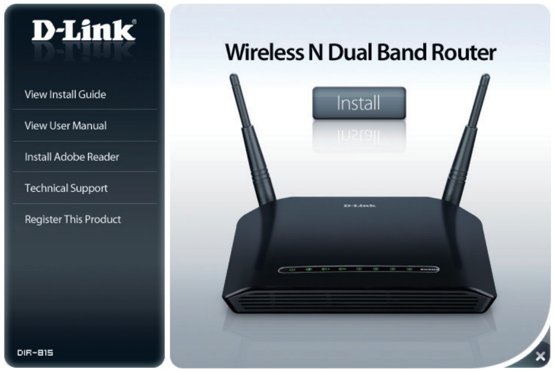
There are several different ways you can configure your router to connect to the Internet and connect to your clients:

- **Quick Router Setup Wizard** - Insert the supplied CD and launch the setup wizard (see below).
- **D-Link Setup Wizard** - This wizard will launch if you do not run the CD wizard and log into the router for the first time. Refer to page 15.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to page 21.

Quick Router Setup Wizard (CD)

To run the **Quick Router Setup Wizard**, insert the CD in the CD-ROM drive. When the autorun screen appears, click **English** (or **French**), and then click the **Install** button.

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



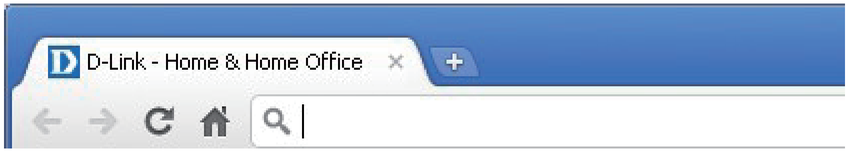
When the Wizard appears, select your language from the drop-down menu and then click **Next** to continue. Follow the on-screen instructions to configure your router.

Once you are finished, you may skip to page 21 and will be able to log into the web-based configuration utility and configure more advanced features.

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**.

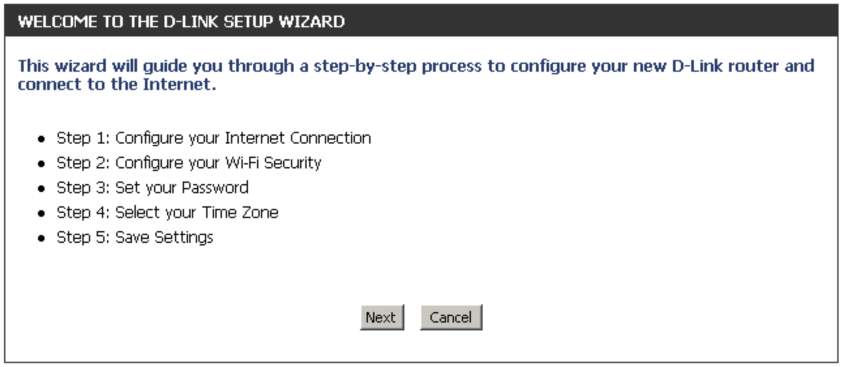
If you have already configured your settings and you would like to access the configuration utility, please refer to page 21.



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.

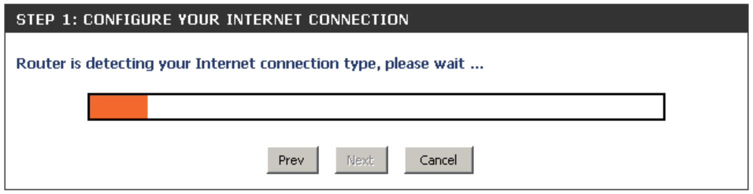


WELCOME TO THE D-LINK SETUP WIZARD

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

- Step 1: Configure your Internet Connection
- Step 2: Configure your Wi-Fi Security
- Step 3: Set your Password
- Step 4: Select your Time Zone
- Step 5: Save Settings

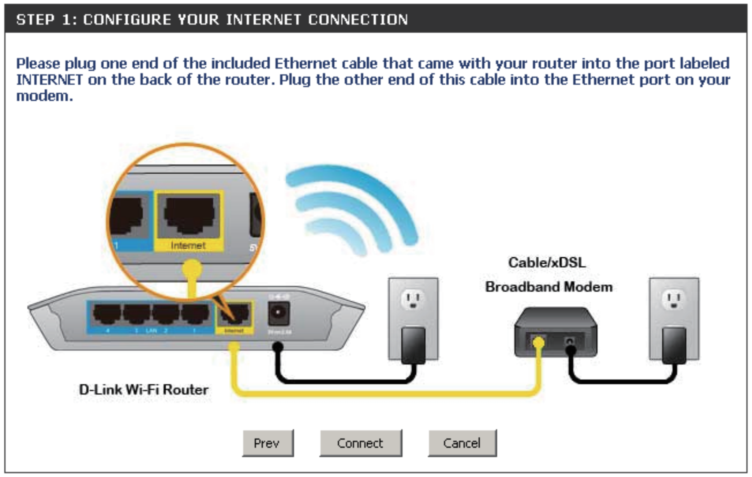
Please wait while your router detects your internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Router is detecting your Internet connection type, please wait ...

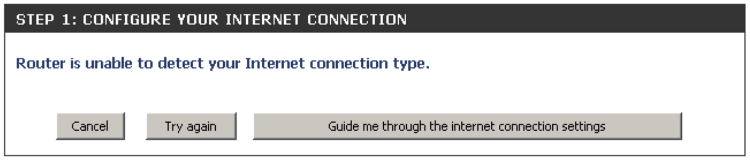
If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Connect your broadband modem to the Internet port and then click **Try Again**.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

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

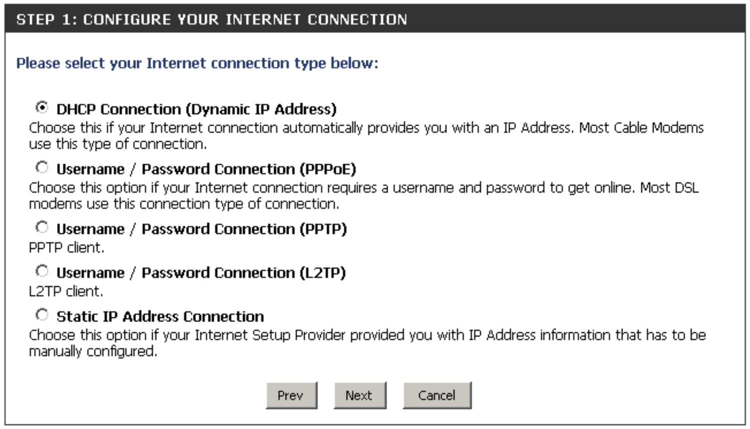
If the router detects an Ethernet connection but does not detect the type of Internet connection you have, this screen will appear. Click **Guide me through the Internet Connection Settings** to display a list of connection types to choose from.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Router is unable to detect your Internet connection type.

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



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Please select your Internet connection type below:

● **DHCP Connection (Dynamic IP Address)**
Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

○ **Username / Password Connection (PPPoE)**
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this connection type of connection.

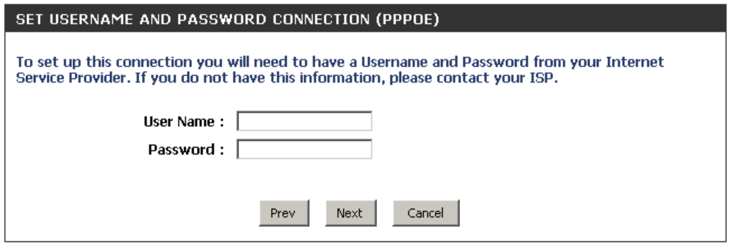
○ **Username / Password Connection (PPTP)**
PPTP client.

○ **Username / Password Connection (L2TP)**
L2TP client.

○ **Static IP Address Connection**
Choose this option if your Internet Setup Provider provided you with IP Address information that has to be manually configured.

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.*



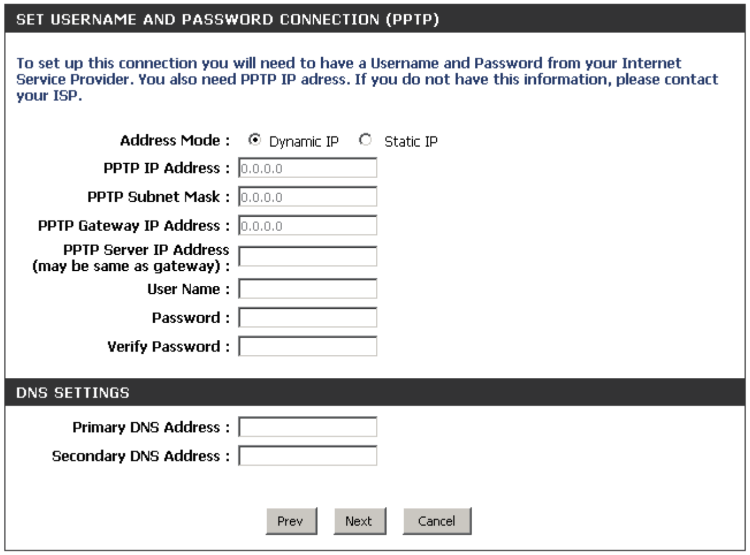
SET USERNAME AND PASSWORD CONNECTION (PPPOE)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. If you do not have this information, please contact your ISP.

User Name :

Password :

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



SET USERNAME AND PASSWORD CONNECTION (PPTP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP adress. If you do not have this information, please contact your ISP.

Address Mode : ● Dynamic IP ○ Static IP

PPTP IP Address : 0.0.0.0

PPTP Subnet Mask : 0.0.0.0

PPTP Gateway IP Address : 0.0.0.0

PPTP Server IP Address (may be same as gateway) :

User Name :

Password :

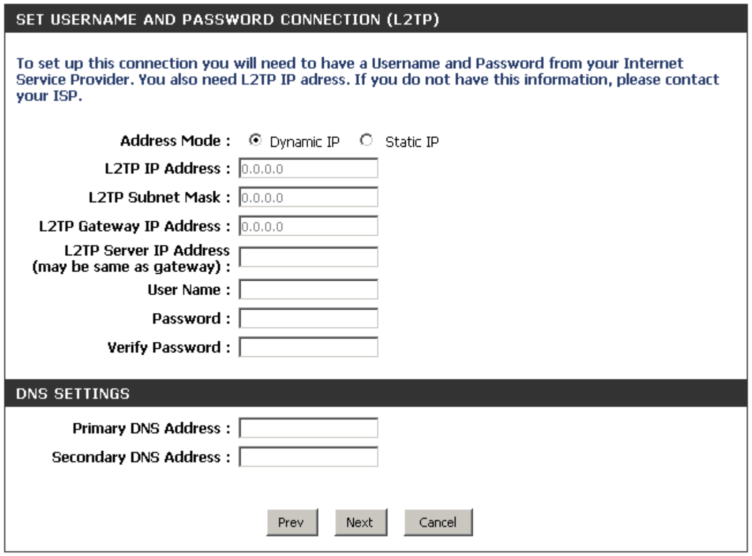
Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

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



SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP adress. If you do not have this information, please contact your ISP.

Address Mode : ● Dynamic IP ○ Static IP

L2TP IP Address : 0.0.0.0

L2TP Subnet Mask : 0.0.0.0

L2TP Gateway IP Address : 0.0.0.0

L2TP Server IP Address (may be same as gateway) :

User Name :

Password :

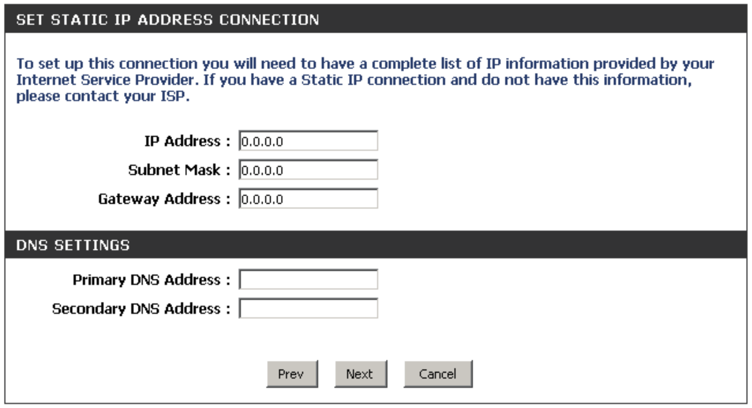
Verify Password :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

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



SET STATIC IP ADDRESS CONNECTION

To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP.

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Gateway Address : 0.0.0.0

DNS SETTINGS

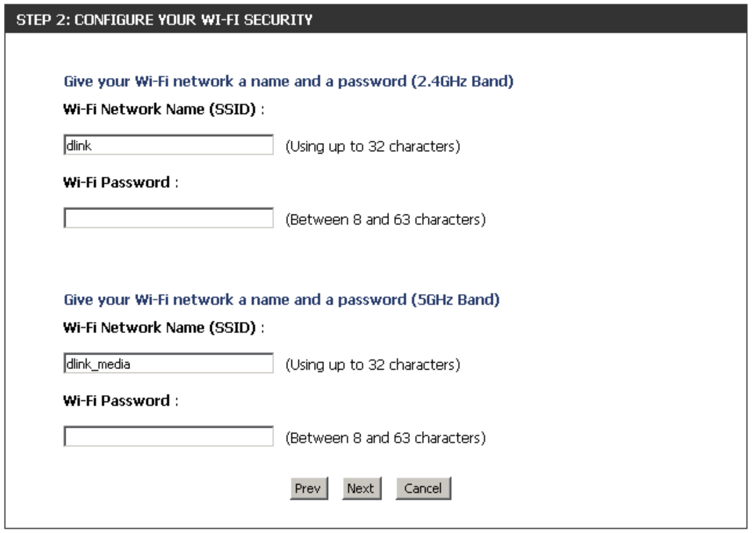
Primary DNS Address :

Secondary DNS Address :

For both the 2.4GHz and 5GHz 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.



STEP 2: CONFIGURE YOUR WI-FI SECURITY

Give your Wi-Fi network a name and a password (2.4GHz Band)

Wi-Fi Network Name (SSID) : dlink (Using up to 32 characters)

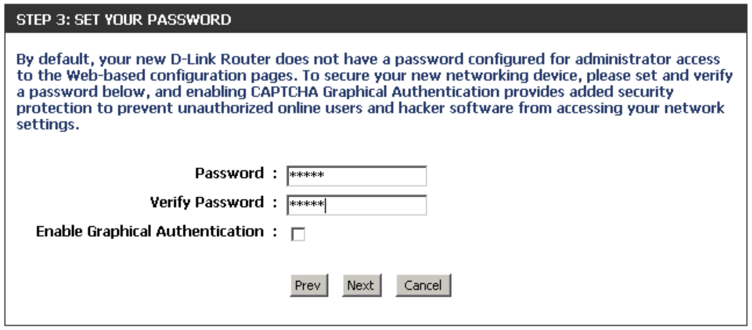
Wi-Fi Password : (Between 8 and 63 characters)

Give your Wi-Fi network a name and a password (5GHz Band)

Wi-Fi Network Name (SSID) : dlink_media (Using up to 32 characters)

Wi-Fi Password : (Between 8 and 63 characters)

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.



STEP 3: SET YOUR PASSWORD

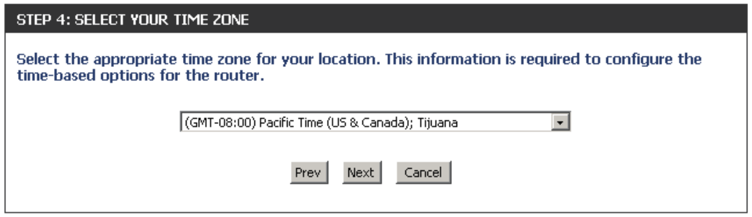
By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below, and enabling CAPTCHA Graphical Authentication provides added security protection to prevent unauthorized online users and hacker software from accessing your network settings.

Password : *****

Verify Password : *****

Enable Graphical Authentication : □

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

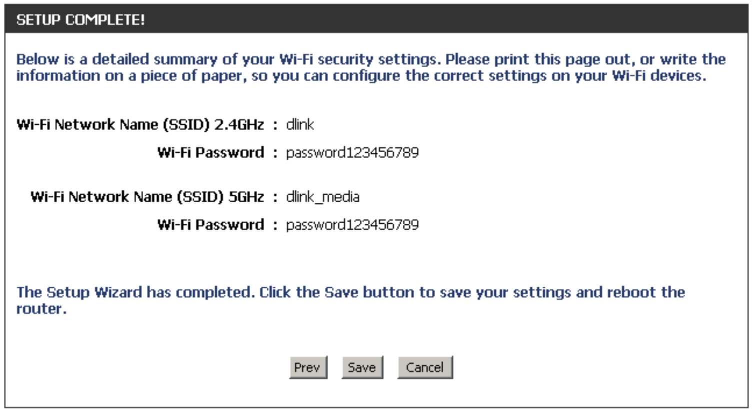


STEP 4: SELECT YOUR TIME ZONE

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

(GMT-08:00) Pacific Time (US & Canada); Tijuana

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



SETUP COMPLETE!

Below is a detailed summary of your Wi-Fi security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your Wi-Fi devices.

Wi-Fi Network Name (SSID) 2.4GHz : dlink

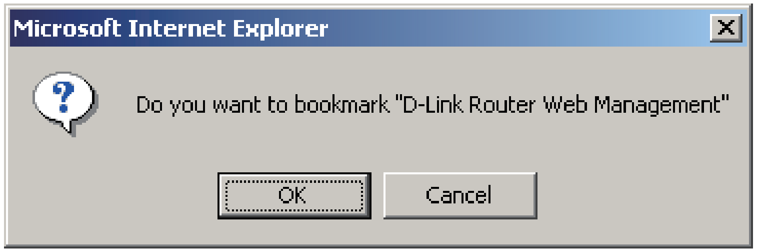
Wi-Fi Password : password123456789

Wi-Fi Network Name (SSID) 5GHz : dlink_media

Wi-Fi Password : password123456789

The Setup Wizard has completed. Click the Save button to save your settings and reboot the router.

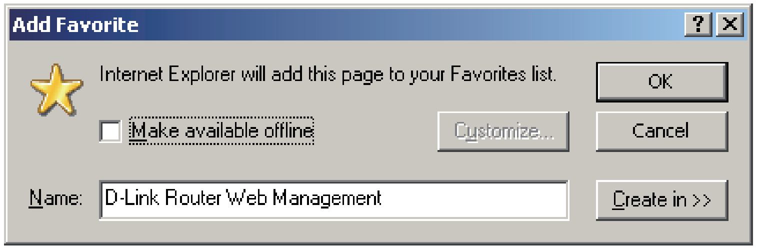
If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.



Microsoft Internet Explorer

Do you want to bookmark "D-Link Router Web Management"

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



Add Favorite

Internet Explorer will add this page to your Favorites list.

□ Make available offline

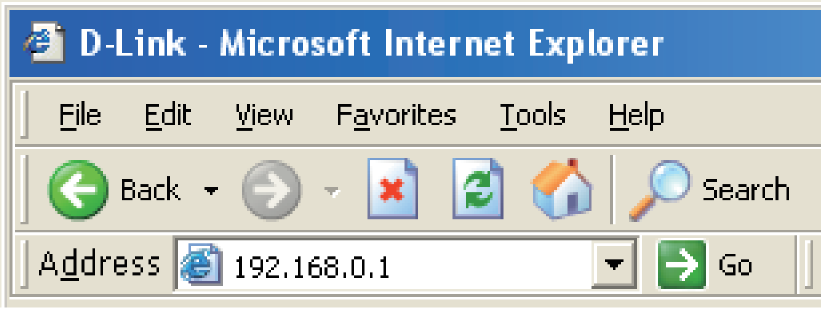
Name: D-Link Router Web Management

The router will now reboot. Please allow a minute or two before logging back in.

Web-based Configuration Utility

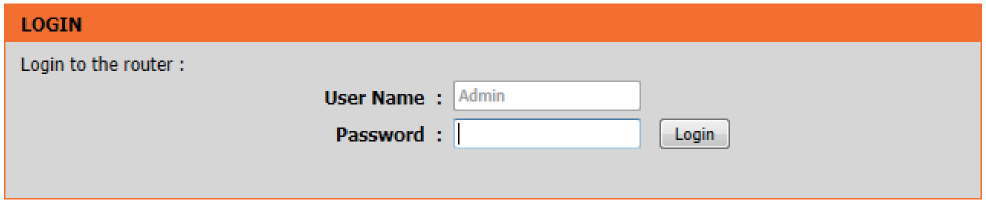
To access the configuration utility, open a web-browser such as Internet Explorer and enter the IP address of the router (**http://192.168.0.1**).

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



192.168.0.1

Enter your password. Leave the password blank by default.


LOGIN

Login to the router :

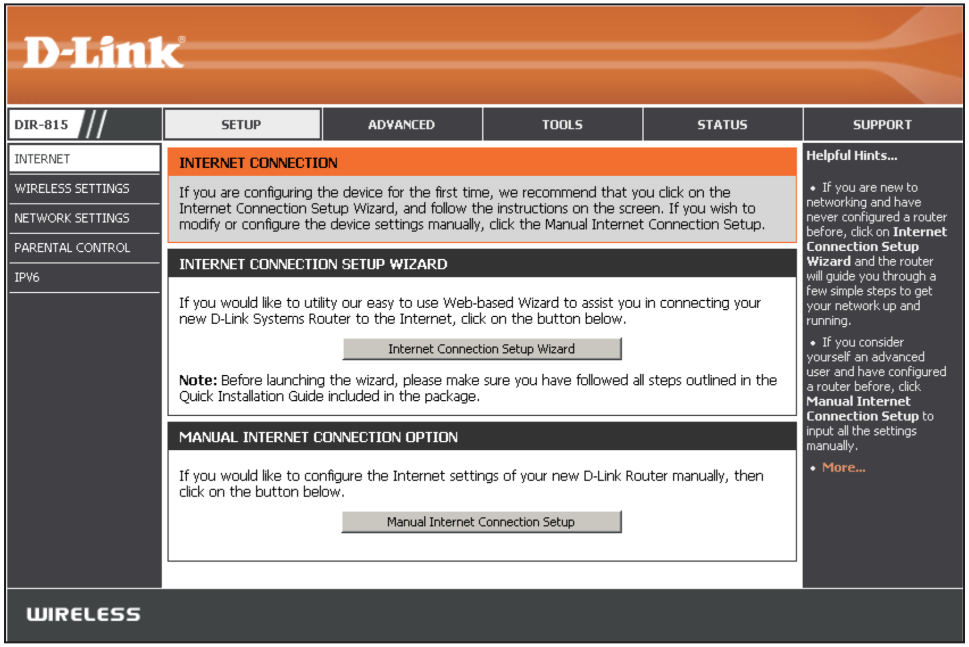
User Name : Admin

Password :

Internet Connection Setup

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

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup Wizard**. You will be directed to the Quick Setup Wizard. Please skip to page 15.



INTERNET CONNECTION

If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

INTERNET CONNECTION SETUP WIZARD

If you would like to utility our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.

Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

MANUAL INTERNET CONNECTION OPTION

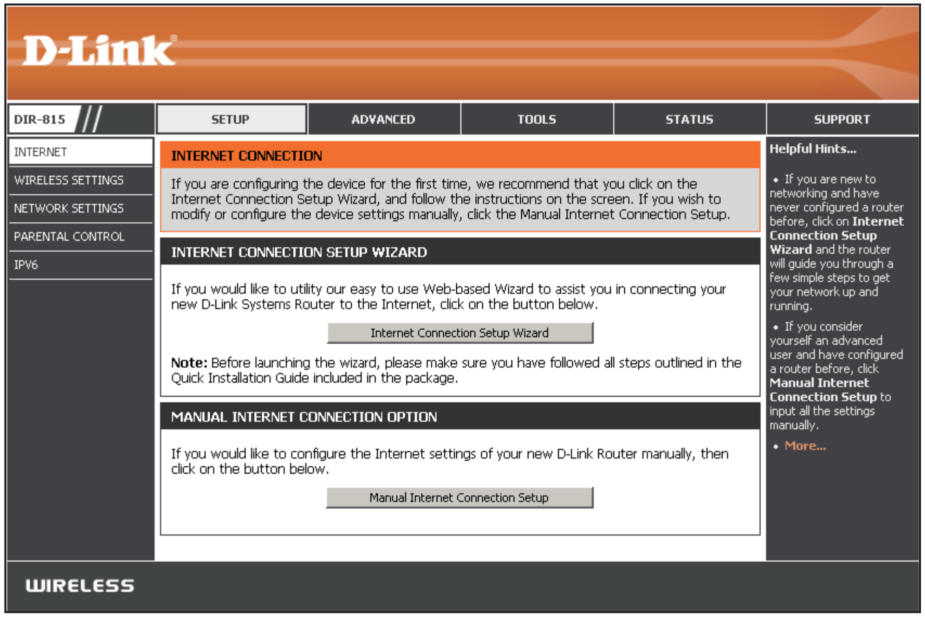
If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

Helpful Hints...

- If you are new to networking and have never configured a router before, click on **Internet Connection Setup Wizard** and the router will guide you through a few simple steps to get your network up and running.
- If you consider yourself an advanced user and have configured a router before, click **Manual Internet Connection Setup** to input all the settings manually.
- More...

Internet Connection Setup Wizard

Click the **Internet Connection Setup Wizard** button to start the Internet Connection Setup Wizard.



INTERNET CONNECTION

If you are configuring the device for the first time, we recommend that you click on the Internet Connection Setup Wizard, and follow the instructions on the screen. If you wish to modify or configure the device settings manually, click the Manual Internet Connection Setup.

INTERNET CONNECTION SETUP WIZARD

If you would like to utility our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.

Note: Before launching the wizard, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

MANUAL INTERNET CONNECTION OPTION

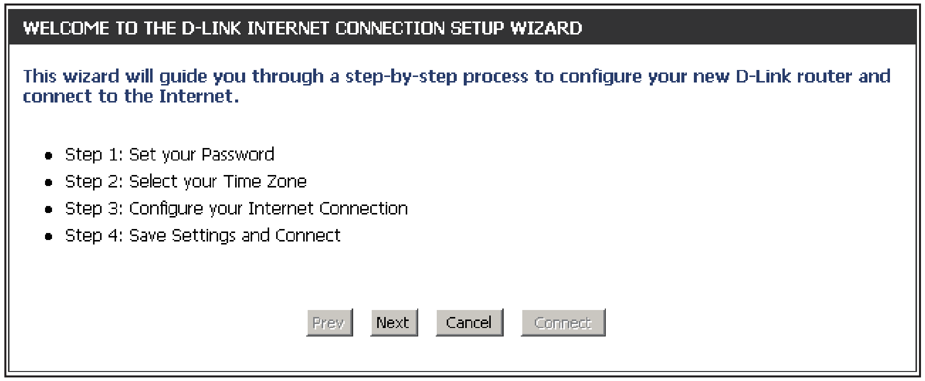
If you would like to configure the Internet settings of your new D-Link Router manually, then click on the button below.

Helpful Hints...

- If you are new to networking and have never configured a router before, click on **Internet Connection Setup Wizard** and the router will guide you through a few simple steps to get your network up and running.
- If you consider yourself an advanced user and have configured a router before, click **Manual Internet Connection Setup** to input all the settings manually.
- More...

The following window appears, summarizing the steps required to complete the Internet Connection Setup Wizard:

Click **Next** to continue.

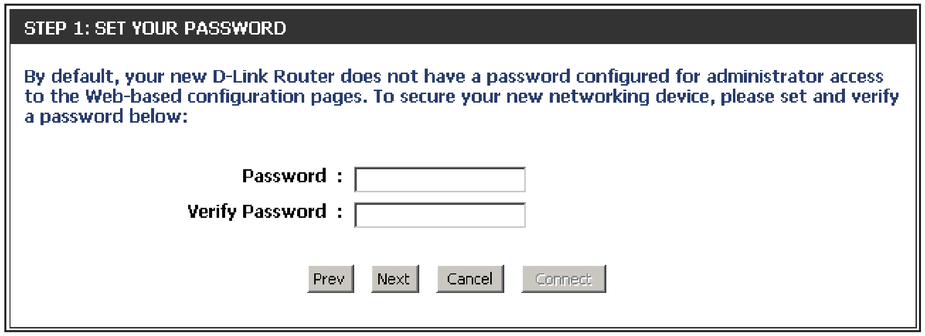


WELCOME TO THE D-LINK INTERNET CONNECTION SETUP WIZARD

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

- Step 1: Set your Password
- Step 2: Select your Time Zone
- Step 3: Configure your Internet Connection
- Step 4: Save Settings and Connect

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



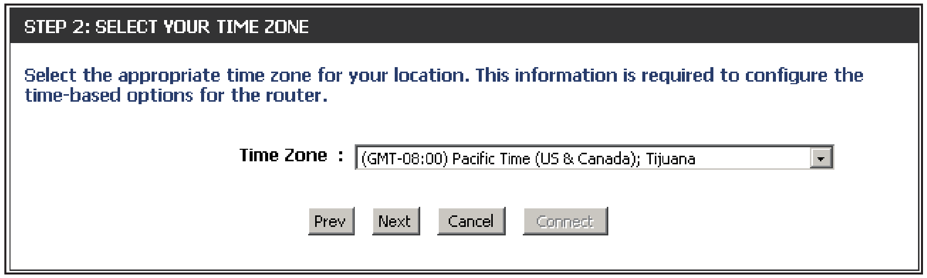
STEP 1: SET YOUR PASSWORD

By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below:

Password :

Verify Password :

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

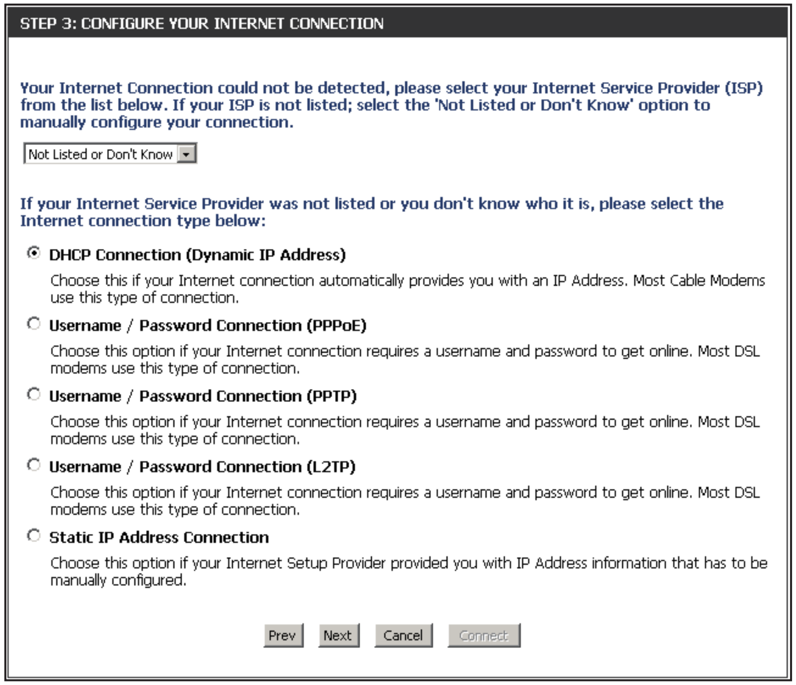


STEP 2: SELECT YOUR TIME ZONE

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

Time Zone : (GMT-08:00) Pacific Time (US & Canada); Tijuana

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



STEP 3: CONFIGURE YOUR INTERNET CONNECTION

Your Internet Connection could not be detected, please select your Internet Service Provider (ISP) from the list below. If your ISP is not listed; select the 'Not Listed or Don't Know' option to manually configure your connection.

Not Listed or Don't Know

If your Internet Service Provider was not listed or you don't know who it is, please select the Internet connection type below:

● DHCP Connection (Dynamic IP Address)

Choose this if your Internet connection automatically provides you with an IP Address. Most Cable Modems use this type of connection.

○ Username / Password Connection (PPPoE)

Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

○ Username / Password Connection (PPTP)

Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

○ Username / Password Connection (L2TP)

Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

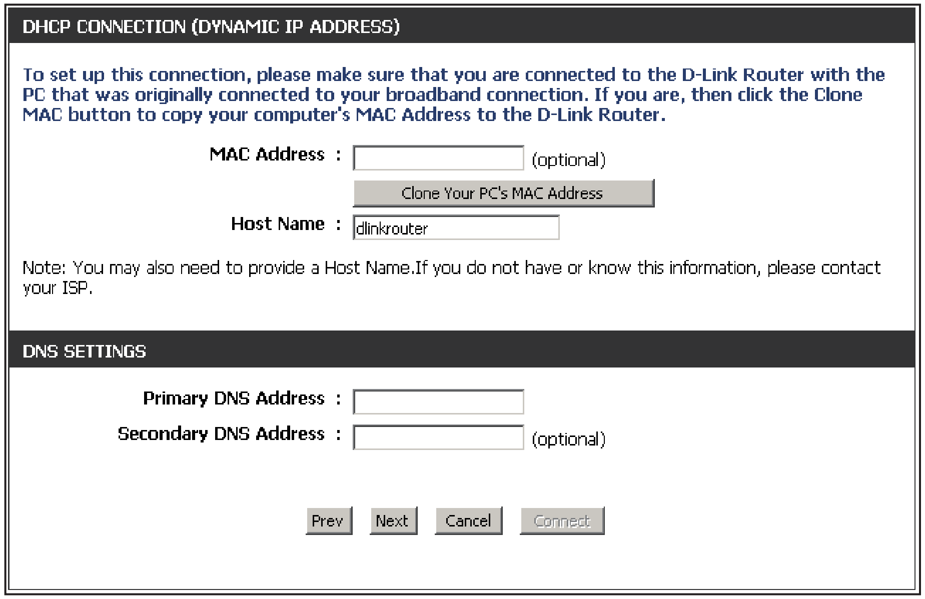
○ Static IP Address Connection

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

If you selected **DHCP Connection (Dynamic IP Address)**, you may need to enter the MAC address of the computer that was last connected directly to your modem. If you are currently using that computer, click **Clone Your PC's MAC Address**.

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

You may enter DNS servers or leave blank to use what your IPS assigns you. Click **Next** to continue.


DHCP CONNECTION (DYNAMIC IP ADDRESS)

To set up this connection, please make sure that you are connected to the D-Link Router with the PC that was originally connected to your broadband connection. If you are, then click the Clone MAC button to copy your computer's MAC Address to the D-Link Router.

MAC Address : (optional)

Host Name : dlinkrouter

Note: You may also need to provide a Host Name.If you do not have or know this information, please contact your ISP.

DNS SETTINGS

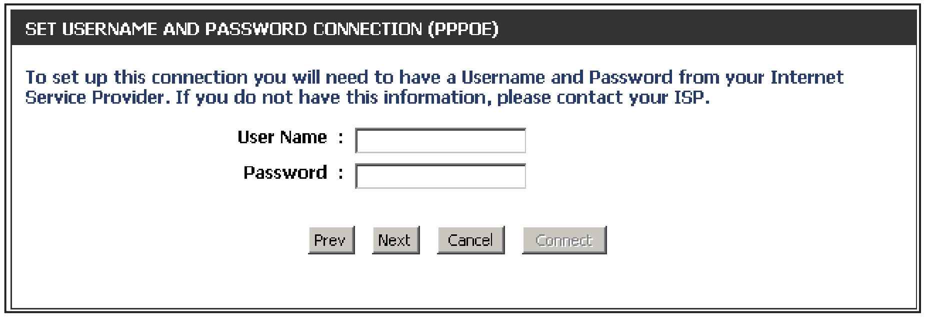
Primary DNS Address :

Secondary DNS Address : (optional)

If you selected **PPPoE**, enter your PPPoE username and password.

Click **Next** to continue.

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


SET USERNAME AND PASSWORD CONNECTION (PPPOE)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. If you do not have this information, please contact your ISP.

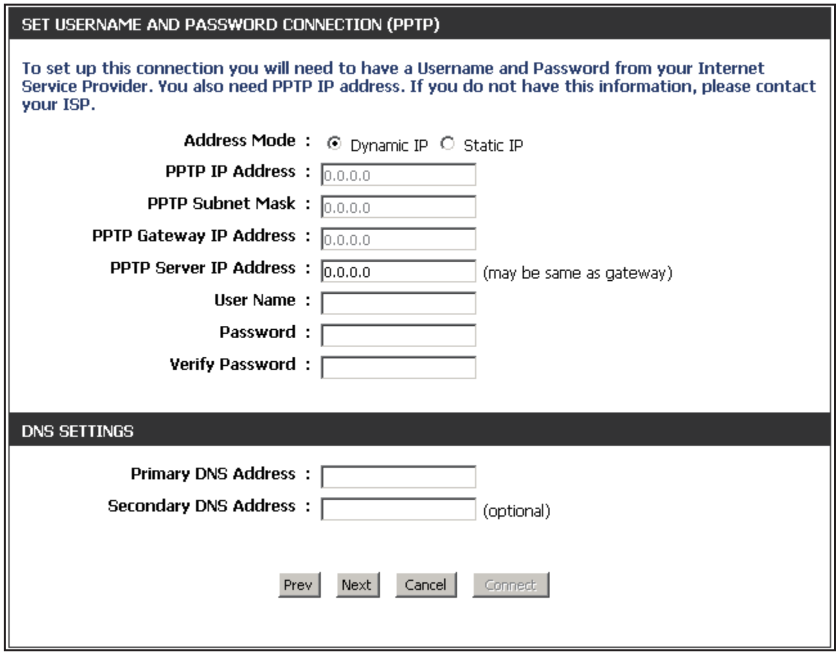
User Name :

Password :

If you selected **PPTP**, enter your PPTP username and password.

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

Click **Next** to continue.



SET USERNAME AND PASSWORD CONNECTION (PPTP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP address. If you do not have this information, please contact your ISP.

Address Mode :	● Dynamic IP ○ Static IP
PPTP IP Address :	0.0.0.0
PPTP Subnet Mask :	0.0.0.0
PPTP Gateway IP Address :	0.0.0.0
PPTP Server IP Address :	0.0.0.0 (may be same as gateway)
User Name :	
Password :	
Verify Password :	

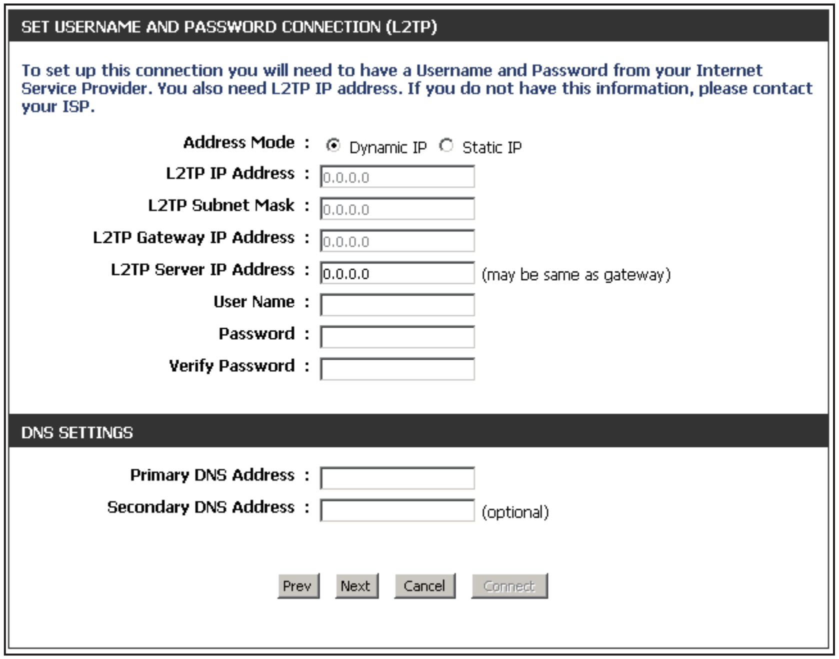
DNS SETTINGS

Primary DNS Address :	
Secondary DNS Address :	(optional)

If you selected **L2TP**, enter your L2TP username and password.

Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, L2TP and DNS server addresses.

Click **Next** to continue.



SET USERNAME AND PASSWORD CONNECTION (L2TP)

To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP address. If you do not have this information, please contact your ISP.

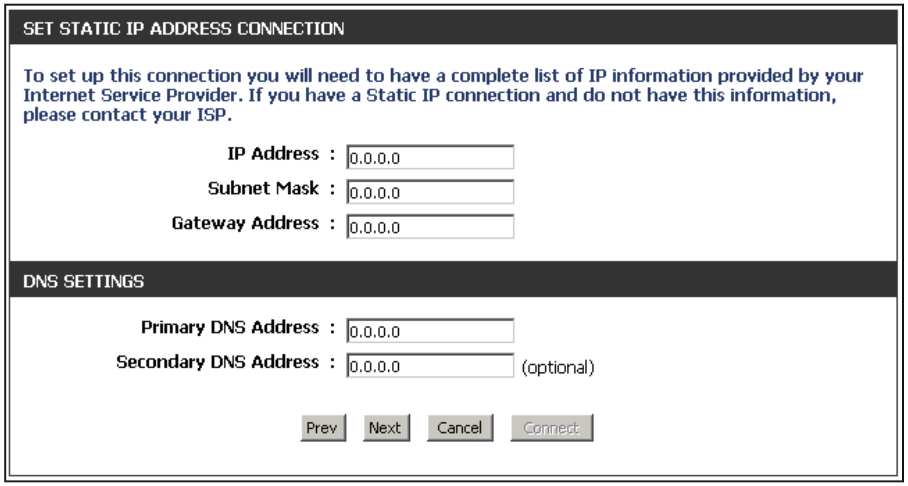
Address Mode :	● Dynamic IP ○ Static IP
L2TP IP Address :	0.0.0.0
L2TP Subnet Mask :	0.0.0.0
L2TP Gateway IP Address :	0.0.0.0
L2TP Server IP Address :	0.0.0.0 (may be same as gateway)
User Name :	
Password :	
Verify Password :	

DNS SETTINGS

Primary DNS Address :	
Secondary DNS Address :	(optional)

If you selected **Static**, enter your network settings supplied by your Internet provider.

Click **Next** to continue.



SET STATIC IP ADDRESS CONNECTION

To set up this connection you will need to have a complete list of IP information provided by your Internet Service Provider. If you have a Static IP connection and do not have this information, please contact your ISP.

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

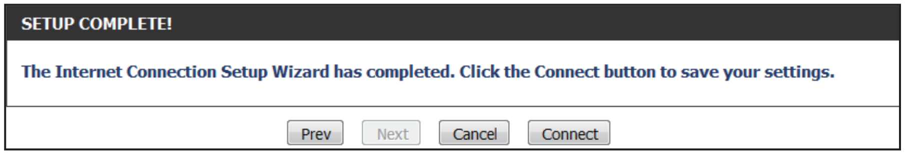
Gateway Address : 0.0.0.0

DNS SETTINGS

Primary DNS Address : 0.0.0.0

Secondary DNS Address : 0.0.0.0 (optional)

Click **Connect** to save your settings.



SETUP COMPLETE!

The Internet Connection Setup Wizard has completed. Click the Connect button to save your settings.

The following window appears to indicate that the settings are being saved. When the Router has finished saving all the changes, the **Setup** > **Internet** window will open.

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

Manual Internet Connection Setup

Static IP

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

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

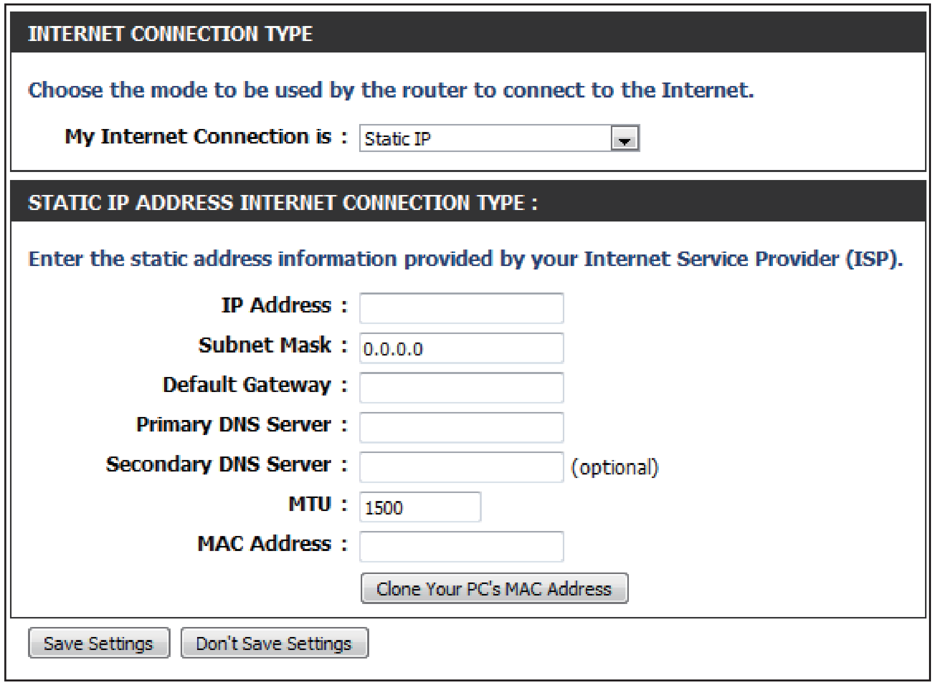
Subnet Mask: Enter the Subnet Mask assigned by your ISP.

Default Gateway: Enter the Gateway assigned by your ISP.

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

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

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



INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : Static IP

STATIC IP ADDRESS INTERNET CONNECTION TYPE :

Enter the static address information provided by your Internet Service Provider (ISP).

IP Address :

Subnet Mask : 0.0.0.0

Default Gateway :

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1500

MAC Address :

Click the **Save Settings** button to save any changes made.

Dynamic IP (DHCP)

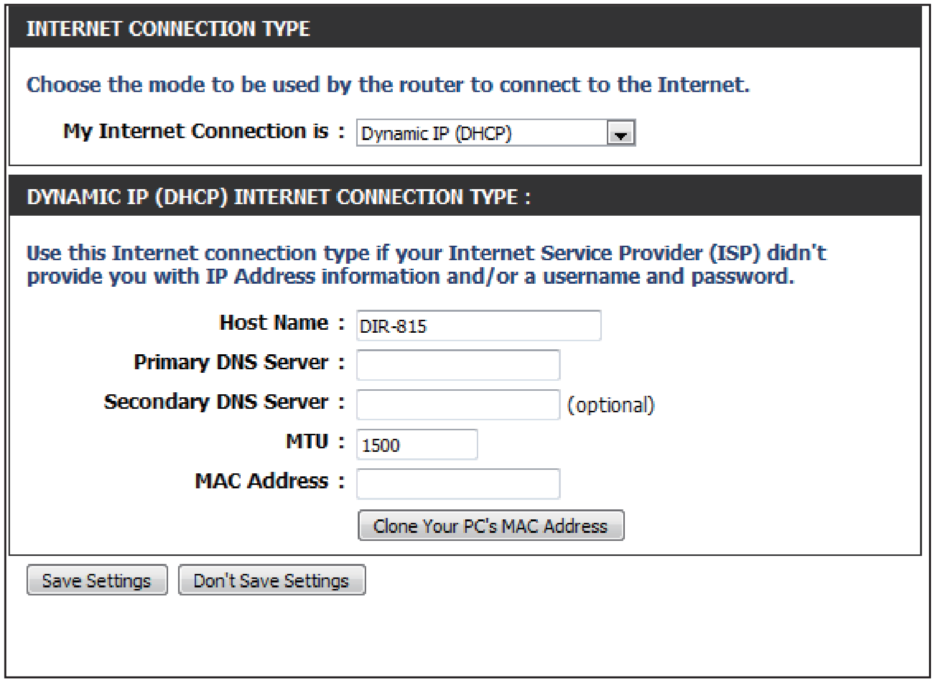
Select **Dynamic IP (DHCP)** from the drop-down menu to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for cable modem services such as Comcast and Cox.

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

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

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

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



INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : Dynamic IP (DHCP)

DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE :

Use this Internet connection type if your Internet Service Provider (ISP) didn't provide you with IP Address information and/or a username and password.

Host Name : DIR-815

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1500

MAC Address :

Click the **Save Settings** button to save any changes made.

PPPoE (Username/Password)

Select **PPPoE (Username/Password)** from the drop-down menu 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.

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

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

User Name: Enter your PPPoE user name.

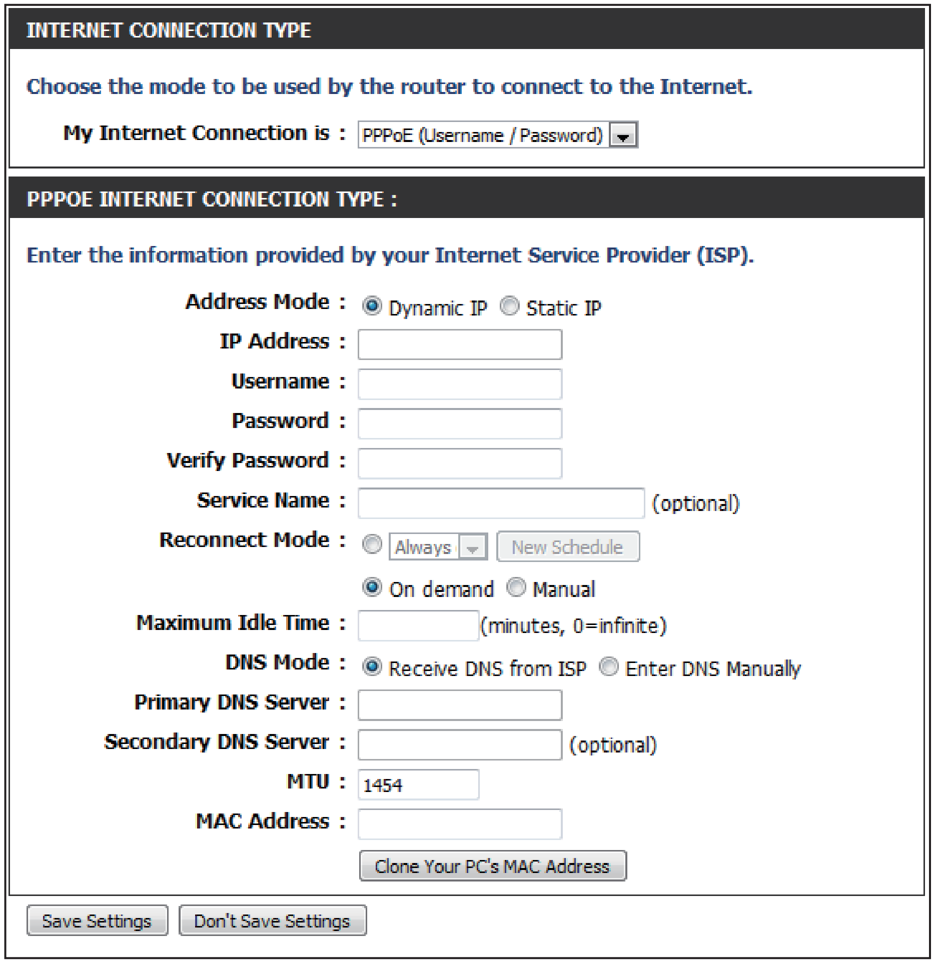
Password: Enter your PPPoE password and then retype the password in the next box.

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

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand** or **Manual** option. To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the **Tools** > **Schedules** window. To create a new schedule, click the **New Schedule** button Refer to “Schedules” on page 97 for more information.

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 PPPoE only).



INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : PPPoE (Username / Password)

PPPOE INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : ● Dynamic IP ○ Static IP

IP Address :

Username :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode : ○ Always New Schedule

● On demand ○ Manual

Maximum Idle Time : (minutes, 0=infinite)

DNS Mode : ● Receive DNS from ISP ○ Enter DNS Manually

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1454

MAC Address :

Clone Your PC's MAC Address

Save Settings Don't Save Settings

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1454 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.

Click the **Save Settings** button to save any changes made.

PPTP

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

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

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

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

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

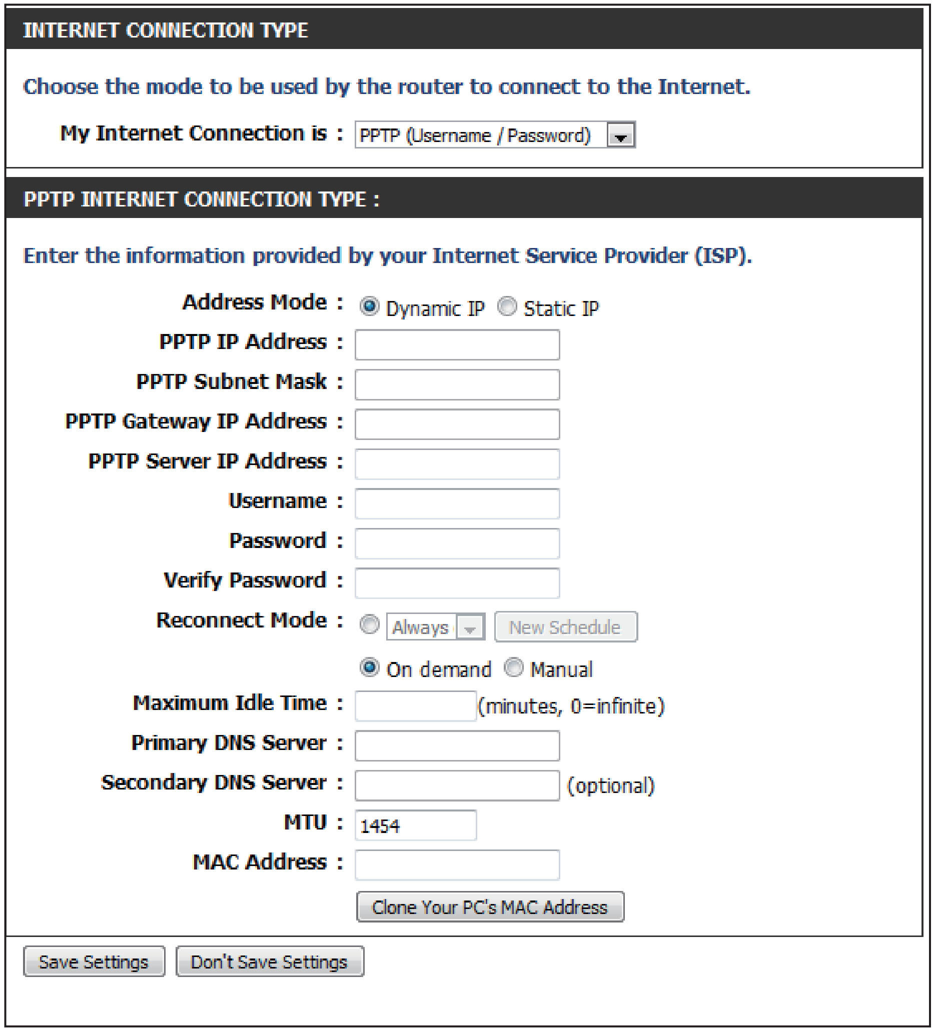
PPTP Server IP Address: Enter the Server IP provided by your ISP (optional).

Username: Enter your PPTP username.

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

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand** or **Manual** option.

To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the **Tools** > **Schedules** window. To create a new schedule, click the **New Schedule** button. Refer to “Schedules” on page 97 for more information.



INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : PPTP (Username / Password)

PPTP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : ● Dynamic IP ○ Static IP

PPTP IP Address :

PPTP Subnet Mask :

PPTP Gateway IP Address :

PPTP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : ○ Always New Schedule

● On demand ○ Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1454

MAC Address :

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

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

MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1454 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.

Click the **Save Settings** button to save any changes made.

L2TP

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

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

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

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

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

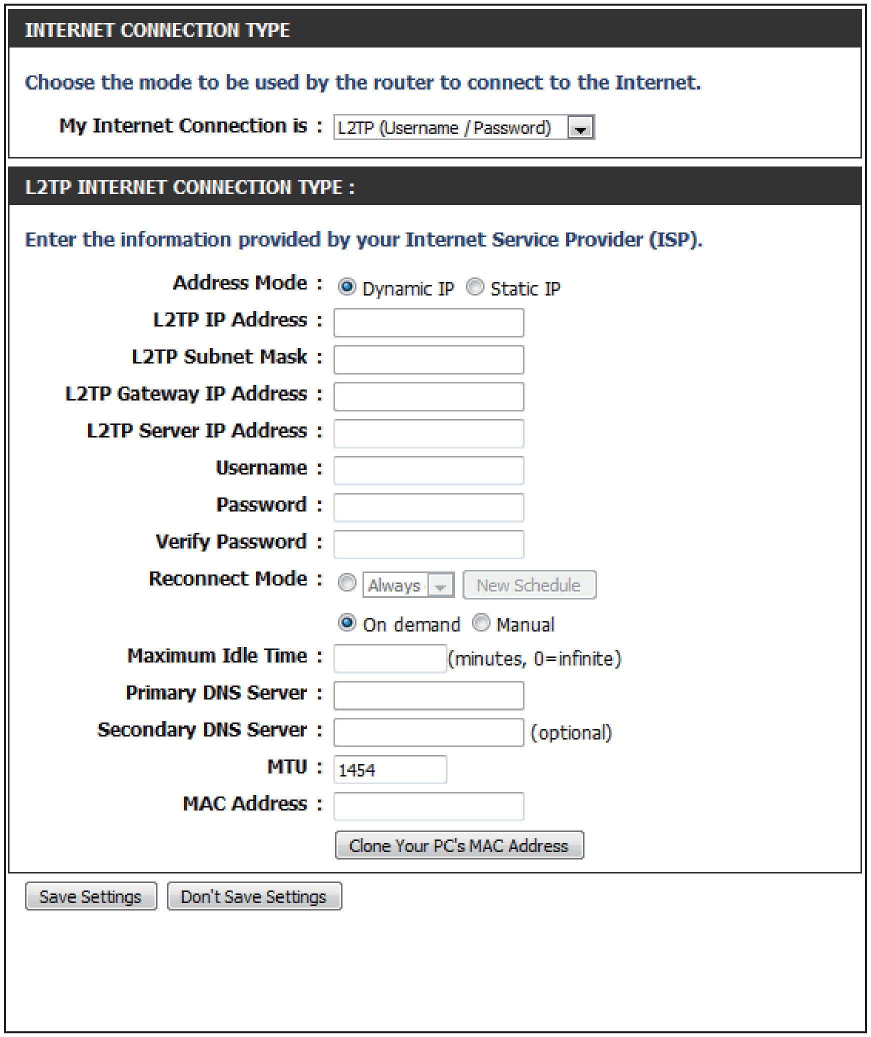
L2TP Server IP Address: Enter the Server IP provided by your ISP (optional).

Username: Enter your L2TP username.

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

Reconnect Mode: Use the radio buttons to specify the reconnect mode. The user can specify a custom schedule or specify the **On Demand** or **Manual** option.

To specify a custom schedule, use the drop-down menu to select one of the schedules that has been defined in the **Tools** > **Schedules** window. To create a new schedule, click the **New Schedule** button. Refer to "Schedules" on page 97 for more information.



INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : L2TP (Username / Password)

L2TP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

Address Mode : ● Dynamic IP ○ Static IP

L2TP IP Address :

L2TP Subnet Mask :

L2TP Gateway IP Address :

L2TP Server IP Address :

Username :

Password :

Verify Password :

Reconnect Mode : ○ Always New Schedule

● On demand ○ Manual

Maximum Idle Time : (minutes, 0=infinite)

Primary DNS Server :

Secondary DNS Server : (optional)

MTU : 1454

MAC Address :

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. 1454 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.

Click the **Save Settings** button to save any changes made.

DS-Lite

Another Internet Connection type is DS-Lite.

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

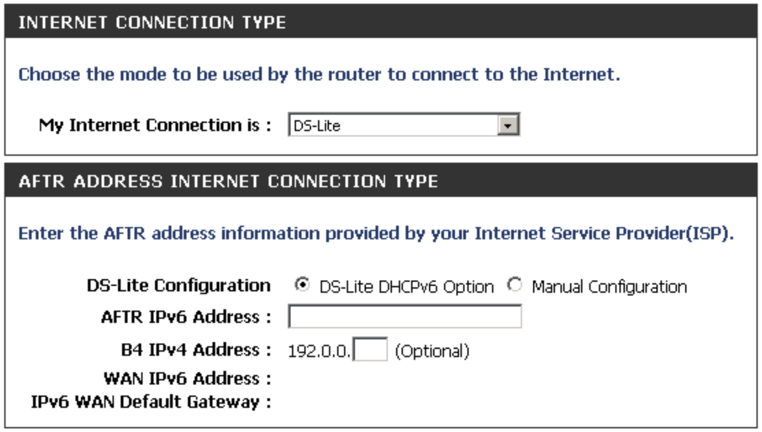
DS-Lite Configuration: Select the DS-Lite DHCPv6 option to let the router allocate the AFTR IPv6 address automatically. Select the Manual Configuration to enter the AFTR IPv6 address in manually.

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

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

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

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



INTERNET CONNECTION TYPE

Choose the mode to be used by the router to connect to the Internet.

My Internet Connection is : DS-Lite

AFTR ADDRESS INTERNET CONNECTION TYPE

Enter the AFTR address information provided by your Internet Service Provider(ISP).

DS-Lite Configuration ● DS-Lite DHCPv6 Option ○ Manual Configuration

AFTR IPv6 Address :

B4 IPv4 Address : 192.0.0. (Optional)

WAN IPv6 Address :

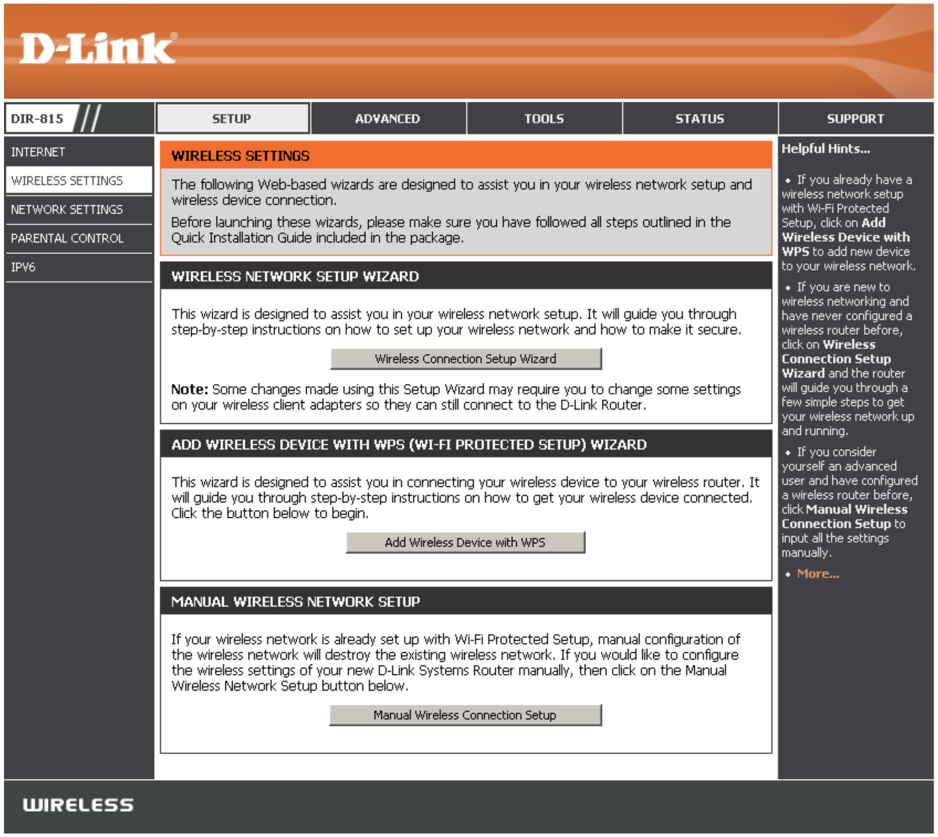
IPv6 WAN Default Gateway :

Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Connection Setup Wizard** and refer to page 41.

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 43.

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



WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

MANUAL WIRELESS NETWORK SETUP

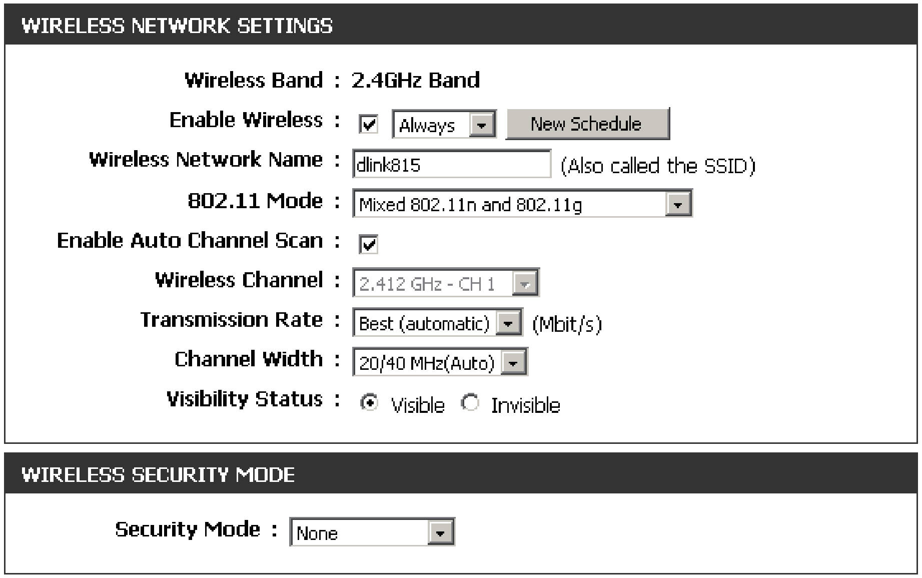
If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

Helpful Hints...

- If you already have a wireless network setup with Wi-Fi Protected Setup, click on **Add Wireless Device with WPS** to add new device to your wireless network.
- If you are new to wireless networking and have never configured a wireless router before, click on **Wireless Connection Setup Wizard** and the router will guide you through a few simple steps to get your wireless network up and running.
- If you consider yourself an advanced user and have configured a wireless router before, click **Manual Wireless Connection Setup** to input all the settings manually.
- More...

Manual Wireless Settings

802.11n/b/g (2.4GHz)



WIRELESS NETWORK SETTINGS

Wireless Band :	2.4GHz Band
Enable Wireless :	☑ Always ▾ New Schedule
Wireless Network Name :	dlink815 (Also called the SSID)
802.11 Mode :	Mixed 802.11n and 802.11g ▾
Enable Auto Channel Scan :	☑
Wireless Channel :	2.412 GHz - CH 1 ▾
Transmission Rate :	Best (automatic) ▾ (Mbit/s)
Channel Width :	20/40 MHz(Auto) ▾
Visibility Status :	● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode :	None ▾

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

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

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

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

Auto Channel Selection: The **Auto Channel Selection** setting can be selected to allow the DIR-815 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-815. 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 Selection**, this option will be greyed out.

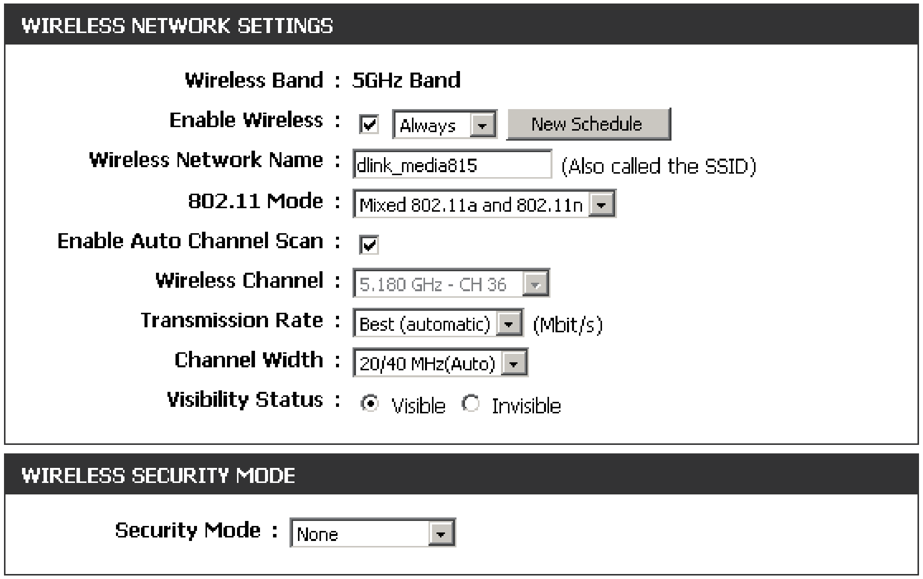
Transmission Rate: Select the transmit rate. It is strongly suggested to select **Best (Automatic)** for best performance.

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.

Visibility Status: Check this box if you do not want the SSID of your wireless network to be broadcast by the DIR-815. If the SSID is hidden, the SSID of the DIR-815 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-815 in order to connect to it.

Wireless Security Mode: Refer to “Wireless Security” on page 40 for more information regarding wireless security.

802.11n/a (5GHz)



WIRELESS NETWORK SETTINGS

Wireless Band : 5GHz Band

Enable Wireless : ☑ Always ▾ [New Schedule]

Wireless Network Name : dlink_media815 (Also called the SSID)

802.11 Mode : Mixed 802.11a and 802.11n ▾

Enable Auto Channel Scan : ☑

Wireless Channel : 5.180 GHz - CH 36 ▾

Transmission Rate : Best (automatic) ▾ (Mbit/s)

Channel Width : 20/40 MHz(Auto) ▾

Visibility Status : ● Visible ○ Invisible

WIRELESS SECURITY MODE

Security Mode : None ▾

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

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

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

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

Auto Channel Selection: The **Auto Channel Selection** setting can be selected to allow the DIR-815 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-815. 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 Selection**, this option will be greyed out.

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

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.

Visibility Status: Check this box if you do not want the SSID of your wireless network to be broadcast by the DIR-815. If the SSID is hidden, the SSID of the DIR-815 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-815 in order to connect to it.

Wireless Security Mode: Refer to "Wireless Security" on the next page for more information regarding wireless security.

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-815 offers the following types of security:

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

What is WPA?

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

The 2 major improvements over WEP:

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

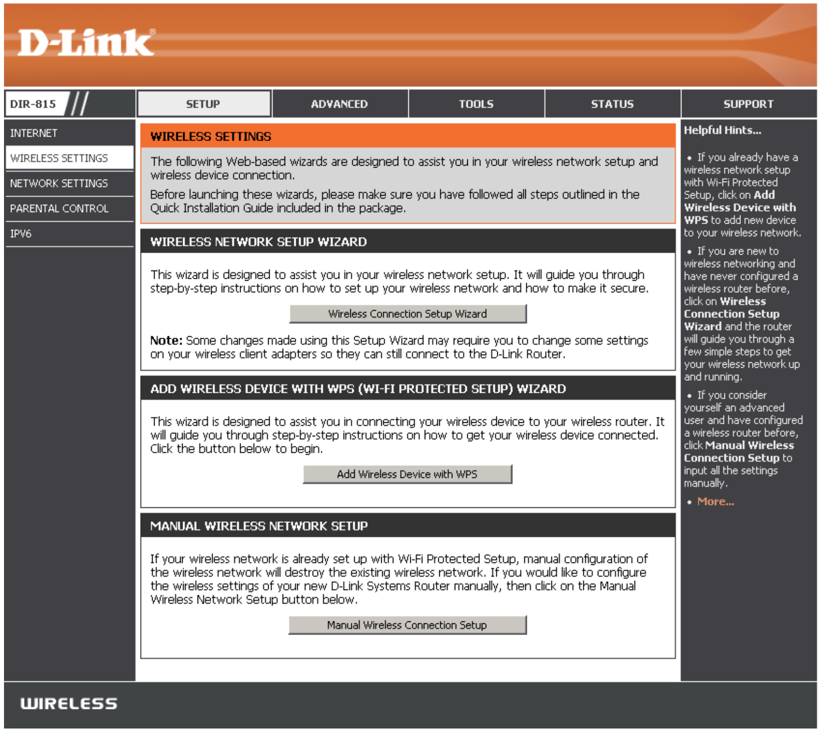
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key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

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

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

Wireless Connection Setup Wizard

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



WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

Before launching these wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

MANUAL WIRELESS NETWORK SETUP

If your wireless network is already set up with Wi-Fi Protected Setup, manual configuration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup button below.

Helpful Hints...

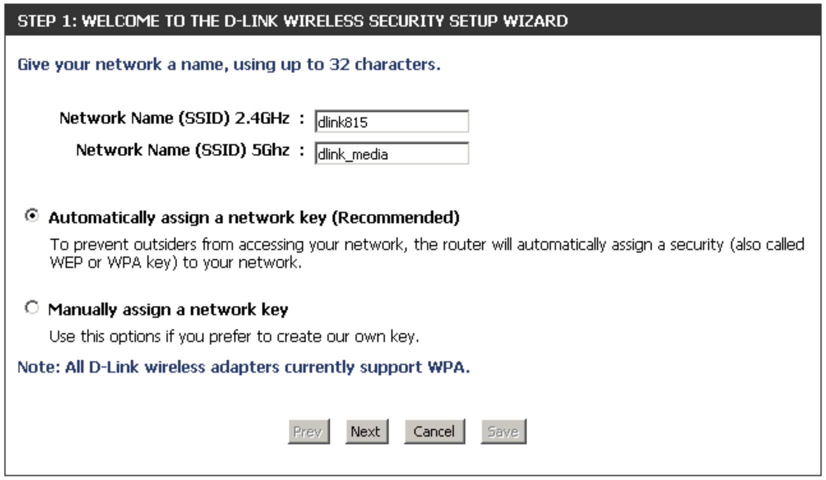
- If you already have a wireless network setup with Wi-Fi Protected Setup, click on **Add Wireless Device with WPS** to add new device to your wireless network.
- If you are new to wireless networking and have never configured a wireless router before, click on **Wireless Connection Setup Wizard** and the router will guide you through a few simple steps to get your wireless network up and running.
- If you consider yourself an advanced user and have configured a wireless router before, click **Manual Wireless Connection Setup** to input all the settings manually.
- **More...**

Check the **Manually set 5GHz band Network Name...** box to manually set your desired wireless network name for the 5GHz band.

Type your desired wireless network name (SSID).

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

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



STEP 1: WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

Give your network a name, using up to 32 characters.

Network Name (SSID) 2.4GHz : dlink815

Network Name (SSID) 5Ghz : dlink_media

● Automatically assign a network key (Recommended)

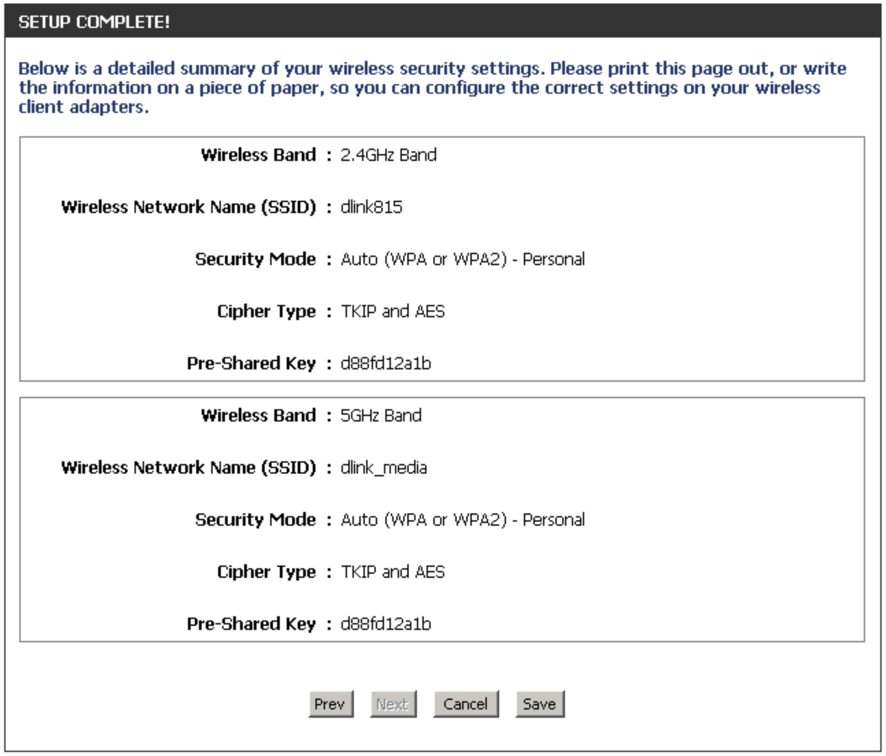
To prevent outsiders from accessing your network, the router will automatically assign a security (also called WEP or WPA key) to your network.

○ Manually assign a network key

Use this options if you prefer to create our own key.

Note: All D-Link wireless adapters currently support WPA.

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



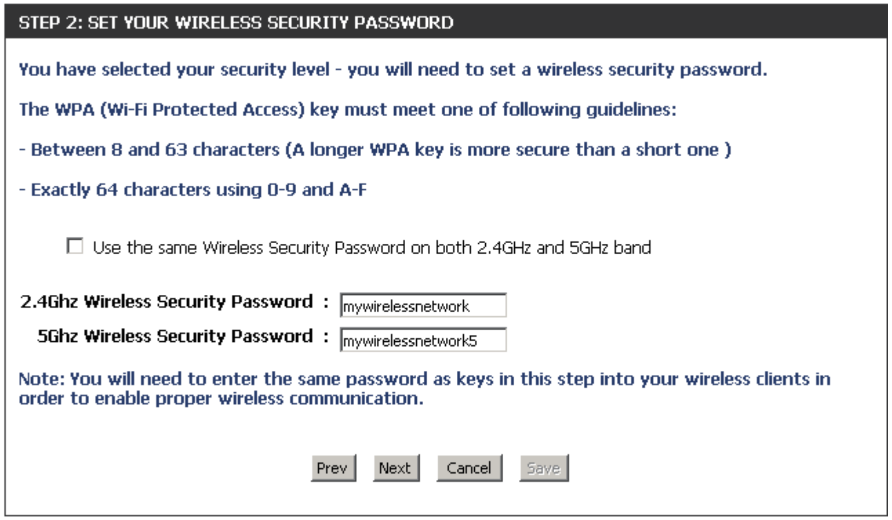
SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Band :	2.4GHz Band
Wireless Network Name (SSID) :	dlink815
Security Mode :	Auto (WPA or WPA2) - Personal
Cipher Type :	TKIP and AES
Pre-Shared Key :	d88fd12a1b

Wireless Band :	5GHz Band
Wireless Network Name (SSID) :	dlink_media
Security Mode :	Auto (WPA or WPA2) - Personal
Cipher Type :	TKIP and AES
Pre-Shared Key :	d88fd12a1b

If you selected **Manually**, the following screen will appear.



STEP 2: SET YOUR WIRELESS SECURITY PASSWORD

You have selected your security level - you will need to set a wireless security password.

The WPA (Wi-Fi Protected Access) key must meet one of following guidelines:

- Between 8 and 63 characters (A longer WPA key is more secure than a short one)

- Exactly 64 characters using 0-9 and A-F

□ Use the same Wireless Security Password on both 2.4GHz and 5GHz band

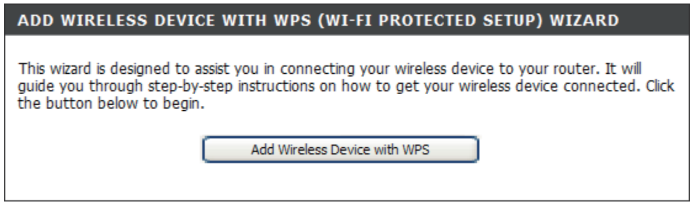
2.4Ghz Wireless Security Password : mywirelessnetwork

5Ghz Wireless Security Password : mywirelessnetwork5

Note: You will need to enter the same password as keys in this step into your wireless clients in order to enable proper wireless communication.

Add Wireless Device with WPS Wizard

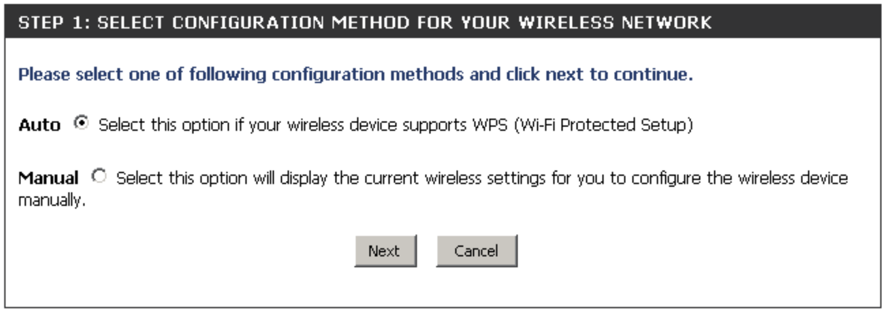
From the **Setup** > **Wireless Settings** screen, click **Add Wireless Device with WPS**.



ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

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



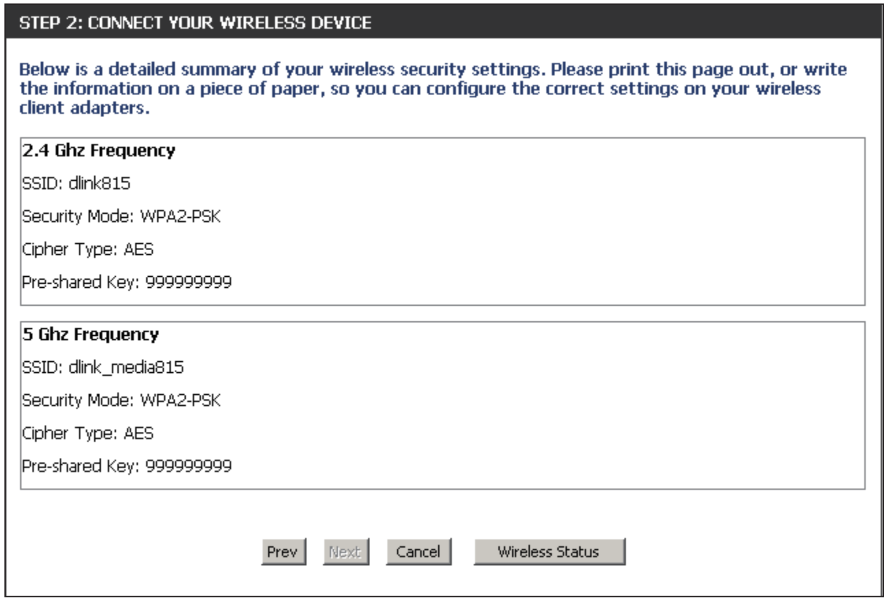
STEP 1: SELECT CONFIGURATION METHOD FOR YOUR WIRELESS NETWORK

Please select one of following configuration methods and click next to continue.

Auto ● Select this option if your wireless device supports WPS (Wi-Fi Protected Setup)

Manual ○ Select this option will display the current wireless settings for you to configure the wireless device manually.

If you select **Manual**, a settings summary screen will appear. Write down the security key and enter this on your wireless clients. Click **OK** to finish.



STEP 2: CONNECT YOUR WIRELESS DEVICE

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

2.4 Ghz Frequency

SSID: dlink815

Security Mode: WPA2-PSK

Cipher Type: AES

Pre-shared Key: 999999999

5 Ghz Frequency

SSID: dlink_media815

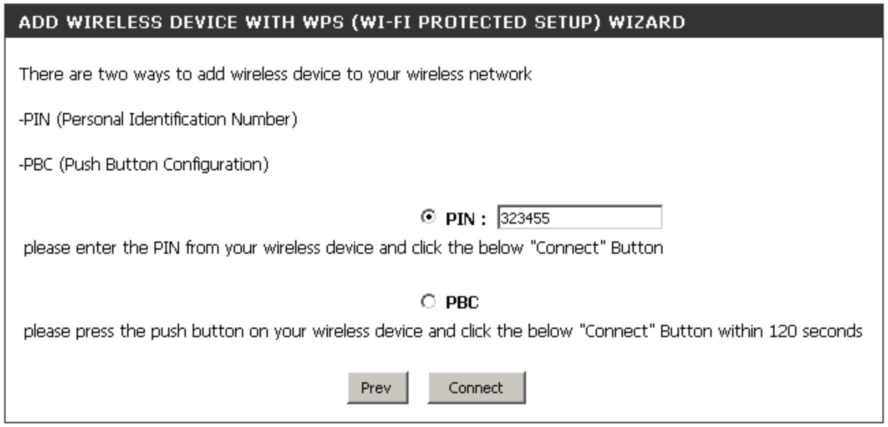
Security Mode: WPA2-PSK

Cipher Type: AES

Pre-shared Key: 999999999

PIN: Select this option to use PIN method. In order to use this method you must know the wireless client's 8 digit PIN and click **Connect**.

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



ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

There are two ways to add wireless device to your wireless network

-PIN (Personal Identification Number)

-PBC (Push Button Configuration)

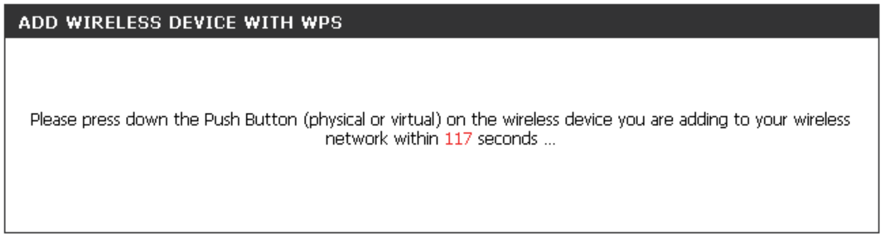
● PIN : 323455

please enter the PIN from your wireless device and click the below "Connect" Button

○ PBC

please press the push button on your wireless device and click the below "Connect" Button within 120 seconds

Once you click **Connect**, you will have a 120 second time limit to apply the settings to your wireless client(s) and successfully establish a connection.



ADD WIRELESS DEVICE WITH WPS

Please press down the Push Button (physical or virtual) on the wireless device you are adding to your wireless network within 117 seconds ...

WPA/WPA2-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**.

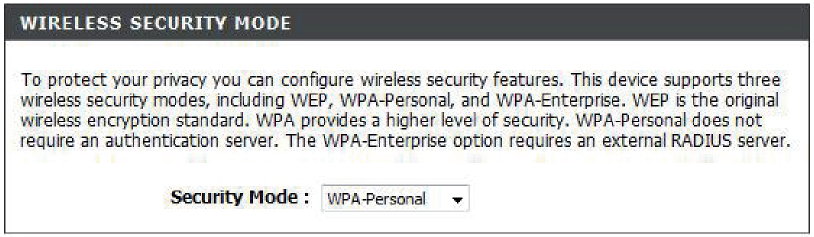
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

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

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

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

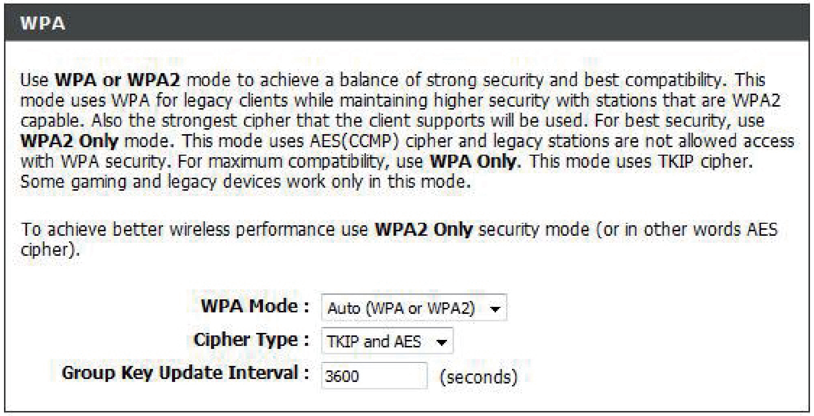
7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WPA-PSK on your adapter and enter the same passphrase as you did on the router.



WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes, including WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal



WPA

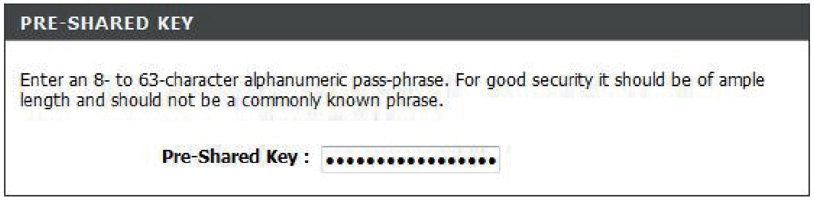
Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : Auto (WPA or WPA2)

Cipher Type : TKIP and AES

Group Key Update Interval : 3600 (seconds)



PRE-SHARED KEY

Enter an 8- to 63-character alphanumeric pass-phrase. For good security it should be of ample length and should not be a commonly known phrase.

Pre-Shared Key : ••••••••••••••••

Configure WPA/WPA2-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.

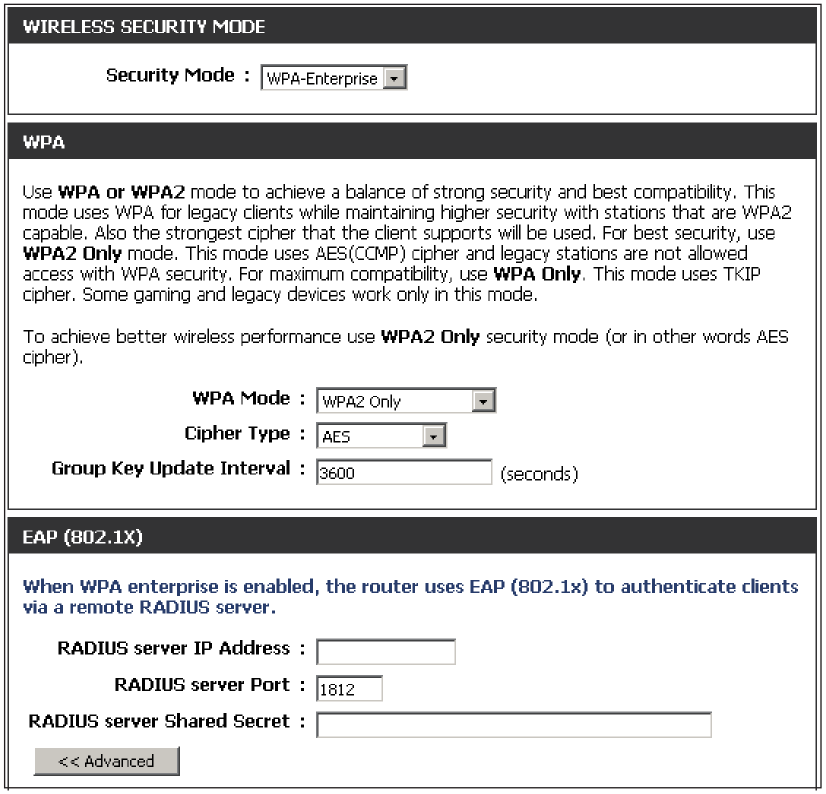
2. Next to *Security Mode*, select **WPA-Enterprise**.

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 *Cypher Type*, select **TKIP and AES**, **TKIP**, or **AES**.

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

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



WIRELESS SECURITY MODE

Security Mode : WPA-Enterprise

WPA

Use **WPA or WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES(CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : WPA2 Only

Cipher Type : AES

Group Key Update Interval : 3600 (seconds)

EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port : 1812

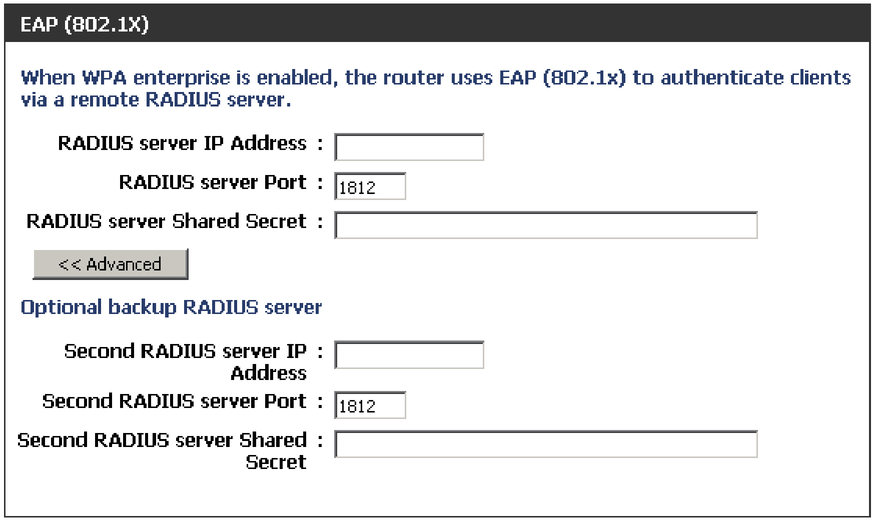
RADIUS server Shared Secret :

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

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

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

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



EAP (802.1X)

When WPA enterprise is enabled, the router uses EAP (802.1x) to authenticate clients via a remote RADIUS server.

RADIUS server IP Address :

RADIUS server Port : 1812

RADIUS server Shared Secret :

Optional backup RADIUS server

Second RADIUS server IP Address :

Second RADIUS server Port : 1812

Second RADIUS server Shared Secret :

Network Settings

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

Router Settings

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

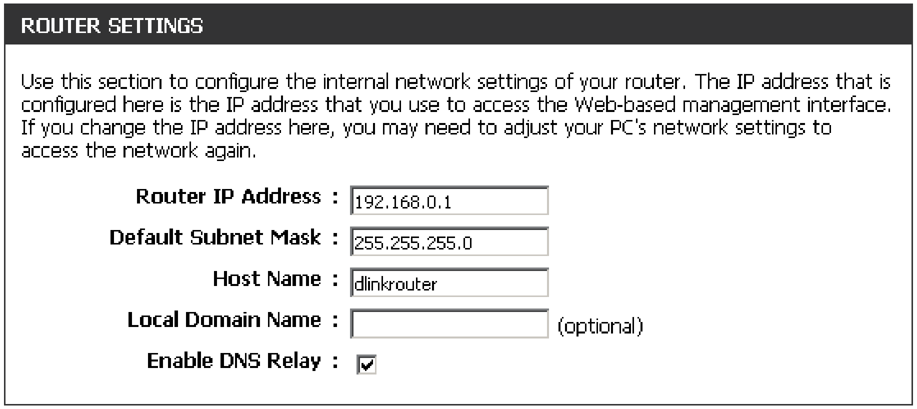
If you change the IP address, once you click **Save Settings**, you will need to enter the new IP address in your browser to get back into the configuration utility.

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

Host Name: Enter a name for the router.

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

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



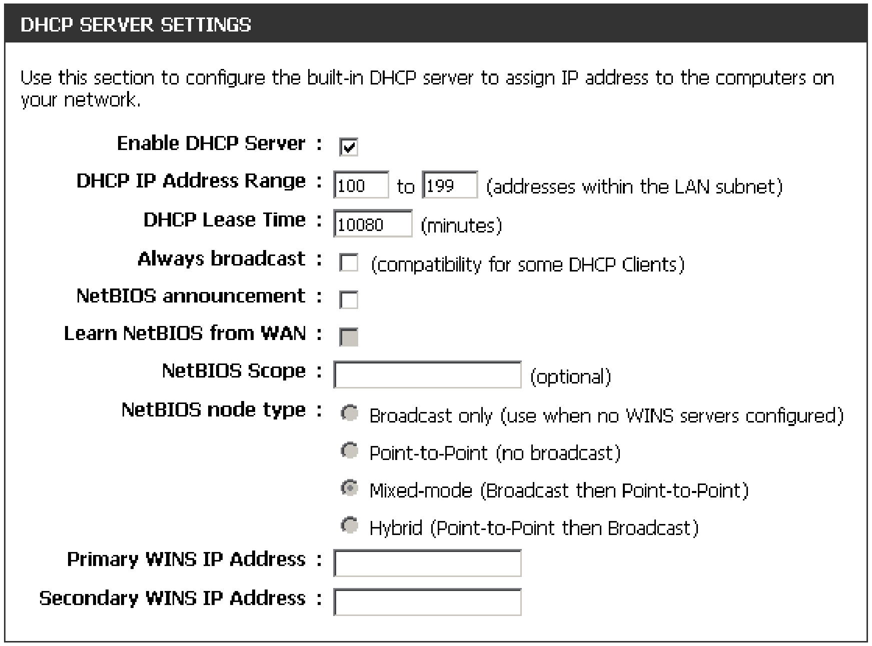
ROUTER SETTINGS

Use this section to configure the internal network settings of your router. The IP address that is configured here is the IP address that you use to access the Web-based management interface. If you change the IP address here, you may need to adjust your PC's network settings to access the network again.

Router IP Address :	192.168.0.1
Default Subnet Mask :	255.255.255.0
Host Name :	dlinkrouter
Local Domain Name :	(optional)
Enable DNS Relay :	☑

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-815 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-815. 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.



DHCP SERVER SETTINGS

Use this section to configure the built-in DHCP server to assign IP address to the computers on your network.

Enable DHCP Server : ☑

DHCP IP Address Range : 100 to 199 (addresses within the LAN subnet)

DHCP Lease Time : 10080 (minutes)

Always broadcast : □ (compatibility for some DHCP Clients)

NetBIOS announcement : □

Learn NetBIOS from WAN : □

NetBIOS Scope : ______ (optional)

NetBIOS node type :
- ○ Broadcast only (use when no WINS servers configured)
- ○ Point-to-Point (no broadcast)
- ● Mixed-mode (Broadcast then Point-to-Point)
- ○ Hybrid (Point-to-Point then Broadcast)

Primary WINS IP Address : ______

Secondary WINS IP Address : ______

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

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

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

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

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

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

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

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

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

WINS IP Address: Enter your WINS Server IP address(es).

DHCP Reservation

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

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

Enable: Check this box to enable the reservation.

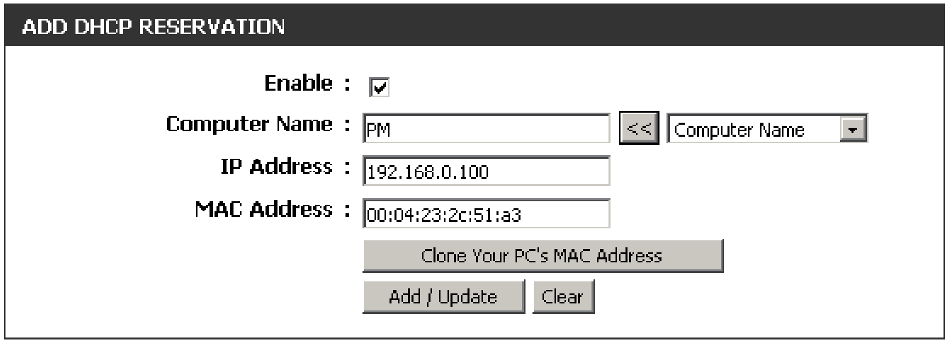
Computer Name: Enter the computer name or select from the drop-down menu and click **<<**.

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

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

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

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



ADD DHCP RESERVATION

Enable : ☑

Computer Name : PM

IP Address : 192.168.0.100

MAC Address : 00:04:23:2c:51:a3

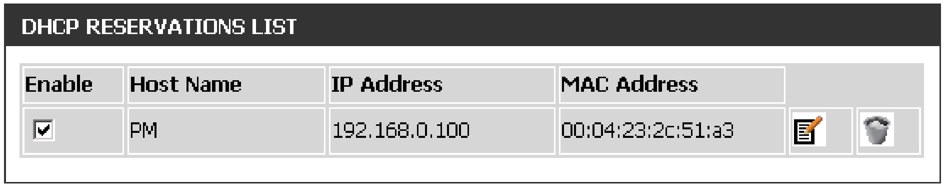
DHCP Reservations List

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

Enable: Check to enable the reservation.

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

Delete: Click to remove the reservation from the list.



DHCP RESERVATIONS LIST

Enable	Host Name	IP Address	MAC Address		
☑	PM	192.168.0.100	00:04:23:2c:51:a3	✎	🗑

Parental Controls

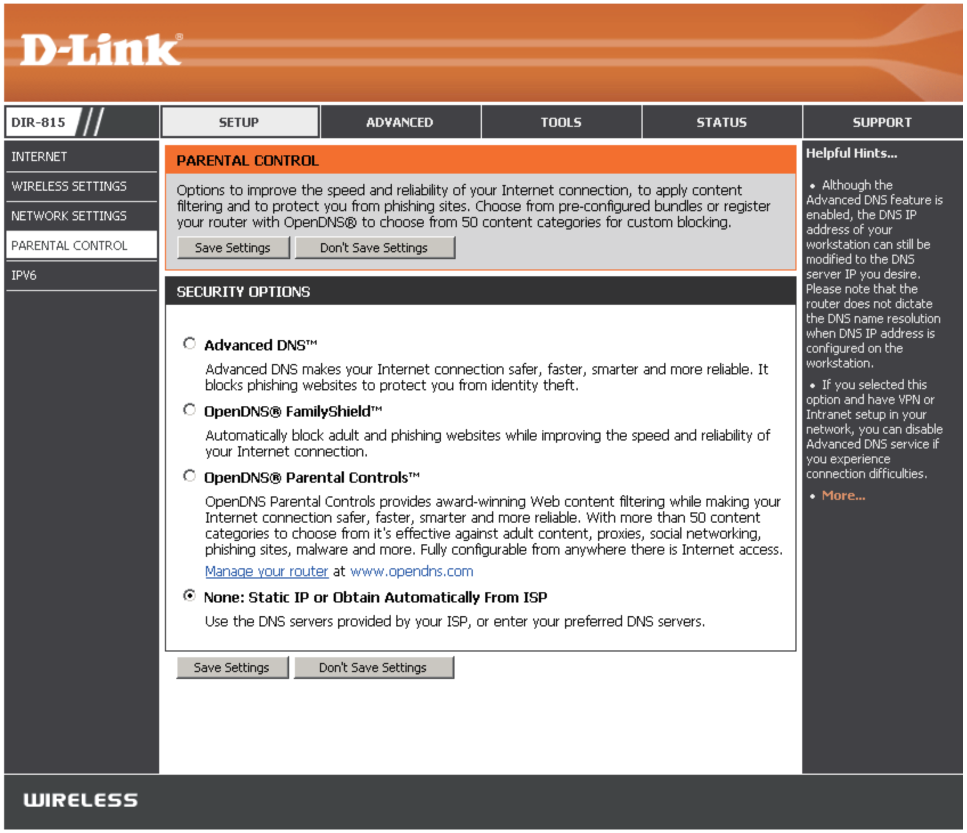
Advanced DNS Service is a free security option that provides anti-phishing protection to your network and offers navigation improvements such as auto-correction of common URL typos.

Advanced DNS: Faster, more reliable Internet browsing.

Open DNS FamilyShield: Includes Advanced DNS™ and automatic protection from malware, phishing, and adult websites. This option uses OpenDNS®.

Open DNS Parental Controls: Includes Advanced DNS™, FamilyShield™, and customizable blocking of malware and phishing sites. You may also customize filtering of web content by category. This option uses OpenDNS®.

None: DNS servers will be provided via DHCP by your ISP or you may manually enter DNS servers.



PARENTAL CONTROL

Options to improve the speed and reliability of your Internet connection, to apply content filtering and to protect you from phishing sites. Choose from pre-configured bundles or register your router with OpenDNS® to choose from 50 content categories for custom blocking.

SECURITY OPTIONS

○ **Advanced DNS™**

Advanced DNS makes your Internet connection safer, faster, smarter and more reliable. It blocks phishing websites to protect you from identity theft.

○ **OpenDNS® FamilyShield™**

Automatically block adult and phishing websites while improving the speed and reliability of your Internet connection.

○ **OpenDNS® Parental Controls™**

OpenDNS Parental Controls provides award-winning Web content filtering while making your Internet connection safer, faster, smarter and more reliable. With more than 50 content categories to choose from it's effective against adult content, proxies, social networking, phishing sites, malware and more. Fully configurable from anywhere there is Internet access.

Manage your router at www.opendns.com

● **None: Static IP or Obtain Automatically From ISP**

Use the DNS servers provided by your ISP, or enter your preferred DNS servers.

Helpful Hints...

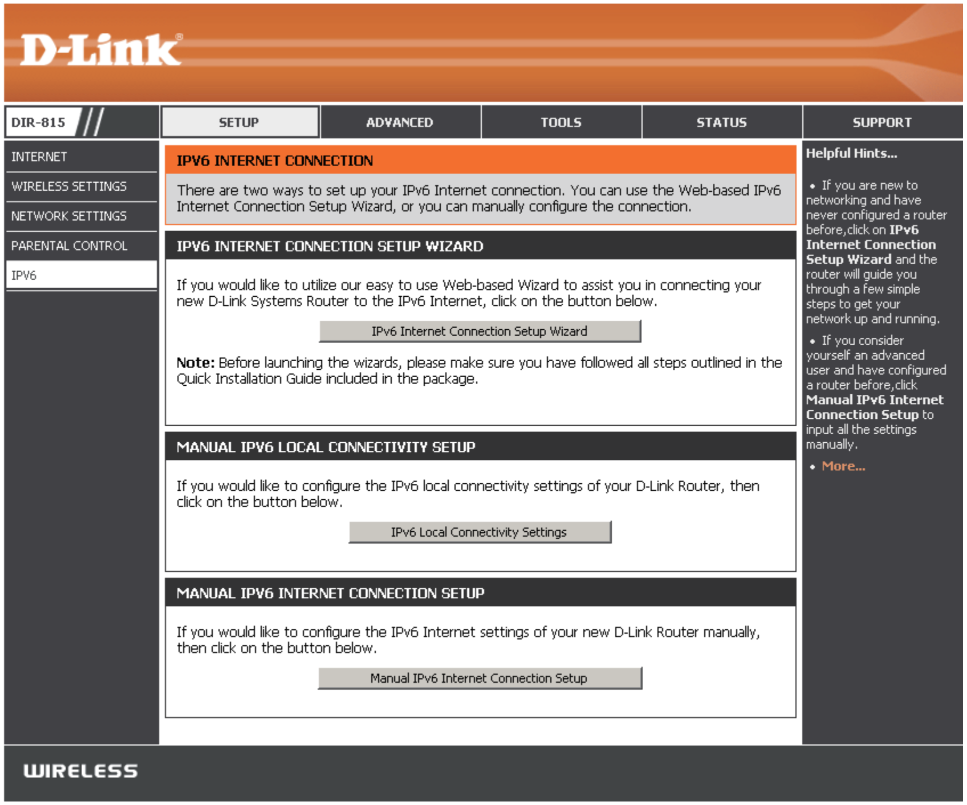
- Although the Advanced DNS feature is enabled, the DNS IP address of your workstation can still be modified to the DNS server IP you desire. Please note that the router does not dictate the DNS name resolution when DNS IP address is configured on the workstation.
- If you selected this option and have VPN or Intranet setup in your network, you can disable Advanced DNS service if you experience connection difficulties.
- More...

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.

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.



IPV6 INTERNET CONNECTION

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

IPV6 INTERNET CONNECTION SETUP WIZARD

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the IPv6 Internet, click on the button below.

Note: Before launching the wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

MANUAL IPV6 LOCAL CONNECTIVITY SETUP

If you would like to configure the IPv6 local connectivity settings of your D-Link Router, then click on the button below.

MANUAL IPV6 INTERNET CONNECTION SETUP

If you would like to configure the IPv6 Internet settings of your new D-Link Router manually, then click on the button below.

Helpful Hints...

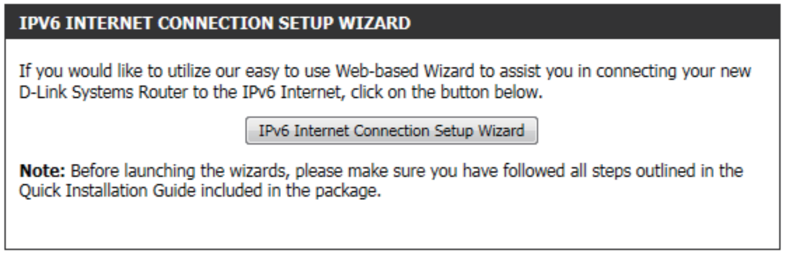
- If you are new to networking and have never configured a router before,click on **IPv6 Internet Connection Setup Wizard** and the router will guide you through a few simple steps to get your network up and running.
- If you consider yourself an advanced user and have configured a router before,click **Manual IPv6 Internet Connection Setup** to input all the settings manually.
- More...

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.

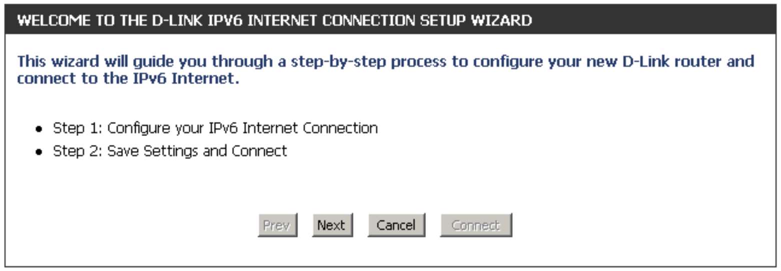


IPV6 INTERNET CONNECTION SETUP WIZARD

If you would like to utilize our easy to use Web-based Wizard to assist you in connecting your new D-Link Systems Router to the IPv6 Internet, click on the button below.

Note: Before launching the wizards, please make sure you have followed all steps outlined in the Quick Installation Guide included in the package.

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

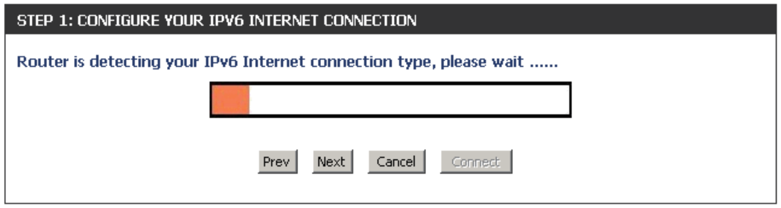


WELCOME TO THE D-LINK IPV6 INTERNET CONNECTION SETUP WIZARD

This wizard will guide you through a step-by-step process to configure your new D-Link router and connect to the IPv6 Internet.

- Step 1: Configure your IPv6 Internet Connection
- Step 2: Save Settings and Connect

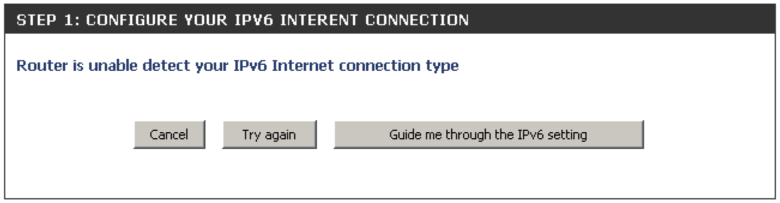
The router will try to detect whether its possible to obtain the IPv6 Internet connection type automatically. If this succeeds then the user will be guided through the input of the appropriate parameters for the connection type found.



STEP 1: CONFIGURE YOUR IPV6 INTERNET CONNECTION

Router is detecting your IPv6 Internet connection type, please wait ......

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

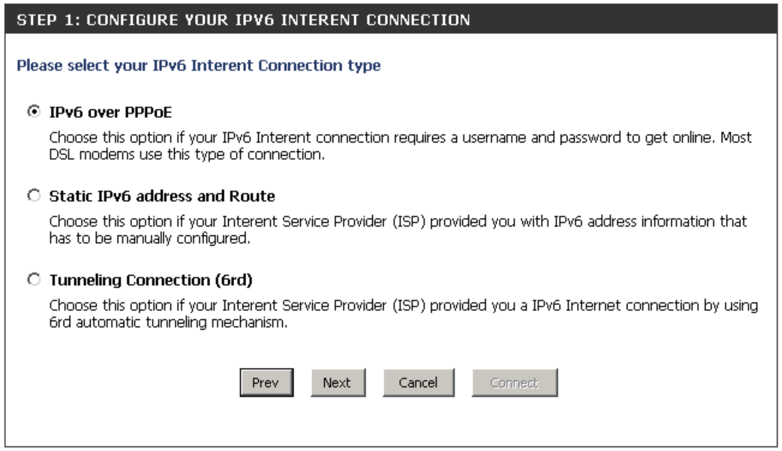

STEP 1: CONFIGURE YOUR IPV6 INTERENT CONNECTION

Router is unable detect your IPv6 Internet connection type

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

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

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


STEP 1: CONFIGURE YOUR IPV6 INTERENT CONNECTION

Please select your IPv6 Interent Connection type

● IPv6 over PPPoE

Choose this option if your IPv6 Interent connection requires a username and password to get online. Most DSL modems use this type of connection.

○ Static IPv6 address and Route

Choose this option if your Interent Service Provider (ISP) provided you with IPv6 address information that has to be manually configured.

○ Tunneling Connection (6rd)

Choose this option if your Interent Service Provider (ISP) provided you a IPv6 Internet connection by using 6rd automatic tunneling mechanism.

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 that requires a username and password to get online. Most DSL modems use this type of connection.

The following parameters will be available for configuration:

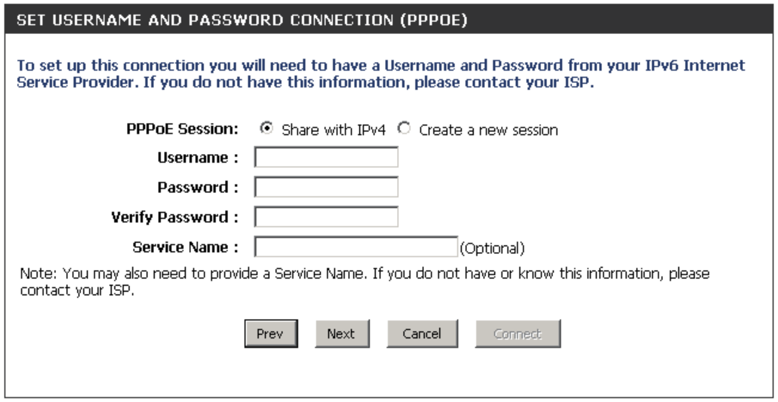
PPPoE Session: Select the PPPoE Session value used here. This option will state that this connection shares it's information with the already configured IPv6 PPPoE connection, or the user can create a new PPPoE connection here.

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

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

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

Service Name: Enter the service name for this connection here. This option is optional.



SET USERNAME AND PASSWORD CONNECTION (PPPOE)

To set up this connection you will need to have a Username and Password from your IPv6 Internet Service Provider. If you do not have this information, please contact your ISP.

PPPoE Session: ● Share with IPv4 ○ Create a new session

Username :

Password :

Verify Password :

Service Name : (Optional)

Note: You may also need to provide a Service Name. If you do not have or know this information, please contact your ISP.

Static IPv6 Address Connection

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

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

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

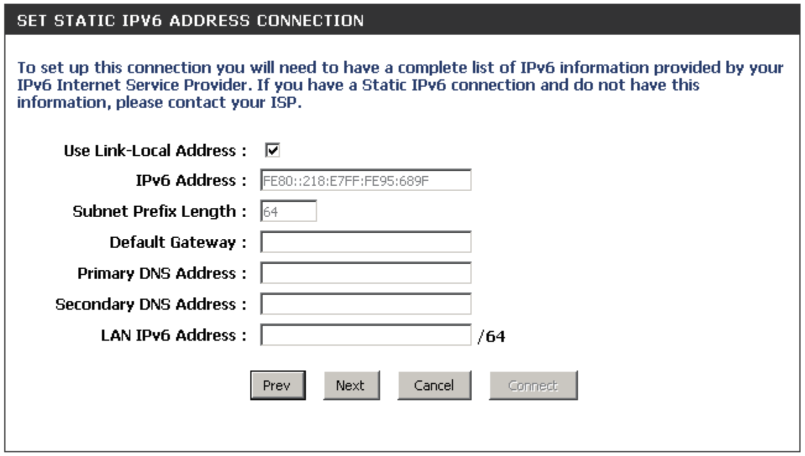
Subnet Prefix Length: Enter the WAN subnet prefix length value used here.

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

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

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

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



SET STATIC IPV6 ADDRESS CONNECTION

To set up this connection you will need to have a complete list of IPv6 information provided by your IPv6 Internet Service Provider. If you have a Static IPv6 connection and do not have this information, please contact your ISP.

Use Link-Local Address : ☑

IPv6 Address : FE80::218:E7FF:FE95:689F

Subnet Prefix Length : 64

Default Gateway :

Primary DNS Address :

Secondary DNS Address :

LAN IPv6 Address : /64

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.

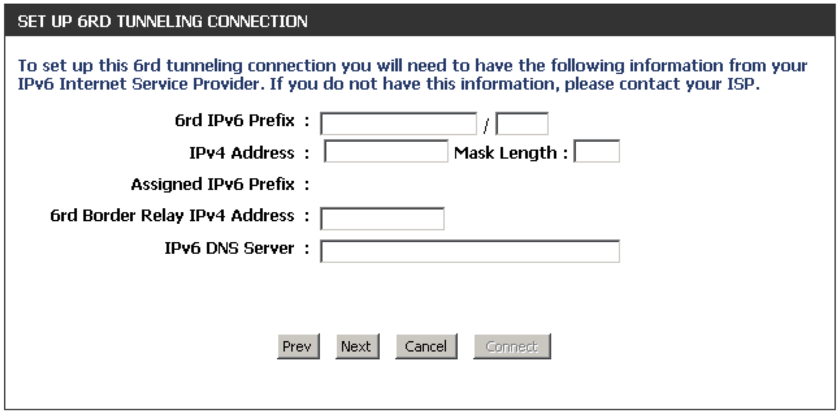
IPv4 Address: Enter the IPv4 address used here.

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.



SET UP 6RD TUNNELING CONNECTION

To set up this 6rd tunneling connection you will need to have the following information from your IPv6 Internet Service Provider. If you do not have this information, please contact your ISP.

6rd IPv6 Prefix : /

IPv4 Address : Mask Length :

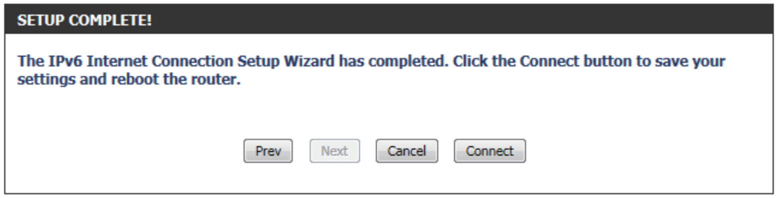
Assigned IPv6 Prefix :

6rd Border Relay IPv4 Address :

IPv6 DNS Server :

The IPv6 Internet Connection Setup Wizard is complete.

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



SETUP COMPLETE!

The IPv6 Internet Connection Setup Wizard has completed. Click the Connect button to save your settings and reboot the router.

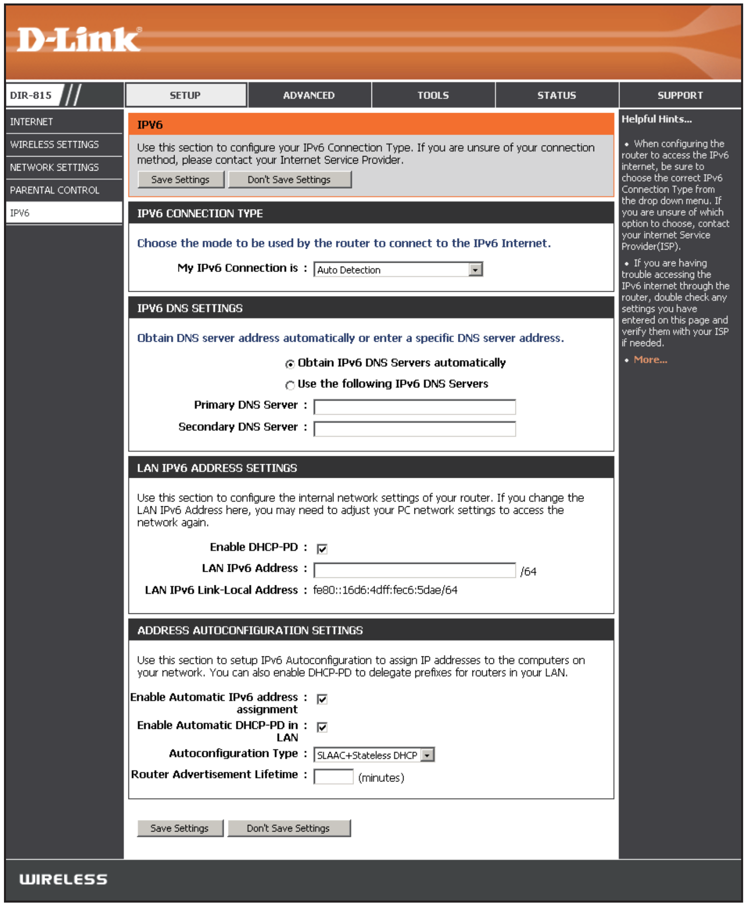
IPv6 Manual Setup

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

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

Auto Detection

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



IPV6

Use this section to configure your IPv6 Connection Type. If you are unsure of your connection method, please contact your Internet Service Provider.

IPV6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : Auto Detection

IPV6 DNS SETTINGS

Obtain DNS server address automatically or enter a specific DNS server address.

● Obtain IPv6 DNS Servers automatically

○ Use the following IPv6 DNS Servers

Primary DNS Server :

Secondary DNS Server :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for routers in your LAN.

Enable Automatic IPv6 address assignment : ☑

Enable Automatic DHCP-PD in LAN : ☑

Autoconfiguration Type : SLAAC+Stateless DHCP

Router Advertisement Lifetime : (minutes)

Helpful Hints...

- When configuring the router to access the IPv6 internet, be sure to choose the correct IPv6 Connection Type from the drop down menu. If you are unsure of which option to choose, contact your internet Service Provider(ISP).
- If you are having trouble accessing the IPv6 internet through the router, double check any settings you have entered on this page and verify them with your ISP if needed.
- More...

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.

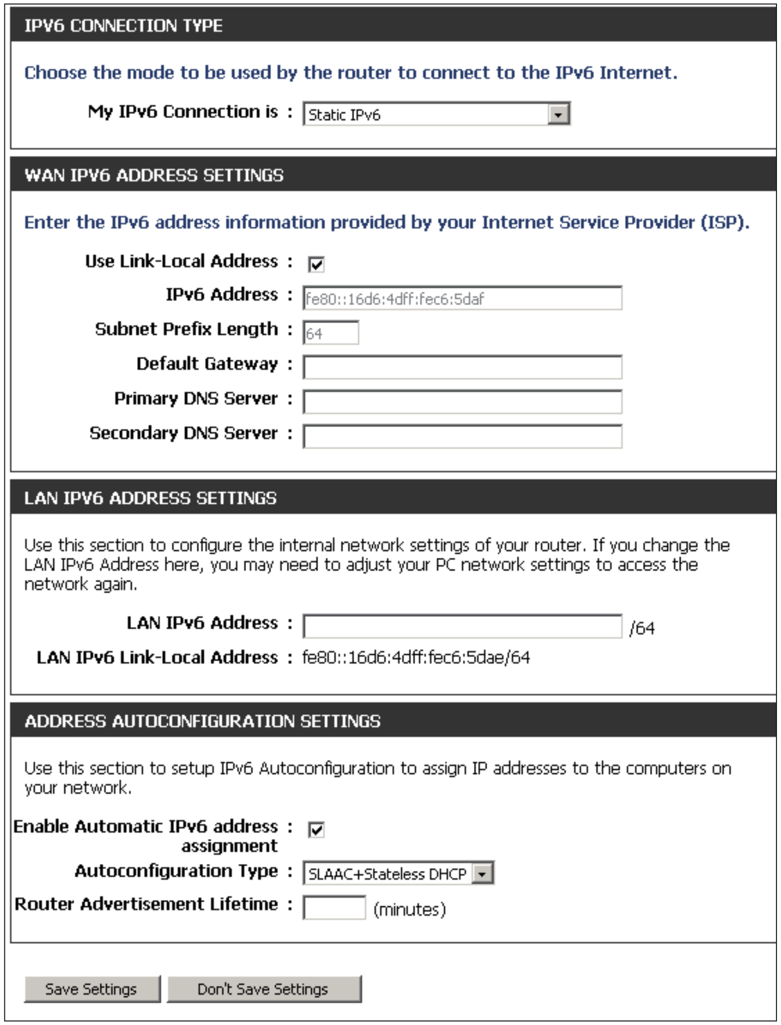
Enable Autoconfiguration: Check to enable Automatic IPv6 address assignment.

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 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : Static IPv6

WAN IPV6 ADDRESS SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

Use Link-Local Address : ☑

IPv6 Address : fe80::16d6:4dff:fec6:5daf

Subnet Prefix Length : 64

Default Gateway :

Primary DNS Server :

Secondary DNS Server :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Automatic IPv6 address assignment : ☑

Autoconfiguration Type : SLAAC+Stateless DHCP

Router Advertisement Lifetime : (minutes)

Autoconfiguration

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

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

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

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

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

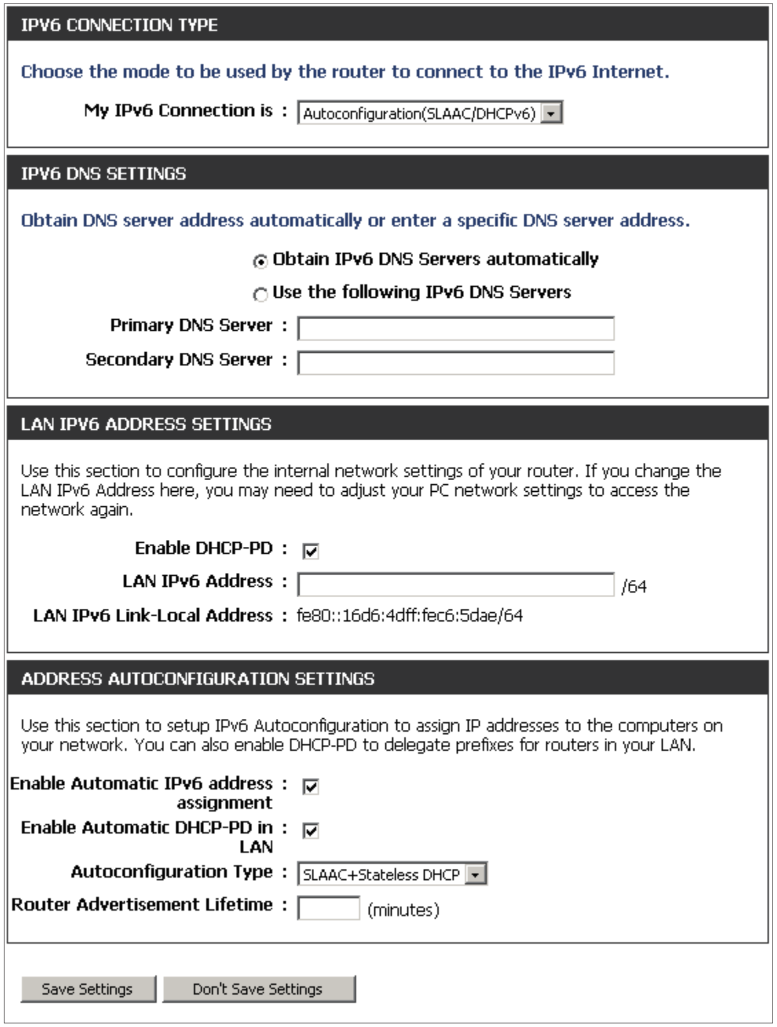
Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful DHCPv6**, **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 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : Autoconfiguration(SLAAC/DHCPv6)

IPV6 DNS SETTINGS

Obtain DNS server address automatically or enter a specific DNS server address.

● Obtain IPv6 DNS Servers automatically

○ Use the following IPv6 DNS Servers

Primary DNS Server :

Secondary DNS Server :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for routers in your LAN.

Enable Automatic IPv6 address assignment : ☑

Enable Automatic DHCP-PD in LAN : ☑

Autoconfiguration Type : SLAAC+Stateless DHCP

Router Advertisement Lifetime : (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.

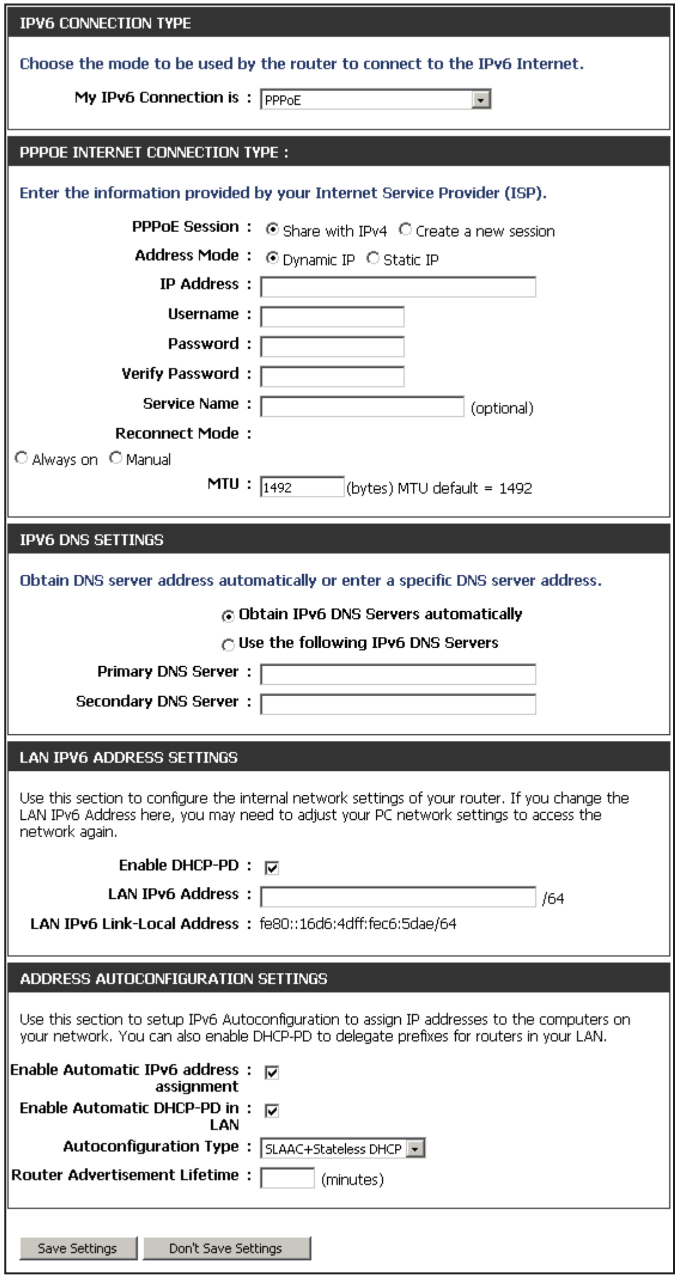
IPv6 DNS Settings: Select either **Obtain DNS server address automatically** or **Use the following DNS Address**.

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

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

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

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.



IPV6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : PPPoE

PPPOE INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (ISP).

PPPoE Session : ● Share with IPv4 ○ Create a new session

Address Mode : ● Dynamic IP ○ Static IP

IP Address :

Username :

Password :

Verify Password :

Service Name : (optional)

Reconnect Mode :

○ Always on ○ Manual

MTU : 1492 (bytes) MTU default = 1492

IPV6 DNS SETTINGS

Obtain DNS server address automatically or enter a specific DNS server address.

● Obtain IPv6 DNS Servers automatically

○ Use the following IPv6 DNS Servers

Primary DNS Server :

Secondary DNS Server :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for routers in your LAN.

Enable Automatic IPv6 address assignment : ☑

Enable Automatic DHCP-PD in LAN : ☑

Autoconfiguration Type : SLAAC+Stateless DHCP

Router Advertisement Lifetime : (minutes)

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).

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

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

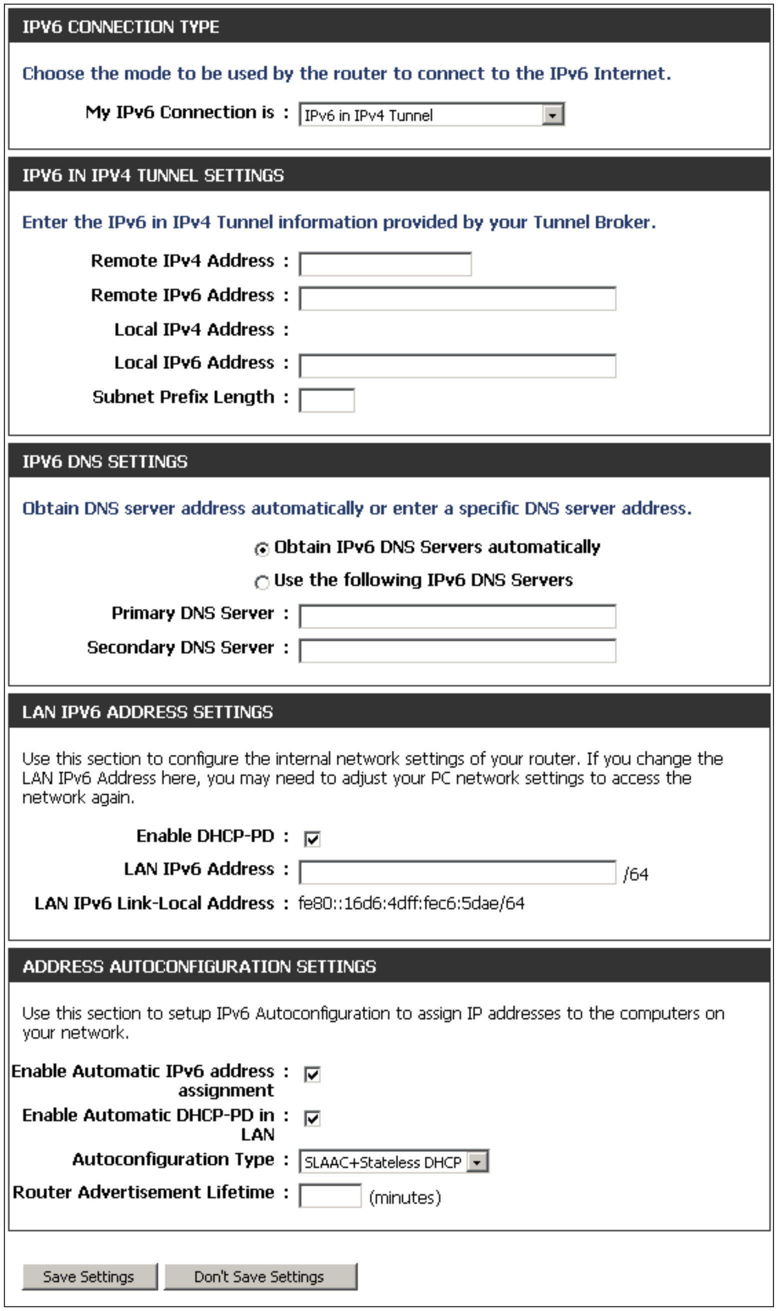
Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful DHCPv6**, **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.

Pv6 Address Lifetime: Enter the Router Advertisement Lifetime (in minutes).



IPV6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : IPv6 in IPv4 Tunnel

IPV6 IN IPV4 TUNNEL SETTINGS

Enter the IPv6 in IPv4 Tunnel information provided by your Tunnel Broker.

Remote IPv4 Address :

Remote IPv6 Address :

Local IPv4 Address :

Local IPv6 Address :

Subnet Prefix Length :

IPV6 DNS SETTINGS

Obtain DNS server address automatically or enter a specific DNS server address.

● Obtain IPv6 DNS Servers automatically

○ Use the following IPv6 DNS Servers

Primary DNS Server :

Secondary DNS Server :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

Enable DHCP-PD : ☑

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Automatic IPv6 address assignment : ☑

Enable Automatic DHCP-PD in LAN : ☑

Autoconfiguration Type : SLAAC+Stateless DHCP

Router Advertisement Lifetime : (minutes)

6 to 4

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

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

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

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

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

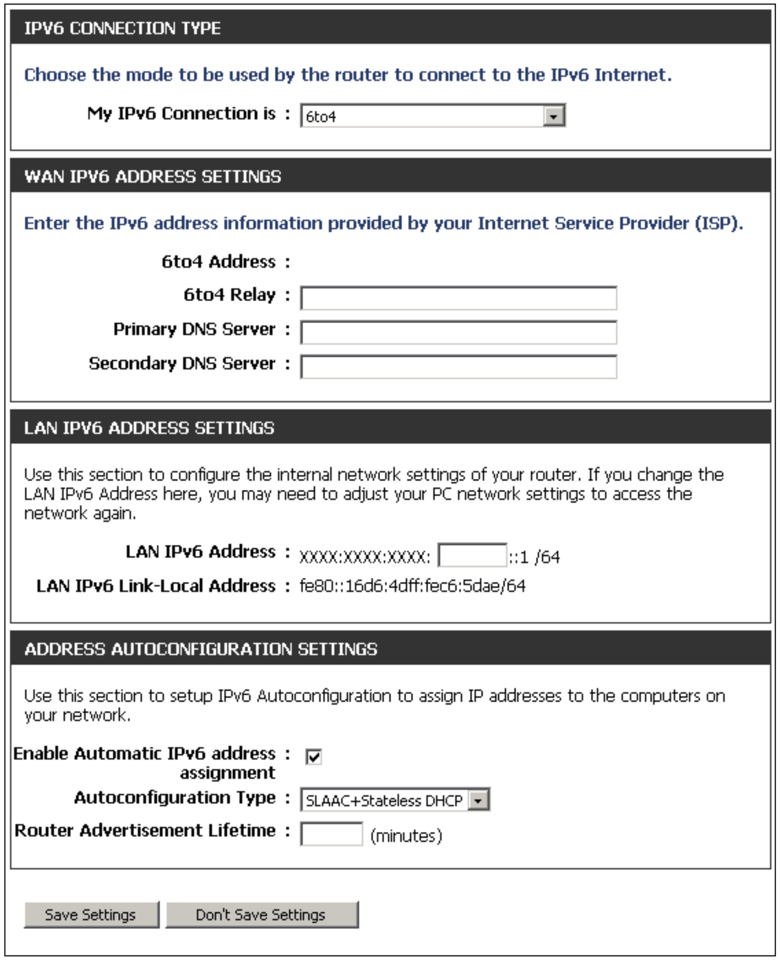
Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

Autoconfiguration Type: Select **Stateful DHCPv6**, **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 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : 6to4

WAN IPV6 ADDRESS SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

6to4 Address :
6to4 Relay :
Primary DNS Server :
Secondary DNS Server :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

LAN IPv6 Address : XXXX:XXXX:XXXX: ::1 /64
LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Automatic IPv6 address assignment : ☑
Autoconfiguration Type : SLAAC+Stateless DHCP
Router Advertisement Lifetime : (minutes)

6rd

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

WAN IPv6 Settings: Enter the address settings supplied by your Internet provider (ISP). Check the **Enable Spoke and Hub Mode** box to have all IPv6 traffic go to the 6rd Border Relay. Please contact your ISP for more information.

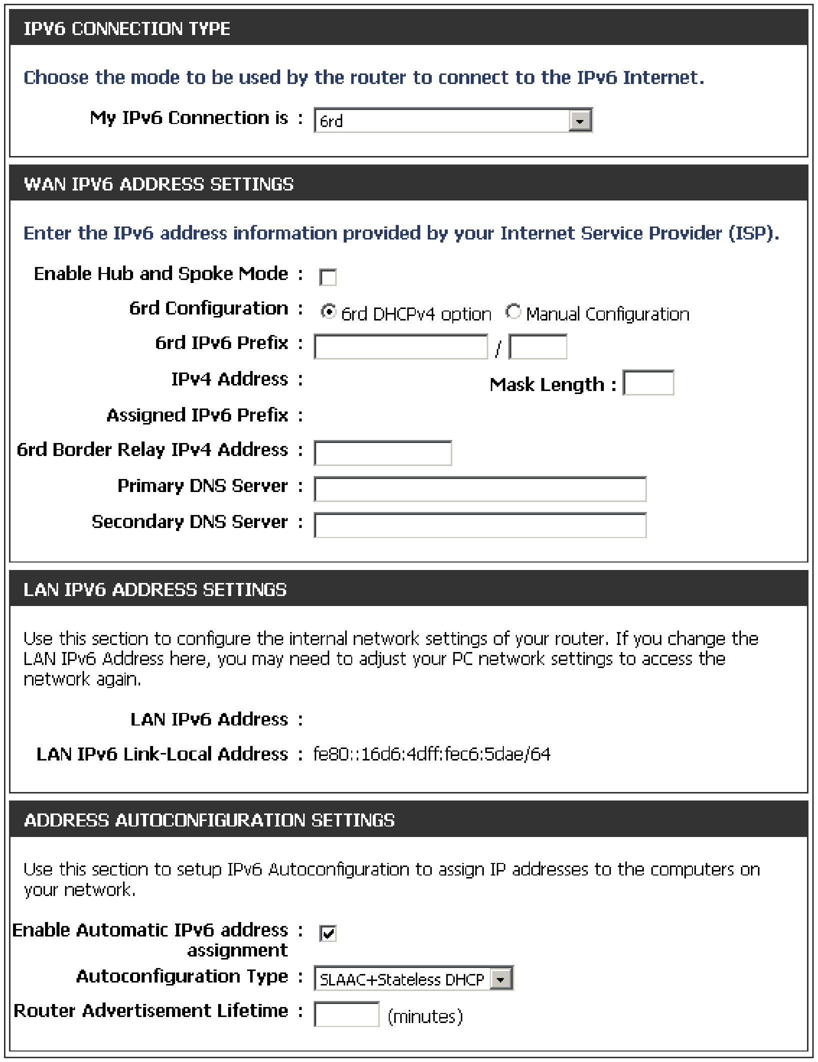
LAN IPv6 Address: Enter the LAN (local) IPv6 address for the router.

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

Enable Autoconfiguration: Check to enable the Autoconfiguration feature.

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

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



IPV6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : 6rd

WAN IPV6 ADDRESS SETTINGS

Enter the IPv6 address information provided by your Internet Service Provider (ISP).

Enable Hub and Spoke Mode : □

6rd Configuration : ● 6rd DHCPv4 option ○ Manual Configuration

6rd IPv6 Prefix : /

IPv4 Address : Mask Length :

Assigned IPv6 Prefix :

6rd Border Relay IPv4 Address :

Primary DNS Server :

Secondary DNS Server :

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

LAN IPv6 Address :

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network.

Enable Automatic IPv6 address assignment : ☑

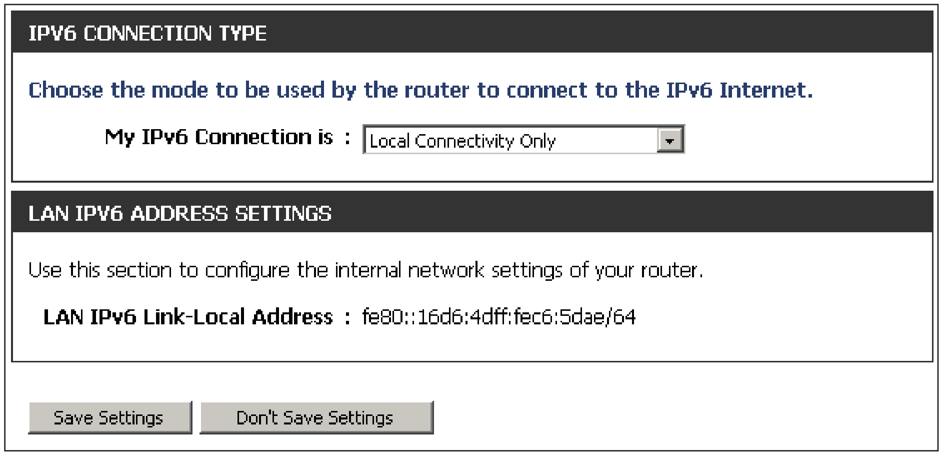
Autoconfiguration Type : SLAAC+Stateless DHCP

Router Advertisement Lifetime : (minutes)

Link-Local Connectivity

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

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



IPV6 CONNECTION TYPE

Choose the mode to be used by the router to connect to the IPv6 Internet.

My IPv6 Connection is : Local Connectivity Only

LAN IPV6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router.

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

Advanced

Virtual Server

The Virtual Server window allows you to open a single port. If you would like to open a range of ports, refer to the next page.

Enable Checkbox: Check the box on the left side to enable the Virtual Server rule.

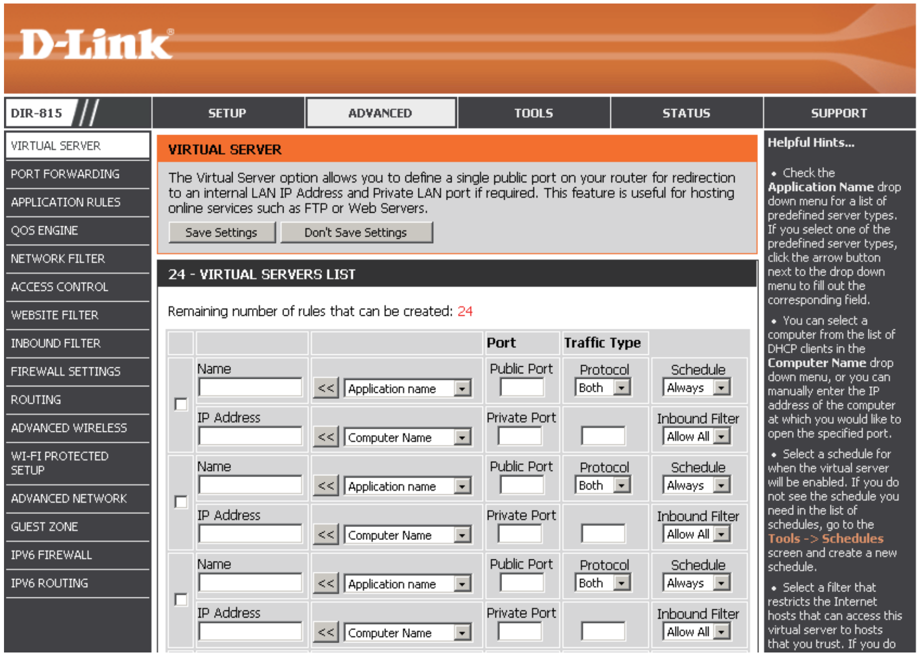
Name: Enter a name for the rule or select an application from the drop-down menu. Select an application and click << to populate the fields.

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

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

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

Schedule Drop-Down Menu: Use the drop-down menu to schedule the time that 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.



VIRTUAL SERVER

The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

24 - VIRTUAL SERVERS LIST

Remaining number of rules that can be created: 24

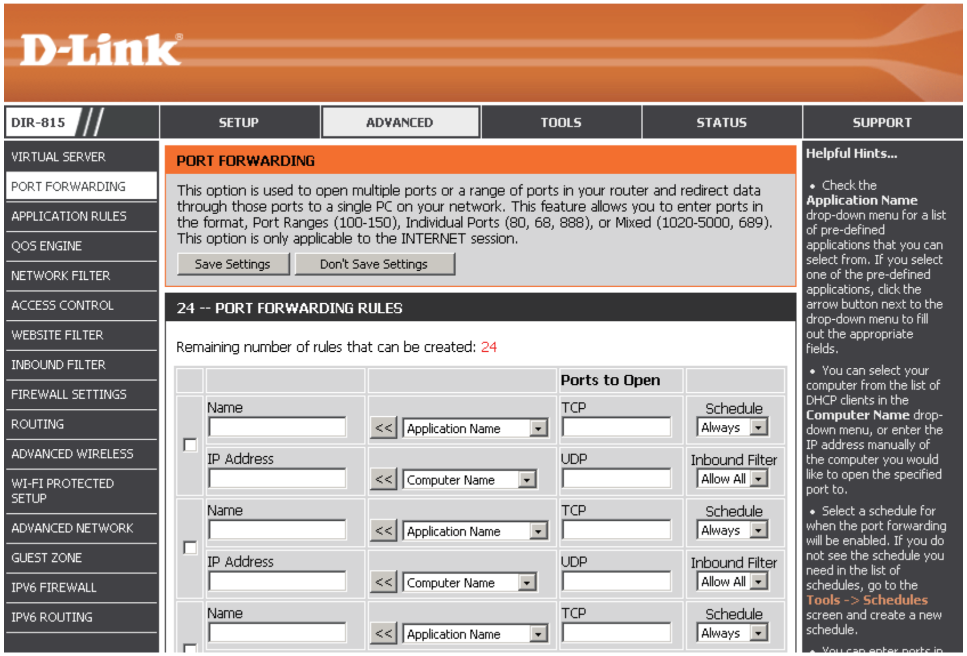
			Port	Traffic Type	
□	Name	<< Application name	Public Port	Protocol Both	Schedule Always
	IP Address	<< Computer Name	Private Port		Inbound Filter Allow All
□	Name	<< Application name	Public Port	Protocol Both	Schedule Always
	IP Address	<< Computer Name	Private Port		Inbound Filter Allow All
□	Name	<< Application name	Public Port	Protocol Both	Schedule Always
	IP Address	<< Computer Name	Private Port		Inbound Filter Allow All

Helpful Hints...

- Check the **Application Name** drop down menu for a list of predefined server types. If you select one of the predefined server types, click the arrow button next to the drop down menu to fill out the corresponding field.
- You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the computer at which you would like to open the specified port.
- Select a schedule for when the virtual server will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools -> Schedules** screen and create a new schedule.
- Select a filter that restricts the Internet hosts that can access this virtual server to hosts that you trust. If you do

Port Forwarding

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



PORT FORWARDING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in the format, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689). This option is only applicable to the INTERNET session.

24 -- PORT FORWARDING RULES

Remaining number of rules that can be created: 24

			Ports to Open	
☐	Name	<< Application Name	TCP	Schedule Always
	IP Address	<< Computer Name	UDP	Inbound Filter Allow All
☐	Name	<< Application Name	TCP	Schedule Always
	IP Address	<< Computer Name	UDP	Inbound Filter Allow All
☐	Name	<< Application Name	TCP	Schedule Always

Helpful Hints...

- Check the **Application Name** drop-down menu for a list of pre-defined applications that you can select from. If you select one of the pre-defined applications, click the arrow button next to the drop-down menu to fill out the appropriate fields.
- You can select your computer from the list of DHCP clients in the **Computer Name** drop-down menu, or enter the IP address manually of the computer you would like to open the specified port to.
- Select a schedule for when the port forwarding will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools -> Schedules** screen and create a new schedule.
- You can enter ports in

Enable Checkbox: Check the box on the left side to enable the Port Forwarding rule.

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

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

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

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

Schedule: Use the drop-down menu to schedule the time that the Port Forwarding 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.

Click the **Save Settings** button to save any changes made.

Application Rules

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DIR-815. 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.

Enable Checkbox: Check the box on the left side to enable the Application Rule.

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

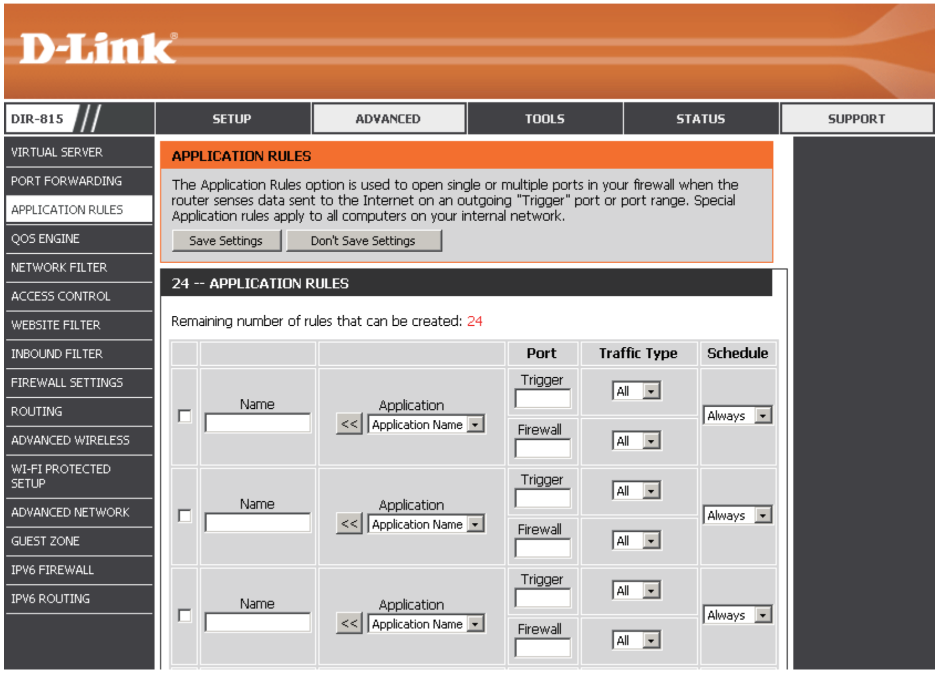
Trigger: This is the port used to trigger the application. It can be either a single port or a range of ports.

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

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 All).

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.



APPLICATION RULES

The Application Rules option is used to open single or multiple ports in your firewall when the router senses data sent to the Internet on an outgoing "Trigger" port or port range. Special Application rules apply to all computers on your internal network.

24 -- APPLICATION RULES

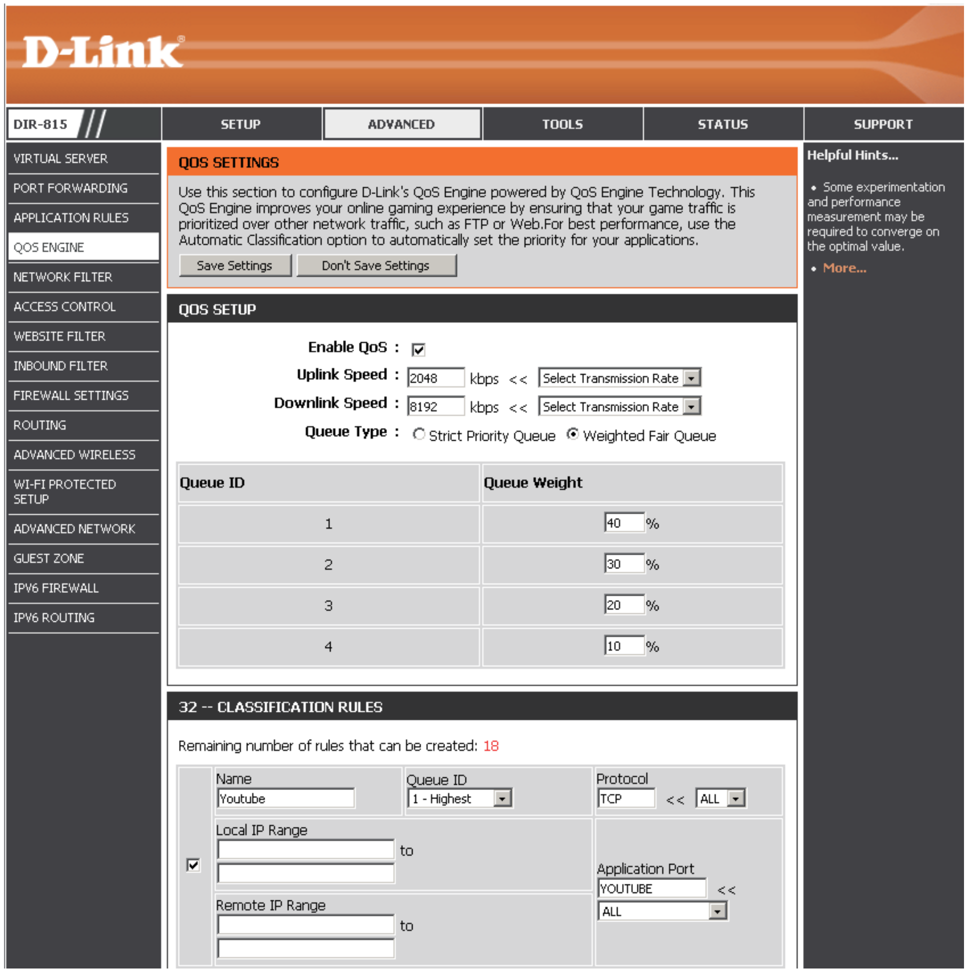
Remaining number of rules that can be created: 24

			Port	Traffic Type	Schedule
□	Name	Application << Application Name	Trigger	All	Always
			Firewall	All	
□	Name	Application << Application Name	Trigger	All	Always
			Firewall	All	
□	Name	Application << Application Name	Trigger	All	Always
			Firewall	All	

Click the **Save Settings** button to save any changes made.

QoS Engine

The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.



QOS SETTINGS

Use this section to configure D-Link's QoS Engine powered by QoS Engine Technology. This QoS Engine improves your online gaming experience by ensuring that your game traffic is prioritized over other network traffic, such as FTP or Web.For best performance, use the Automatic Classification option to automatically set the priority for your applications.

Helpful Hints...

- Some experimentation and performance measurement may be required to converge on the optimal value.

QOS SETUP

Enable QoS : ☑

Uplink Speed : 2048 kbps << Select Transmission Rate

Downlink Speed : 8192 kbps << Select Transmission Rate

Queue Type : ○ Strict Priority Queue ● Weighted Fair Queue

Queue ID	Queue Weight
1	40 %
2	30 %
3	20 %
4	10 %

32 -- CLASSIFICATION RULES

Remaining number of rules that can be created: 18

☑ Name: Youtube; Queue ID: 1 - Highest; Protocol: TCP << ALL

Local IP Range: to

Remote IP Range: to

Application Port: YOUTUBE << ALL

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

Upload Speed: Enter an uplink speed or select the transmission uplink speed from the drop-down menu.

Download Speed: Enter a downlink speed or select the transmission downlink speed from the drop-down menu.

Queue: Select either **Strict Priority Queue** (fixed) or **Weighted Fair Queue** (percentage).

Enable: Check to enabled your classification rule.

Name: Enter a name for your classification rule.

Queue ID: Select the queue ID (priority) from the drop-down menu.

Local IP Range: Specify a single local IP by entering the IP in the top box or enter a range of IPs (first IP of the range in the top box and the last IP of the range in the bottom one).

Remote IP Range: Specify a single remote IP by entering the IP in the top box or enter a range of IPs (first IP of the range in the top box and the last IP of the range in the bottom one).

Protocol: Use the Protocol drop-down menu to select the traffic type.

Application Port: Select the application service from drop-down menu or input application service directly.

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 Broadband Router.

Configure MAC Filtering: Select **Turn MAC Filtering OFF**, **Turn MAC Filtering ON and ALLOW computers listed to access the network**, or **Turn MAC Filtering ON and DENY computers listed to access the network** from the drop-down menu.

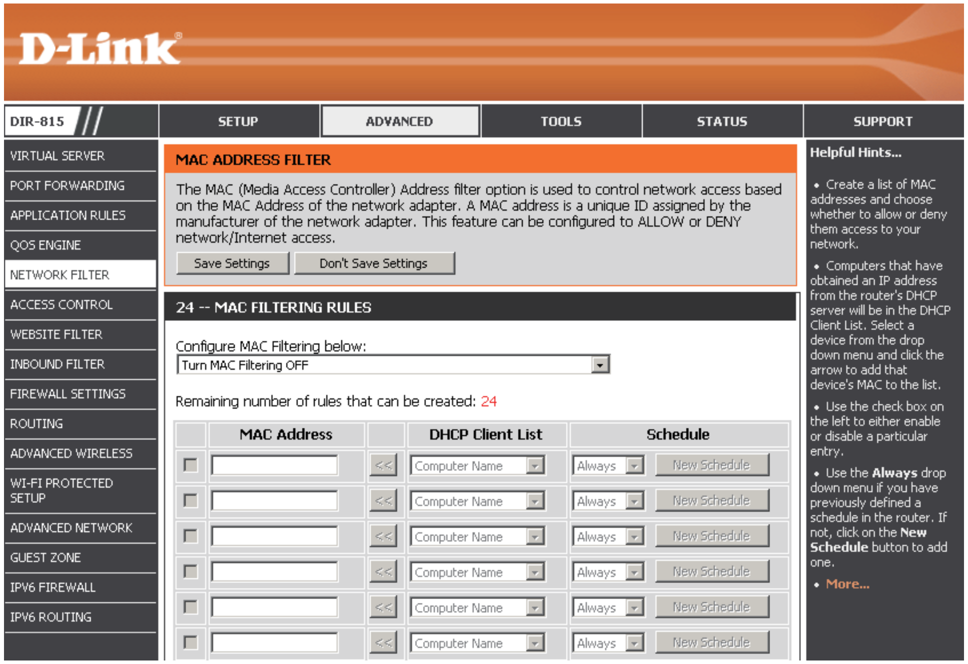
Enable Checkbox: Check the box on the left side to enable the Network Filter.

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

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

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

Schedule: The schedule of time when the Network Filter will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the **New Schedule** button to create your own schedule.



MAC ADDRESS FILTER

The MAC (Media Access Controller) Address filter option is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of the network adapter. This feature can be configured to ALLOW or DENY network/Internet access.

24 -- MAC FILTERING RULES

Configure MAC Filtering below:
Turn MAC Filtering OFF

Remaining number of rules that can be created: 24

	MAC Address		DHCP Client List	Schedule	
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule
□		<<	Computer Name	Always	New Schedule

Helpful Hints...

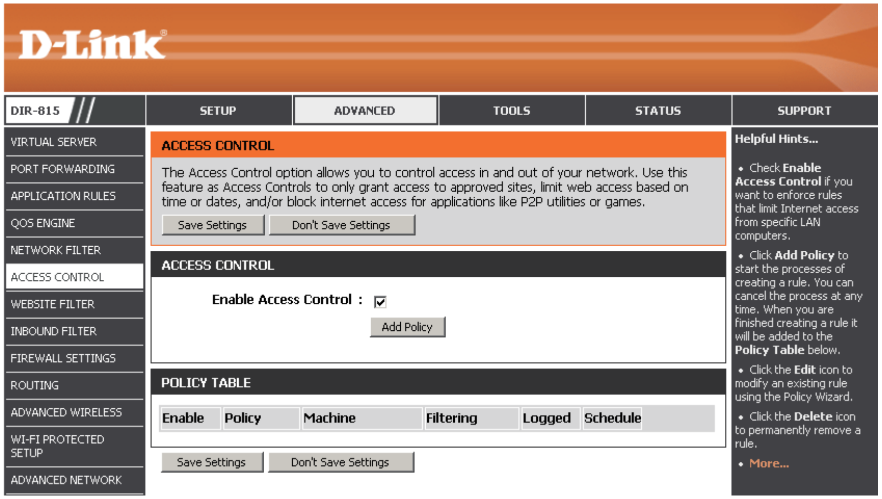
- Create a list of MAC addresses and choose whether to allow or deny them access to your network.
- Computers that have obtained an IP address from the router's DHCP server will be in the DHCP Client List. Select a device from the drop down menu and click the arrow to add that device's MAC to the list.
- Use the check box on the left to either enable or disable a particular entry.
- Use the **Always** drop down menu if you have previously defined a schedule in the router. If not, click on the **New Schedule** button to add one.
- More...

Click the **Save Settings** button to save any changes made.

Access Control

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

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



ACCESS CONTROL

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

ACCESS CONTROL

Enable Access Control : ☑

POLICY TABLE

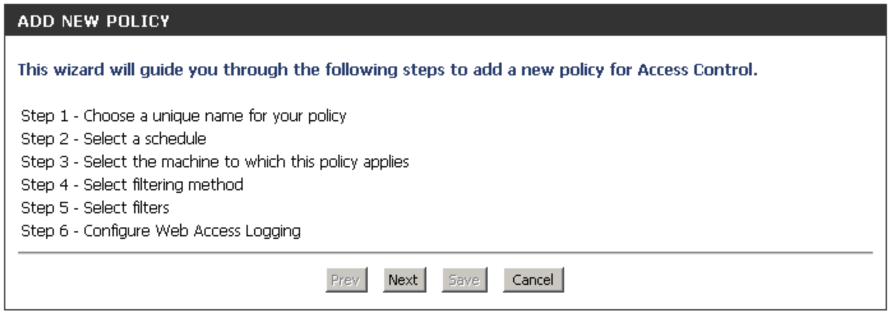
Enable	Policy	Machine	Filtering	Logged	Schedule

Helpful Hints...

- Check **Enable Access Control** if you want to enforce rules that limit Internet access from specific LAN computers.
- Click **Add Policy** to start the processes of creating a rule. You can cancel the process at any time. When you are finished creating a rule it will be added to the **Policy Table** below.
- Click the **Edit** icon to modify an existing rule using the Policy Wizard.
- Click the **Delete** icon to permanently remove a rule.
- More...

Access Control Wizard

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

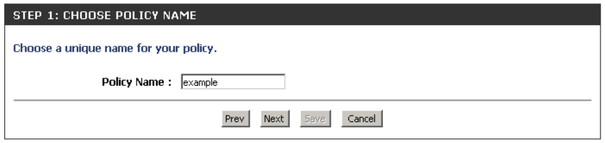


ADD NEW POLICY

This wizard will guide you through the following steps to add a new policy for Access Control.

Step 1 - Choose a unique name for your policy
Step 2 - Select a schedule
Step 3 - Select the machine to which this policy applies
Step 4 - Select filtering method
Step 5 - Select filters
Step 6 - Configure Web Access Logging

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

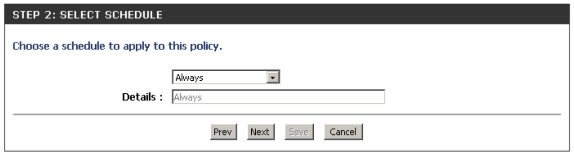


STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name : example

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



STEP 2: SELECT SCHEDULE

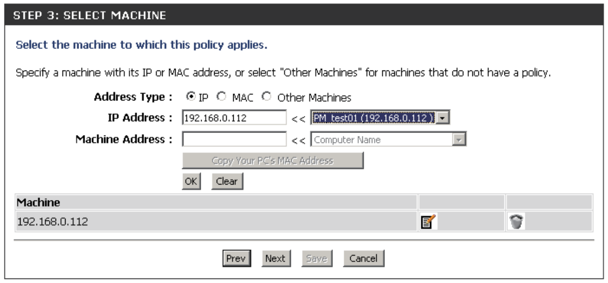
Choose a schedule to apply to this policy.

Always

Details : Always

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).



STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select "Other Machines" for machines that do not have a policy.

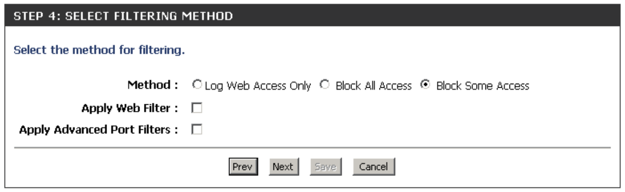
Address Type : ● IP ○ MAC ○ Other Machines

IP Address : 192.168.0.112 << PM_test01 (192.168.0.112)

Machine Address : << Computer Name

Machine		
192.168.0.112		

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



STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

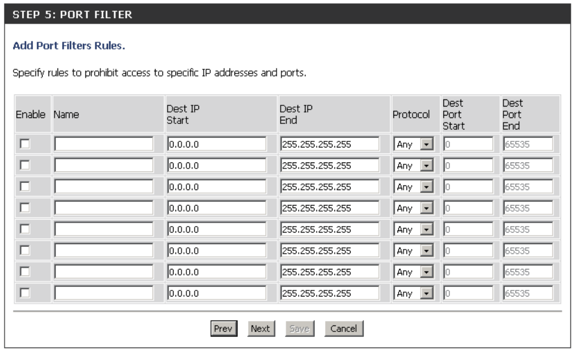
Method : ○ Log Web Access Only ○ Block All Access ● Block Some Access

Apply Web Filter : □

Apply Advanced Port Filters : □

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.



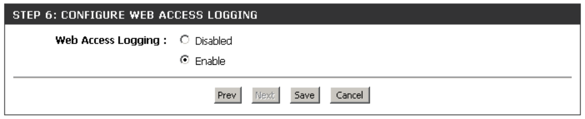
STEP 5: PORT FILTER

Add Port Filters Rules.

Specify rules to prohibit access to specific IP addresses and ports.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535
□		0.0.0.0	255.255.255.255	Any	0	65535

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

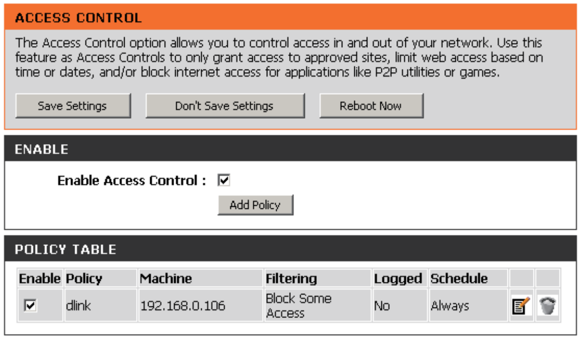


STEP 6: CONFIGURE WEB ACCESS LOGGING

Web Access Logging : ○ Disabled
● Enable

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

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



ACCESS CONTROL

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

ENABLE

Enable Access Control : ☑

POLICY TABLE

Enable	Policy	Machine	Filtering	Logged	Schedule		
☑	dlink	192.168.0.106	Block Some Access	No	Always		

Website Filter

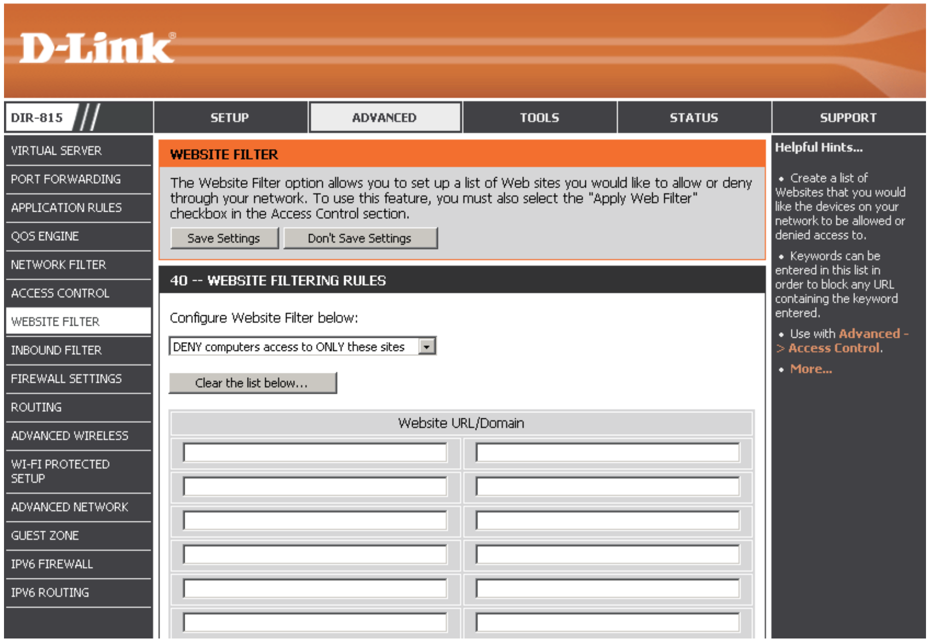
Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network.

Configure Web Filtering: Select **Turn OFF Website Filtering**, **ALLOW computers access to ONLY these sites**, or **DENY computers access to ONLY these sites** from the drop-down menu.

Enable Checkbox: Check the box on the left side to enable the Website Filter.

Website URL: Enter the keywords or URLs that you want to allow or block.

Schedule: The schedule of time when the Website Filter will be enabled. The schedule may be set to Always, which will allow the particular service to always be enabled. Click the **New Schedule** button to create your own schedule.



WEBSITE FILTER

The Website Filter option allows you to set up a list of Web sites you would like to allow or deny through your network. To use this feature, you must also select the "Apply Web Filter" checkbox in the Access Control section.

40 -- WEBSITE FILTERING RULES

Configure Website Filter below: DENY computers access to ONLY these sites

Helpful Hints...

- Create a list of Websites that you would like the devices on your network to be allowed or denied access to.
- Keywords can be entered in this list in order to block any URL containing the keyword entered.
- Use with Advanced -> Access Control.
- More...

Click the **Save Settings** button to save any changes made.

Inbound Filters

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

Name: Enter a name for the inbound filter rule.

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

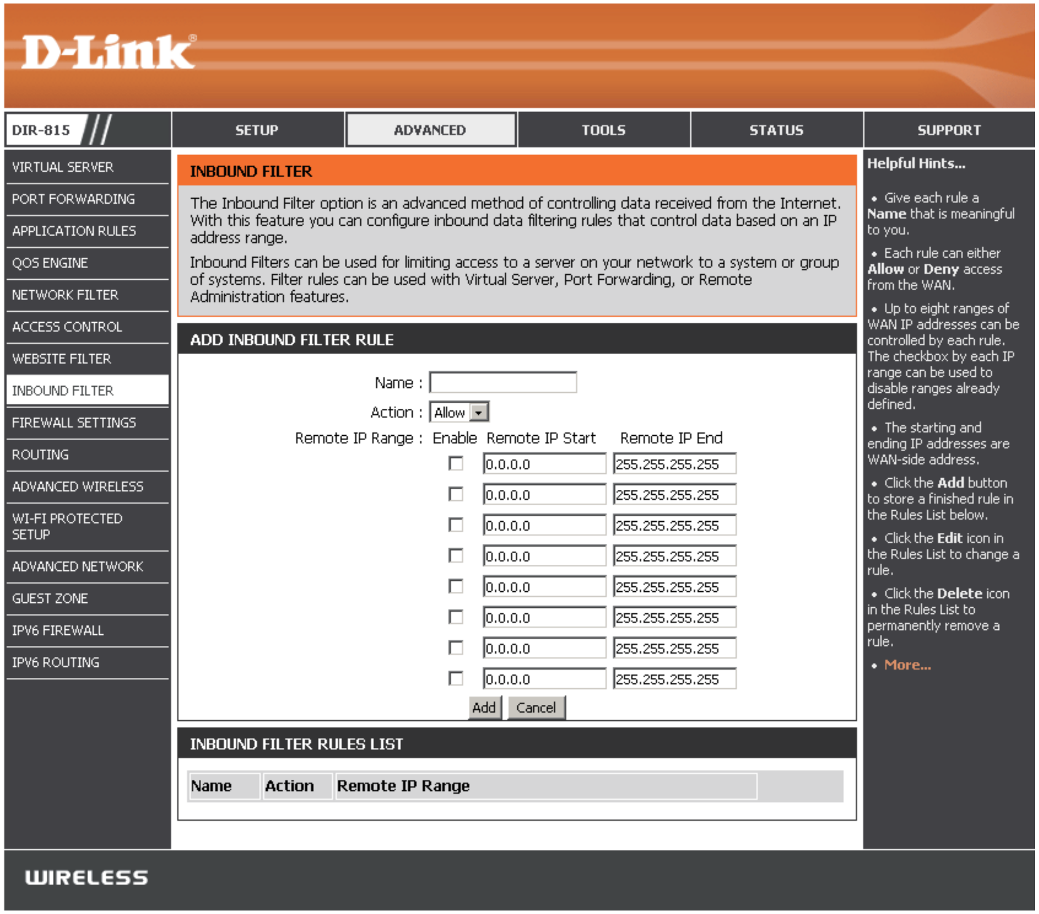
Enable: Check to enable rule.

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

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

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

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



INBOUND FILTER

The Inbound Filter option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on an IP address range.

Inbound Filters can be used for limiting access to a server on your network to a system or group of systems. Filter rules can be used with Virtual Server, Port Forwarding, or Remote Administration features.

ADD INBOUND FILTER RULE

Name :

Action : Allow

Remote IP Range : Enable	Remote IP Start	Remote IP End
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255
□	0.0.0.0	255.255.255.255

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range

Helpful Hints...

- Give each rule a **Name** that is meaningful to you.
- Each rule can either **Allow** or **Deny** access from the WAN.
- Up to eight ranges of WAN IP addresses can be controlled by each rule. The checkbox by each IP range can be used to disable ranges already defined.
- The starting and ending IP addresses are WAN-side address.
- Click the **Add** button to store a finished rule in the Rules List below.
- Click the **Edit** icon in the Rules List to change a rule.
- Click the **Delete** icon in the Rules List to permanently remove a rule.
- **More...**

Firewall Settings

A firewall protects your network from the outside world. The DIR-815 offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you can enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

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

NAT Endpoint Filtering: Select one of the following for TCP and UDP ports:
Endpoint Independent - Any incoming traffic sent to an open port will be forwarded to the application that opened the port. The port will close if idle for 5 minutes.

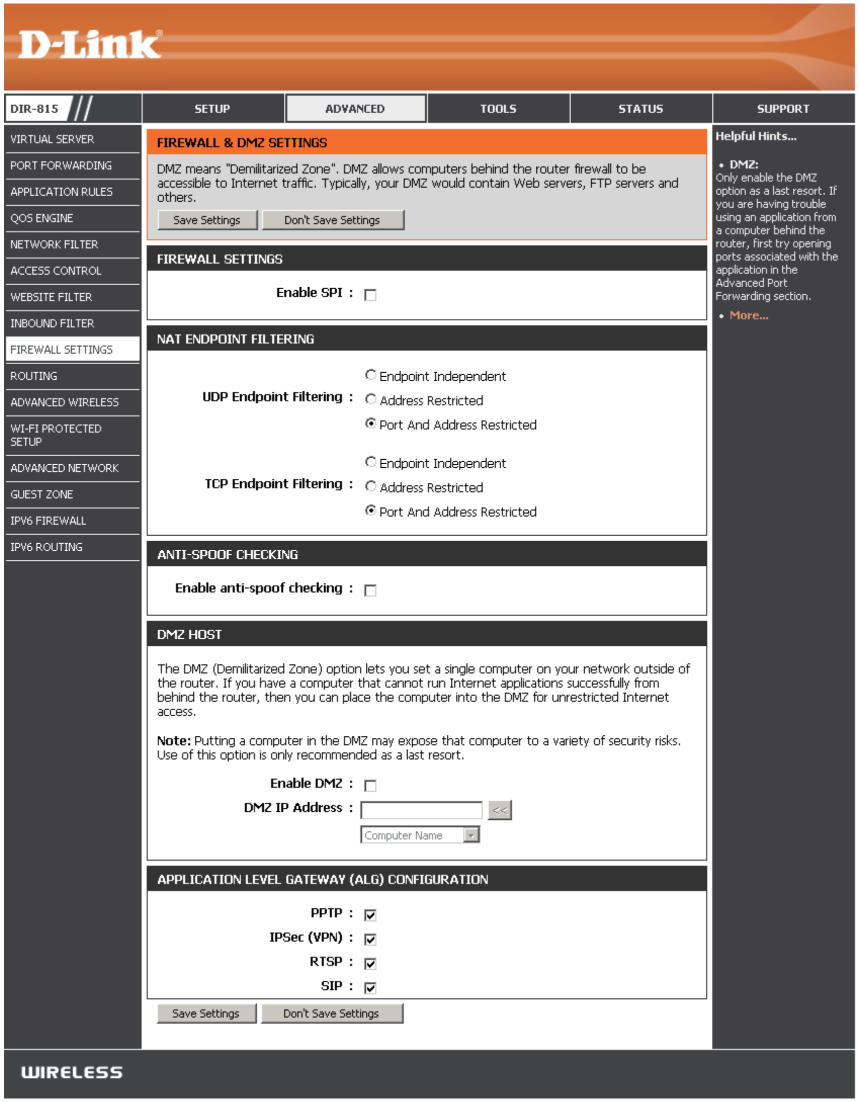
Address Restricted - Incoming traffic must match the IP address of the outgoing connection.

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

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

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

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



FIREWALL & DMZ SETTINGS

DMZ means "Demilitarized Zone". DMZ allows computers behind the router firewall to be accessible to Internet traffic. Typically, your DMZ would contain Web servers, FTP servers and others.

FIREWALL SETTINGS

Enable SPI : □

NAT ENDPOINT FILTERING

UDP Endpoint Filtering : ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

TCP Endpoint Filtering : ○ Endpoint Independent ○ Address Restricted ● Port And Address Restricted

ANTI-SPOOF CHECKING

Enable anti-spoof checking : □

DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting 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.

Enable DMZ : □

DMZ IP Address : Computer Name

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP : ☑

IPSec (VPN) : ☑

RTSP : ☑

SIP : ☑

Helpful Hints...

- **DMZ:** Only enable the DMZ option as a last resort. If you are having trouble using an application from a computer behind the router, first try opening ports associated with the application in the Advanced Port Forwarding section.

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

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

IPSEC (VPN): Allows multiple VPN 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 application that uses 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.

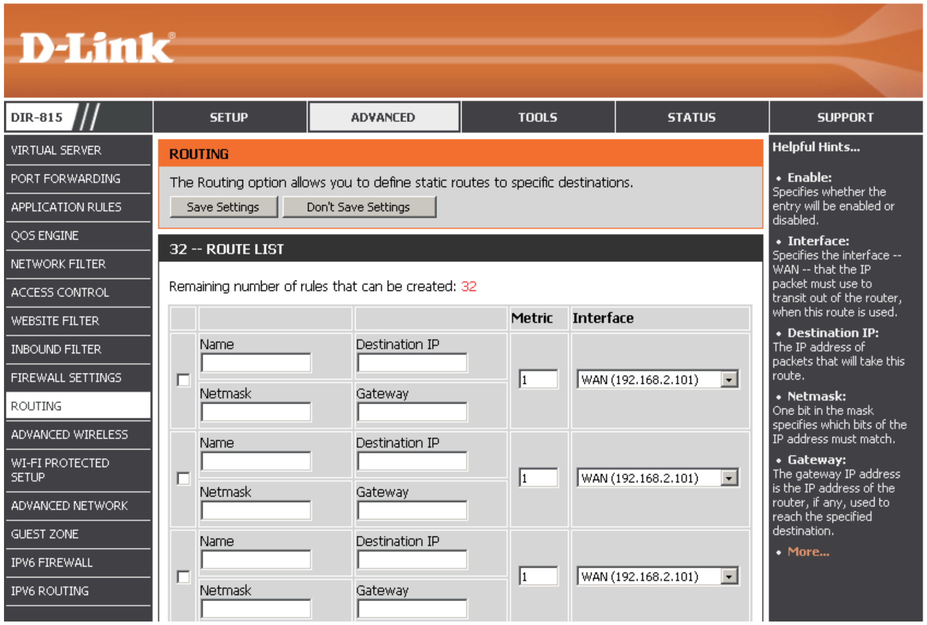
Destination IP: Enter the IP address of packets that will take this route.

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.



ROUTING

The Routing option allows you to define static routes to specific destinations.

32 -- ROUTE LIST

Remaining number of rules that can be created: 32

			Metric	Interface
□	Name	Destination IP	1	WAN (192.168.2.101)
	Netmask	Gateway		
□	Name	Destination IP	1	WAN (192.168.2.101)
	Netmask	Gateway		
□	Name	Destination IP	1	WAN (192.168.2.101)
	Netmask	Gateway		

Helpful Hints...

- **Enable:** Specifies whether the entry will be enabled or disabled.
- **Interface:** Specifies the interface -- WAN -- that the IP packet must use to transit out of the router, when this route is used.
- **Destination IP:** The IP address of packets that will take this route.
- **Netmask:** One bit in the mask specifies which bits of the IP address must match.
- **Gateway:** The gateway IP address is the IP address of the router, if any, used to reach the specified destination.
- More...

Click the **Save Settings** button to save any changes made.

Advanced Wireless Settings

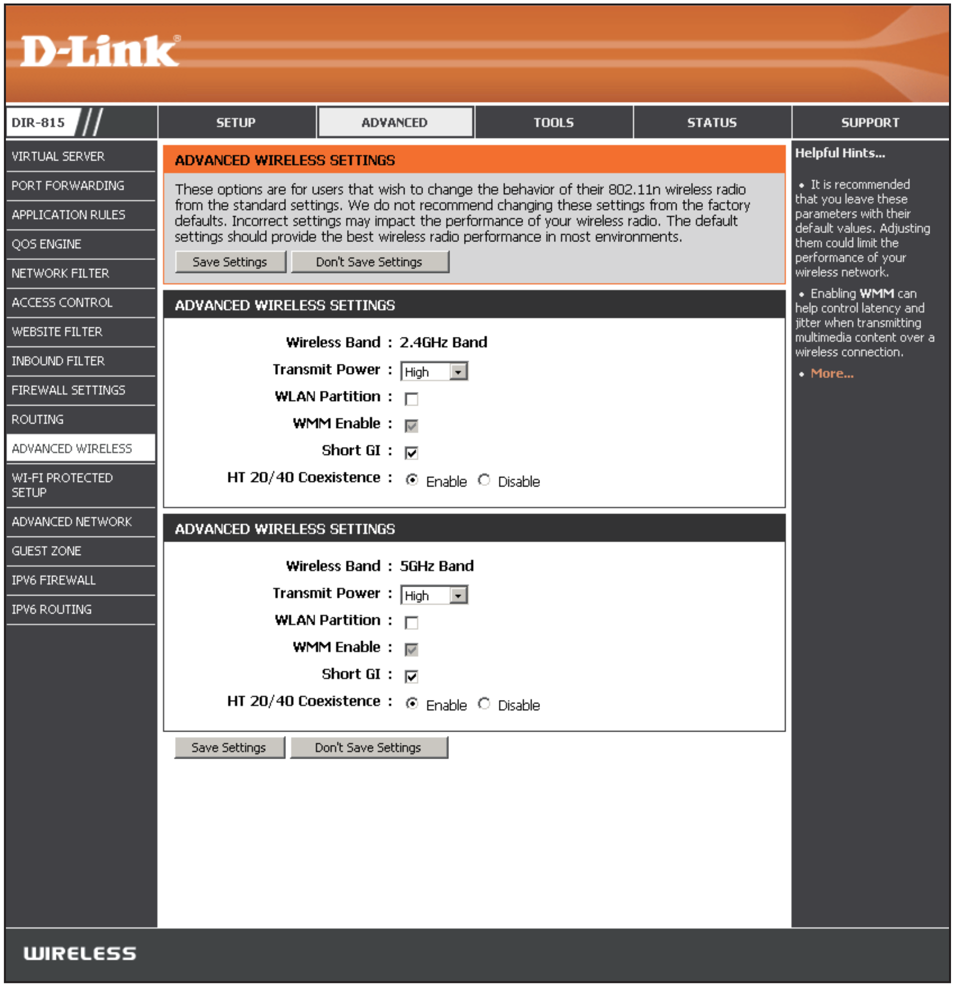
Transmit Power: Set the transmit power of the antennas.

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 (2.4GHz only): 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.



ADVANCED WIRELESS SETTINGS

These options are for users that wish to change the behavior of their 802.11n wireless radio from the standard settings. We do not recommend changing these settings from the factory defaults. Incorrect settings may impact the performance of your wireless radio. The default settings should provide the best wireless radio performance in most environments.

ADVANCED WIRELESS SETTINGS

Wireless Band : 2.4GHz Band
Transmit Power : High
WLAN Partition : □
WMM Enable : ☑
Short GI : ☑
HT 20/40 Coexistence : ● Enable ○ Disable

ADVANCED WIRELESS SETTINGS

Wireless Band : 5GHz Band
Transmit Power : High
WLAN Partition : □
WMM Enable : ☑
Short GI : ☑
HT 20/40 Coexistence : ● Enable ○ Disable

Helpful Hints...

- It is recommended that you leave these parameters with their default values. Adjusting them could limit the performance of your wireless network.
- Enabling **WMM** can help control latency and jitter when transmitting multimedia content over a wireless connection.
- More...

Click the **Save Settings** button to save any changes made.

Wi-Fi Protected Setup (WPS)

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

Enable: Enable the Wi-Fi Protected Setup feature.

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

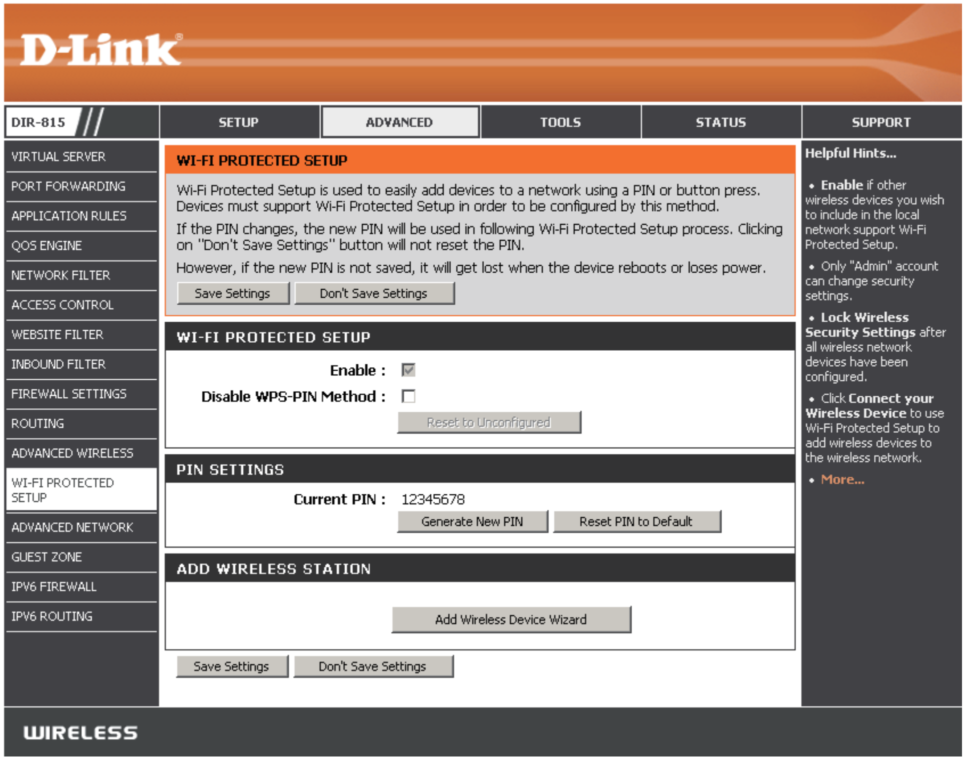
Disable WPS-PIN Method: Check to disable the WPS PIN method of securing your network. This will not affect the Push-Button method.

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

Current PIN: Shows the current PIN.

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

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



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

If the PIN changes, the new PIN will be used in following Wi-Fi Protected Setup process. Clicking on "Don't Save Settings" button will not reset the PIN.

However, if the new PIN is not saved, it will get lost when the device reboots or loses power.

WI-FI PROTECTED SETUP

Enable : ☑

Disable WPS-PIN Method : □

PIN SETTINGS

Current PIN : 12345678

ADD WIRELESS STATION

Helpful Hints...

- **Enable** if other wireless devices you wish to include in the local network support Wi-Fi Protected Setup.
- Only "Admin" account can change security settings.
- **Lock Wireless Security Settings** after all wireless network devices have been configured.
- Click **Connect your Wireless Device** to use Wi-Fi Protected Setup to add wireless devices to the wireless network.
- More...

Add Wireless Station: Click the **Connect your Wireless Device** button to start the Wireless Connection Setup Wizard. This wizard helps you add wireless devices to the wireless network.

The wizard will either display the wireless network settings to guide you through manual configuration, prompt you to enter the PIN for the device, or ask you to press the WPS button on the device. If the device supports Wi-Fi Protected Setup and has a WPS button, you can add it to the network by pressing the WPS button on the device and then the WPS button on the router within 2 minutes. The button will light solid blue for 5 seconds when the device has successfully been added to the network.

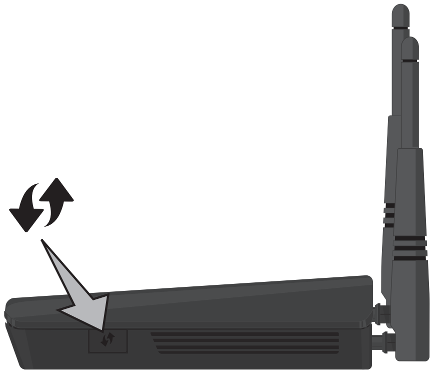
There are several ways to add a wireless device to your network. A “registrar” controls access to the wireless network. A registrar only allows devices onto the wireless network if you have entered the PIN, or pressed a special Wi-Fi Protected Setup button on the device. The router acts as a registrar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

Click the **Save Settings** button to save any changes made.

WPS Button

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

Refer to page 107 for more information.



Advanced Network

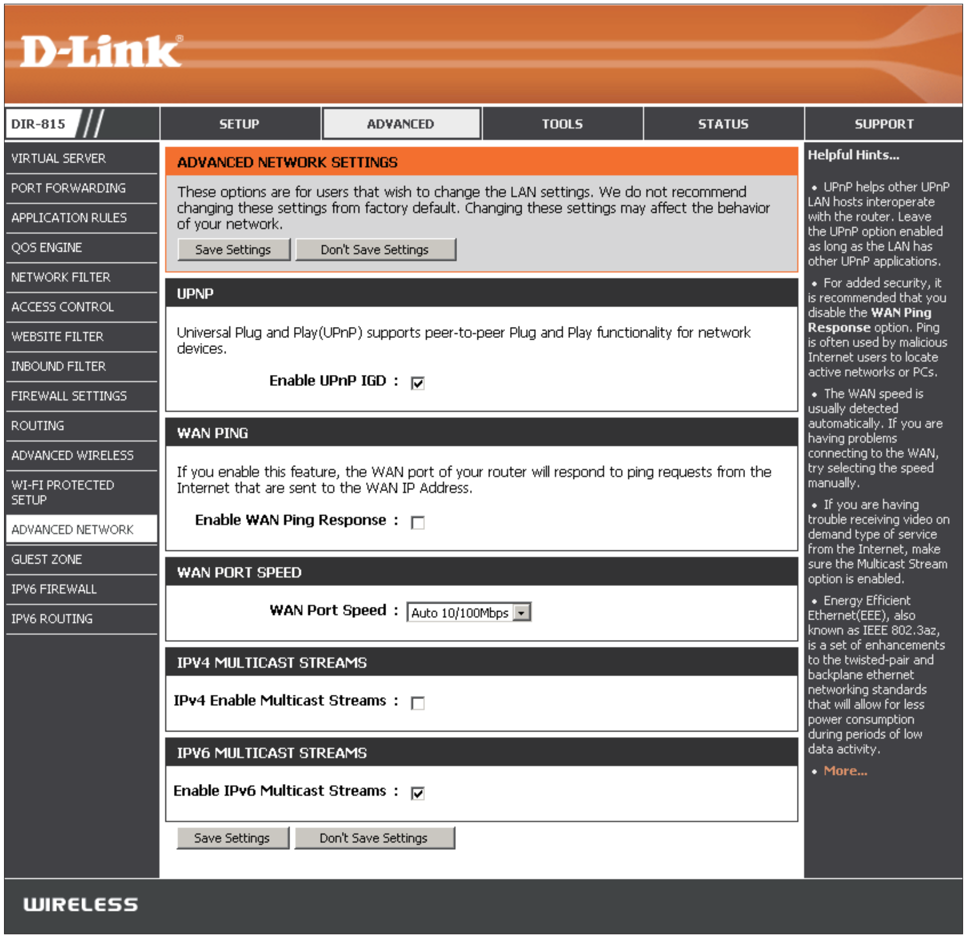
Enable UPnP: To use the Universal Plug and Play (UPnP™) feature click on **Enabled**. UPNP provides compatibility with networking equipment, software and peripherals.

Enable WAN Ping Response: Unchecking the box will not allow the DIR-815 to respond to pings. Blocking the Ping may provide some extra security from hackers. Check the box to allow the Internet port to be "pinged".

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

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

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



ADVANCED NETWORK SETTINGS

These options are for users that wish to change the LAN settings. We do not recommend changing these settings from factory default. Changing these settings may affect the behavior of your network.

UPNP

Universal Plug and Play(UPnP) supports peer-to-peer Plug and Play functionality for network devices.

Enable UPnP IGD : ☑

WAN PING

If you enable this feature, the WAN port of your router will respond to ping requests from the Internet that are sent to the WAN IP Address.

Enable WAN Ping Response : □

WAN PORT SPEED

WAN Port Speed : Auto 10/100Mbps

IPV4 MULTICAST STREAMS

IPv4 Enable Multicast Streams : □

IPV6 MULTICAST STREAMS

Enable IPv6 Multicast Streams : ☑

Helpful Hints...

- UPnP helps other UPnP LAN hosts interoperate with the router. Leave the UPnP option enabled as long as the LAN has other UPnP applications.
- For added security, it is recommended that you disable the **WAN Ping Response** option. Ping is often used by malicious Internet users to locate active networks or PCs.
- The WAN speed is usually detected automatically. If you are having problems connecting to the WAN, try selecting the speed manually.
- If you are having trouble receiving video on demand type of service from the Internet, make sure the Multicast Stream option is enabled.
- Energy Efficient Ethernet(EEE), also known as IEEE 802.3az, is a set of enhancements to the twisted-pair and backplane ethernet networking standards that will allow for less power consumption during periods of low data activity.
- More...

Click the **Save Settings** button to save any changes made.

Guest Zone

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

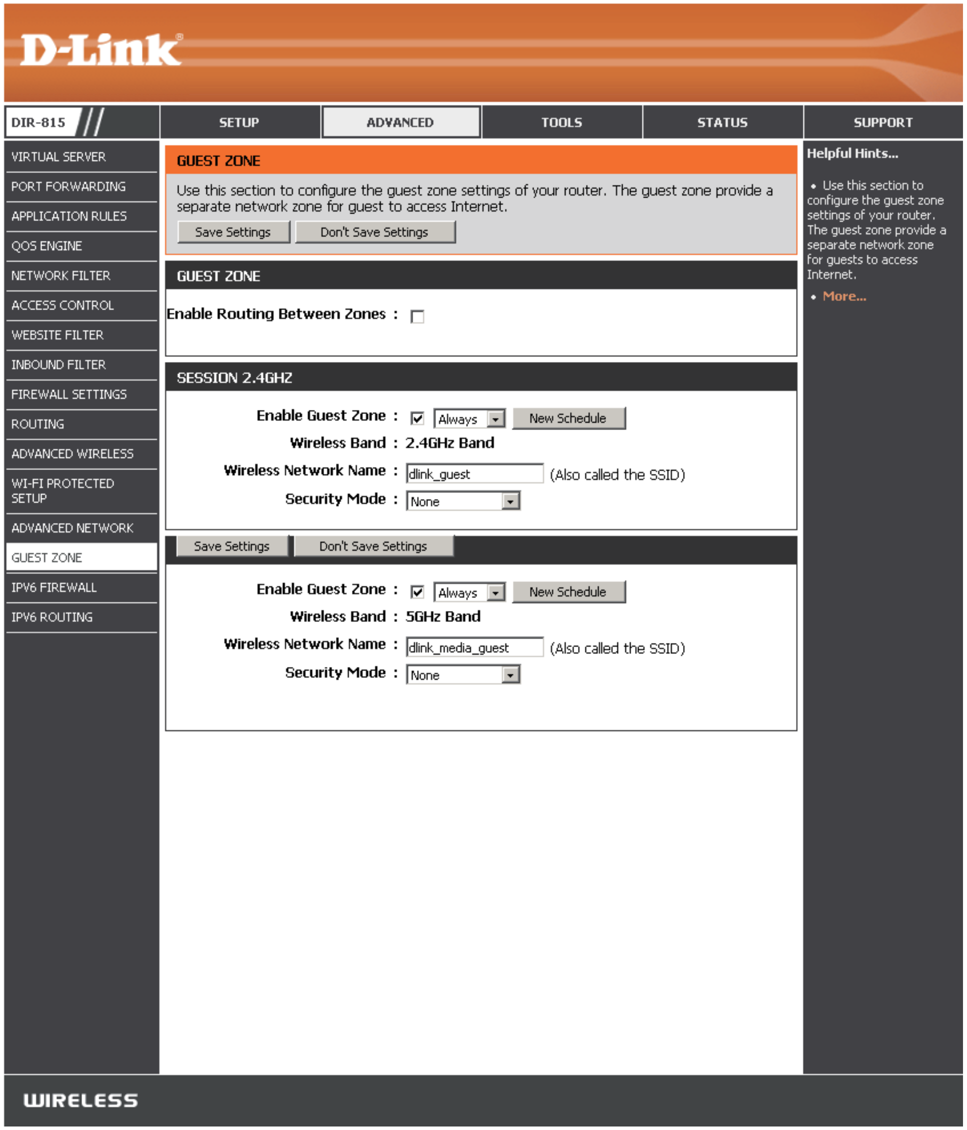
Enable Guest Zone: Check to enable the Guest Zone feature.

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.

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.



GUEST ZONE

Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guest to access Internet.

GUEST ZONE

Enable Routing Between Zones : □

SESSION 2.4GHZ

Enable Guest Zone : ☑ Always

Wireless Band : 2.4GHz Band

Wireless Network Name : dlink_guest (Also called the SSID)

Security Mode : None

Enable Guest Zone : ☑ Always

Wireless Band : 5GHz Band

Wireless Network Name : dlink_media_guest (Also called the SSID)

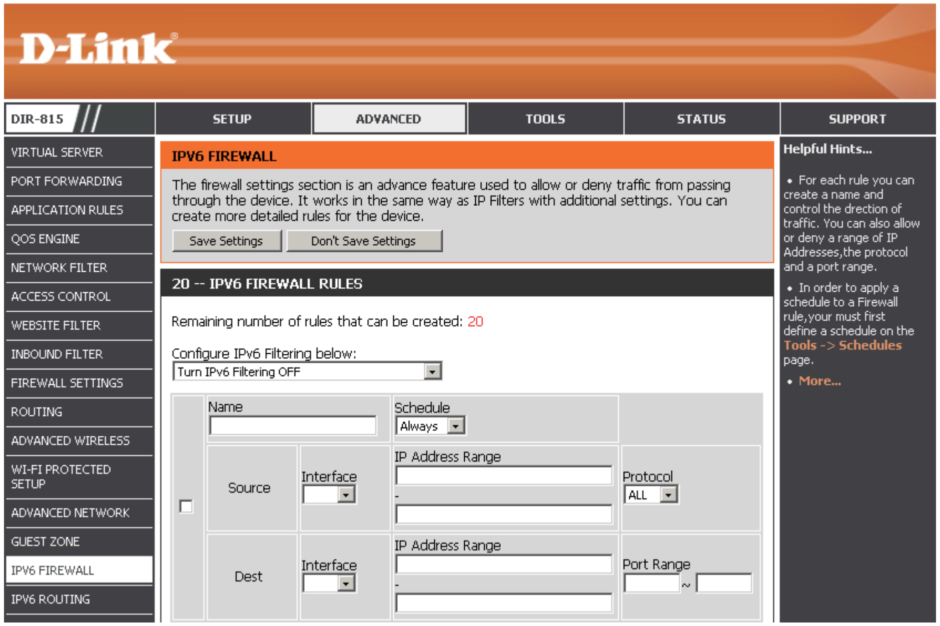
Security Mode : None

Helpful Hints...

- Use this section to configure the guest zone settings of your router. The guest zone provide a separate network zone for guests to access Internet.

IPv6 Firewall

The DIR-815’s IPv6 Firewall feature allows you to configure which kind of IPv6 traffic is allowed to pass through the device. The DIR-815’s IPv6 Firewall functions in a similar way to the IP Filters feature.



IPV6 FIREWALL

The firewall settings section is an advance feature used to allow or deny traffic from passing through the device. It works in the same way as IP Filters with additional settings. You can create more detailed rules for the device.

20 -- IPV6 FIREWALL RULES

Remaining number of rules that can be created: 20

Configure IPv6 Filtering below: Turn IPv6 Filtering OFF

□	Name		Schedule: Always	
	Source	Interface	IP Address Range	Protocol: ALL
	Dest	Interface	IP Address Range	Port Range ~

Helpful Hints...

- For each rule you can create a name and control the direction of traffic. You can also allow or deny a range of IP Addresses,the protocol and a port range.
- In order to apply a schedule to a Firewall rule,your must first define a schedule on the Tools -> Schedules page.
- More...

Enable Checkbox: Check the box on the left side to enable the IPv6 firewall rule.

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

Action: Use the radio buttons to *Allow* or *Deny* transport of the IPv6 data packets according to the criteria defined in the firewall rule.

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

Enter the source IPv6 address range in the adjacent **IP Address Range** field.
Use the **Dest** drop-down menu to specify the interface that connects to the destination IP addresses of the firewall rule.

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

Select 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.

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 top port range field and enter the last port in the field underneath.

Click the **Save Settings** button to save any changes made.

IPv6 Routing

This page 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.

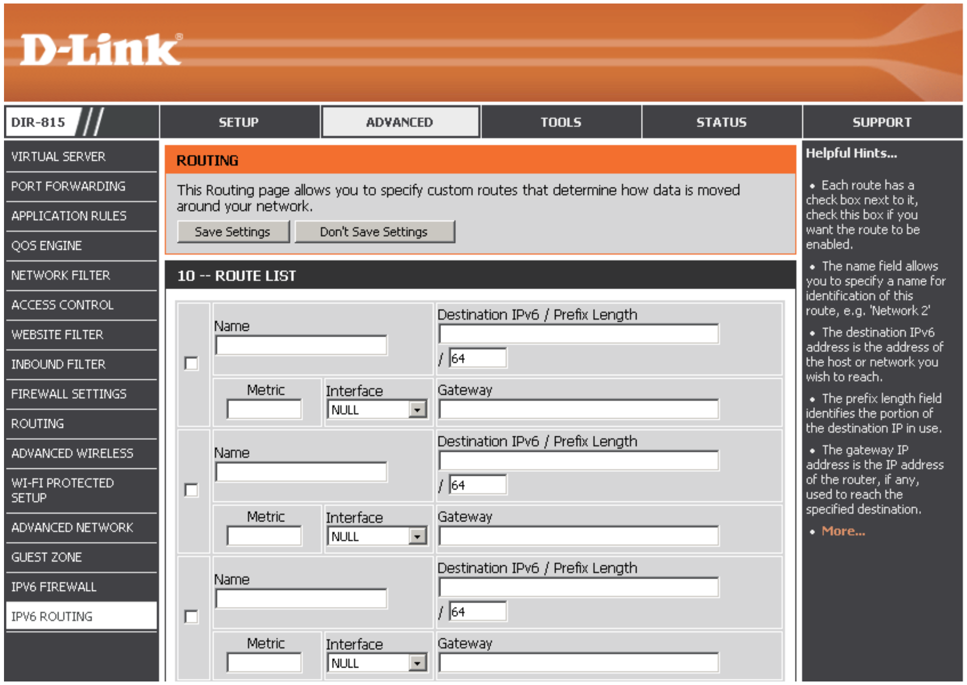
Name: Enter a specific name to identify this route.

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

Metric: Enter the metric value for this rule here.

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

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



ROUTING

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

10 -- ROUTE LIST

□	Name		Destination IPv6 / Prefix Length / 64
	Metric	Interface NULL	Gateway
□	Name		Destination IPv6 / Prefix Length / 64
	Metric	Interface NULL	Gateway
□	Name		Destination IPv6 / Prefix Length / 64
	Metric	Interface NULL	Gateway

Helpful Hints...

- Each route has a check box next to it, check this box if you want the route to be enabled.
- The name field allows you to specify a name for identification of this route, e.g. 'Network 2'
- The destination IPv6 address is the address of the host or network you wish to reach.
- The prefix length field identifies the portion of the destination IP in use.
- The gateway IP address is the IP address of the router, if any, used to reach the specified destination.

Tools

Admin

This page will allow you to change the Administrator password and configure the authentication settings. This window also allows you to enable Remote Management, via the Internet.

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

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.

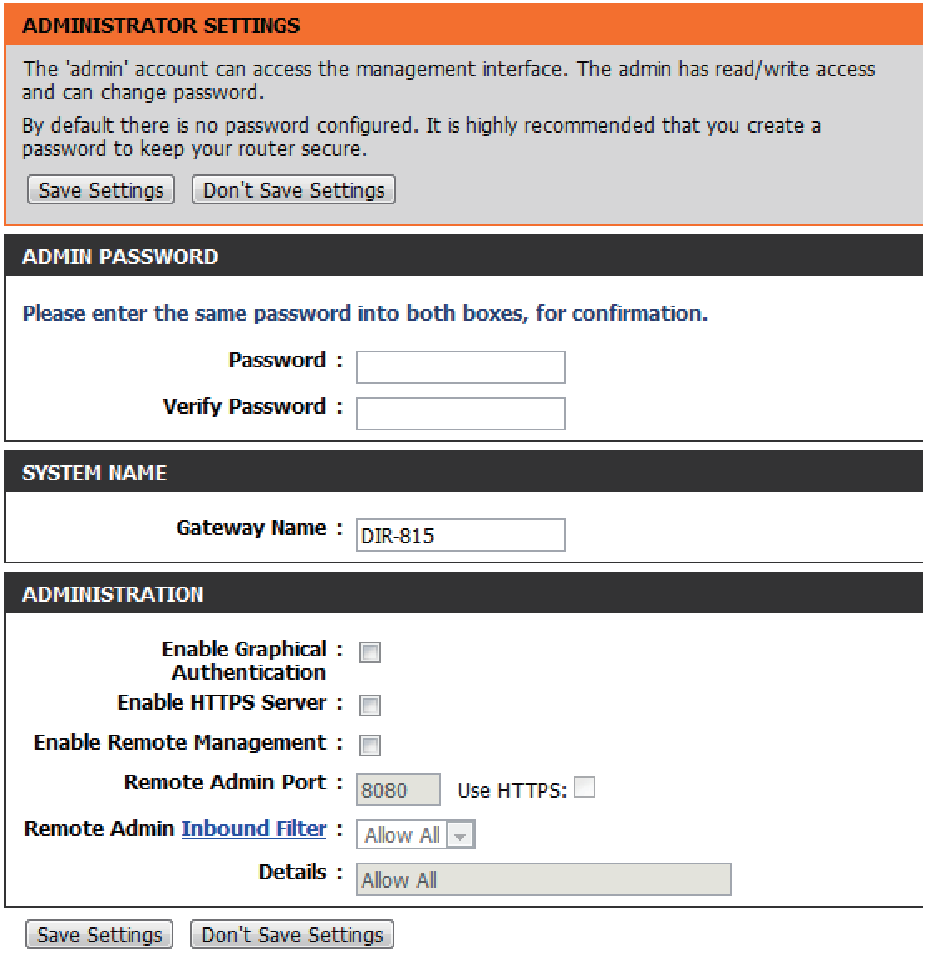
Enable HTTPS Server: Check to enable HTTPS to connect to the router securely. This means to connect to the router, you must enter **https://192.168.0.1** (for example) instead of **http://192.168.0.1**.

Enable Remote Management: Remote management allows the DIR-815 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-815 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-815 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.



ADMINISTRATOR SETTINGS

The 'admin' account can access the management interface. The admin has read/write access and can change password.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :

Verify Password :

SYSTEM NAME

Gateway Name : DIR-815

ADMINISTRATION

Enable Graphical Authentication : □

Enable HTTPS Server : □

Enable Remote Management : □

Remote Admin Port : 8080 Use HTTPS: □

Remote Admin Inbound Filter : Allow All

Details : Allow All

Click the **Save Settings** button to save any changes made.

Time

The Time window 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.

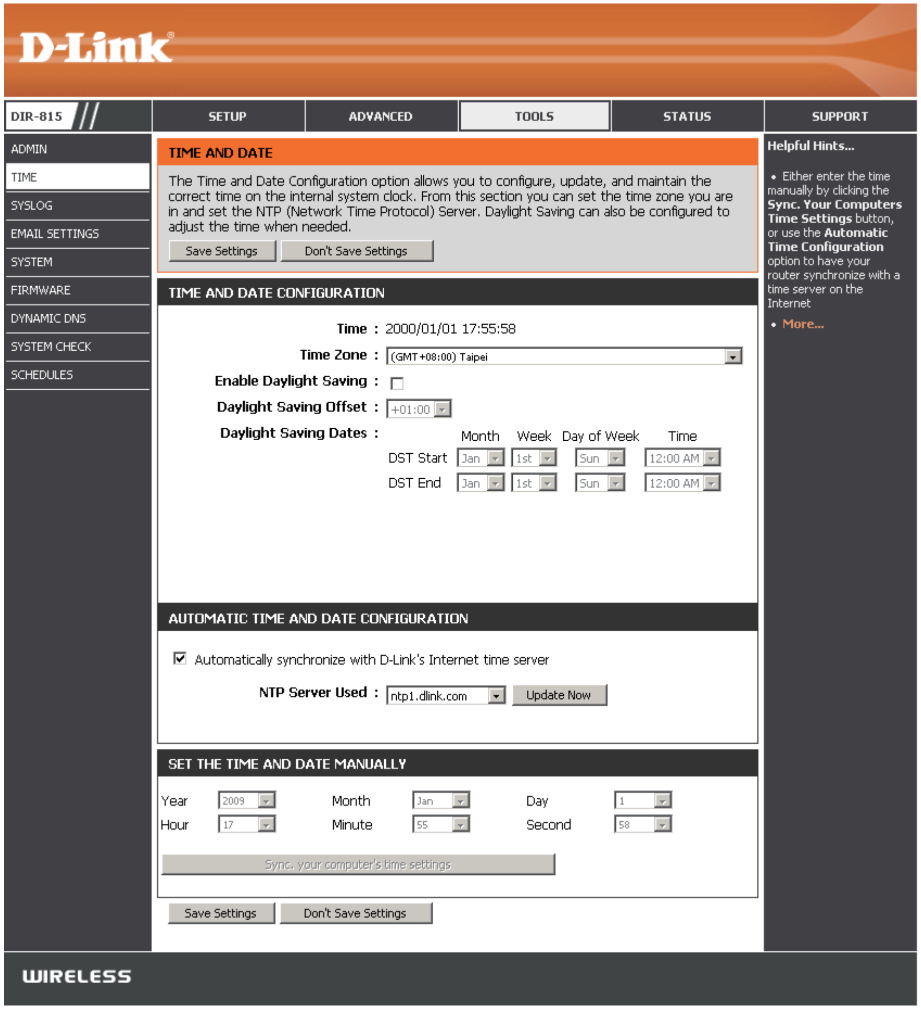
Enable Daylight Saving: To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

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

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

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.



TIME AND DATE

The Time and Date Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone you are in and set the NTP (Network Time Protocol) Server. Daylight Saving can also be configured to adjust the time when needed.

TIME AND DATE CONFIGURATION

Time : 2000/01/01 17:55:58

Time Zone : (GMT+08:00) Taipei

Enable Daylight Saving : □

Daylight Saving Offset : +01:00

Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Jan	1st	Sun	12:00 AM
DST End	Jan	1st	Sun	12:00 AM

AUTOMATIC TIME AND DATE CONFIGURATION

☑ Automatically synchronize with D-Link's Internet time server

NTP Server Used : ntp1.dlink.com

SET THE TIME AND DATE MANUALLY

Year	2009	Month	Jan	Day	1
Hour	17	Minute	55	Second	58

Helpful Hints...

- Either enter the time manually by clicking the **Sync. Your Computers Time Settings** button, or use the **Automatic Time Configuration** option to have your router synchronize with a time server on the Internet

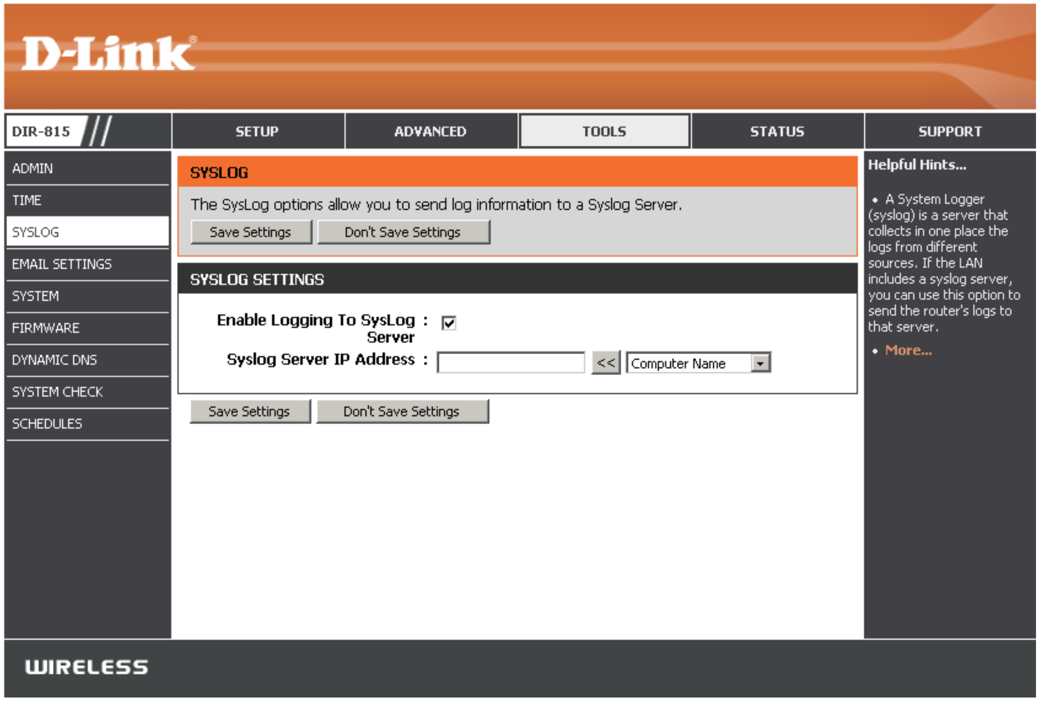
Click the **Save Settings** button to save any changes made.

SysLog

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

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

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



SYSLOG

The SysLog options allow you to send log information to a Syslog Server.

SYSLOG SETTINGS

Enable Logging To SysLog Server : ☑

Syslog Server IP Address : Computer Name

Helpful Hints...

- A System Logger (syslog) is a server that collects in one place the logs from different sources. If the LAN includes a syslog server, you can use this option to send the router's logs to that server.

Email Settings

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

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

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

Email Subject: Enter the text that you want to appear in the subject line of the e-mail that is sent.

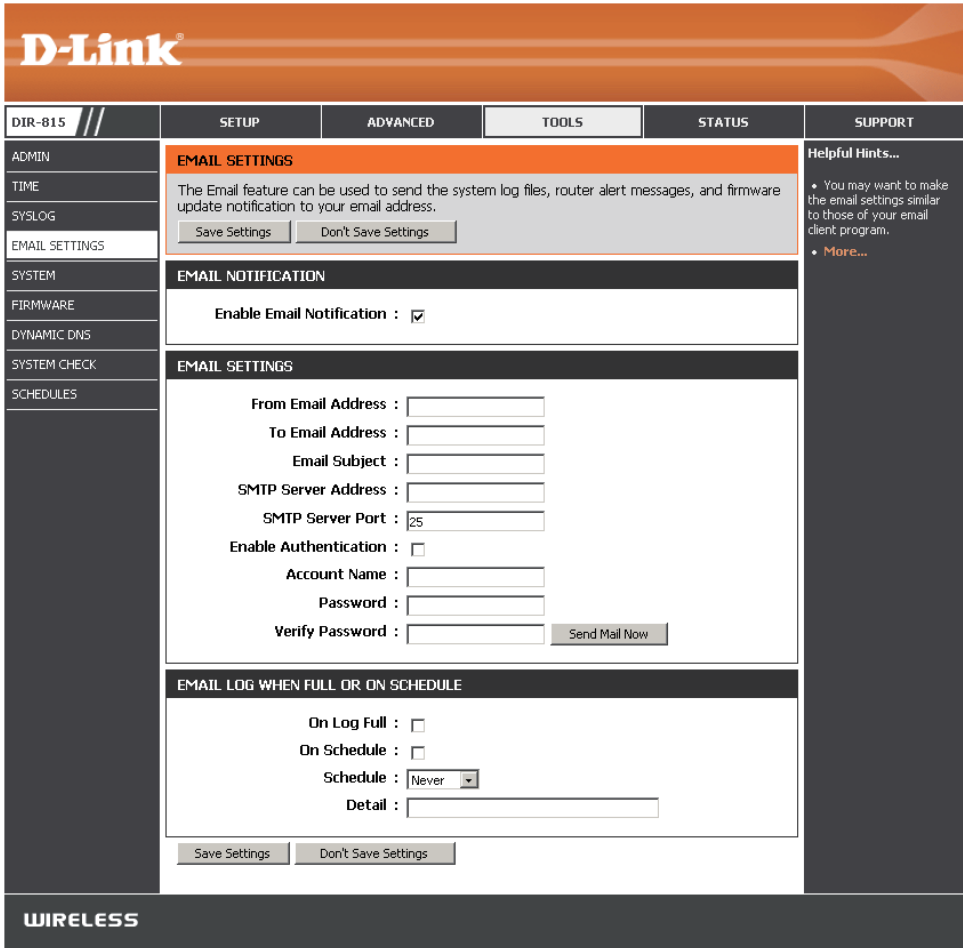
SMTP Server Address: Enter the SMTP server address for sending email. If your SMTP server requires authentication, select this option.

Account Name: Enter your account for sending email.

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

Send Mail Now: Click this button to send a test email from the Router to verify that the email settings have been configured correctly.

Click the **Save Settings** button to save any changes made.



EMAIL SETTINGS

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

Save Settings | Don't Save Settings

EMAIL NOTIFICATION

Enable Email Notification : ☑

EMAIL SETTINGS

From Email Address :
To Email Address :
Email Subject :
SMTP Server Address :
SMTP Server Port : 25
Enable Authentication : □
Account Name :
Password :
Verify Password : Send Mail Now

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full : □
On Schedule : □
Schedule : Never
Detail :

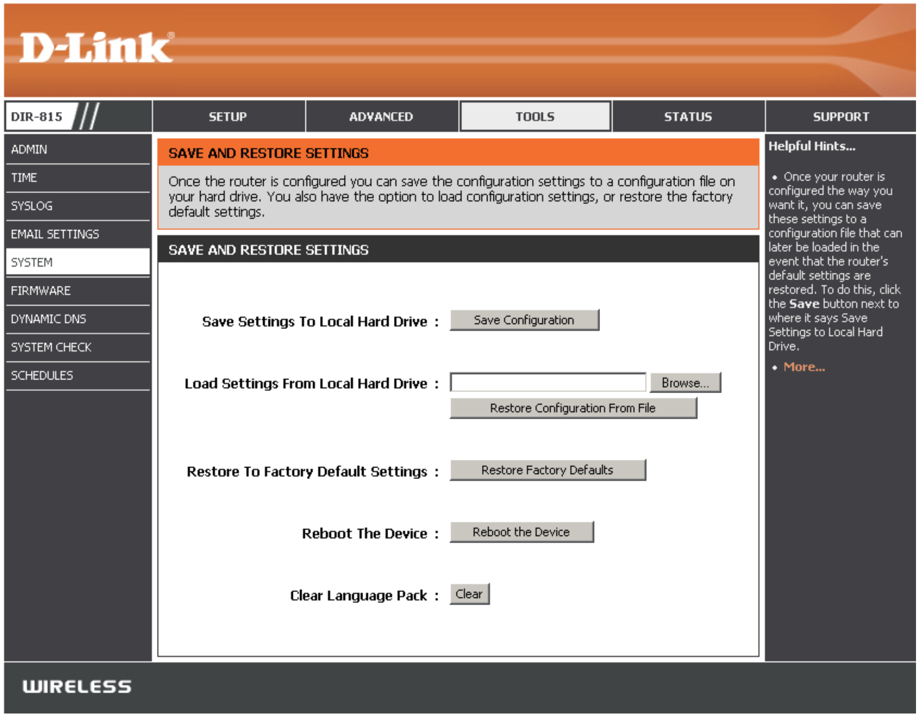
Save Settings | Don't Save Settings

Helpful Hints...

- You may want to make the email settings similar to those of your email client program.
- More...

System

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



SAVE AND RESTORE SETTINGS

Once the router is configured you can save the configuration settings to a configuration file on your hard drive. You also have the option to load configuration settings, or restore the factory default settings.

SAVE AND RESTORE SETTINGS

Save Settings To Local Hard Drive : Save Configuration

Load Settings From Local Hard Drive : Browse... Restore Configuration From File

Restore To Factory Default Settings : Restore Factory Defaults

Reboot The Device : Reboot the Device

Clear Language Pack : Clear

Helpful Hints...

- Once your router is configured the way you want it, you can save these settings to a configuration file that can later be loaded in the event that the router's default settings are restored. To do this, click the **Save** button next to where it says Save Settings to Local Hard Drive.
- More...

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

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

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

Reboot Device: Click to reboot the router.

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

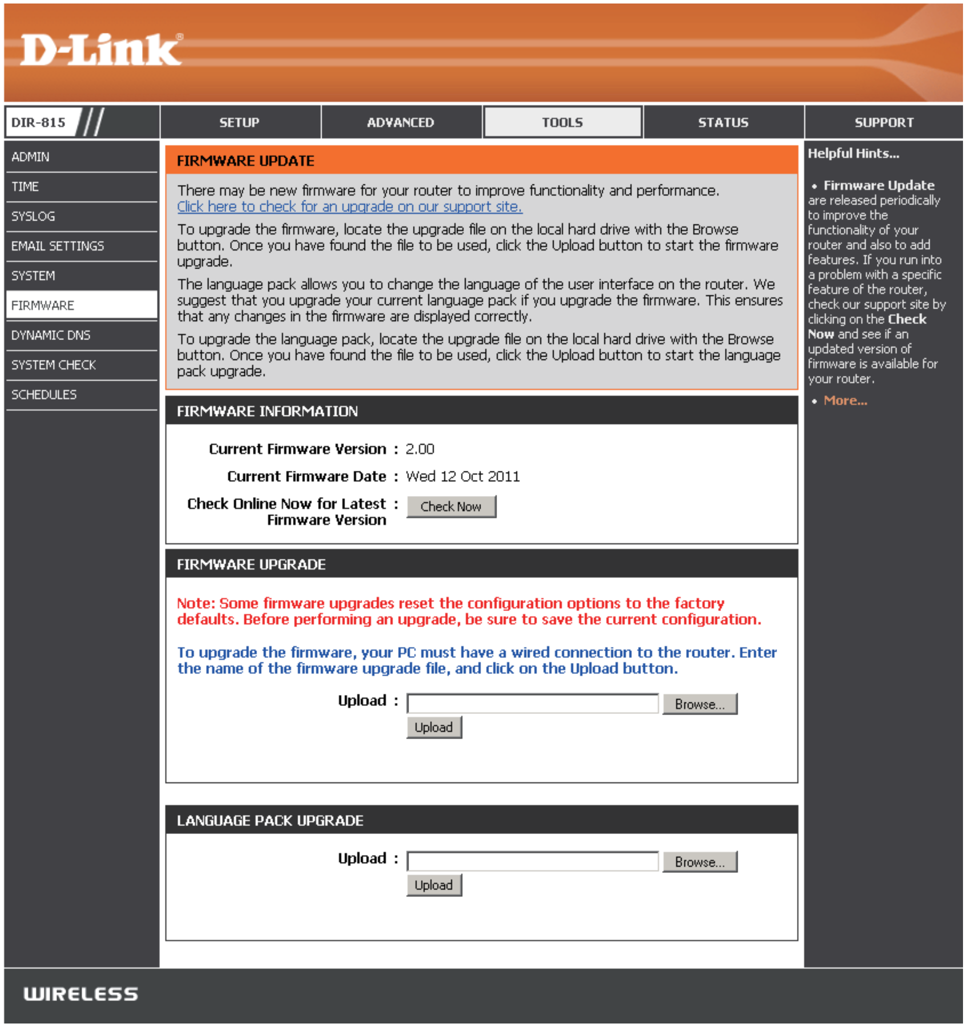
Firmware

Use the Firmware window to upgrade the firmware of the Router and install language packs. If you plan to install new firmware, make sure the firmware you want to use is on the local hard drive of the computer. If you want to install a new language pack, make sure that you have the language pack available. Please check the D-Link support site for firmware updates at **http://support.dlink.com**. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Information: This section displays information about the firmware that is loaded on the Router. Click the **Check Now** button to find out if there is an updated firmware; if so, download the new firmware to your hard drive.

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

Language Pack Upgrade: If you want to change the Router's language pack, click **Browse** to locate the language pack. Click **Upload** to complete the load the new language pack.



FIRMWARE UPDATE

There may be new firmware for your router to improve functionality and performance.
Click here to check for an upgrade on our support site.

To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the firmware upgrade.

The language pack allows you to change the language of the user interface on the router. We suggest that you upgrade your current language pack if you upgrade the firmware. This ensures that any changes in the firmware are displayed correctly.

To upgrade the language pack, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Upload button to start the language pack upgrade.

FIRMWARE INFORMATION

Current Firmware Version : 2.00
Current Firmware Date : Wed 12 Oct 2011
Check Online Now for Latest Firmware Version : Check Now

FIRMWARE UPGRADE

Note: Some firmware upgrades reset the configuration options to the factory defaults. Before performing an upgrade, be sure to save the current configuration.

To upgrade the firmware, your PC must have a wired connection to the router. Enter the name of the firmware upgrade file, and click on the Upload button.

Upload :

LANGUAGE PACK UPGRADE

Upload :

Helpful Hints...

- **Firmware Update** are released periodically to improve the functionality of your router and also to add features. If you run into a problem with a specific feature of the router, check our support site by clicking on the **Check Now** and see if an updated version of firmware is available for your router.
- More...

Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) using a domain name that you have purchased (www.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.

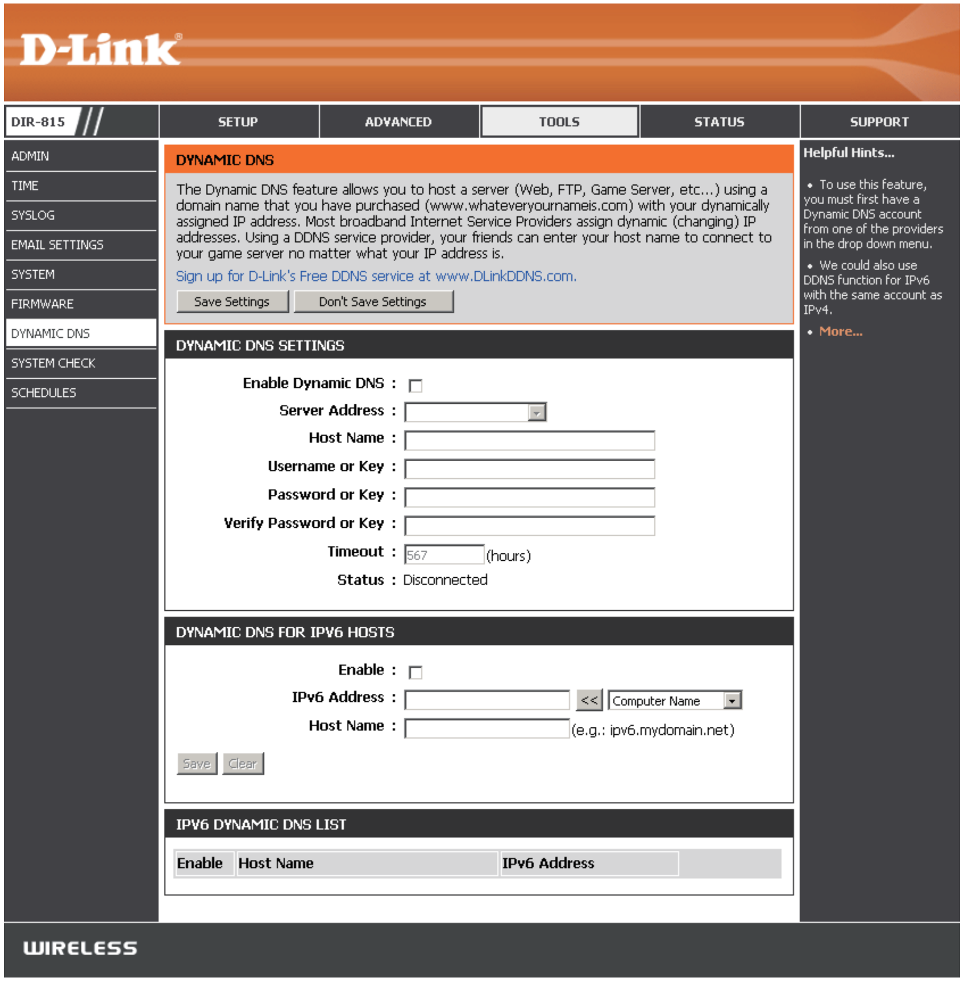
Timeout: Enter a timeout time (in hours).

Status: Displays the current connection status.

DDNS for IPv6 Hosts

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

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



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 (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 your host name to connect to your game server no matter what your IP address is.

Sign up for D-Link's Free DDNS service at www.DLinkDDNS.com.

DYNAMIC DNS SETTINGS

Enable Dynamic DNS : □
Server Address :
Host Name :
Username or Key :
Password or Key :
Verify Password or Key :
Timeout : 567 (hours)
Status : Disconnected

DYNAMIC DNS FOR IPV6 HOSTS

Enable : □
IPv6 Address : << Computer Name
Host Name : (e.g.: ipv6.mydomain.net)

IPV6 DYNAMIC DNS LIST

Enable	Host Name	IPv6 Address

Helpful Hints...

- To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu.
- We could also use DDNS function for IPv6 with the same account as IPv4.
- More...

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

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

Enable: Check to enable the entry.

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

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

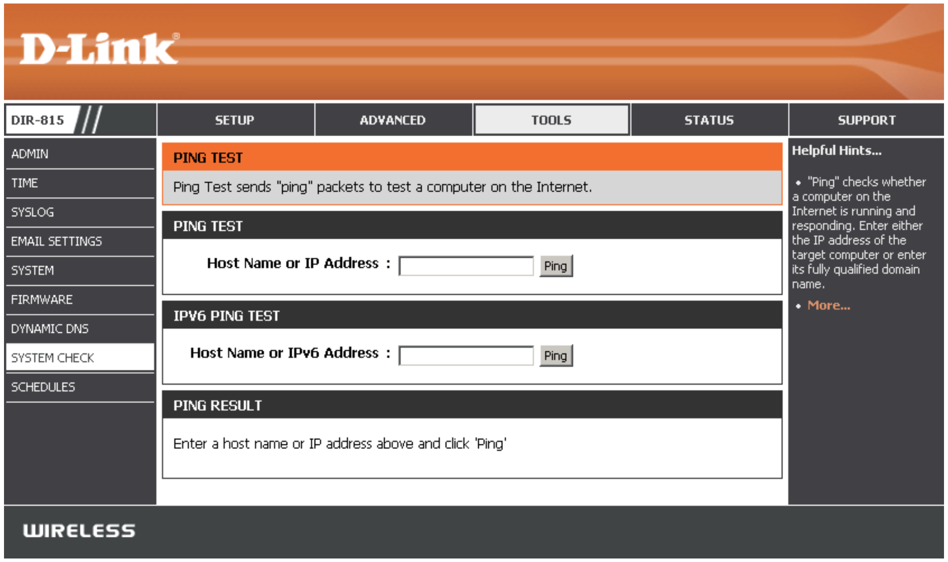
Edit/Delete: Click the edit icon to make changes to the entry or click the delete icon to remove the entry.

System Check

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

IPv6 Ping Test: The IPv6 Ping Test is used to send IPv6 Ping packets to test if a computer is on the Internet. Enter the IPv6 Address that you wish to Ping, and click **Ping**. Click **Stop** to stop sending IPv6 Ping packets

Ping Results: The results of your Ping/IPv6 Ping attempts will be displayed here.



PING TEST

Ping Test sends "ping" packets to test a computer on the Internet.

PING TEST

Host Name or IP Address :

IPV6 PING TEST

Host Name or IPv6 Address :

PING RESULT

Enter a host name or IP address above and click 'Ping'

Helpful Hints...

- "Ping" checks whether a computer on the Internet is running and responding. Enter either the IP address of the target computer or enter its fully qualified domain name.

Schedules

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

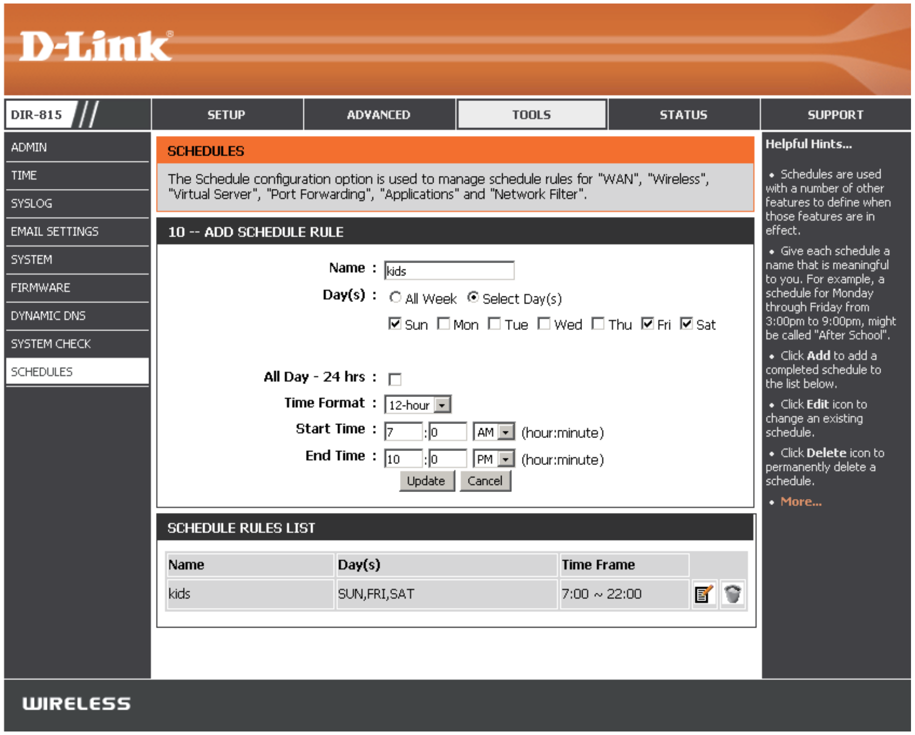
Name: Enter a name for your new schedule.

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

Time: Check **All Day - 24hrs** or enter a *Start Time* and *End Time* for your schedule.

Add: Click **Add** to save your schedule. You must click the **Add** button 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.



SCHEDULES

The Schedule configuration option is used to manage schedule rules for "WAN", "Wireless", "Virtual Server", "Port Forwarding", "Applications" and "Network Filter".

10 -- ADD SCHEDULE RULE

Name : kids

Day(s) : ○ All Week ● Select Day(s)

☑ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☑ Fri ☑ Sat

All Day - 24 hrs : ☐

Time Format : 12-hour

Start Time : 7 : 0 AM (hour:minute)

End Time : 10 : 0 PM (hour:minute)

SCHEDULE RULES LIST

Name	Day(s)	Time Frame	
kids	SUN,FRI,SAT	7:00 ~ 22:00	

Helpful Hints...

- Schedules are used with a number of other features to define when those features are in effect.
- Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".
- Click **Add** to add a completed schedule to the list below.
- Click **Edit** icon to change an existing schedule.
- Click **Delete** icon to permanently delete a schedule.
- More...

Status

Device Info

This page displays the current information for the DIR-815. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

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

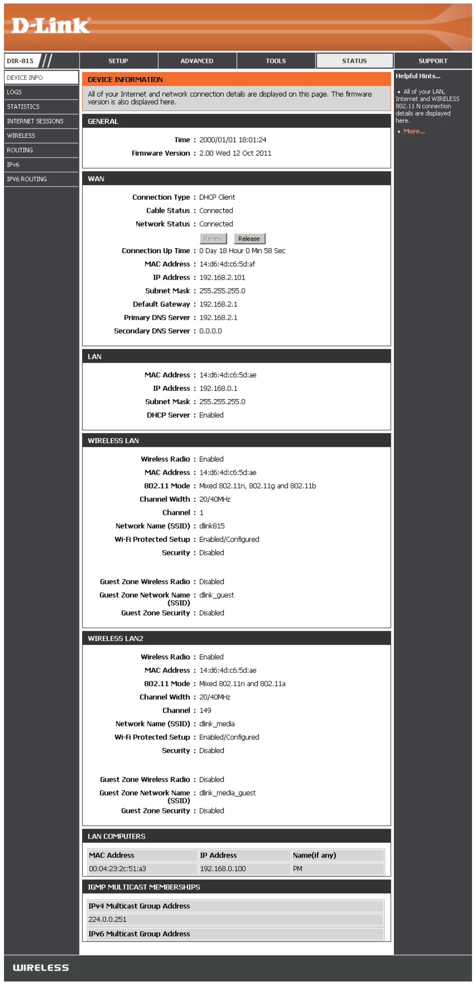
General: Displays the router's time and firmware version.

WAN: Displays the MAC address and the public IP settings

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

Wireless LAN: Displays the wireless MAC address and your wireless settings such as SSID and Channel. The first Wireless LAN section is for the 2.4GHz segment and the second section is for the 5GHz segment.

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).



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

Helpful Hints...

- All of your LAN, Internet and WIRELESS 802.11 N connection details are displayed here.
- More...

GENERAL

Time : 2000/01/01 18:01:24
Firmware Version : 2.00 Wed 12 Oct 2011

WAN

Connection Type : DHCP Client
Cable Status : Connected
Network Status : Connected
Connection Up Time : 0 Day 18 Hour 0 Min 58 Sec
MAC Address : 14:d6:4d:c6:5d:af
IP Address : 192.168.2.101
Subnet Mask : 255.255.255.0
Default Gateway : 192.168.2.1
Primary DNS Server : 192.168.2.1
Secondary DNS Server : 0.0.0.0

LAN

MAC Address : 14:d6:4d:c6:5d:ae
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

Wireless Radio : Enabled
MAC Address : 14:d6:4d:c6:5d:ae
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Channel Width : 20/40MHz
Channel : 1
Network Name (SSID) : dlink815
Wi-Fi Protected Setup : Enabled/Configured
Security : Disabled

Guest Zone Wireless Radio : Disabled
Guest Zone Network Name (SSID) : dlink_guest
Guest Zone Security : Disabled

WIRELESS LAN2

Wireless Radio : Enabled
MAC Address : 14:d6:4d:c6:5d:ae
802.11 Mode : Mixed 802.11n and 802.11a
Channel Width : 20/40MHz
Channel : 149
Network Name (SSID) : dlink_media
Wi-Fi Protected Setup : Enabled/Configured
Security : Disabled

Guest Zone Wireless Radio : Disabled
Guest Zone Network Name (SSID) : dlink_media_guest
Guest Zone Security : Disabled

LAN COMPUTERS

MAC Address	IP Address	Name(if any)
00:04:23:2c:51:a3	192.168.0.100	PM

IGMP MULTICAST MEMBERSHIPS

IPv4 Multicast Group Address
224.0.0.251
IPv6 Multicast Group Address

Logs

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

Save Log File: Click the **Save** button save the Router's log entries to a log file on your computer.

Log Type: Use the radio buttons to select the types of messages that you want to display from the log. **System**, **Firewall & Security**, and **Router Status** messages can be selected.

Log Level: There are three levels of message importance: **Critical**, **Warning**, and **Information**. Select the levels that you want displayed in the log.

Log Files: Use this section to view and manage the Router's log entries.

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

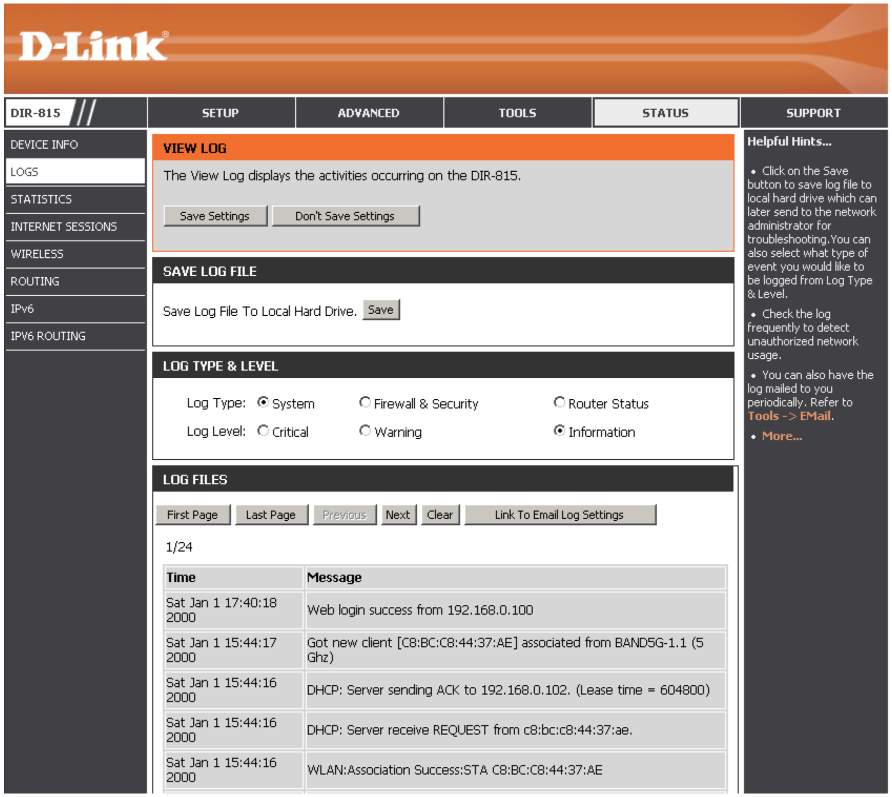
Last Page: Click this button to view the last page of the Router logs.

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

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

Clear: Clears all of the log contents.

Link to Log Settings: Click this button to open the **Tools** > **Email Settings** screen so that you can change the Email configuration for sending logs.



VIEW LOG

The View Log displays the activities occurring on the DIR-815.

SAVE LOG FILE

Save Log File To Local Hard Drive.

LOG TYPE & LEVEL

Log Type: ● System ○ Firewall & Security ○ Router Status

Log Level: ○ Critical ○ Warning ● Information

LOG FILES

1/24

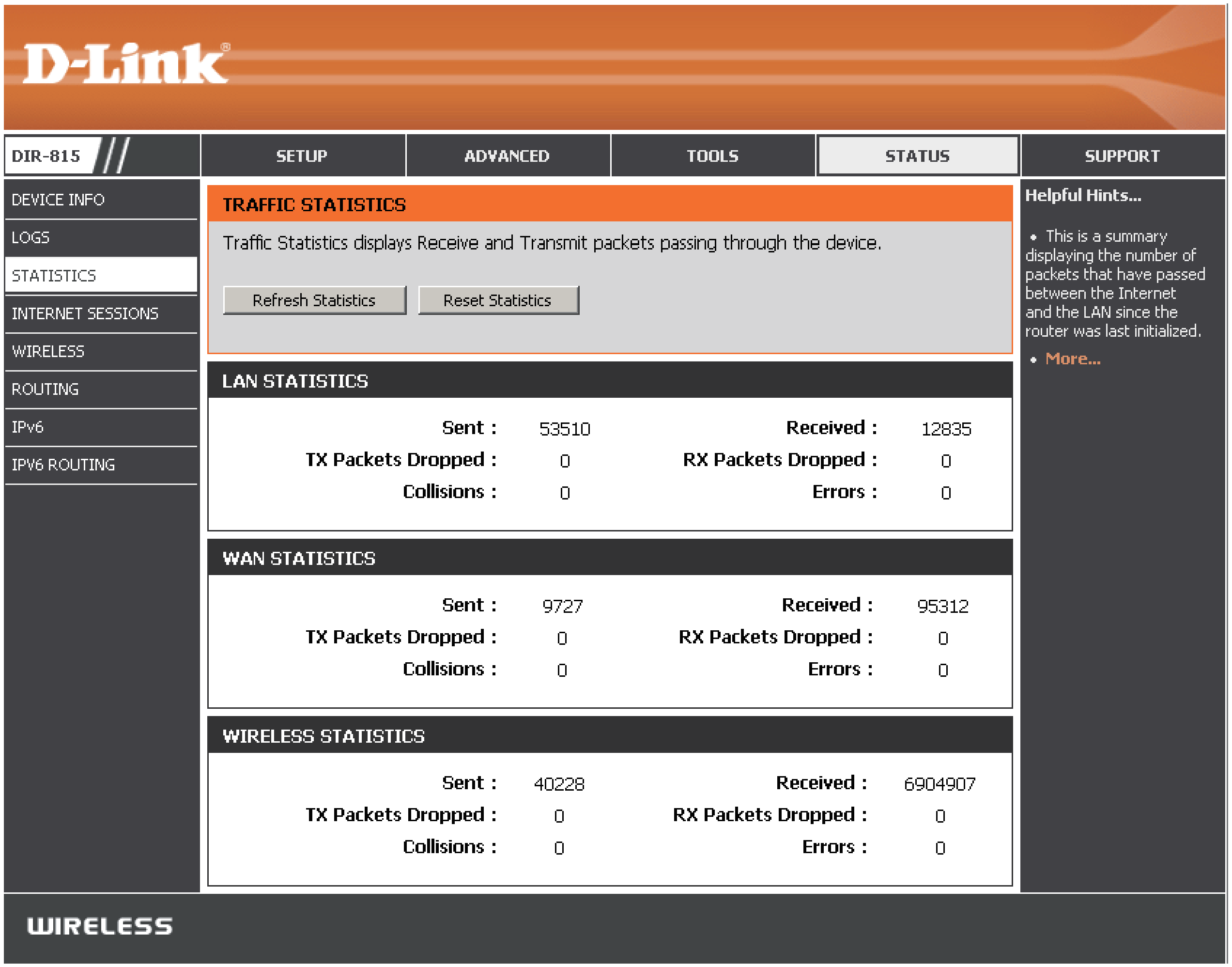
Time	Message
Sat Jan 1 17:40:18 2000	Web login success from 192.168.0.100
Sat Jan 1 15:44:17 2000	Got new client [C8:BC:C8:44:37:AE] associated from BAND5G-1.1 (5 Ghz)
Sat Jan 1 15:44:16 2000	DHCP: Server sending ACK to 192.168.0.102. (Lease time = 604800)
Sat Jan 1 15:44:16 2000	DHCP: Server receive REQUEST from c8:bc:c8:44:37:ae.
Sat Jan 1 15:44:16 2000	WLAN:Association Success:STA C8:BC:C8:44:37:AE

Helpful Hints...

- Click on the Save button to save log file to local hard drive which can later send to the network administrator for troubleshooting. You can also select what type of event you would like to be logged from Log Type & Level.
- Check the log frequently to detect unauthorized network usage.
- You can also have the log mailed to you periodically. Refer to **Tools -> EMail**.
- **More...**

Statistics

The screen below displays the **Traffic Statistics**. Here you can view the amount of packets that pass through the DIR-815 on both the WAN, LAN ports and both the 802.11n/g (2.4GHz) and 802.11n/a (5GHz) wireless bands. The traffic counter will reset if the device is rebooted.



TRAFFIC STATISTICS

Traffic Statistics displays Receive and Transmit packets passing through the device.

LAN STATISTICS

Sent :	53510	Received :	12835
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

WAN STATISTICS

Sent :	9727	Received :	95312
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

WIRELESS STATISTICS

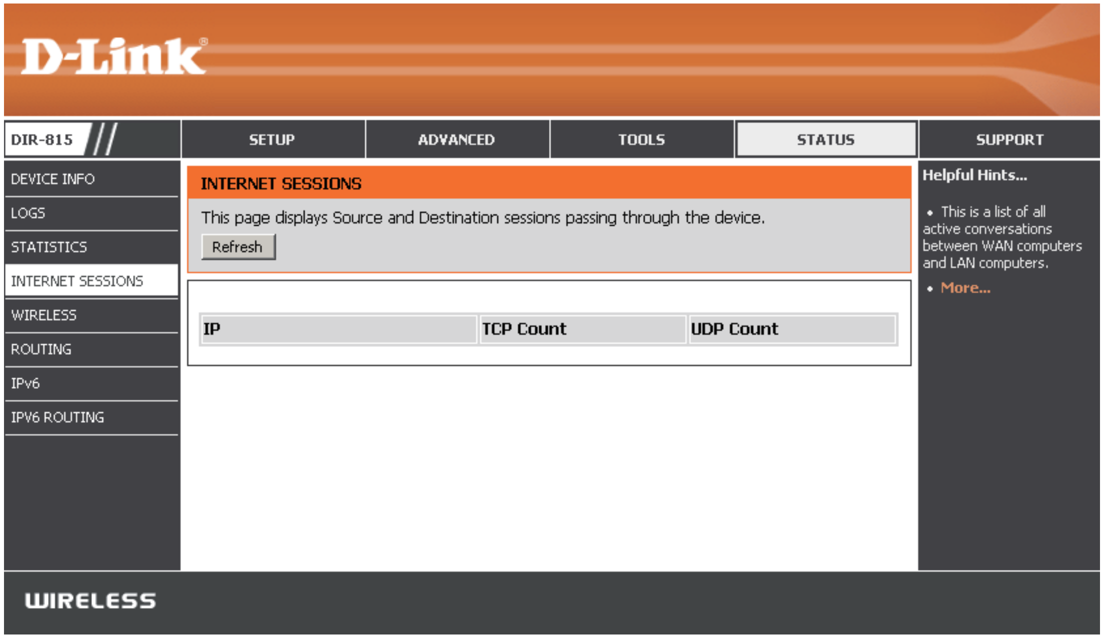
Sent :	40228	Received :	6904907
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

Helpful Hints...

- This is a summary displaying the number of packets that have passed between the Internet and the LAN since the router was last initialized.
- More...

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.



INTERNET SESSIONS

This page displays Source and Destination sessions passing through the device.

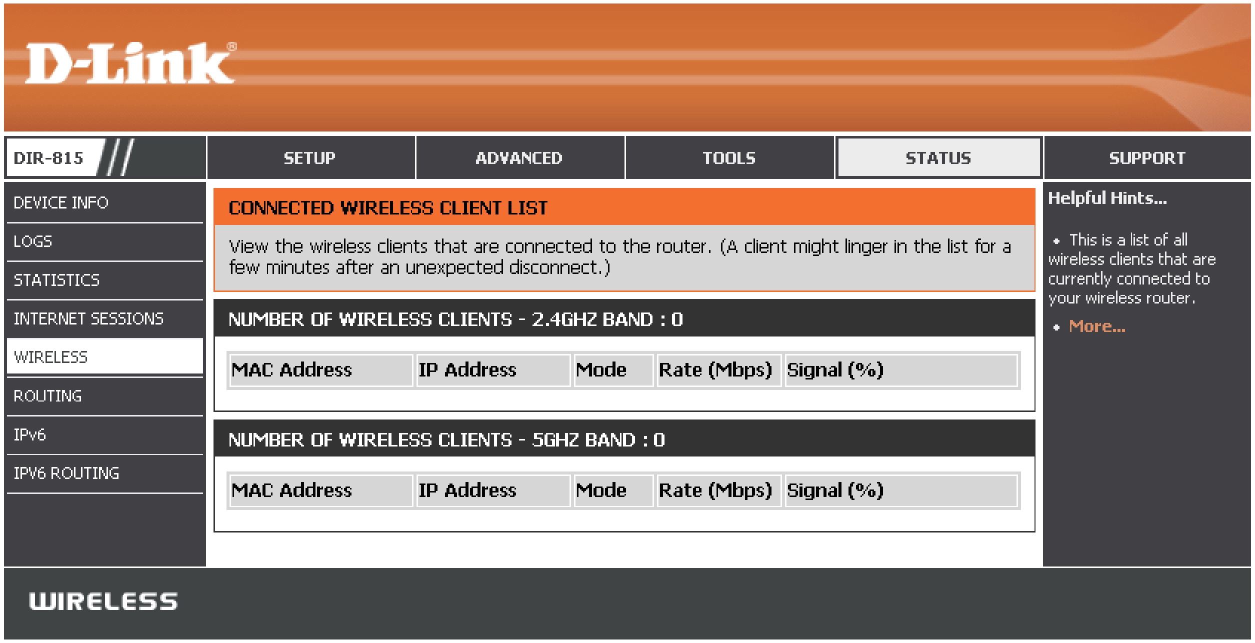
IP	TCP Count	UDP Count

Helpful Hints...

- This is a list of all active conversations between WAN computers and LAN computers.

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.



CONNECTED WIRELESS CLIENT LIST

View the wireless clients that are connected to the router. (A client might linger in the list for a few minutes after an unexpected disconnect.)

NUMBER OF WIRELESS CLIENTS - 2.4GHZ BAND : 0

MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)

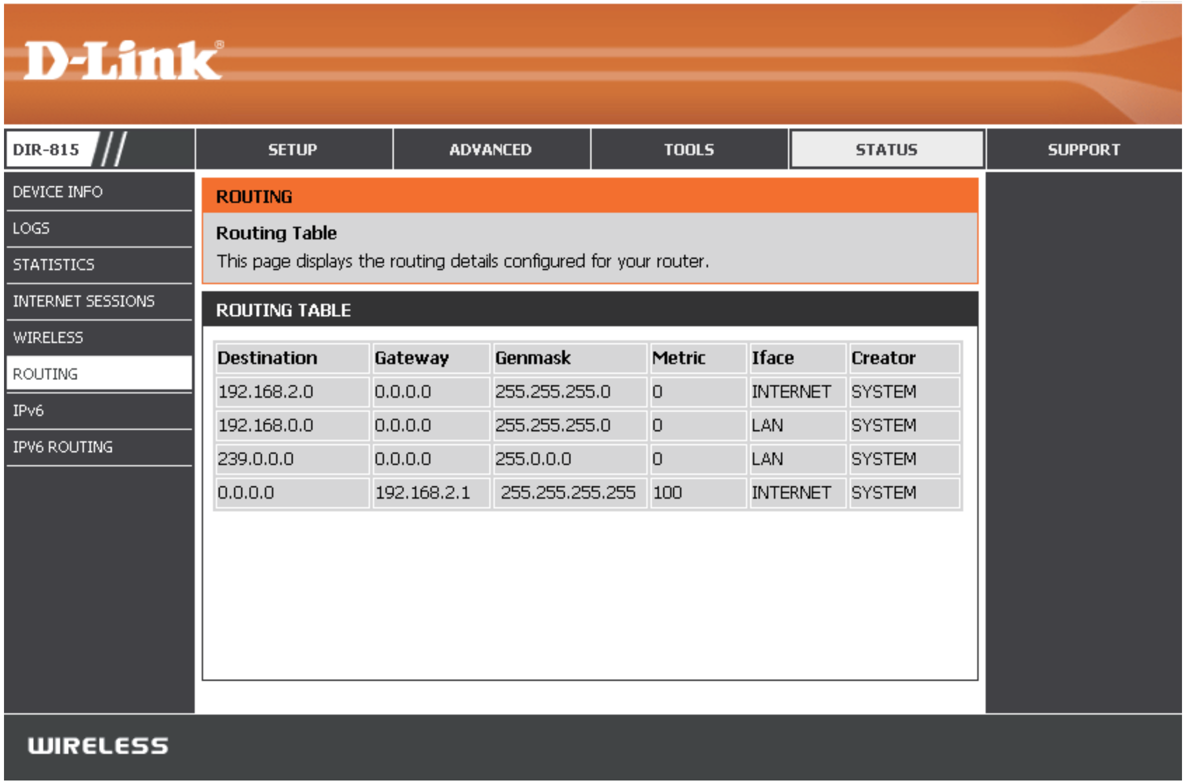
NUMBER OF WIRELESS CLIENTS - 5GHZ BAND : 0

MAC Address	IP Address	Mode	Rate (Mbps)	Signal (%)

- This is a list of all wireless clients that are currently connected to your wireless router.

Routing

This page will display your current routing table.



ROUTING

Routing Table

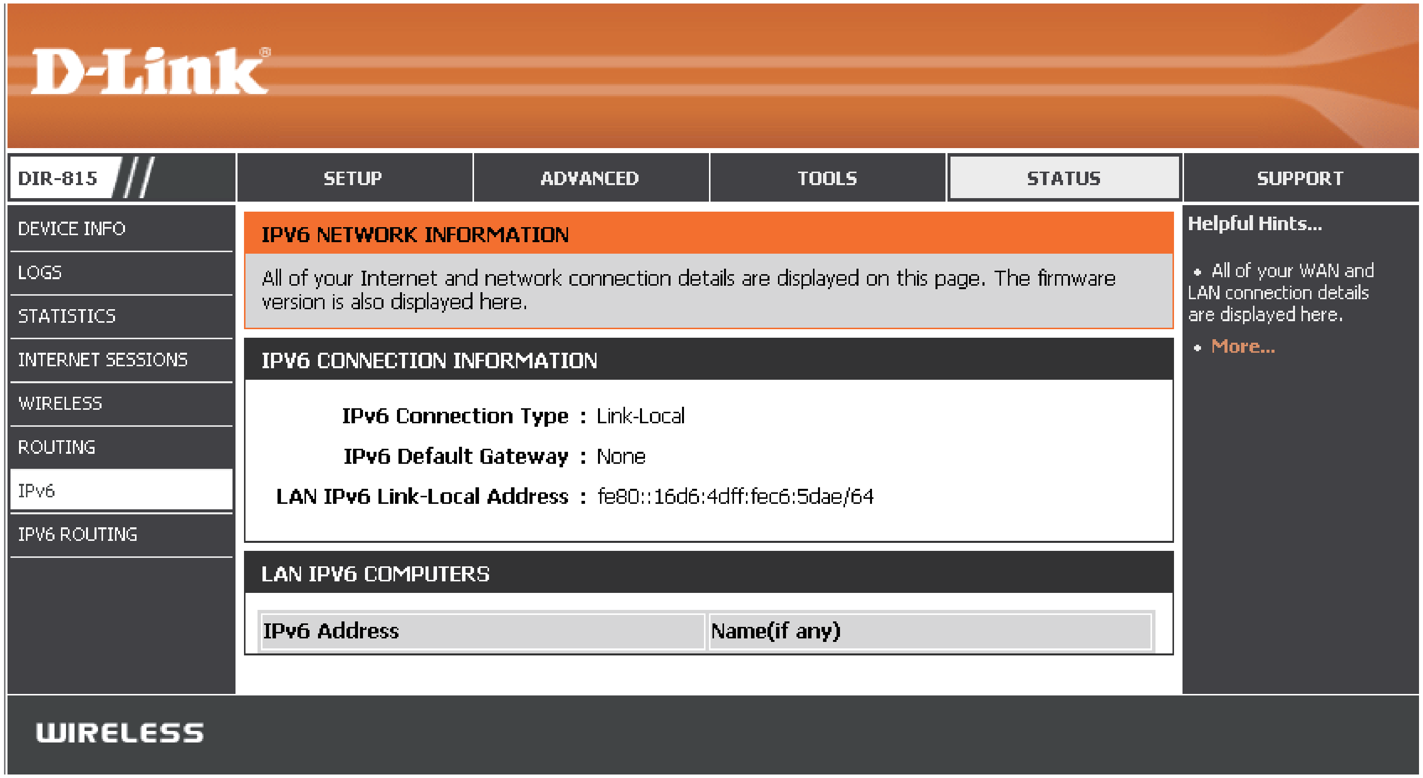
This page displays the routing details configured for your router.

ROUTING TABLE

Destination	Gateway	Genmask	Metric	Iface	Creator
192.168.2.0	0.0.0.0	255.255.255.0	0	INTERNET	SYSTEM
192.168.0.0	0.0.0.0	255.255.255.0	0	LAN	SYSTEM
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN	SYSTEM
0.0.0.0	192.168.2.1	255.255.255.255	100	INTERNET	SYSTEM

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 NETWORK INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

IPV6 CONNECTION INFORMATION

IPv6 Connection Type : Link-Local

IPv6 Default Gateway : None

LAN IPv6 Link-Local Address : fe80::16d6:4dff:fec6:5dae/64

LAN IPV6 COMPUTERS

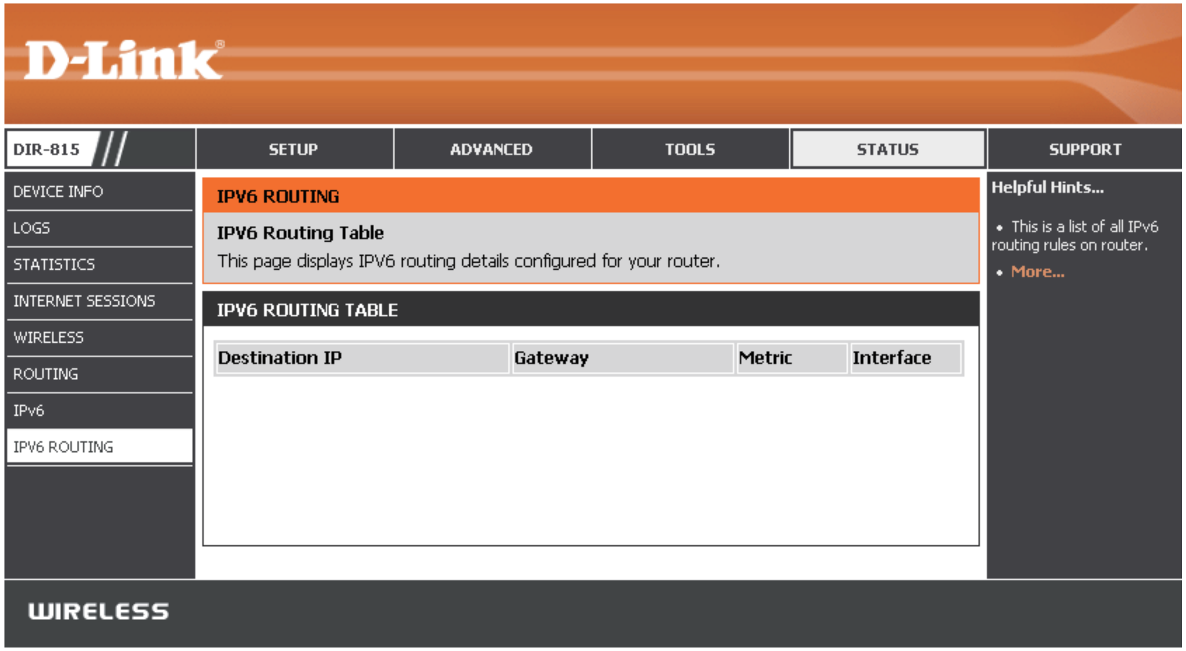
IPv6 Address	Name(if any)

Helpful Hints...

- All of your WAN and LAN connection details are displayed here.
- More...

IPV6 Routing

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



IPV6 ROUTING

IPV6 Routing Table

This page displays IPV6 routing details configured for your router.

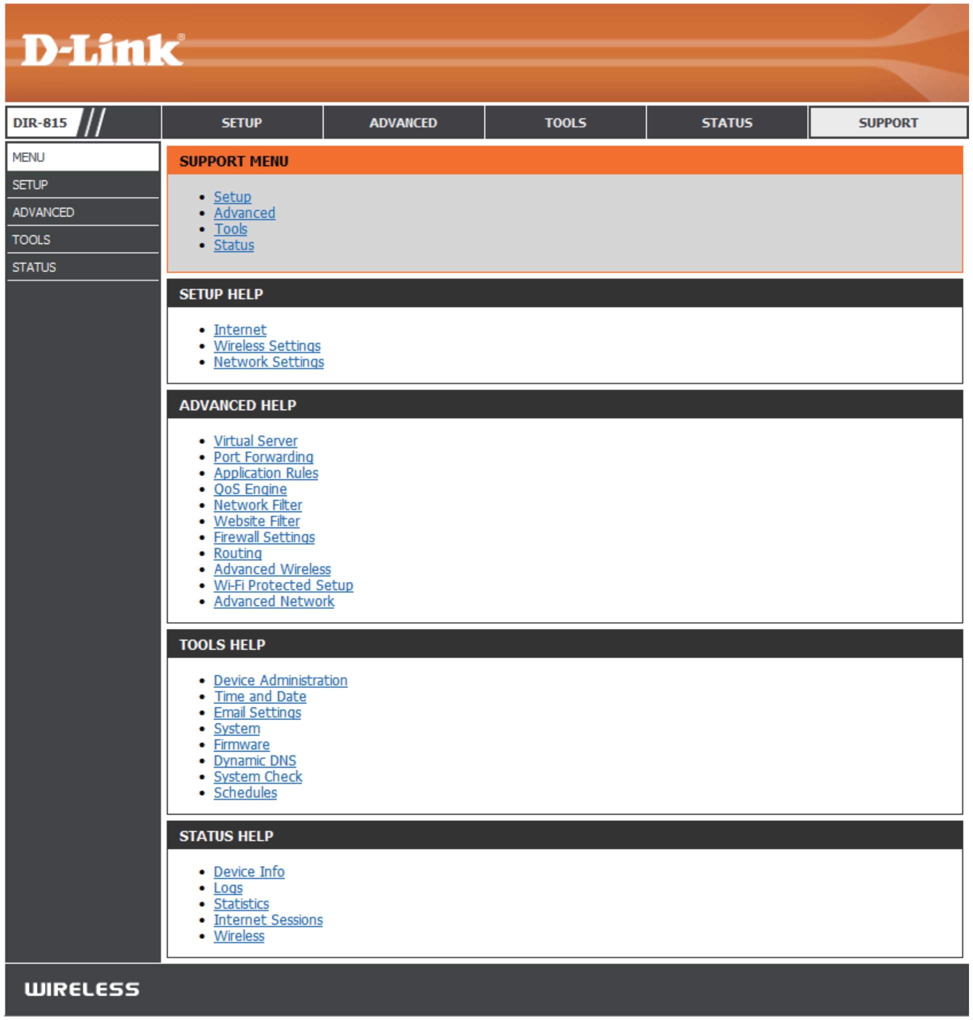
IPV6 ROUTING TABLE

Destination IP	Gateway	Metric	Interface

Helpful Hints...

- This is a list of all IPv6 routing rules on router.
- More...

Support



SUPPORT MENU

- Setup
- Advanced
- Tools
- Status

SETUP HELP

- Internet
- Wireless Settings
- Network Settings

ADVANCED HELP

- Virtual Server
- Port Forwarding
- Application Rules
- QoS Engine
- Network Filter
- Website Filter
- Firewall Settings
- Routing
- Advanced Wireless
- Wi-Fi Protected Setup
- Advanced Network

TOOLS HELP

- Device Administration
- Time and Date
- Email Settings
- System
- Firmware
- Dynamic DNS
- System Check
- Schedules

STATUS HELP

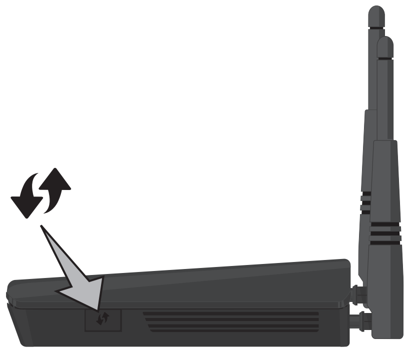
- Device Info
- Logs
- Statistics
- Internet Sessions
- Wireless

Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DIR-815 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-815 for about 1 second. The WPS button 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).

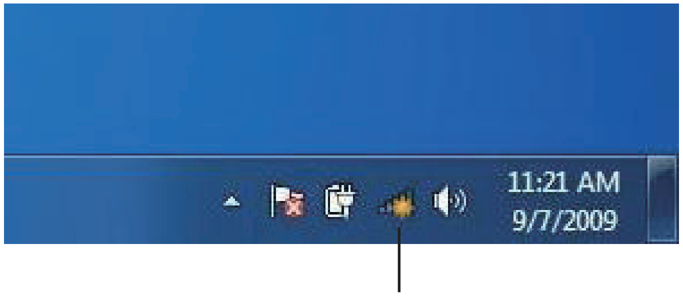
Step 3 - Allow up to 1 minute to configure. Once the WPS light stops blinking, you will be connected and your wireless connection will be secure with WPA2.

Windows® 7

WPA/WPA2

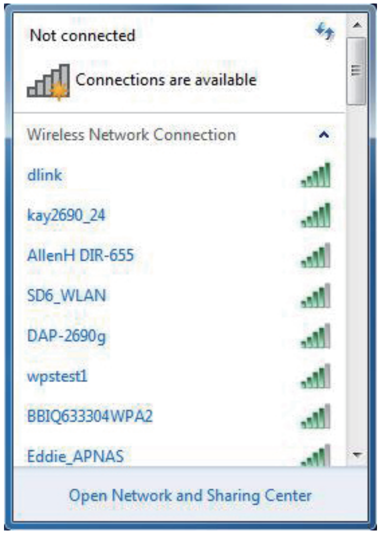
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

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



Wireless Icon

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



Not connected

Connections are available

Wireless Network Connection

dlink

kay2690_24

AllenH DIR-655

SD6_WLAN

DAP-2690g

wpstest1

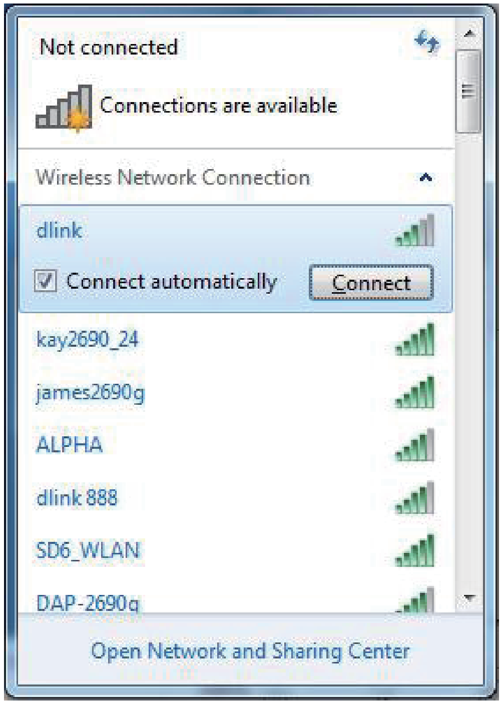
BBIQ633304WPA2

Eddie_APNAS

Open Network and Sharing Center

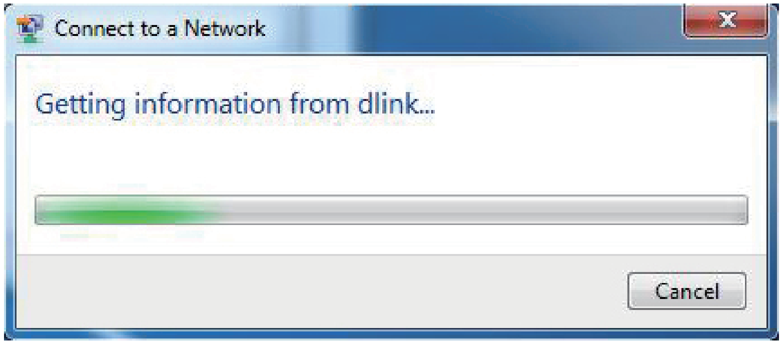
3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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

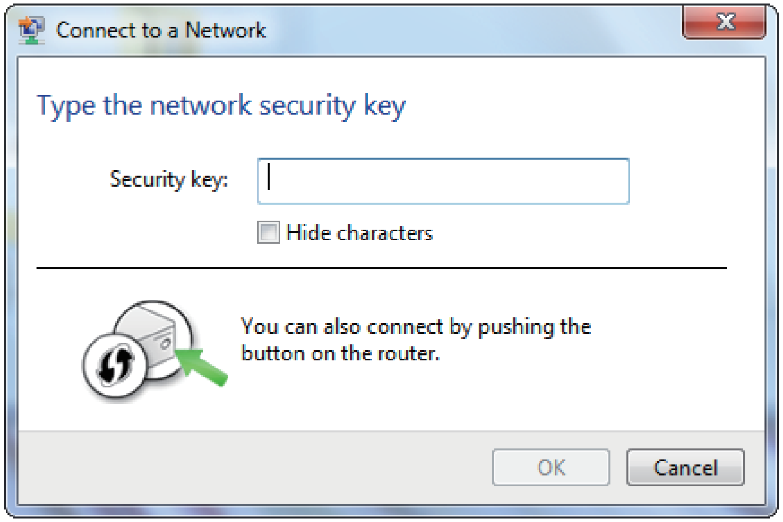

Not connected

Connections are available

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


Getting information from dlink...

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



Type the network security key

Security key:

□ Hide characters

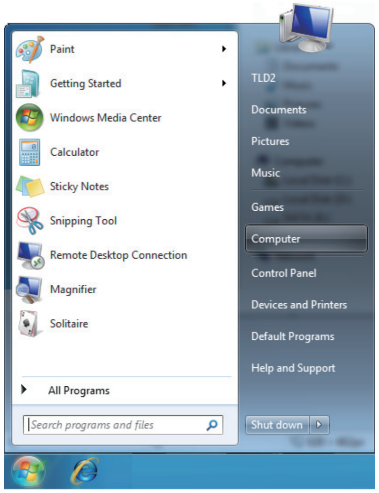
You can also connect by pushing the button on the router.

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.

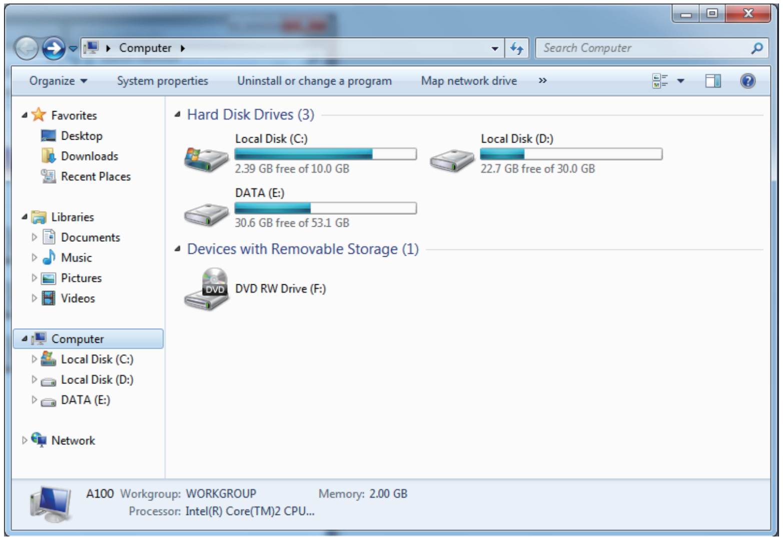
WPS

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

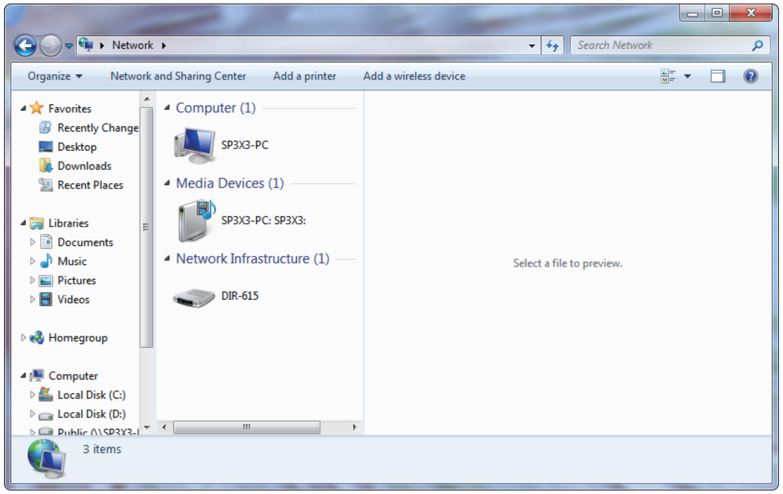
1. Click the **Start** button and select **Computer** from the Start menu.



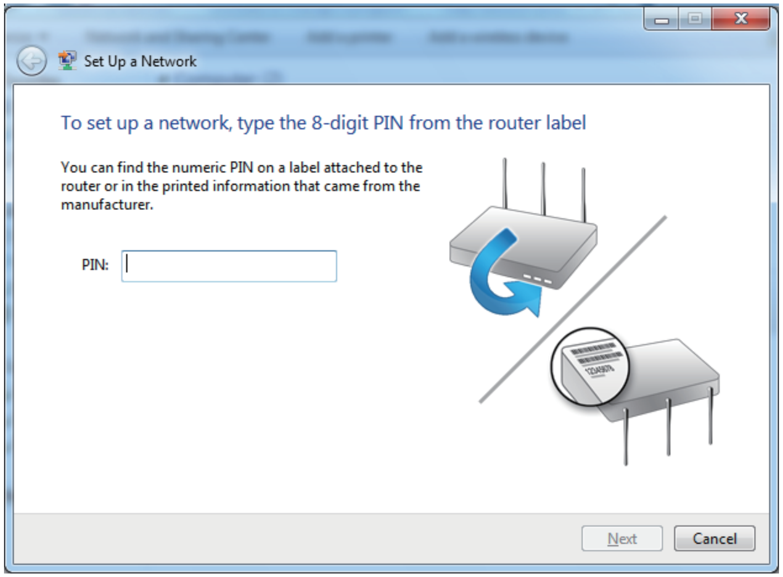
2. Click the **Network** option.



3. Double-click the DIR-815.



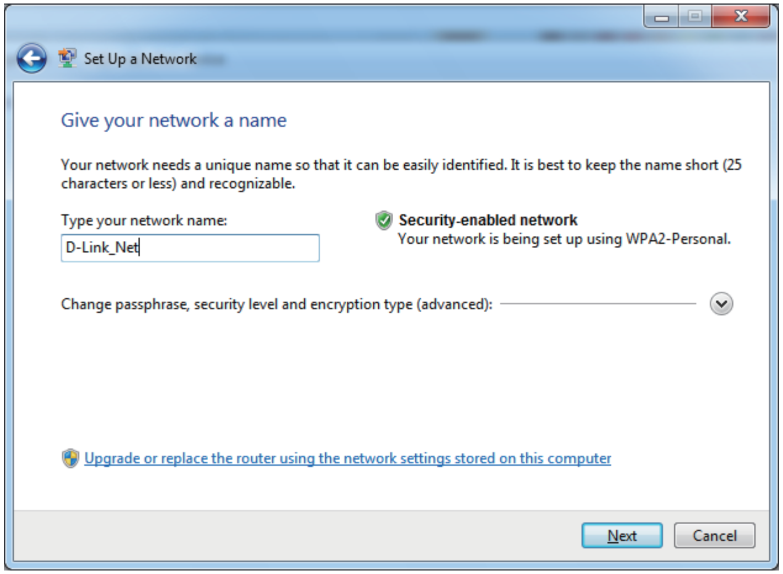
4. Input the WPS PIN number (displayed in the WPS window on the Router's LCD screen or in the **Setup** > **Wireless Setup** menu in the Router's Web UI) and click **Next**.



To set up a network, type the 8-digit PIN from the router label

You can find the numeric PIN on a label attached to the router or in the printed information that came from the manufacturer.

5. Type a name to identify the network.



Give your network a name

Your network needs a unique name so that it can be easily identified. It is best to keep the name short (25 characters or less) and recognizable.

Type your network name: D-Link_Net

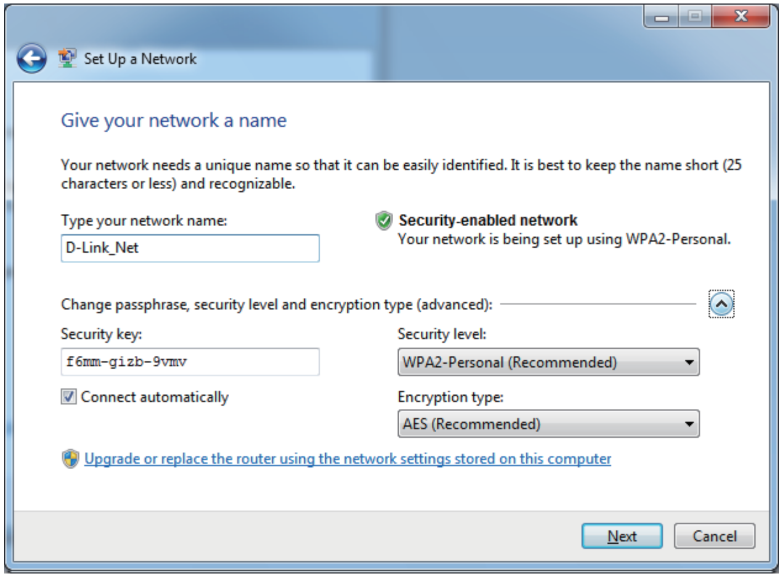
Security-enabled network
Your network is being set up using WPA2-Personal.

Change passphrase, security level and encryption type (advanced):

Upgrade or replace the router using the network settings stored on this computer
Next
Cancel

6. To configure advanced settings, click the ⌄ icon.

Click **Next** to continue.



Give your network a name

Your network needs a unique name so that it can be easily identified. It is best to keep the name short (25 characters or less) and recognizable.

Type your network name: D-Link_Net

Security-enabled network
Your network is being set up using WPA2-Personal.

Change passphrase, security level and encryption type (advanced):

Security key: f6mm-gizb-9vmv

Security level: WPA2-Personal (Recommended)

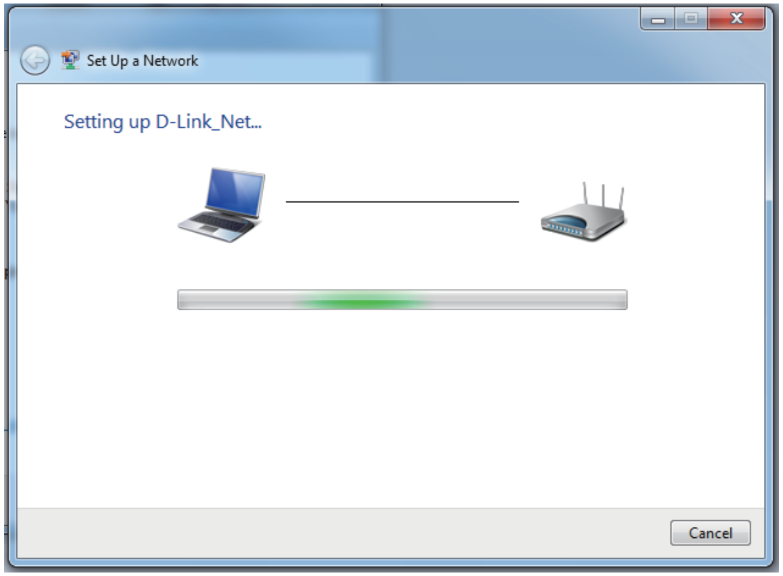
☑ Connect automatically

Encryption type: AES (Recommended)

Upgrade or replace the router using the network settings stored on this computer
Next
Cancel

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

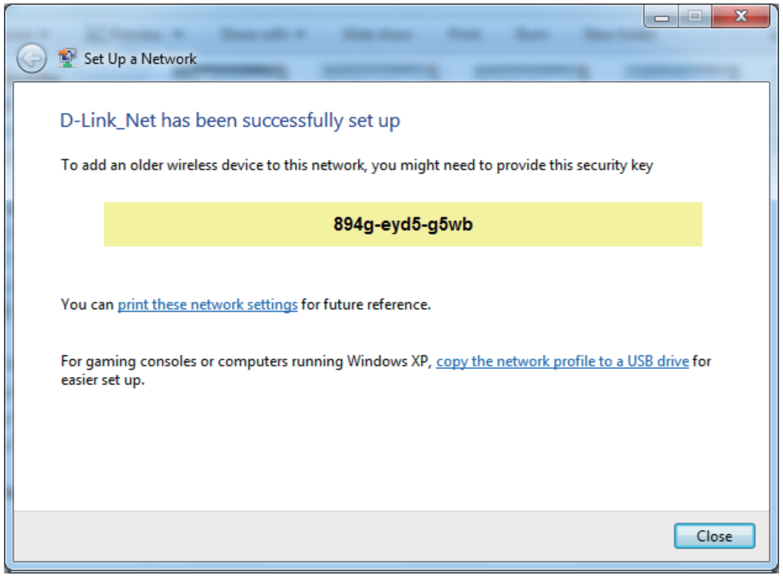
   Wait for the configuration to complete.



Setting up D-Link_Net...

8. The following window informs you that WPS on the DIR-815 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.



D-Link_Net has been successfully set up

To add an older wireless device to this network, you might need to provide this security key

894g-eyd5-g5wb

You can print these network settings for future reference.

For gaming consoles or computers running Windows XP, copy the network profile to a USB drive for easier set up.

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

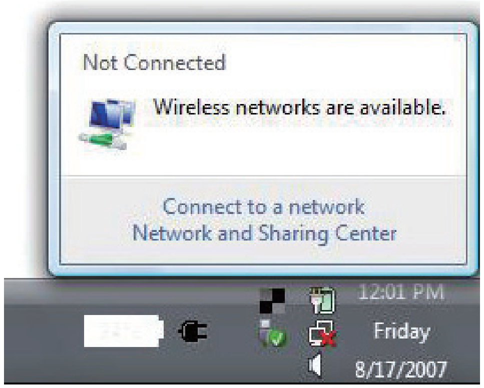
Windows Vista®

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**.

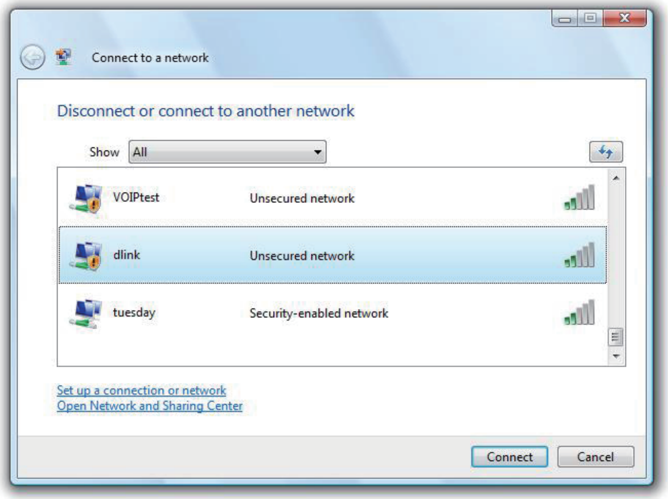


Not Connected

Wireless networks are available.

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.



Connect to a network

Disconnect or connect to another network

Show: All

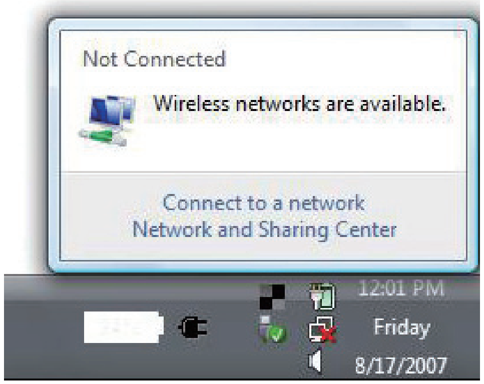
VOIPtest	Unsecured network
dlink	Unsecured network
tuesday	Security-enabled network

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

WPA/WPA2

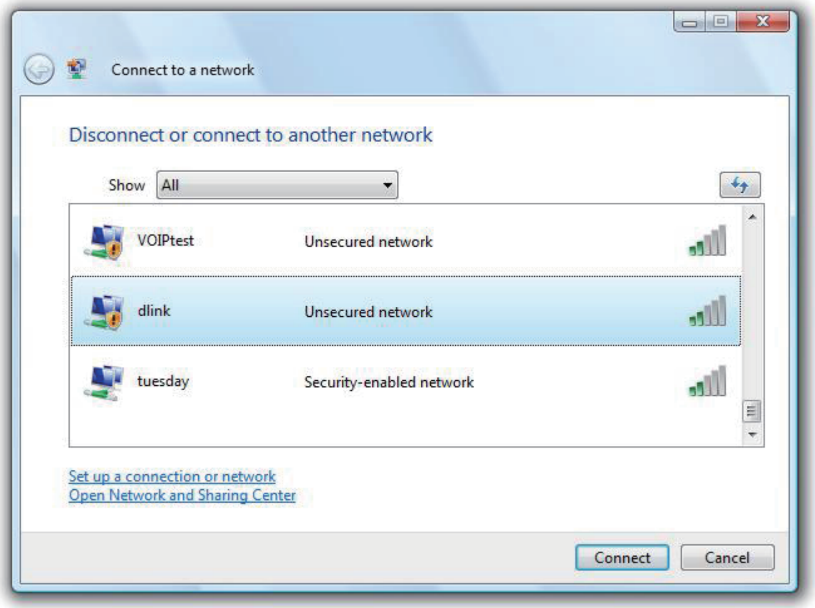
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

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**.



Wireless networks are available.

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

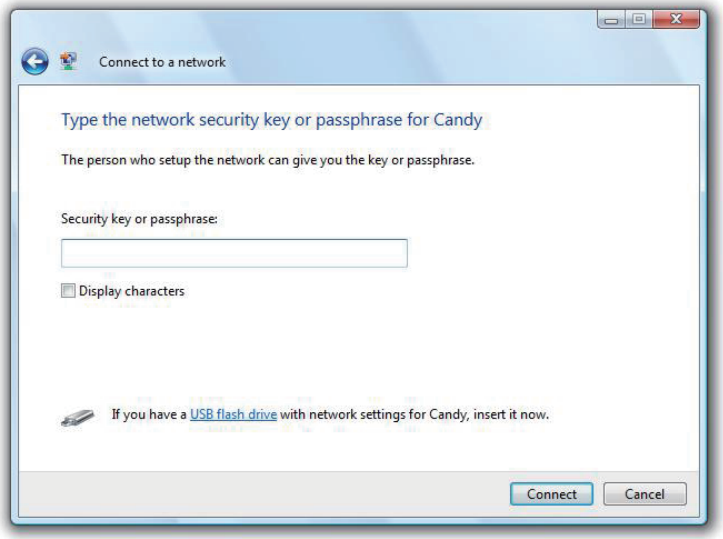

Connect to a network
Show
All
Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

Disconnect or connect to another network

VOIPtest	Unsecured network
dlink	Unsecured network
tuesday	Security-enabled network

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

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



Connect to a network

Type the network security key or passphrase for Candy

The person who setup the network can give you the key or passphrase.

Security key or passphrase:

□ Display characters

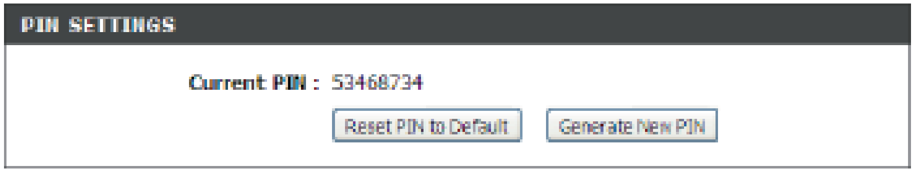
If you have a USB flash drive with network settings for Candy, insert it now.

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.



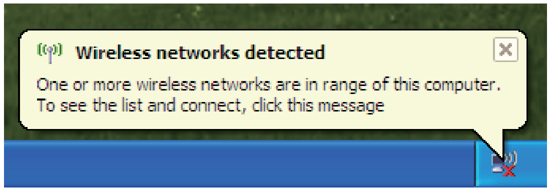
Current PIN : 53468734

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.

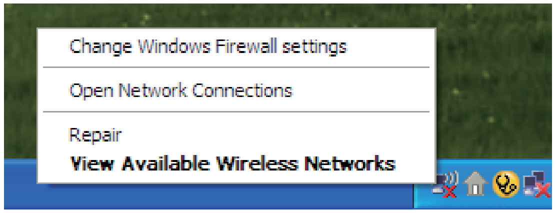


Wireless networks detected

One or more wireless networks are in range of this computer.
To see the list and connect, click this message

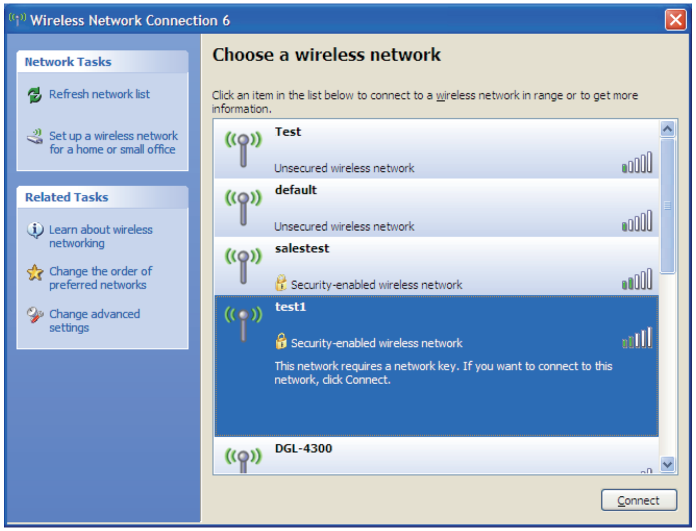
or

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


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

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

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



Wireless Network Connection 6

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

salestest
Security-enabled wireless network

test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

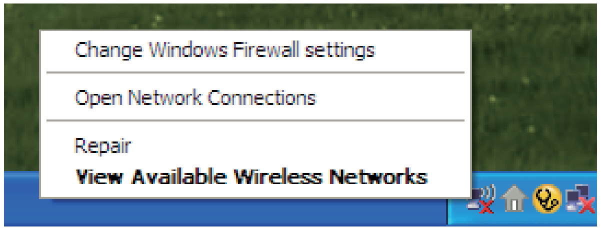
DGL-4300

Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

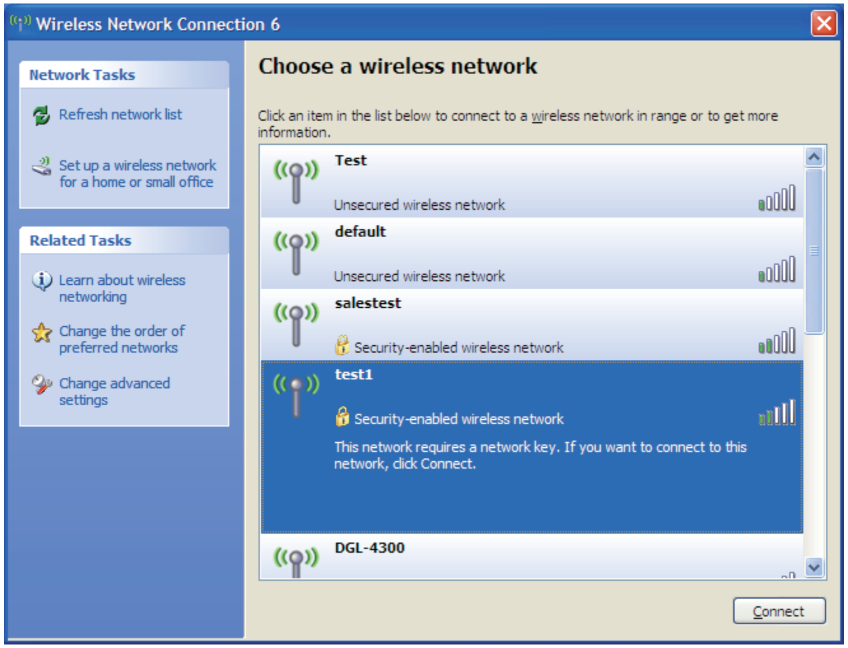
WPA/WPA2

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**.


Change Windows Firewall settings
Open Network Connections
Repair
View Available Wireless Networks

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


Wireless Network Connection 6
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

Test
Unsecured wireless network

default
Unsecured wireless network

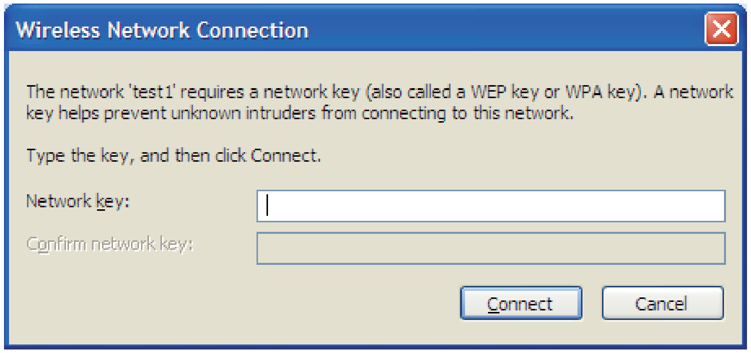
salestest
Security-enabled wireless network

test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

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

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



The network 'test1' requires a network key (also called a WEP key or WPA key). A network key helps prevent unknown intruders from connecting to this network.

Type the key, and then click Connect.

Network key:

Confirm network key:

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-815. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

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

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

  - Microsoft Internet Explorer 6 and higher
  - Mozilla Firefox 3 and higher
  - Google Chrome 8 and higher
  - Apple Safari 4 and higher

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

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

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

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

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

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

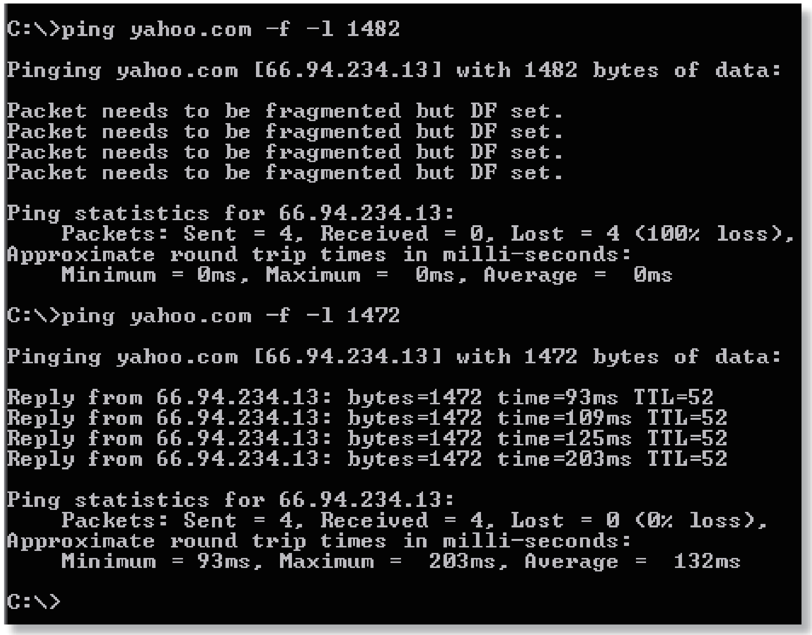
- Click on **Start** and then click **Run**.

- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, and XP 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, etc.
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-815 wireless network Cardbus adapters.

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

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

Networking Basics

Check your IP address

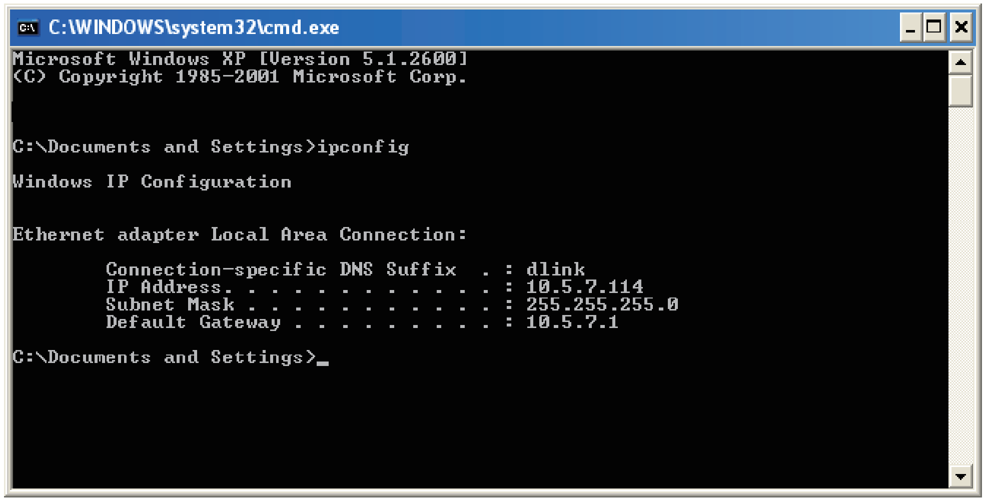
After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : dlink
        IP Address. . . . . . . . . . . . : 10.5.7.114
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.5.7.1

C:\Documents and 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** > **Change Adapter Settings.**

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

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

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

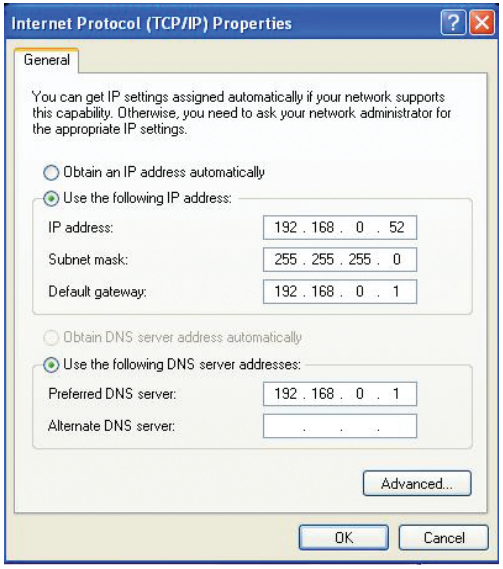
Step 2
Right-click on the **Local Area Connection** which represents your network adapter and select **Properties**.

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

Step 4
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 0 . 52
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server: . . .

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

Technical Specifications

Standards

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

Security

- WEP™
- WPA™ - Personal/Enterprise
- WPA2™ - Personal/Enterprise

Wireless Signal Rates[1]

IEEE 802.11n 2.4GHz (HT20/40):

• 144.4Mbps (300) · 130Mbps (270)
• 115.6Mbps (240) · 86.7Mbps (180)
• 72.2Mbps (150) · 65Mbps (135)
• 57.8Mbps (120) · 43.3Mbps (90)
• 28.9Mbps (60) · 21.7Mbps (45)
•14.4Mbps (30) · 7.2Mbps (15)

IEEE 802.11n 5GHz (HT20/40):

• 144.4Mbps (300) · 130Mbps (270)
• 115.6Mbps (240) · 86.7Mbps (180)
• 72.2Mbps (150) · 65Mbps (135)
• 57.8Mbps (120) · 43.3Mbps (90)
• 28.9Mbps (60) · 21.7Mbps (45)
•14.4Mbps (30) · 7.2Mbps (15)

MSC (0-15)

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

Wireless Frequency Range[2]

- 2.4GHz to 2.483GHz
- 5.15GHz to 5.25GHz[3]
- 5.725GHz to 5.825GHz[3]

Antenna Type

- Two (2) external antennas

Operating Temperature

- 32°F to 104°F (0°C to 40°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- CE
- IC
- C-Tick
- CSA International

Dimensions

- L = 6.25 inches (158.87 mm)
- W = 4.72 inches (120.04 mm)
- H = 1.27 inches (32.18 mm)

Warranty

- 1 Year

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

[2] Frequency Range varies depending on country's regulation

[3] The DIR-815 does not include 5.25-5.35GHz & 5.47-5.725GHz in some regions.

Trademarks:

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

Copyright Statement:

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

CE Mark Warning:

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

FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

FCC Caution:

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

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

ICC Notice:

Operation is subject to the following two conditions:

1) This device may not cause interference and
2) This device must accept any interference, including interference that may cause undesired operation of the device.

IMPORTANT NOTE:
IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

(i) The device for the band 5150-5250 MHz is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems;
(ii) The maximum antenna gain (2dBi) permitted (for devices in the band 5725-5825 MHz) to comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate, as stated in section A9.2(3).

In addition, users should also be cautioned to take note that high-power radars are allocated as primary users (meaning they have priority) of the bands 5250-5350 MHz and 5650-5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

(1) Ce périphérique ne doit pas causer d'interférence et.
(2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

GPL Code Statement

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

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

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

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

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

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

GNU GENERAL PUBLIC LICENSE
Version 3, 29 June 2007

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

Preamble

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

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

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

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

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

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

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

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

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

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

TERMS AND CONDITIONS

0. Definitions.

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

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

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

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

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

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

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

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

1. Source Code.

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

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

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

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

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

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

2. Basic Permissions.

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

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

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

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

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

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

4. Conveying Verbatim Copies.

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

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

5. Conveying Modified Source Versions.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Additional Terms.

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

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

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

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

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

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

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

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

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

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

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

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

8. Termination.

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

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

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

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

9. Acceptance Not Required for Having Copies.

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

10. Automatic Licensing of Downstream Recipients.

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

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

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

11. Patents.

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

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

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

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

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

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

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

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

12. No Surrender of Others' Freedom.

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

13. Use with the GNU Affero General Public License.

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

14. Revised Versions of this License.

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

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

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

15. Disclaimer of Warranty.

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

16. Limitation of Liability.

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

17. Interpretation of Sections 15 and 16.

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