D-Link®

Version 2.1 | 07/05/2011

User Manual

Wireless N 150 Home Router

DIR-601

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	October 8, 2009	• Revision A1 with firmware version 1.0
1.1	March 24, 2010	• Updated with minor changes
2.0	April 26, 2011	• Updated to hardware revision B1
2.1	July 5, 2011	• Updated firmware version 2.00

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

D-Link DIR-601 Wireless N 150 Home Router	
Power Adapter	
Ethernet Cable	
CD-ROM	

Note: Using a power supply with a different voltage rating than the one included with the DIR-601 will cause damage and void the warranty for this product.

System Requirements

Network Requirements	• An Ethernet-based Cable or DSL modem • IEEE 802.11n/g wireless clients • 10/100 Ethernet
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer® 6.0 and higher • Mozilla Firefox 3.0 and higher • Google™ Chrome 2.0 and higher • Apple Safari 3.0 and 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® XP with Service Pack 2, Vista® or Windows® 7 • An installed Ethernet adapter • CD-ROM drive

Features

- **Faster Wireless Networking** - The DIR-601 provides up to 150Mbps.* This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Compatible with 802.11g Devices** - The DIR-601 is still fully compatible with the IEEE 802.11g standard, so it can connect with existing 802.11g PCI, USB and Cardbus adapters.

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

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

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

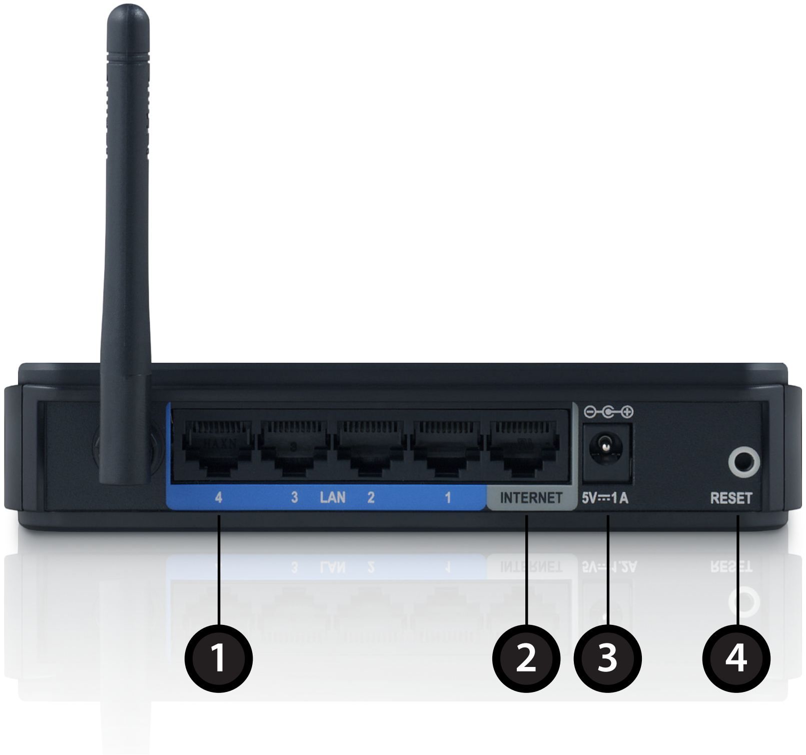
    - **Secure Multiple/Concurrent Sessions** - The DIR-601 can pass through VPN sessions. It supports multiple and concurrent IPSec and PPTP sessions, so users behind the DIR-601 can securely access corporate networks.

- **User-friendly Setup Wizard** - Through its easy-to-use Web-based user interface, you can configure your router to your specific settings within minutes.

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

Hardware Overview

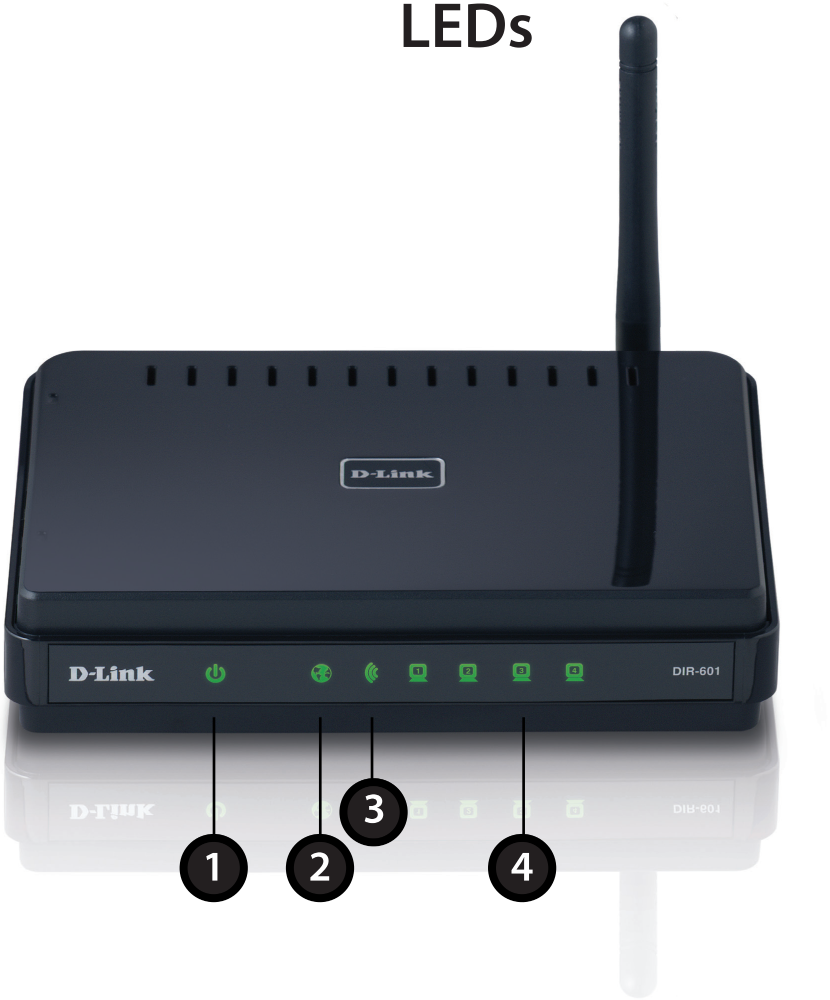
Connections



1	LAN Ports (1-4)	Connect Ethernet devices such as computers, switches, and hubs.
2	Internet Port	The auto MDI/MDIX Internet port is the connection for the Ethernet cable to the cable or DSL modem.
3	Power Receptor	The Power LED will illuminate red when the camera is receiving power.
4	Reset	Pressing the Reset button restores the router to its original factory default settings.

Hardware Overview

LEDs



1	Power LED	A solid light indicates a proper connection to the power supply.
2	Internet LED	A solid light indicates connection on the Internet port. This LED blinks during data transmission.
3	WLAN LED	A solid light indicates that the wireless segment is ready. This LED blinks during wireless data transmission.
4	Local Network LEDs	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

Installation

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

Before you Begin

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

- 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.

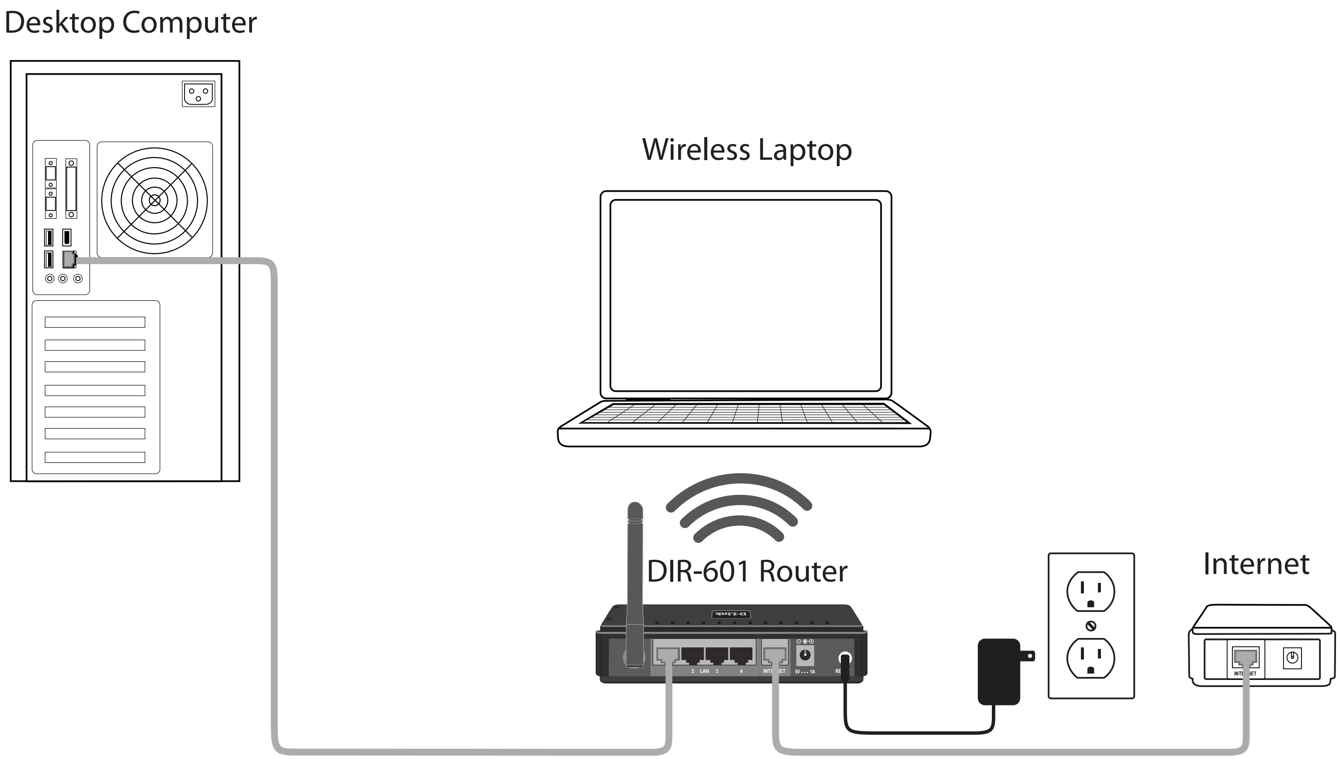
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or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

Network Diagram



Connect to Cable/DSL/Satellite Modem

If you are connecting the router to a cable/DSL/satellite modem, please follow the steps below:

1. Place the router in an open and central location. Do not plug the power adapter into the router.

2. Turn the power off on your modem. If there is no on/off switch, then unplug the modem's power adapter. Shut down your computer.

3. Unplug the Ethernet cable (that connects your computer to your modem) from your computer and place it into the Internet port on the router.

4. Plug an Ethernet cable into one of the four LAN ports on the router. Plug the other end into the Ethernet port on your computer.

5. Turn on or plug in your modem. Wait for the modem to boot (about 30 seconds).

6. Plug the power adapter to the router and connect to an outlet or power strip. Wait about 30 seconds for the router to boot.

7. Turn on your computer.

8. Verify the link lights on the router. The power light, Internet light, and the LAN light (the port that your computer is plugged into) should be lit. If not, make sure your computer, modem, and router are powered on and verify the cable connections are correct.

9. Skip to page 12 to configure your router.

Connect to Another Router

If you are connecting the D-Link router to another router to use as a wireless access point and/or switch, you will have to do the following before connecting the router 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 and 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 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 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.

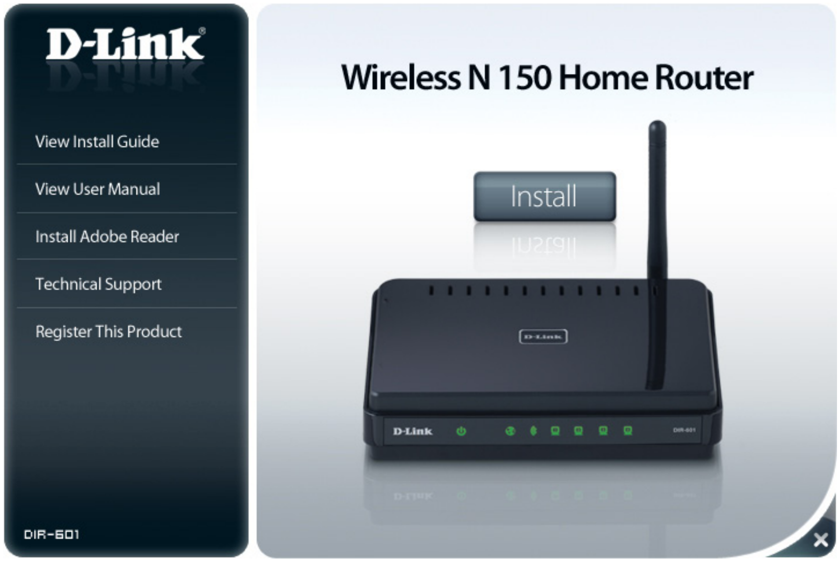
Getting Started

The DIR-601 includes a Quick Router Setup Wizard CD. Follow the simple steps below to run the Setup Wizard to guide you quickly through the installation process. You may manually configure your router without the wizard. Refer to the next page to manually setup your router.

Insert the **Quick Router Setup Wizard CD** in the CD-ROM drive. The step-by-step instructions that follow are shown in Windows® XP or Vista®. The steps and screens are similar for the other Windows® operating systems.

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

When the autorun screen appears, click **Install** and follow the on-screen instructions.



Note: *It is recommended to write down the login password on the provided CD holder.*

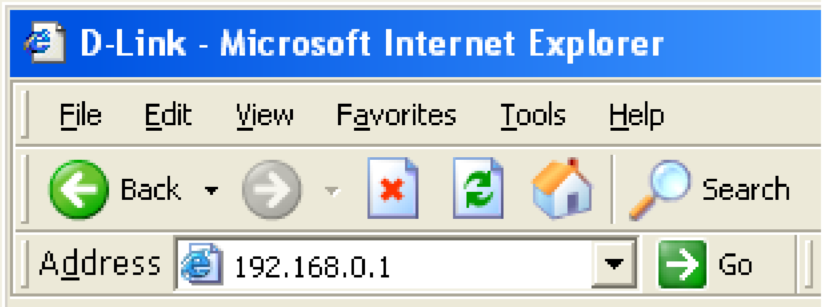
Configuration

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

***Note:** If you have successfully completed the setup on your router with the CD, the Quick Setup Wizard will not appear. Please refer to page 20.*

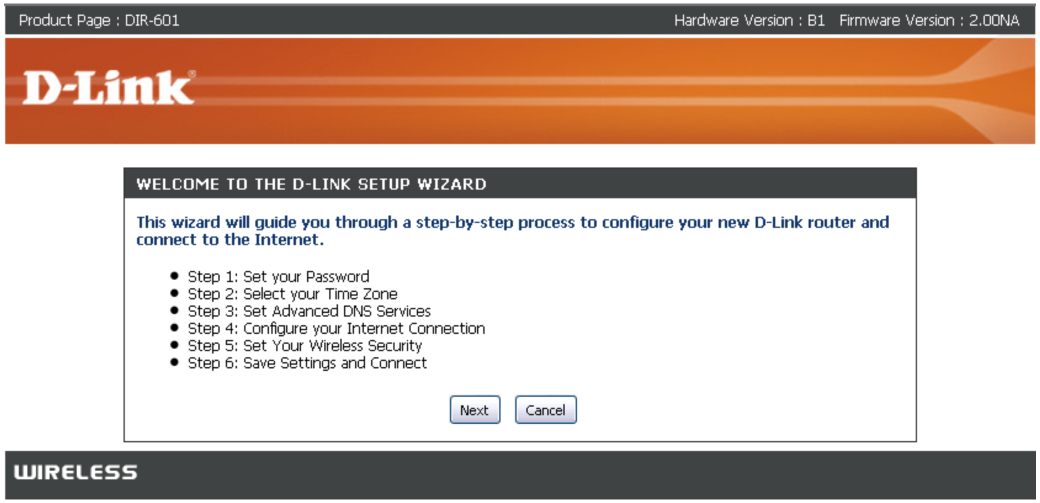
Quick Setup Wizard

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



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.

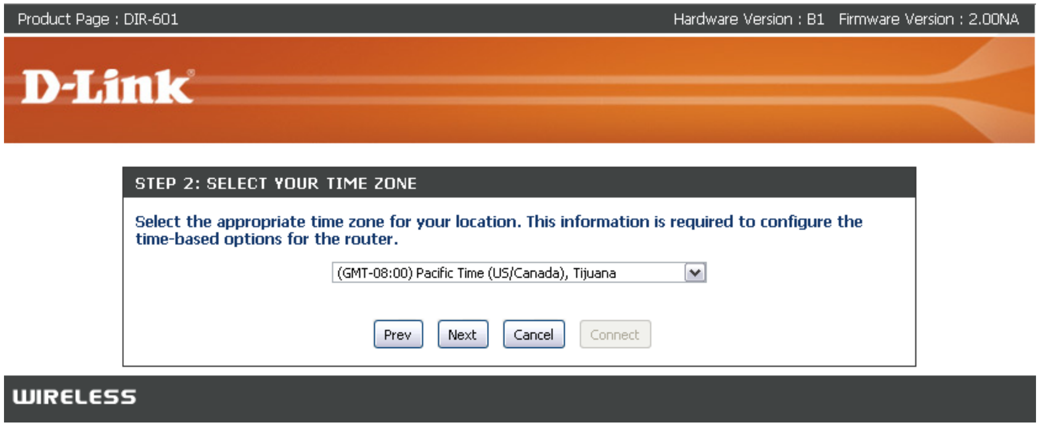


WELCOME TO THE D-LINK SETUP WIZARD

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: Set your Password
- Step 2: Select your Time Zone
- Step 3: Set Advanced DNS Services
- Step 4: Configure your Internet Connection
- Step 5: Set Your Wireless Security
- Step 6: Save Settings and Connect

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

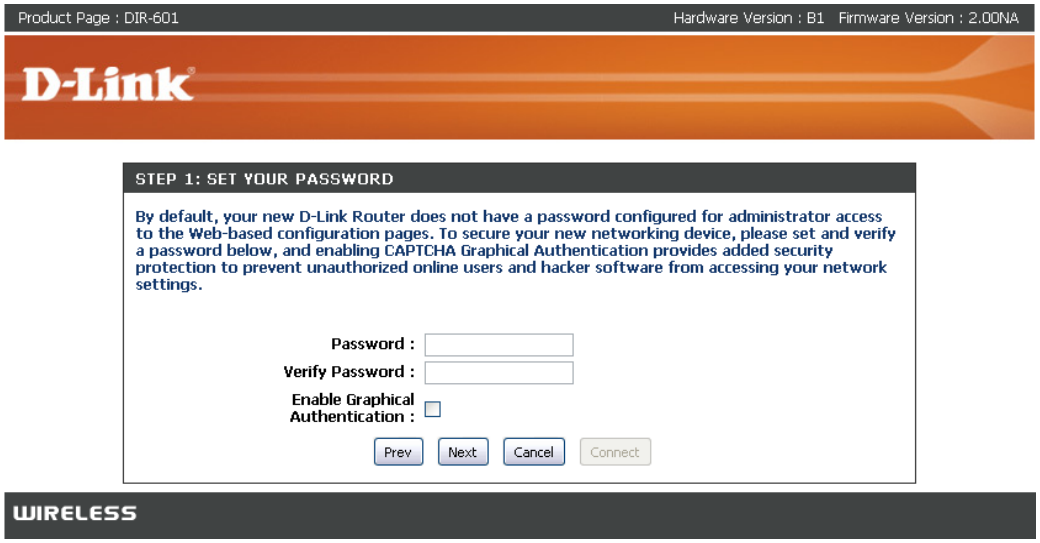


STEP 2: SELECT YOUR TIME ZONE

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

(GMT-08:00) Pacific Time (US/Canada), Tijuana

In order to secure your new networking device, please enter a password and click **Next**.



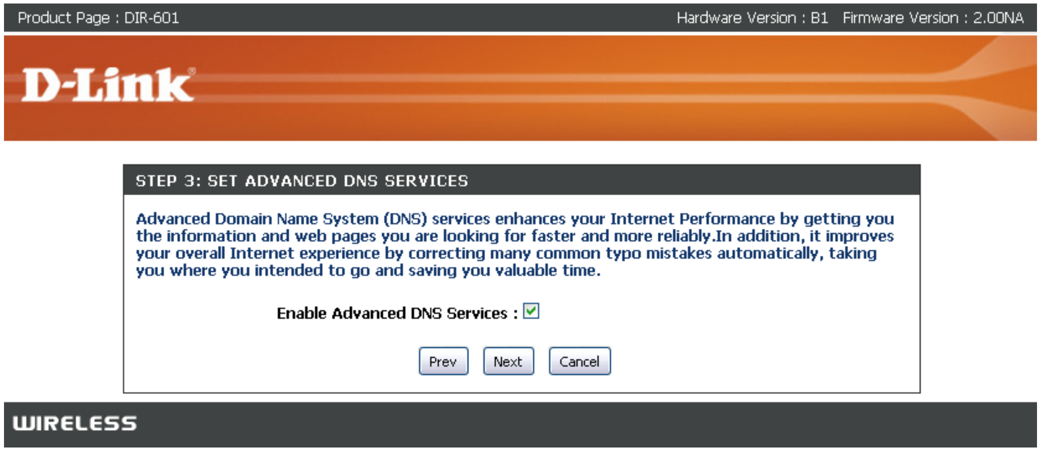
STEP 1: SET YOUR PASSWORD

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, 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 E**nable Advanced DNS Services** to allow this function to improve your overall Internet experience.

Click **Next** to continue.

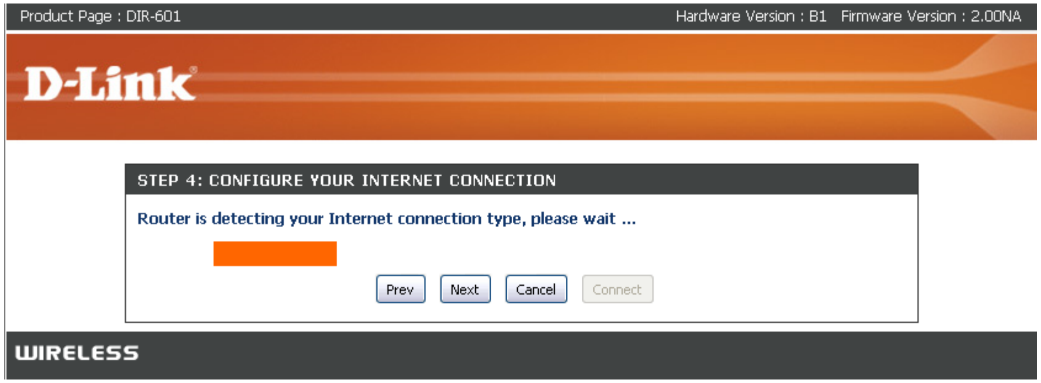


STEP 3: SET ADVANCED DNS SERVICES

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

Enable Advanced DNS Services : ☑

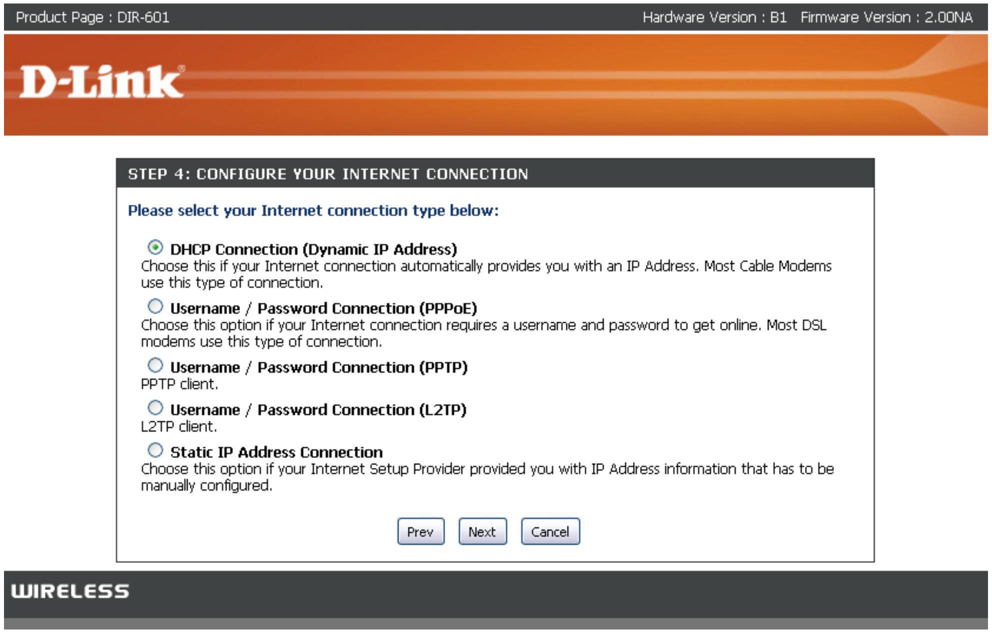
Please wait while your router detects your internet connection type.



STEP 4: CONFIGURE YOUR INTERNET CONNECTION

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

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



STEP 4: 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.

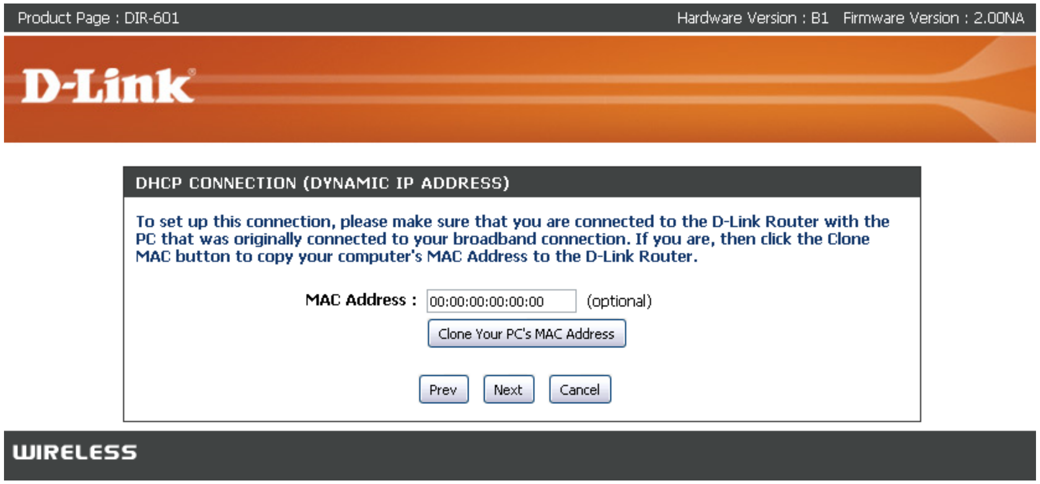
○ Username / Password Connection (PPPoE)
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

○ 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 you selected DHCP Connection, make suer that you are connected to the D-Link router with the PC that was originally connected to your broadband connection. Then, click the Clone MAC button to copy your computer's MAC address. Click **Next** to continue.


Product Page : DIR-601
Hardware Version : B1 Firmware Version : 2.00NA
D-Link
Clone Your PC's MAC Address
Prev
Next
Cancel
WIRELESS

DHCP CONNECTION (DYNAMIC IP ADDRESS)

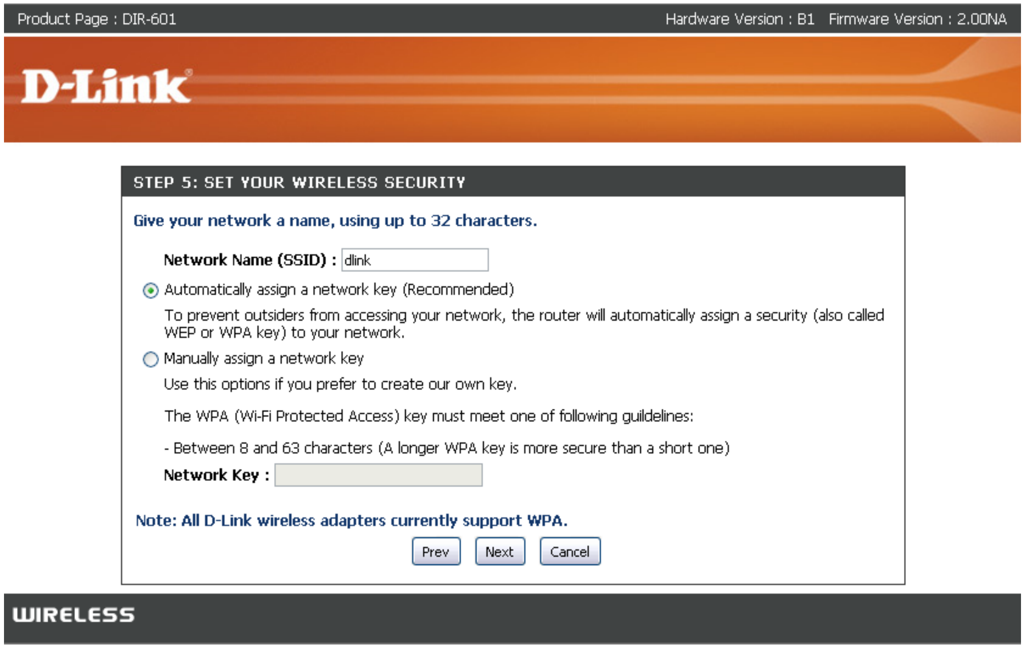
To set up this connection, please make sure that you are connected to the D-Link Router with the PC that was originally connected to your broadband connection. If you are, then click the Clone MAC button to copy your computer's MAC Address to the D-Link Router.

MAC Address : 00:00:00:00:00:00 (optional)

Please give your network a name using up to 32 characters.

It is highly recommended that you have a security key for your network. If you would like the router to automatically assign a security key, choose **Automatically assign a network key** or you may choose **Manually assign a network key and** you may enter your own Network key.

Click **Next** to continue.



STEP 5: SET YOUR WIRELESS SECURITY

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

Network Name (SSID) : dlink

● 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.

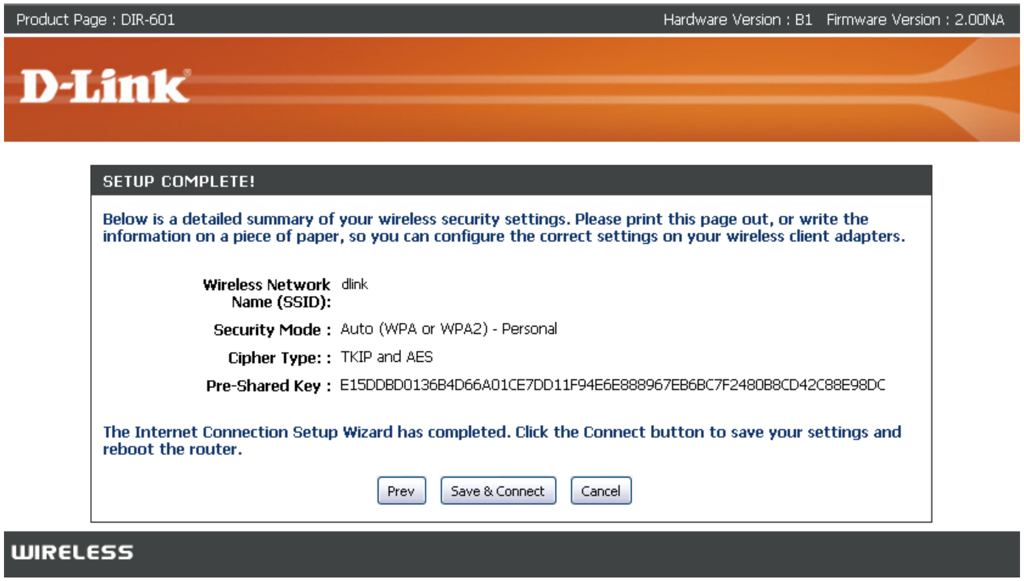
The WPA (Wi-Fi Protected Access) key must meet one of following guildelines:

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

Network Key :

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

Once this screen appears, your setup is complete. Click **Save & Connect** to reboot the router.



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 Network Name (SSID): dlink

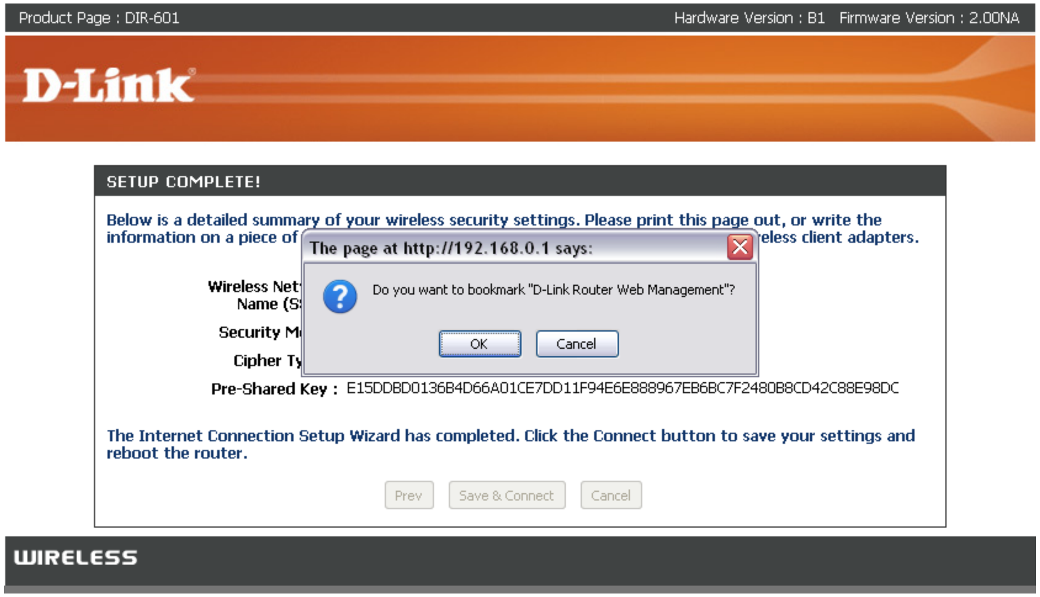
Security Mode : Auto (WPA or WPA2) - Personal

Cipher Type: : TKIP and AES

Pre-Shared Key : E15DDBD0136B4D66A01CE7DD11F94E6E888967EB6BC7F2480B8CD42C88E98DC

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

Before your router reboots, you will be asked if you want to bookmark '**D-Link Router Web Management**,' click **Ok** to finish.



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 eless client adapters.

The page at http://192.168.0.1 says:

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

Wireless Net Name (S

Security M

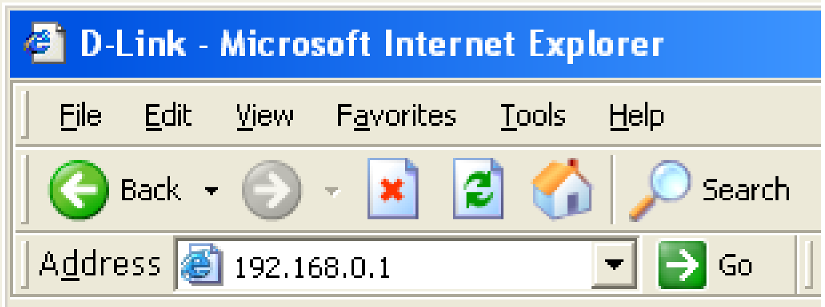
Cipher Ty

Pre-Shared Key : E15DDBD0136B4D66A01CE7DD11F94E6E888967EB6BC7F2480B8CD42C88E98DC

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

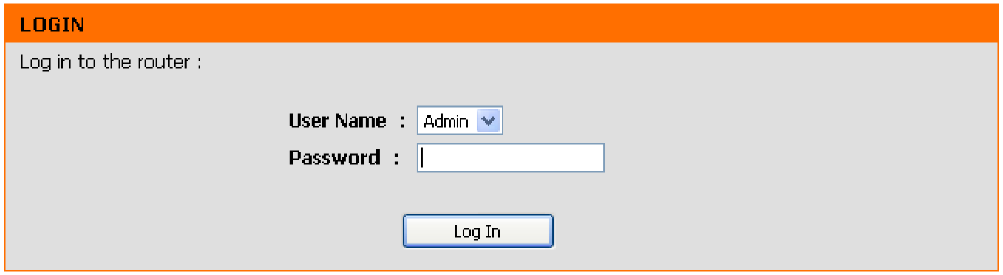
Web-based Configuration Utility

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



Address 192.168.0.1

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



LOGIN

Log in to the router :

User Name : Admin

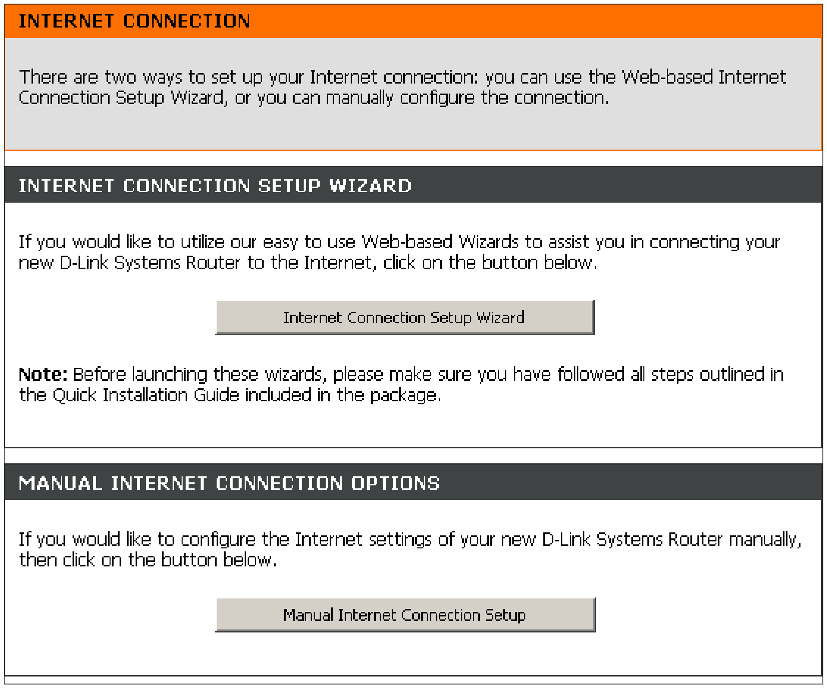
Password :

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

Internet Connection Setup Wizard

Once logged into the web interface of the router, the **Setup > Internet** page will appear. Click the **Internet Connection Setup Wizard** button to quickly configure your router using the setup wizard.

If you want to enter your settings without running the wizard, click **Manual Internet Configuration Wizard**.



INTERNET CONNECTION

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

INTERNET CONNECTION SETUP WIZARD

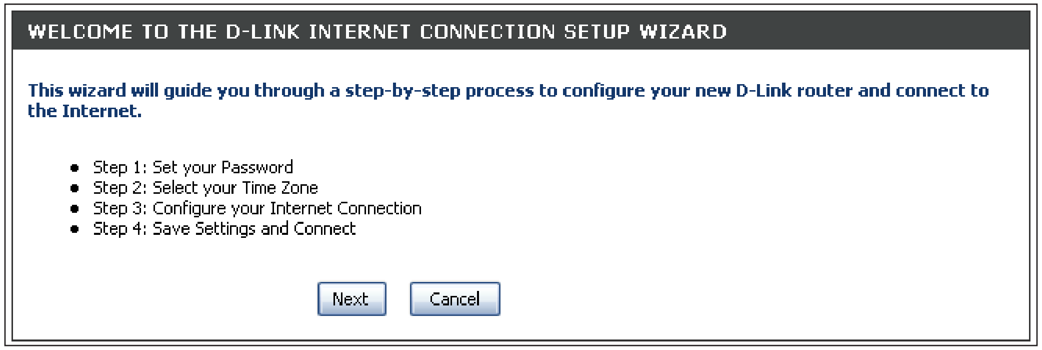
If you would like to utilize our easy to use Web-based Wizards to assist you in connecting your new D-Link Systems Router to the Internet, click on the button below.

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

MANUAL INTERNET CONNECTION OPTIONS

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

Click **Next** to continue.

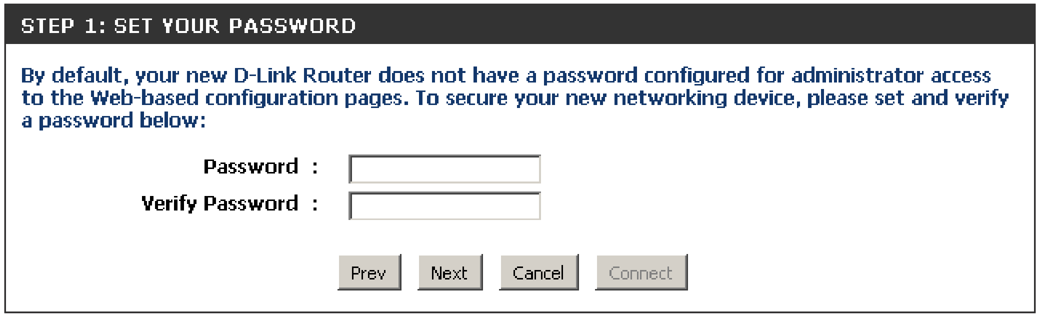


WELCOME TO THE D-LINK INTERNET CONNECTION SETUP WIZARD

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.



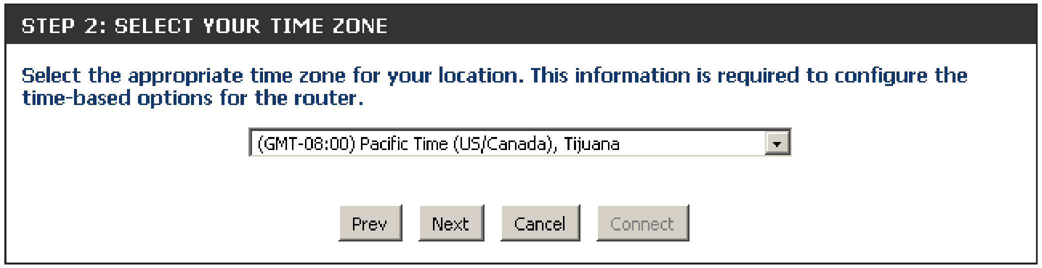
STEP 1: SET YOUR PASSWORD

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.

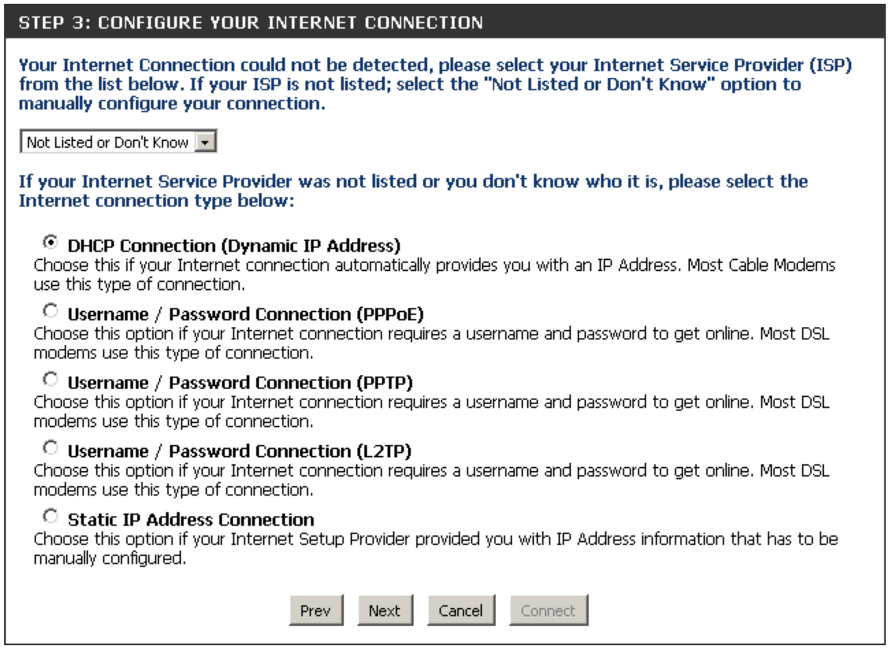


STEP 2: SELECT YOUR TIME ZONE

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

(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.

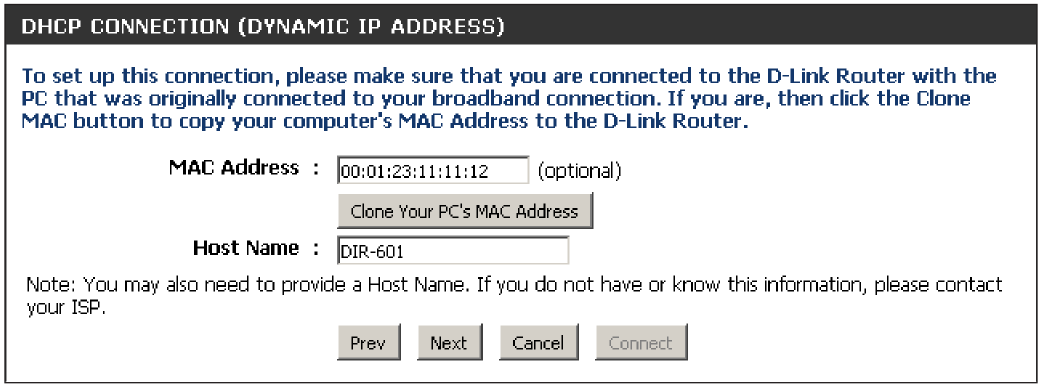
○ **Username / Password Connection (PPTP)**
Choose this option if your Internet connection requires a username and password to get online. Most DSL modems use this type of connection.

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

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



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 : 00:01:23:11:11:12 (optional)

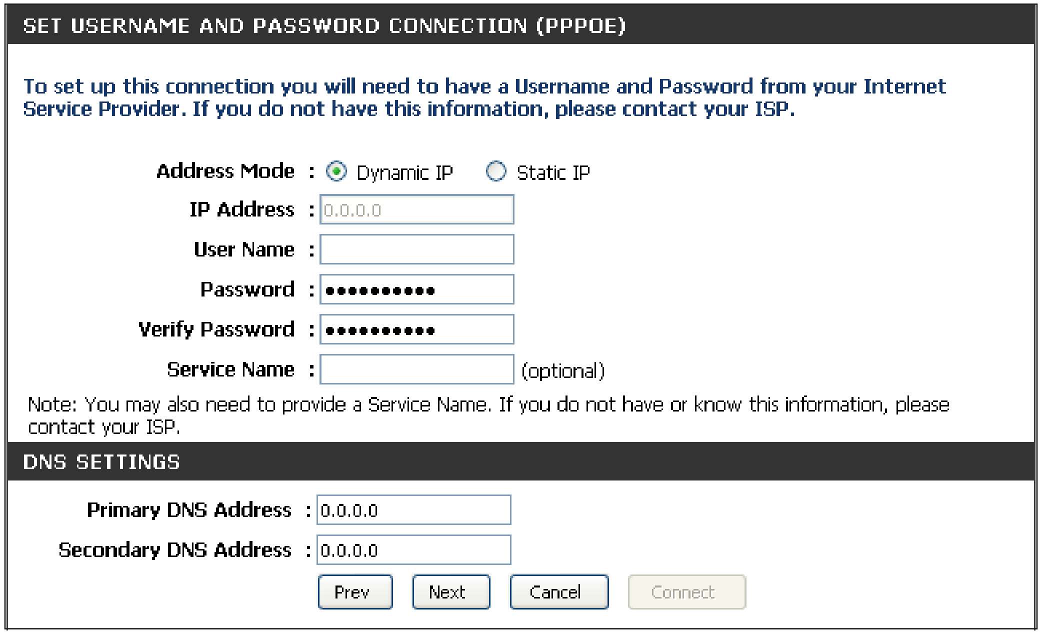
Host Name : DIR-601

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

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

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

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


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.

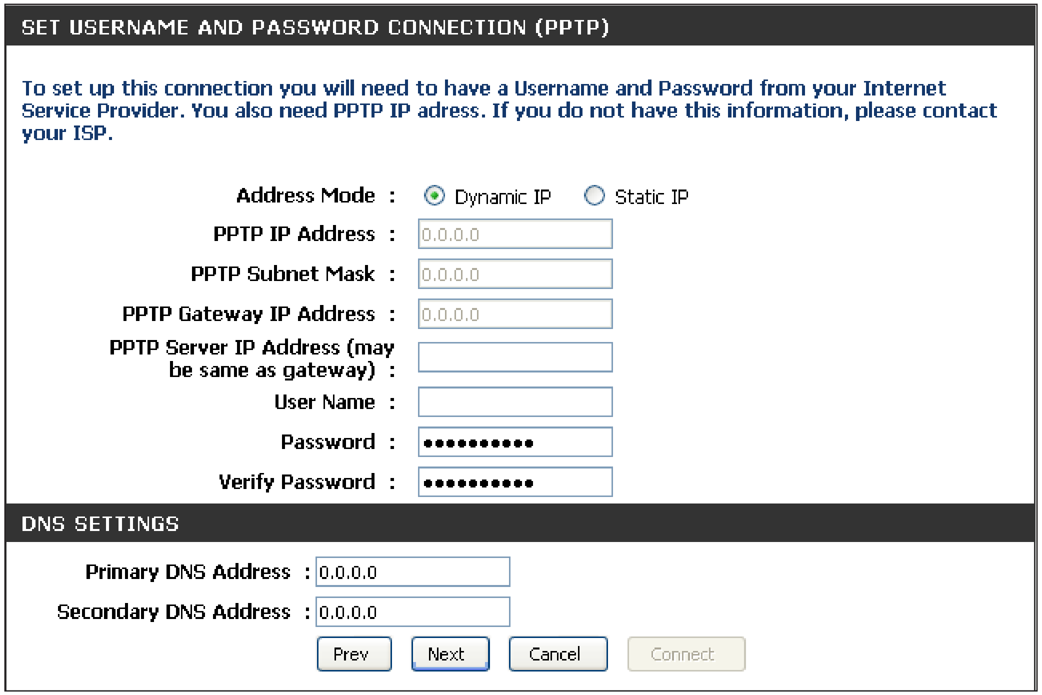
Address Mode : ● Dynamic IP ○ Static IP
IP Address : 0.0.0.0
User Name :
Password : ●●●●●●●●●●
Verify Password : ●●●●●●●●●●
Service Name : (optional)

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

DNS SETTINGS

Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0

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


SET USERNAME AND PASSWORD CONNECTION (PPTP)

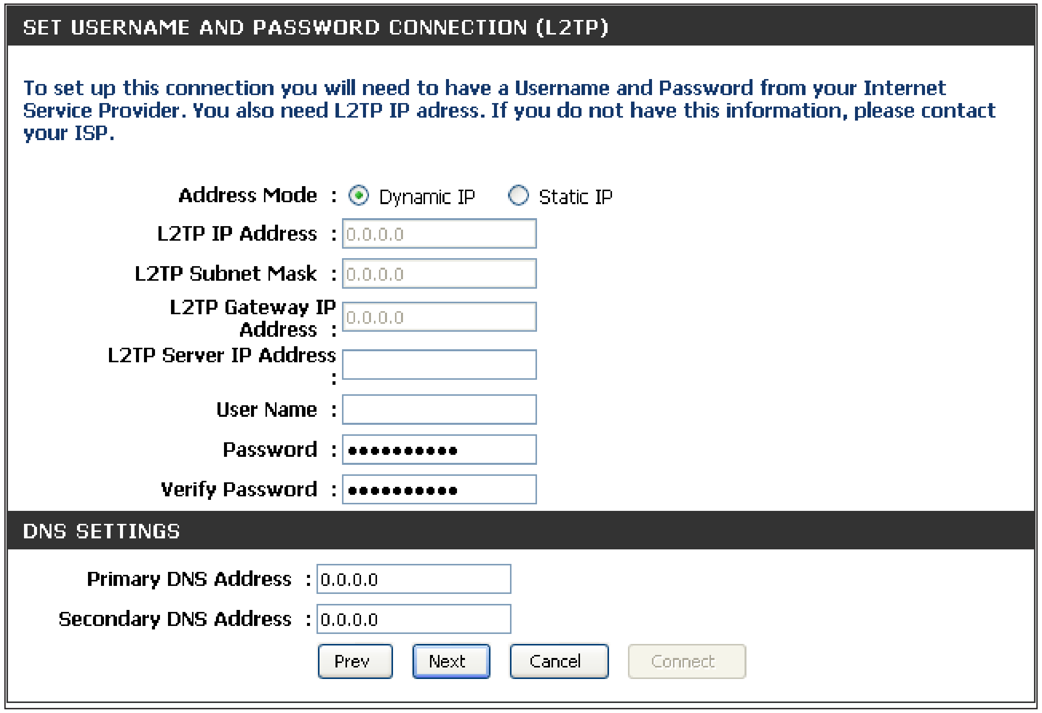
To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need PPTP IP adress. If you do not have this information, please contact your ISP.

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 : 0.0.0.0
Secondary DNS Address : 0.0.0.0

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



SET USERNAME AND PASSWORD CONNECTION (L2TP)

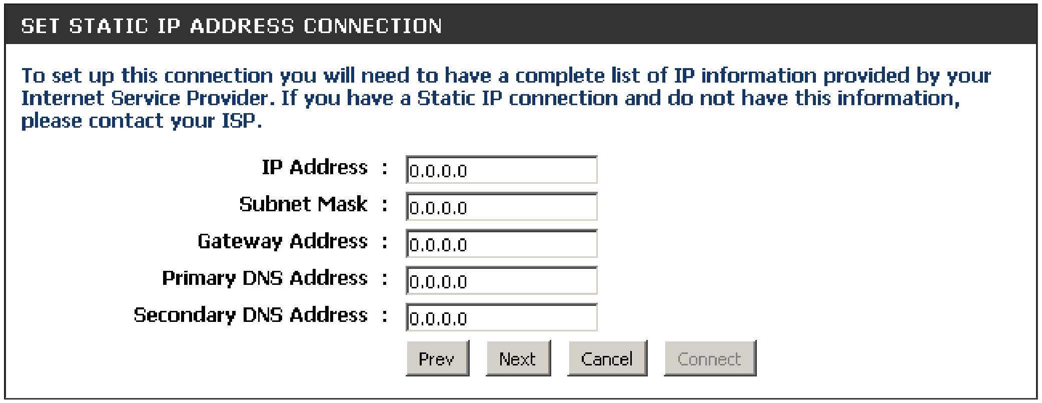
To set up this connection you will need to have a Username and Password from your Internet Service Provider. You also need L2TP IP adress. If you do not have this information, please contact your ISP.

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 :
User Name :
Password : ●●●●●●●●●●
Verify Password : ●●●●●●●●●●

DNS SETTINGS

Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0

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

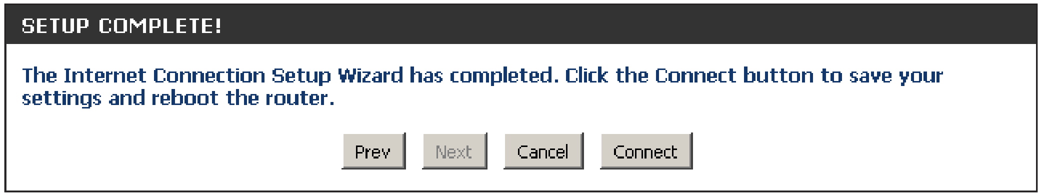


SET STATIC IP ADDRESS CONNECTION

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
Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0

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



SETUP COMPLETE!

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

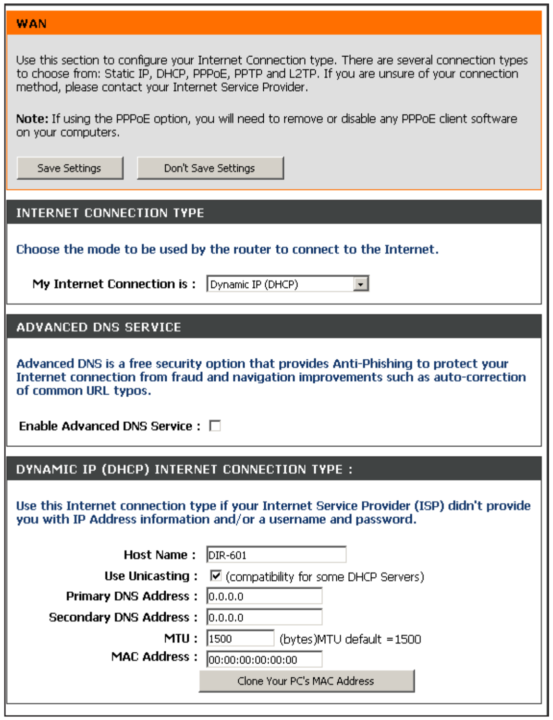
Manual Configuration

Dynamic (Cable)

If you opt to set up your Internet connection manually, you will be redirected to a WAN page that allows you to select your Internet type and enter the correct configuration parameters.

Select your Internet connection type using the “**My Internet Connection is”** drop-down menu.

Click the **Save Settings** button when you have configured the connection.



Use this section to configure your Internet Connection type. There are several connection types to choose from: Static IP, DHCP, PPPoE, PPTP and L2TP. If you are unsure of your connection method, please contact your Internet Service Provider.

Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.

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

My Internet Connection is : Dynamic IP (DHCP)

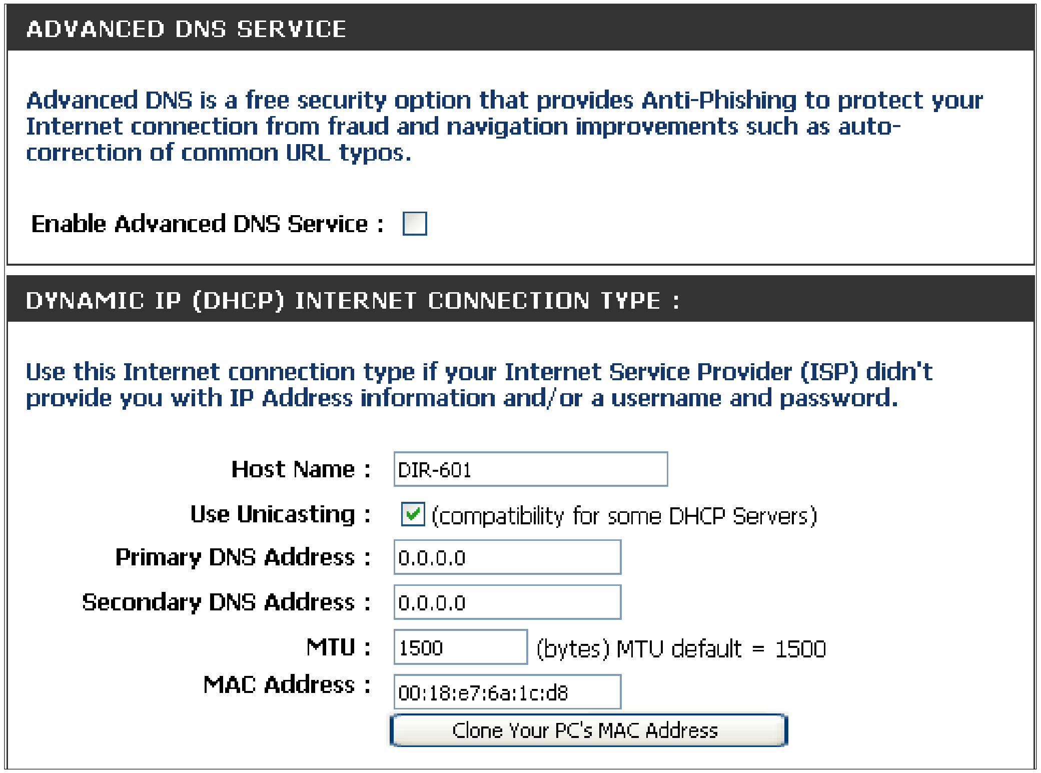
Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service : □

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-601
Use Unicasting : ☑ (compatibility for some DHCP Servers)
Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0
MTU : 1500 (bytes)MTU default =1500
MAC Address : 00:00:00:00:00:00

Dynamic IP Address (DHCP)



ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service : □

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-601

Use Unicasting : ☑ (compatibility for some DHCP Servers)

Primary DNS Address : 0.0.0.0

Secondary DNS Address : 0.0.0.0

MTU : 1500 (bytes) MTU default = 1500

MAC Address : 00:18:e7:6a:1c:d8

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

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

Host Name: The Host Name is optional but may be required by some ISPs.

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

DNS Addresses: Enter the Primary DNS server IP address assigned by your ISP.

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

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

PPPoE (DSL)

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

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

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

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

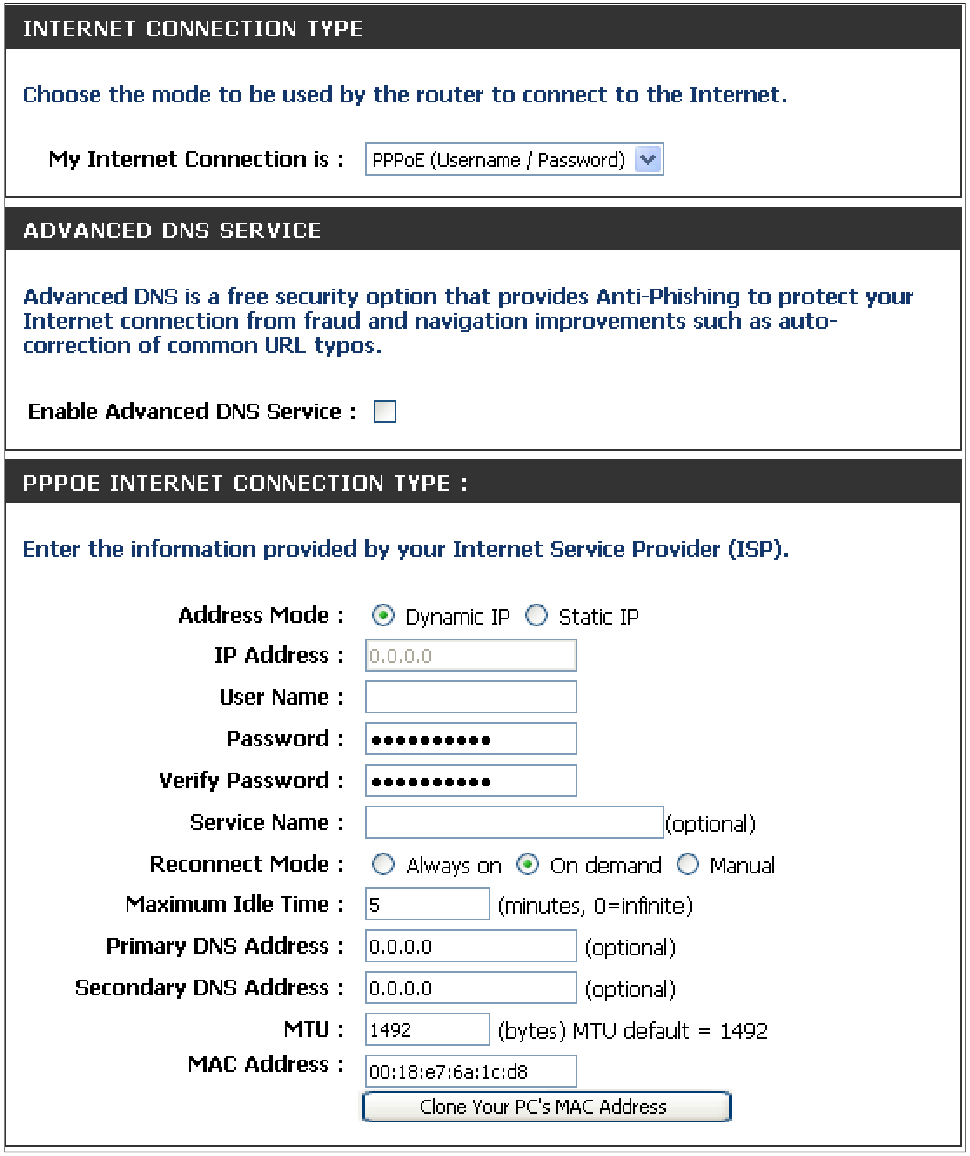
Address Mode: Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

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).



INTERNET CONNECTION TYPE

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

My Internet Connection is : PPPoE (Username / Password)

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service : □

PPPOE INTERNET CONNECTION TYPE :

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

Address Mode :	● Dynamic IP ○ Static IP
IP Address :	0.0.0.0
User Name :	
Password :	••••••••••
Verify Password :	••••••••••
Service Name :	(optional)
Reconnect Mode :	○ Always on ● On demand ○ Manual
Maximum Idle Time :	5 (minutes, 0=infinite)
Primary DNS Address :	0.0.0.0 (optional)
Secondary DNS Address :	0.0.0.0 (optional)
MTU :	1492 (bytes) MTU default = 1492
MAC Address :	00:18:e7:6a:1c:d8

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

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

DNS Addresses: Enter the Primary and Secondary DNS Server Addresses (Static PPPoE only).

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

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

PPTP

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

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

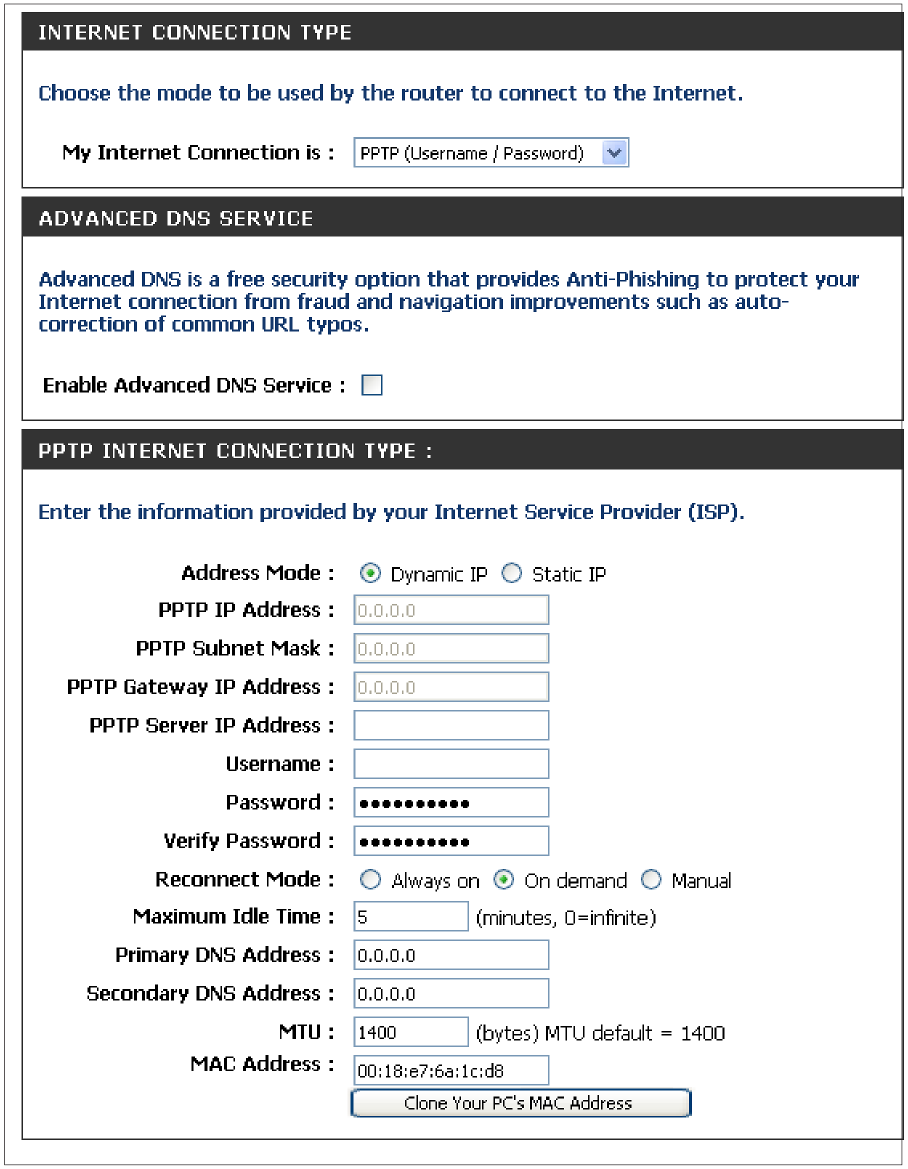
Enabled Advanced DNS Service: Advanced Domain Name System (DNS) services enhances your Internet performance by getting you the information and web pages you are looking for faster and more reliably. In addition, it improves your overall Internet experience by correcting many common typo mistakes automatically,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

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

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

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

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



INTERNET CONNECTION TYPE

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

My Internet Connection is : PPTP (Username / Password)

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service : □

PPTP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (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 :
Username :
Password : ••••••••••
Verify Password : ••••••••••
Reconnect Mode : ○ Always on ● On demand ○ Manual
Maximum Idle Time : 5 (minutes, 0=infinite)
Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0
MTU : 1400 (bytes) MTU default = 1400
MAC Address : 00:18:e7:6a:1c:d8

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

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

Username: Enter your PPTP username.

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

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

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

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

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

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

L2TP

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

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

Enabled Advanced DNS Service: Advanced Domain Name System (DNS) services enhances your Internet performance by getting you the information and web pages you are looking for faster and more reliably. In addition, it improves your overall Internet experience by correcting many common typo mistakes automatically, taking you where you intended to go and saving you valuable time.
Disclaimer: *D-Link makes no warranty as to the availability, reliability, functionality and operation of the Advanced DNS service or its features.*

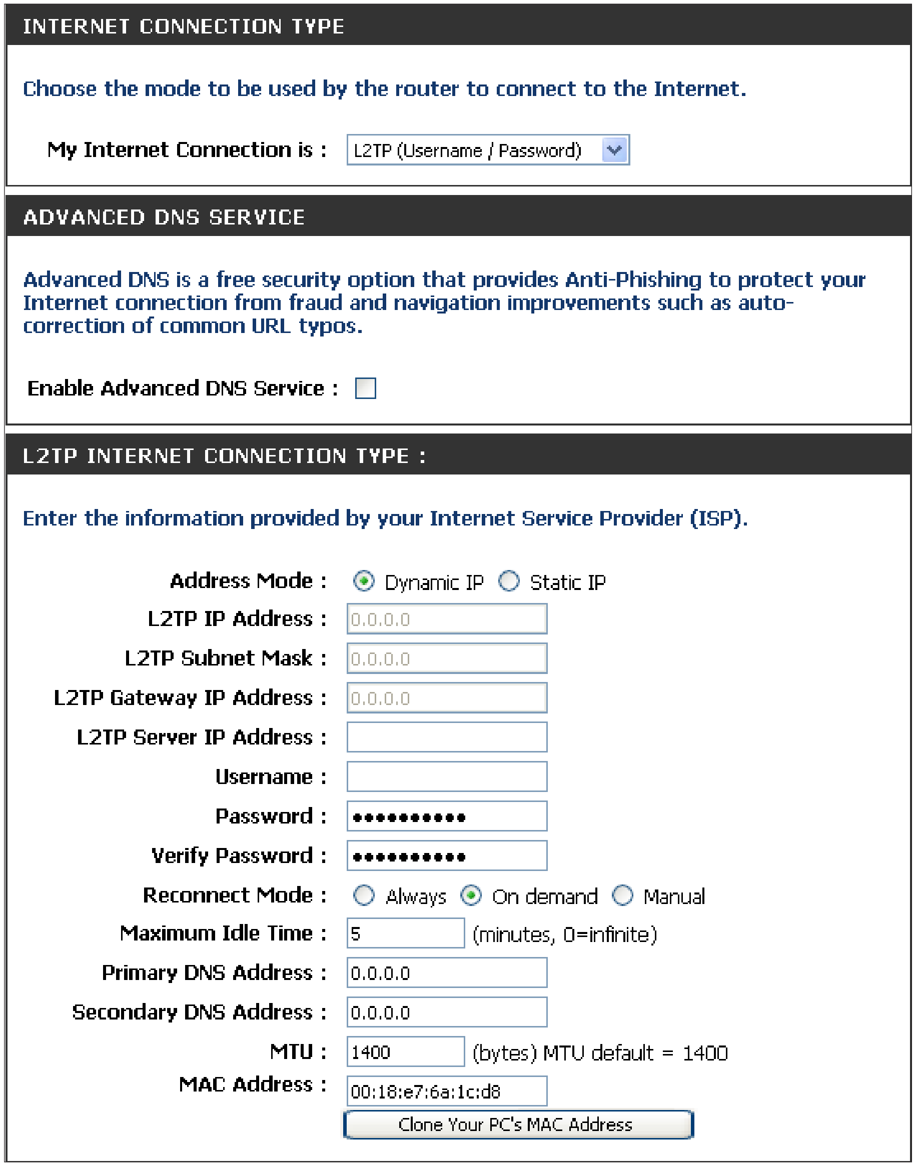
Address Mode: Select **Static** if your ISP assigned you the IP address, subnet mask, gateway, and DNS server addresses. In most cases, select **Dynamic**.

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

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

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

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



INTERNET CONNECTION TYPE

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

My Internet Connection is : L2TP (Username / Password)

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service : □

L2TP INTERNET CONNECTION TYPE :

Enter the information provided by your Internet Service Provider (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 :
Username :
Password : ••••••••••
Verify Password : ••••••••••
Reconnect Mode : ○ Always ● On demand ○ Manual
Maximum Idle Time : 5 (minutes, 0=infinite)
Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0
MTU : 1400 (bytes) MTU default = 1400
MAC Address : 00:18:e7:6a:1c:d8

Username: Enter your L2TP username.

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

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

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

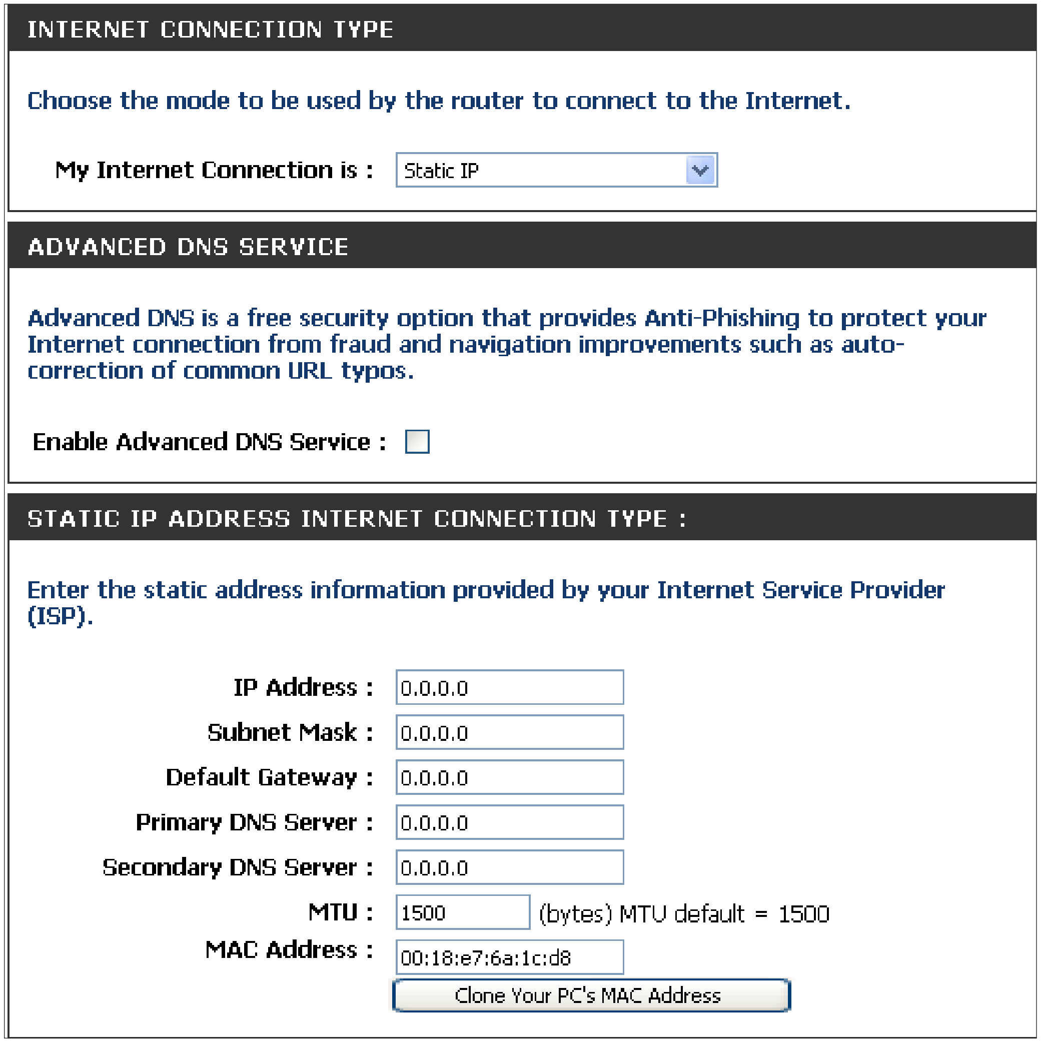
DNS Servers: Enter the Primary and Secondary DNS Server Addresses (Static L2TP only).

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

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

Static IP Address

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



INTERNET CONNECTION TYPE

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

My Internet Connection is : Static IP

ADVANCED DNS SERVICE

Advanced DNS is a free security option that provides Anti-Phishing to protect your Internet connection from fraud and navigation improvements such as auto-correction of common URL typos.

Enable Advanced DNS Service : □

STATIC IP ADDRESS INTERNET CONNECTION TYPE :

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

IP Address : 0.0.0.0

Subnet Mask : 0.0.0.0

Default Gateway : 0.0.0.0

Primary DNS Server : 0.0.0.0

Secondary DNS Server : 0.0.0.0

MTU : 1500 (bytes) MTU default = 1500

MAC Address : 00:18:e7:6a:1c:d8

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

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

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

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

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

Default Gateway: Enter the Gateway assigned by your ISP.

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

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

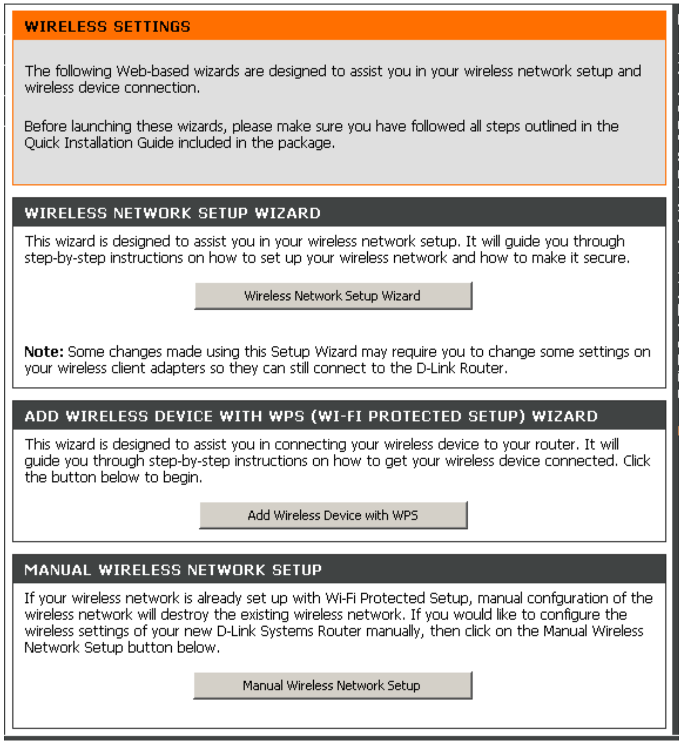
MAC Address: The default MAC Address is set to the Internet port's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP. You can use the **Clone Your PC's MAC Address** button to replace the Internet port's MAC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

Wireless Settings

If you want to configure the wireless settings on your router using the wizard, click **Wireless Connection Setup Wizard** and refer to page 76.

Click **Add Wireless Device with WPS** if you want to add a wireless device using Wi-Fi Protected Setup (WPS) and refer to page 78.

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.

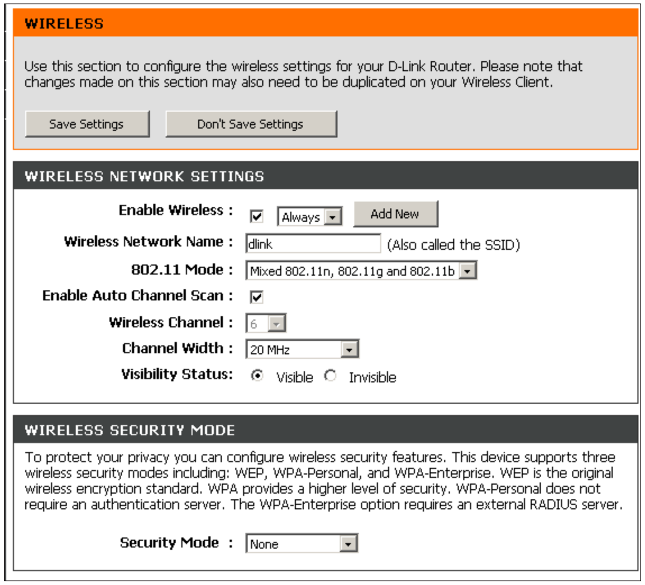
ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

This wizard is designed to assist you in connecting your wireless device to your 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 confguration 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.

Manual Wireless Network Setup



WIRELESS

Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

WIRELESS NETWORK SETTINGS

Enable Wireless : ☑ Always

Wireless Network Name : dlink (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan : ☑

Wireless Channel : 6

Channel Width : 20 MHz

Visibility Status: ● Visible ○ Invisible

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 : 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. Click **Add New** to create your own time schedule to enable the wireless function.

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

802.11 Mode: Select one of the following:

802.11g Only - Select if all of your wireless clients are 802.11g.

802.11n Only - Select only if all of your wireless clients are 802.11n.

Mixed 802.11n and 802.11g - Select if you are using a mix of 802.11n and 802.11g wireless clients.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DIR-601 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DIR-601. By default the channel is set to 6. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you enable **Auto Channel Scan**, this option will be greyed out.

Channel Width: Select the Channel Width:
Auto 20/40 - 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. This is the default setting.
40MHz - Select if you are using only 802.11n wireless clients.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DIR-601. If Invisible is selected, the SSID of the DIR-601 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DIR-601 in order to connect to it.

Wireless Security: Refer to page 75 for more information regarding wireless security.

Network Settings

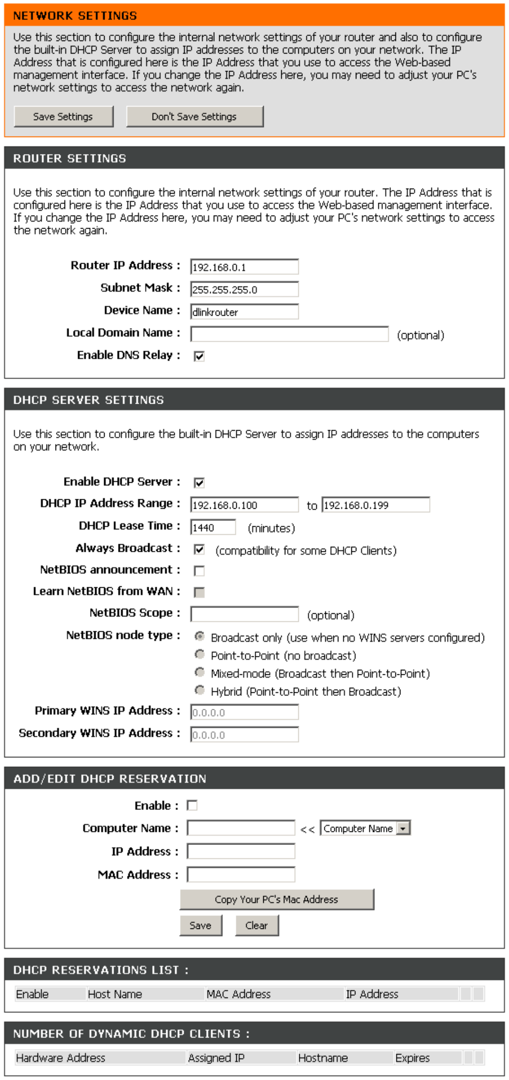
This section will allow you to change the local network settings of the router and to configure the DHCP settings.

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

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

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

Enable DNS Relay: Enter the Domain name (Optional).
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.



NETWORK SETTINGS

Use this section to configure the internal network settings of your router and also to configure the built-in DHCP Server to assign IP addresses to the computers on your network. 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 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
Subnet Mask : 255.255.255.0
Device Name : dlinkrouter
Local Domain Name : (optional)
Enable DNS Relay : ☑

DHCP SERVER SETTINGS

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

Enable DHCP Server : ☑
DHCP IP Address Range : 192.168.0.100 to 192.168.0.199
DHCP Lease Time : 1440 (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 : 0.0.0.0
Secondary WINS IP Address : 0.0.0.0

ADD/EDIT DHCP RESERVATION

Enable : □
Computer Name : << Computer Name
IP Address :
MAC Address :

DHCP RESERVATIONS LIST :

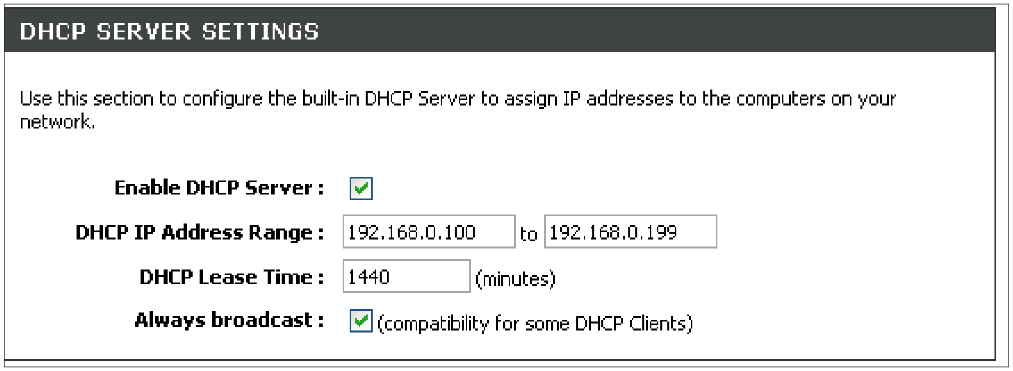
Enable	Host Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS :

Hardware Address	Assigned IP	Hostname	Expires

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DIR-601 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-601. 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 addresses to the computers on your network.

Enable DHCP Server : ☑

DHCP IP Address Range : 192.168.0.100 to 192.168.0.199

DHCP Lease Time : 1440 (minutes)

Always broadcast : ☑ (compatibility for some DHCP Clients)

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.*

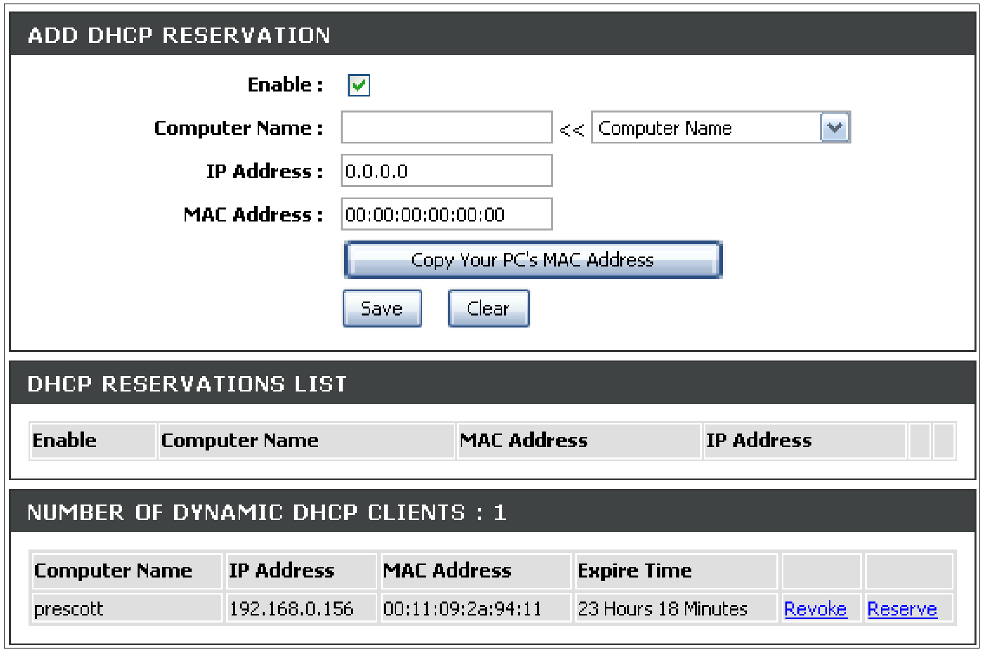
Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes.

Always Broadcast: Enable this feature to broadcast your LAN/WLAN network.

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.*



ADD DHCP RESERVATION

Enable :	☑
Computer Name :	<< Computer Name
IP Address :	0.0.0.0
MAC Address :	00:00:00:00:00:00

DHCP RESERVATIONS LIST

Enable	Computer Name	MAC Address	IP Address

NUMBER OF DYNAMIC DHCP CLIENTS : 1

Computer Name	IP Address	MAC Address	Expire Time		
prescott	192.168.0.156	00:11:09:2a:94:11	23 Hours 18 Minutes	Revoke	Reserve

Enable: Check this box to enable the reservation.

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

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

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

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

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

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

Revoke: Click **Revoke** to cancel the lease for a specific LAN device and free an entry in the lease table. Do this only if the device no longer needs the leased IP address, because, for example, it has been removed from the network.
Note: *The Revoke option will not disconnect a PC with a current network session from the network; you would need to use MAC Address Filter to do that. Revoke will only free up a DHCP Address for the very next requester. If the previous owner is still available, those two devices may both receive an IP Address Conflict error, or the second device may still not receive an IP Address; in that case, you may still need to extend the "DHCP IP Address Range" to address the issue, it is located in the DHCP Server section.*

Virtual Server

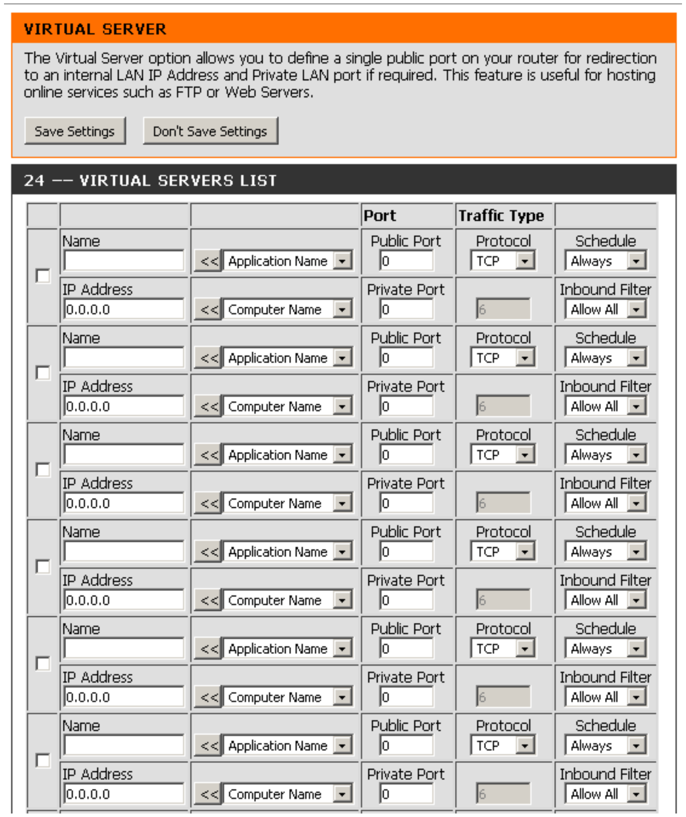
The DIR-601 can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DIR-601 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DIR-601 are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling Virtual Server. Depending on the requested service, the DIR-601 redirects the external service request to the appropriate server within the LAN network.

The DIR-601 is also capable of port-redirection meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

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

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



VIRTUAL SERVER

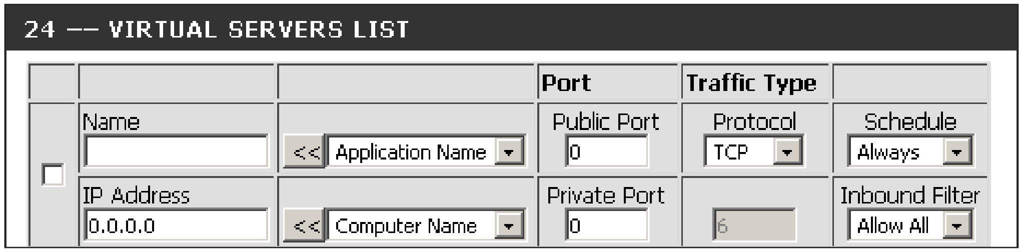
The Virtual Server option allows you to define a single public port on your router for redirection to an internal LAN IP Address and Private LAN port if required. This feature is useful for hosting online services such as FTP or Web Servers.

Save Settings | Don't Save Settings

24 -- VIRTUAL SERVERS LIST

			Port	Traffic Type	
□	Name	<< Application Name	Public Port 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	Private Port 0	6	Inbound Filter Allow All
□	Name	<< Application Name	Public Port 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	Private Port 0	6	Inbound Filter Allow All
□	Name	<< Application Name	Public Port 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	Private Port 0	6	Inbound Filter Allow All
□	Name	<< Application Name	Public Port 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	Private Port 0	6	Inbound Filter Allow All
□	Name	<< Application Name	Public Port 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	Private Port 0	6	Inbound Filter Allow All
□	Name	<< Application Name	Public Port 0	Protocol TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	Private Port 0	6	Inbound Filter Allow All

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



24 -- VIRTUAL SERVERS LIST

			Port	Traffic Type	
□	Name [ ]	<< Application Name ▾	Public Port 0	Protocol TCP ▾	Schedule Always ▾
	IP Address 0.0.0.0	<< Computer Name ▾	Private Port 0	6	Inbound Filter Allow All ▾

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

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

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

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

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

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

Port Forwarding

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

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

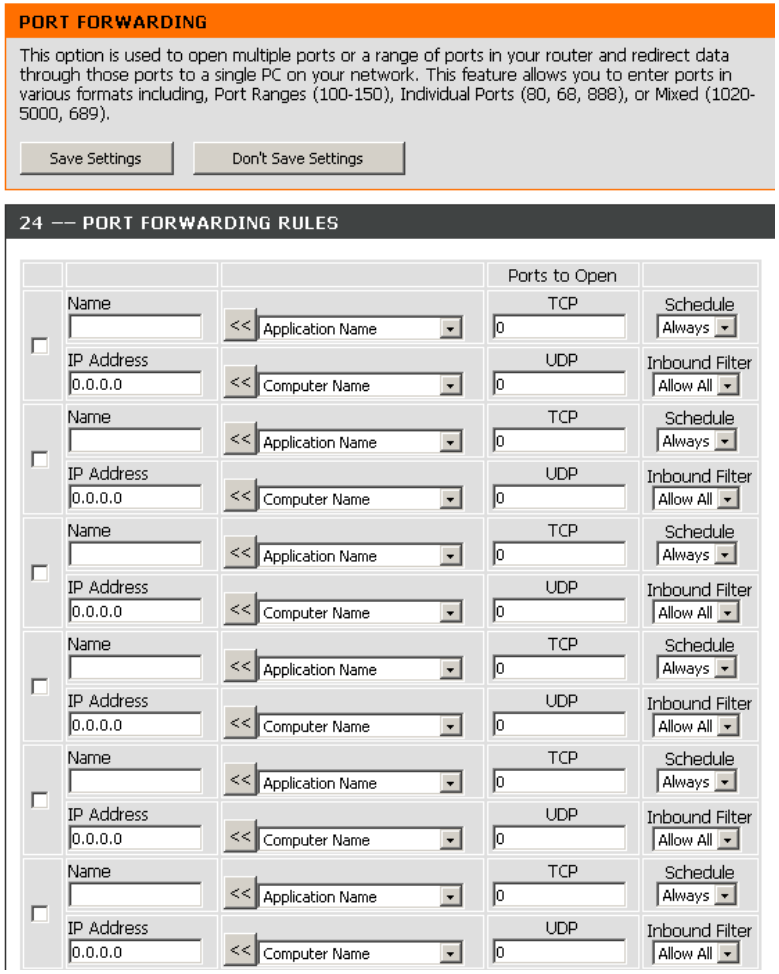
IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), you computer will be listed in the "Computer Name" drop-down menu. Select your computer and click **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

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

Example: 24,1009,3000-4000

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

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



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 various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).

24 -- PORT FORWARDING RULES

				Ports to Open	
☐	Name	<<	Application Name	TCP 0	Schedule Always
	IP Address 0.0.0.0	<<	Computer Name	UDP 0	Inbound Filter Allow All
☐	Name	<<	Application Name	TCP 0	Schedule Always
	IP Address 0.0.0.0	<<	Computer Name	UDP 0	Inbound Filter Allow All
☐	Name	<<	Application Name	TCP 0	Schedule Always
	IP Address 0.0.0.0	<<	Computer Name	UDP 0	Inbound Filter Allow All
☐	Name	<<	Application Name	TCP 0	Schedule Always
	IP Address 0.0.0.0	<<	Computer Name	UDP 0	Inbound Filter Allow All
☐	Name	<<	Application Name	TCP 0	Schedule Always
	IP Address 0.0.0.0	<<	Computer Name	UDP 0	Inbound Filter Allow All
☐	Name	<<	Application Name	TCP 0	Schedule Always
	IP Address 0.0.0.0	<<	Computer Name	UDP 0	Inbound Filter Allow All

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-601. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the firewall (public) ports associated with the trigger port to open them for inbound traffic.

The DIR-601 provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

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

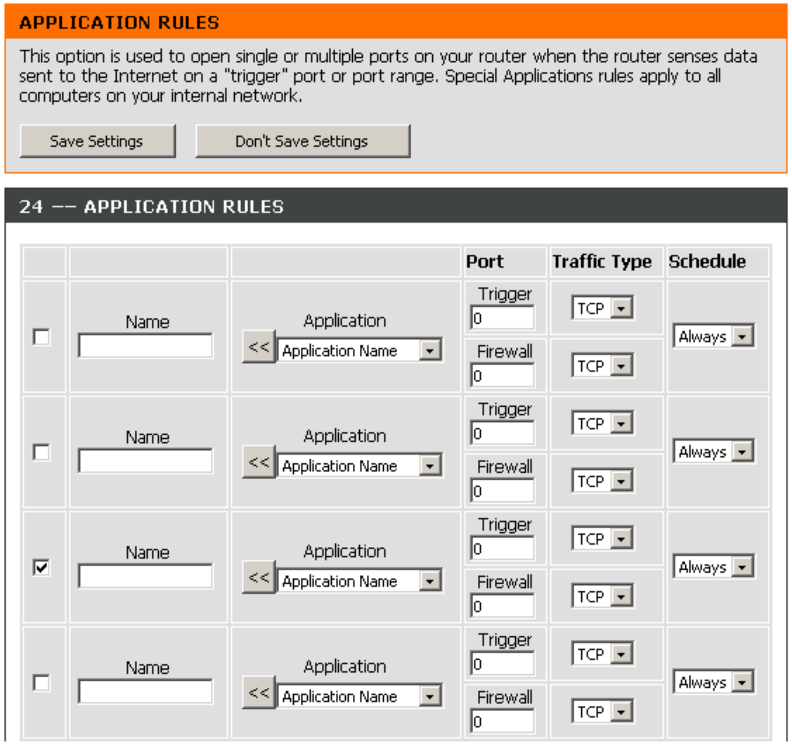
Trigger: This is the port used to trigger the application. It can be either a single port or a range of ports.

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

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

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

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



APPLICATION RULES

This option is used to open single or multiple ports on your router when the router senses data sent to the Internet on a "trigger" port or port range. Special Applications rules apply to all computers on your internal network.

Save Settings | Don't Save Settings

24 -- APPLICATION RULES

			Port	Traffic Type	Schedule
□	Name	Application << Application Name	Trigger 0	TCP	Always
			Firewall 0	TCP	
□	Name	Application << Application Name	Trigger 0	TCP	Always
			Firewall 0	TCP	
☑	Name	Application << Application Name	Trigger 0	TCP	Always
			Firewall 0	TCP	
□	Name	Application << Application Name	Trigger 0	TCP	Always
			Firewall 0	TCP	

QoS Engine

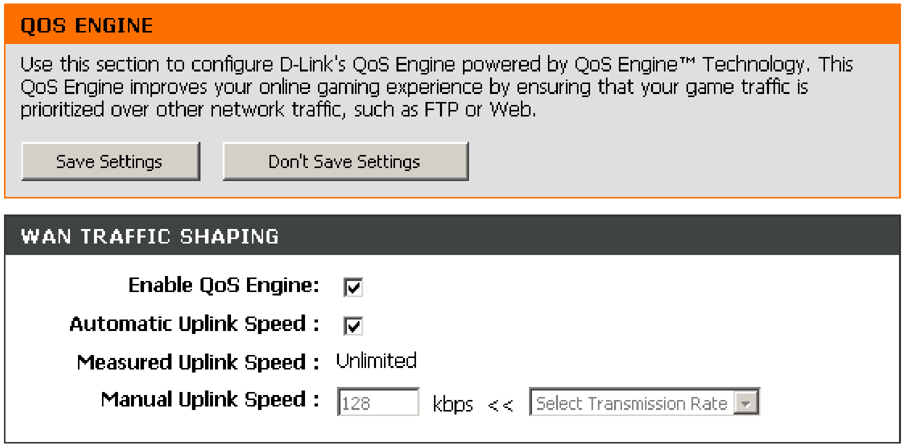
The QoS Engine option helps improve your network gaming performance by prioritizing applications. By default the QoS Engine settings are disabled and application priority is not classified automatically.

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

Automatic Uplink Speed: This option is enabled by default when the QoS Engine option is enabled. This option will allow your router to automatically determine the uplink speed of your Internet connection.

Measured Uplink Speed: This displays the detected uplink speed.

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



QOS ENGINE

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.

WAN TRAFFIC SHAPING

Enable QoS Engine: ☑

Automatic Uplink Speed : ☑

Measured Uplink Speed : Unlimited

Manual Uplink Speed : 128 kbps << Select Transmission Rate

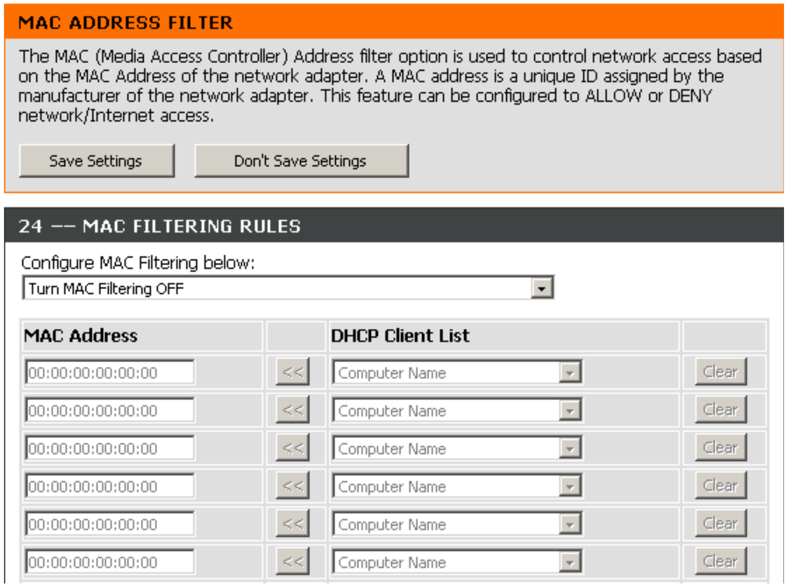
Network Filters

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

Configure MAC Filtering: Select Turn MAC Filtering Off, allow MAC addresses listed below, or deny MAC addresses listed below from the drop-down menu.

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

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


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

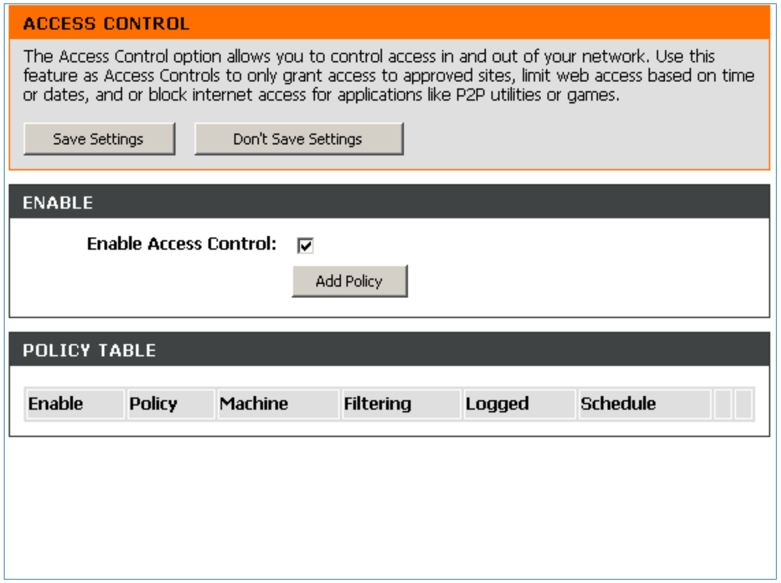
Configure MAC Filtering below:
Turn MAC Filtering OFF

MAC Address		DHCP Client List	
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear
00:00:00:00:00:00	<<	Computer Name	Clear

Access Control

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

Add Policy: Check the **Enable Access Control** check box and 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.

ENABLE

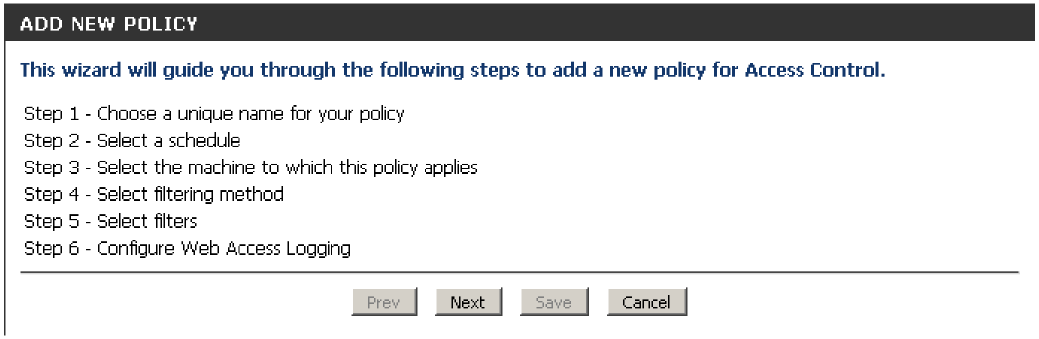
Enable Access Control: ☑

POLICY TABLE

Enable	Policy	Machine	Filtering	Logged	Schedule

Access Control Wizard

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

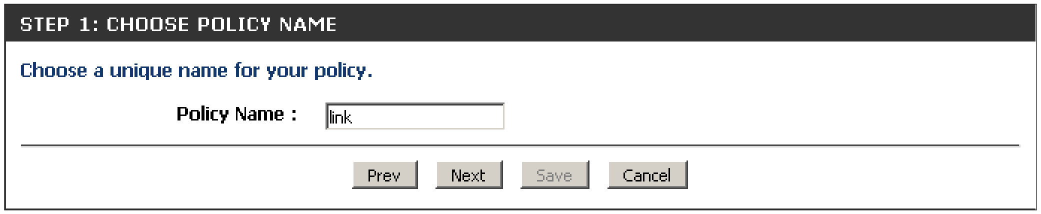


ADD NEW POLICY

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.

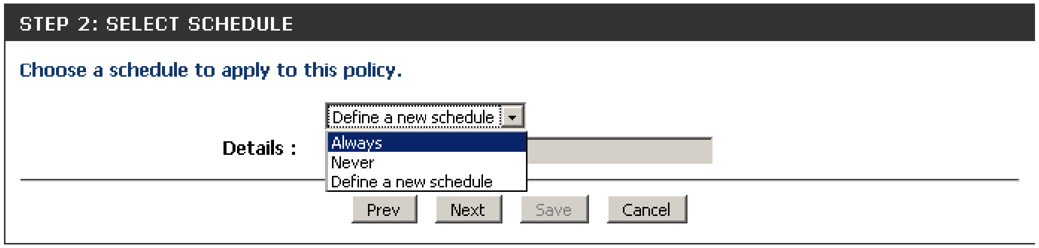


STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name : link

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



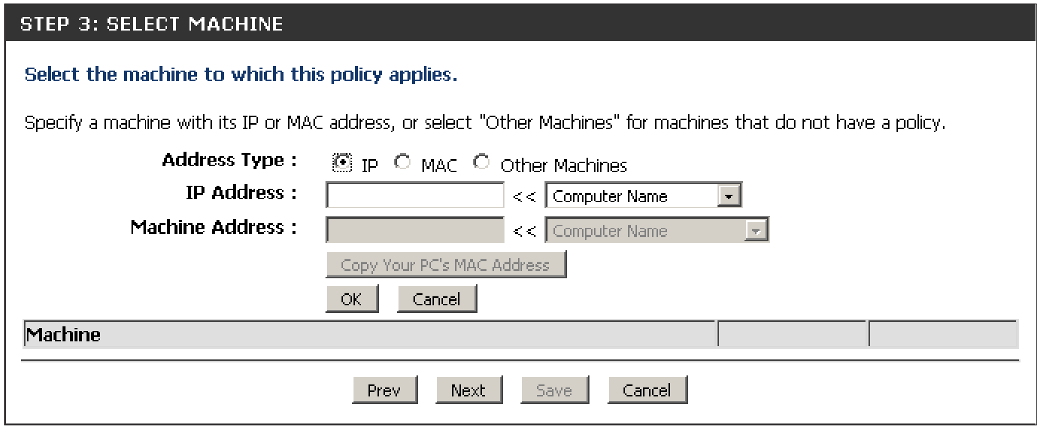
STEP 2: SELECT SCHEDULE

Choose a schedule to apply to this policy.

Details : Define a new schedule

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.



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.

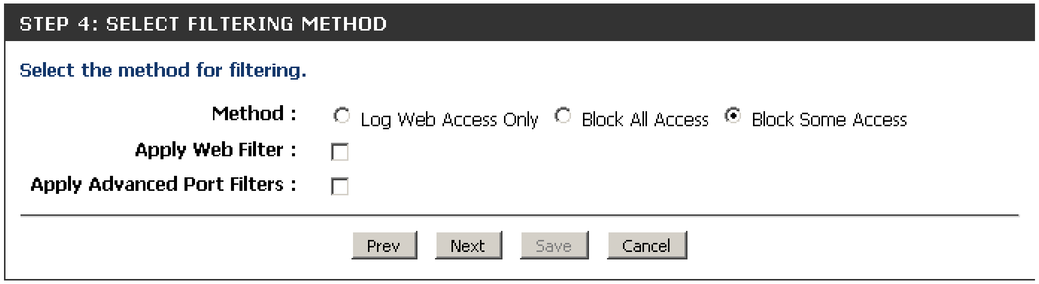
Address Type : ● IP ○ MAC ○ Other Machines

IP Address : << Computer Name

Machine Address : << Computer Name

Machine		

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



STEP 4: SELECT FILTERING METHOD

Select the method for filtering.

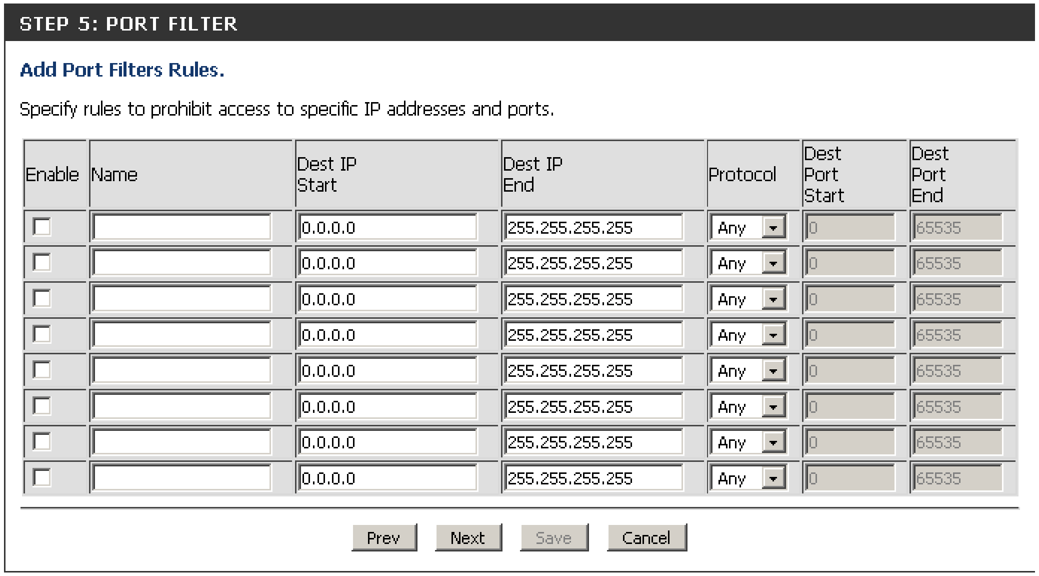
Method : ○ Log Web Access Only ○ Block All Access ● Block Some Access

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

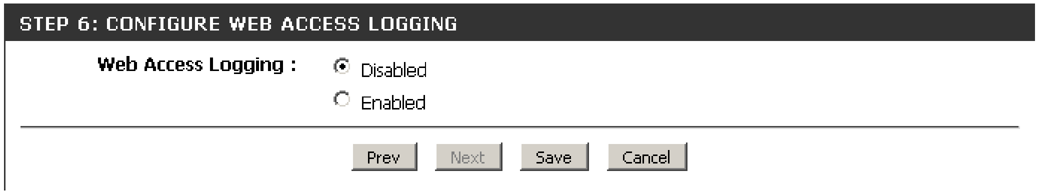
Add Port Filters Rules.

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**.

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



STEP 6: CONFIGURE WEB ACCESS LOGGING

Web Access Logging : ● Disabled
○ Enabled

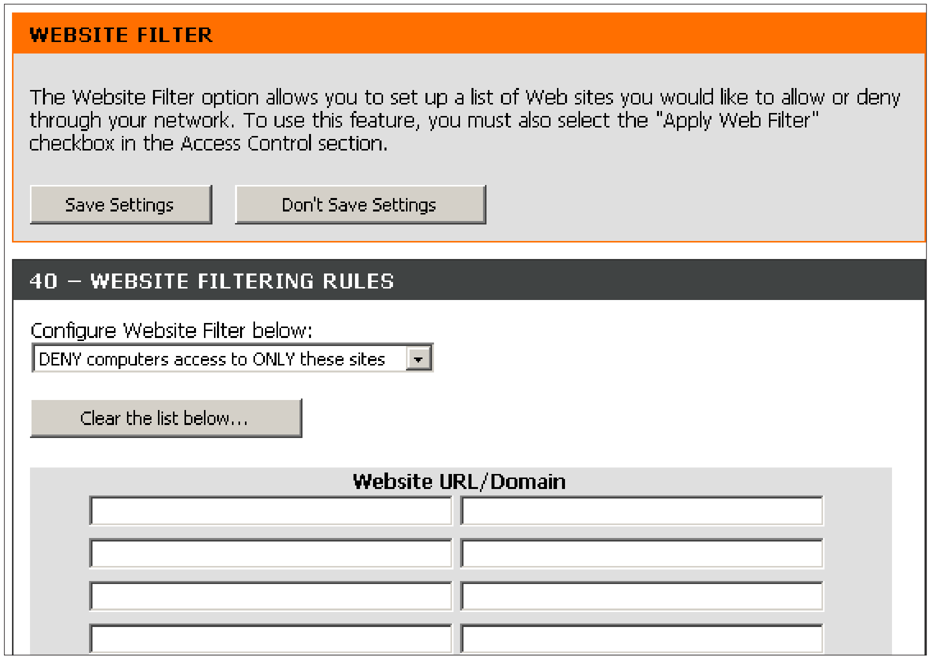
Website Filters

Website Filters are used to allow you to set up a list of allowed Web sites that can be used by multiple users through the network. To use this feature select to **Allow** or **Deny**, enter the domain or website and click **Add**, and then click **Save Settings**. You must also select **Apply Web Filter** under the Access Control section (page 46).

Configure Website Filter Below: Select **Deny** or **Allow** computers access to only these sites.

Clear the list below: Click to delete all entries in the list.

Website URL/ Domain: Enter the keywords or URLs that you want to allow or deny.



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

Inbound Filters

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

Name: Enter a name for the inbound filter rule.

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

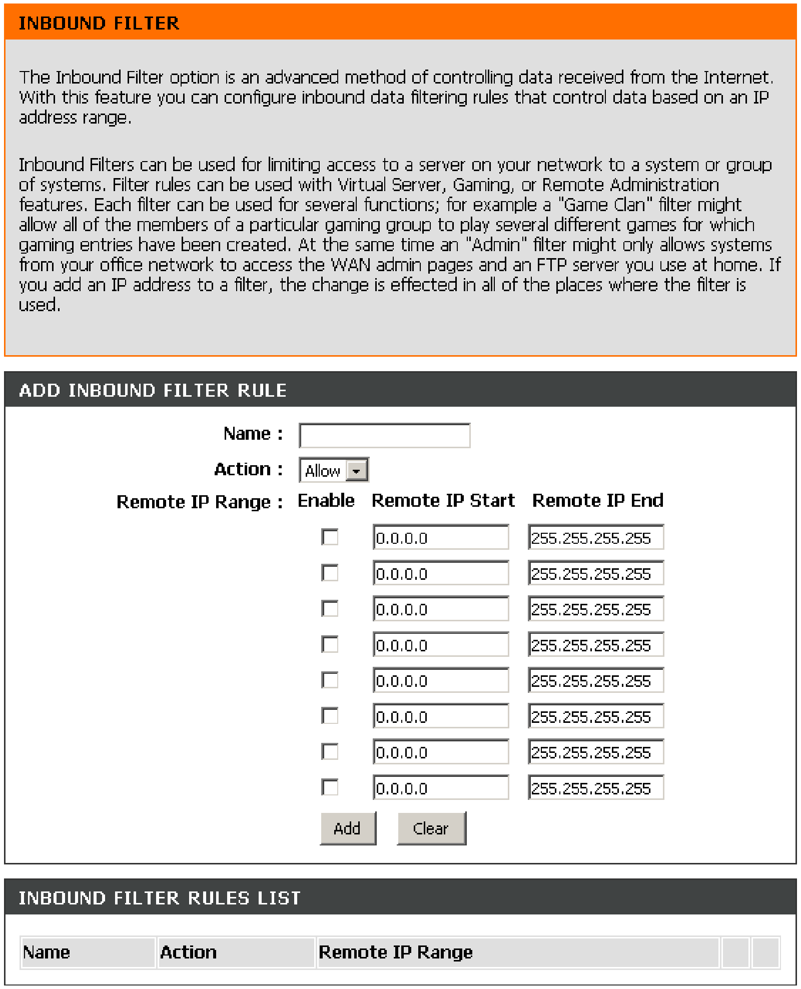
Enable: Check to enable rule.

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

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

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

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



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, Gaming, or Remote Administration features. Each filter can be used for several functions; for example a "Game Clan" filter might allow all of the members of a particular gaming group to play several different games for which gaming entries have been created. At the same time an "Admin" filter might only allows systems from your office network to access the WAN admin pages and an FTP server you use at home. If you add an IP address to a filter, the change is effected in all of the places where the filter is used.

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

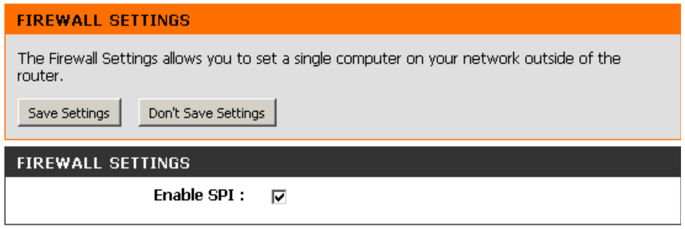
Name	Action	Remote IP Range		

Firewall Settings

A firewall protects your network from the outside world. The D-Link DIR-601 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.

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

Enable Anti-Spoof Checking: Enable this option to provide protection from certain kinds of "spoofing" attacks.



FIREWALL SETTINGS

The Firewall Settings allows you to set a single computer on your network outside of the router.

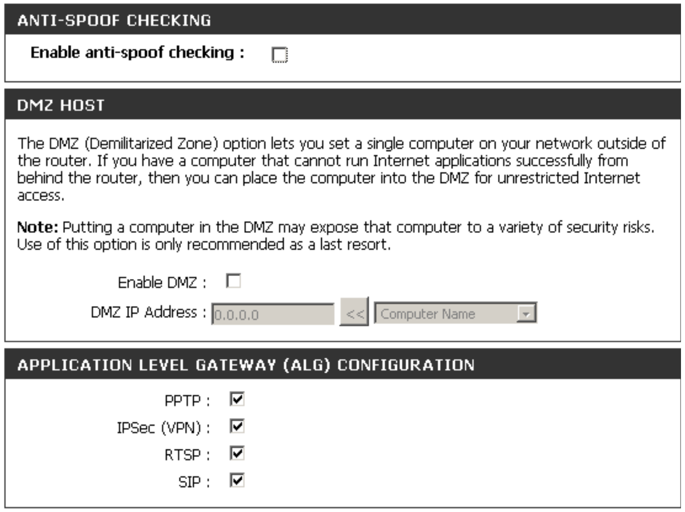
FIREWALL SETTINGS

Enable SPI : ☑

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

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

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



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 : 0.0.0.0 << Computer Name

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP : ☑

IPSec (VPN) : ☑

RTSP : ☑

SIP : ☑

Routing

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

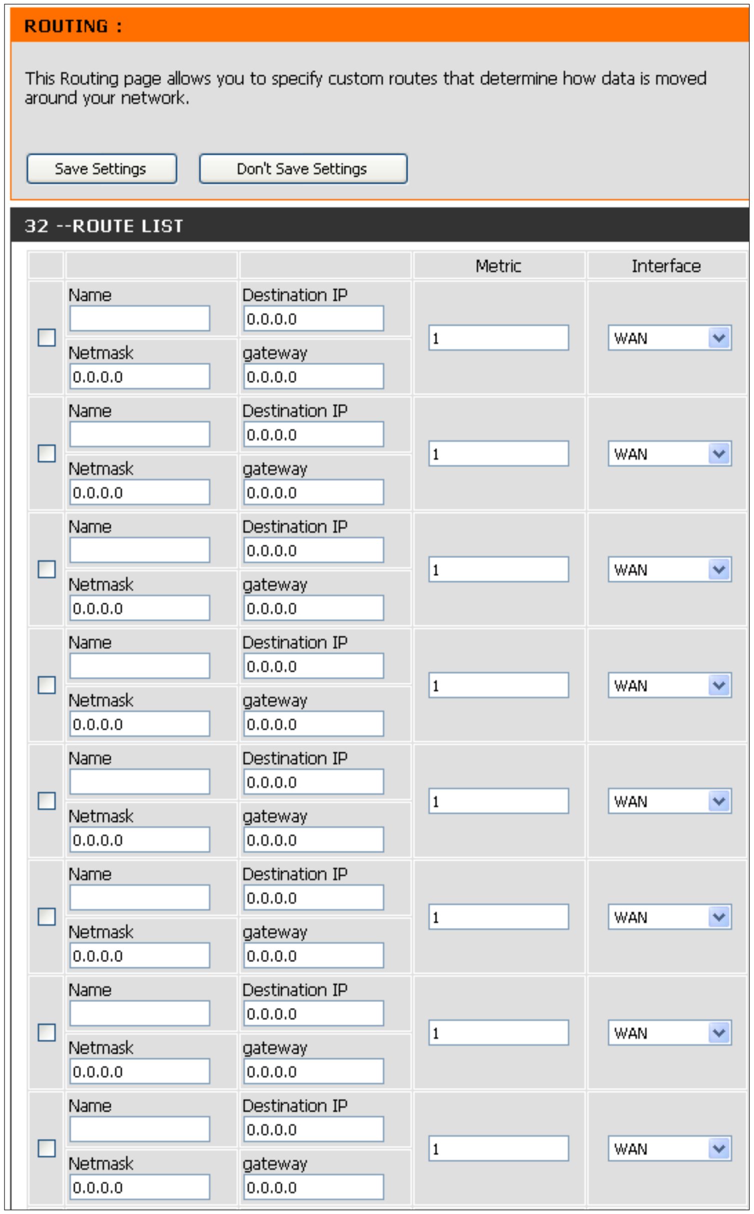
Destination IP: Enter the IP address of packets that will take this route.

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 :

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

32 --ROUTE LIST

			Metric	Interface
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN
☐	Name Netmask 0.0.0.0	Destination IP 0.0.0.0 gateway 0.0.0.0	1	WAN

Advanced Wireless Settings

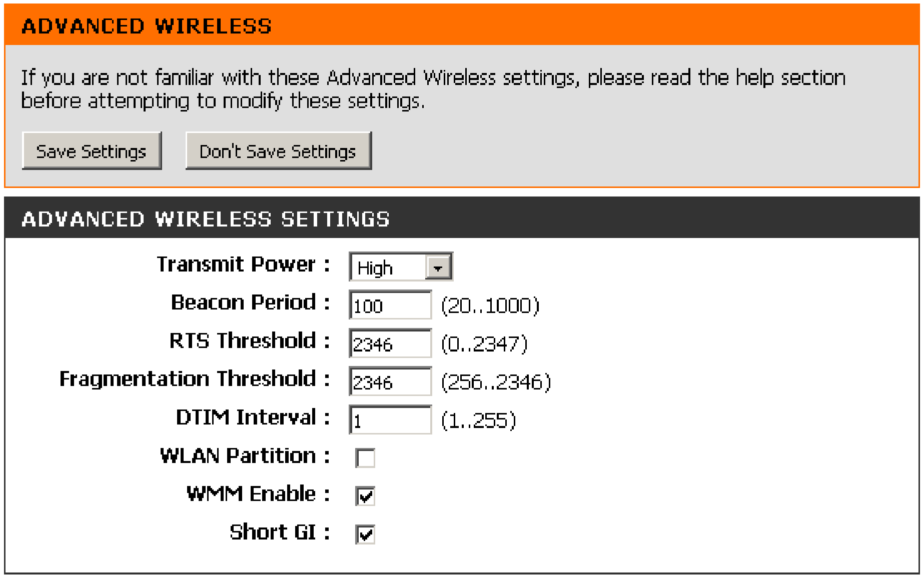
Transmit Power: Set the transmit power of the antennas.

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

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

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

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



ADVANCED WIRELESS

If you are not familiar with these Advanced Wireless settings, please read the help section before attempting to modify these settings.

ADVANCED WIRELESS SETTINGS

Transmit Power :	High	
Beacon Period :	100	(20..1000)
RTS Threshold :	2346	(0..2347)
Fragmentation Threshold :	2346	(256..2346)
DTIM Interval :	1	(1..255)
WLAN Partition :	□	
WMM Enable :	☑	
Short GI :	☑	

WLAN Partition: This feature enables client isolation. If enabling, all clients will not be able to view or access each other's information or within the network.

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.

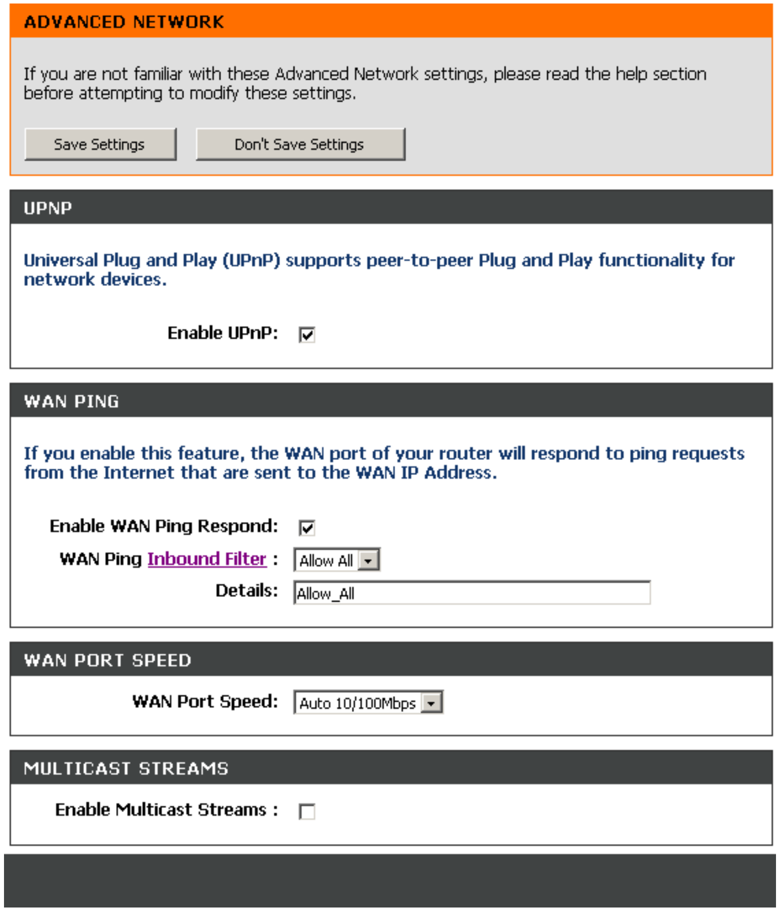
Advanced Network Settings

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

WAN Ping: Unchecking the box will not allow the DIR-601 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.

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



ADVANCED NETWORK

If you are not familiar with these Advanced Network settings, please read the help section before attempting to modify these settings.

UPNP

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

Enable UPnP: ☑

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 Respond: ☑

WAN Ping Inbound Filter : Allow All

Details: Allow_All

WAN PORT SPEED

WAN Port Speed: Auto 10/100Mbps

MULTICAST STREAMS

Enable Multicast Streams : □

Administrator Settings

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

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

User Password: Enter the new password for the User login. If you login as the User, you can only see the settings, but cannot change them.

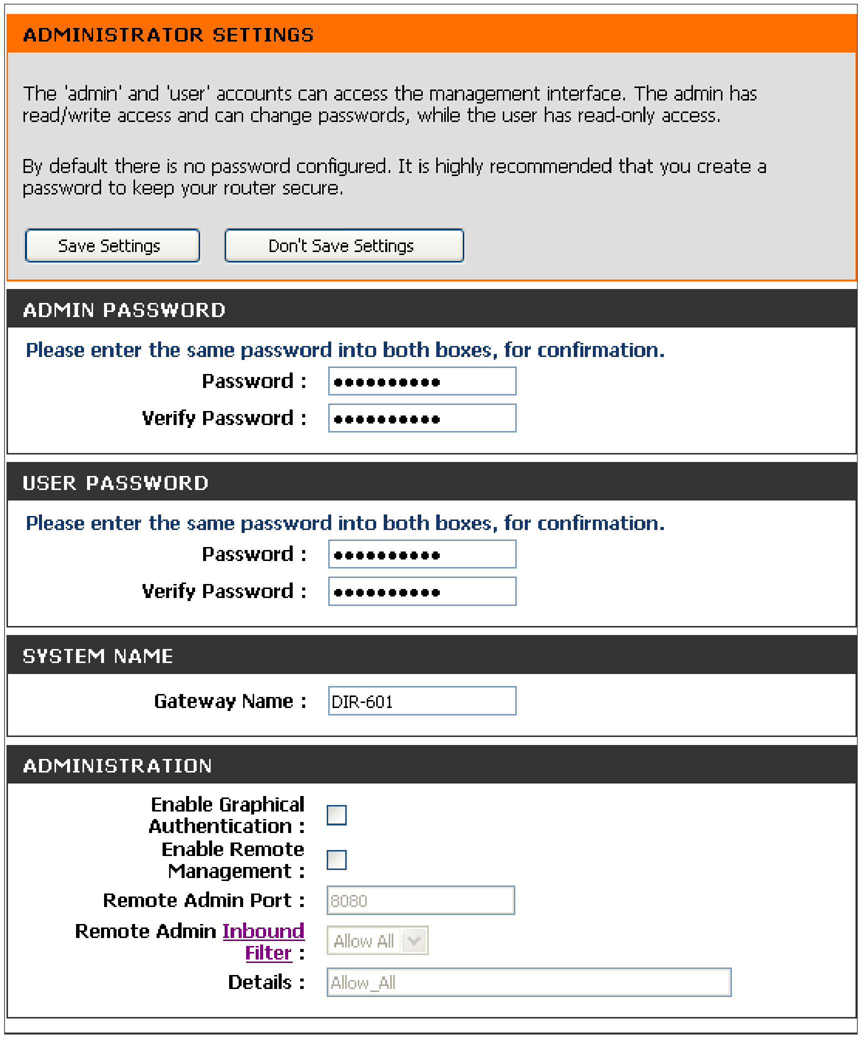
Gateway Name: Enter a name for the DIR-601 router.

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.

Remote Management: Remote management allows the DIR-601 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

Remote Admin Port: The port number used to access the DIR-601. Example: http://x.x.x.x:8080 whereas x.x.x.x is the Internet IP address of the DIR-601 and 8080 is the port used for the Web Management interface.

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.



ADMINISTRATOR SETTINGS

The 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access.

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 : ••••••••••

USER PASSWORD

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

Password : ••••••••••

Verify Password : ••••••••••

SYSTEM NAME

Gateway Name : DIR-601

ADMINISTRATION

Enable Graphical Authentication : □

Enable Remote Management : □

Remote Admin Port : 8080

Remote Admin Inbound Filter : Allow All

Details : Allow_All

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

Time Settings

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

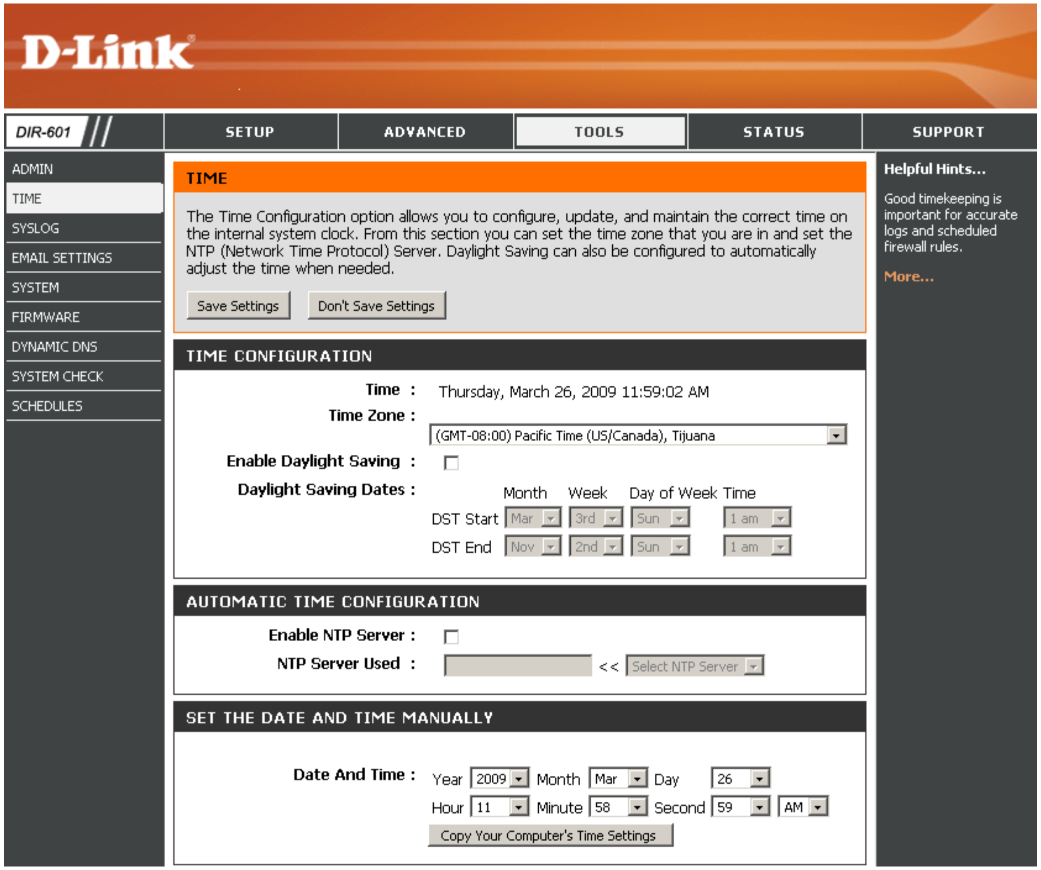
Time Zone: Select the Time Zone from the drop-down menu.

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

Enable NTP Server: NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

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

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



TIME

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

TIME CONFIGURATION

Time : Thursday, March 26, 2009 11:59:02 AM

Time Zone : (GMT-08:00) Pacific Time (US/Canada), Tijuana

Enable Daylight Saving : □

Daylight Saving Dates :

	Month	Week	Day of Week	Time
DST Start	Mar	3rd	Sun	1 am
DST End	Nov	2nd	Sun	1 am

AUTOMATIC TIME CONFIGURATION

Enable NTP Server : □

NTP Server Used : << Select NTP Server

SET THE DATE AND TIME MANUALLY

Date And Time : Year 2009 Month Mar Day 26
Hour 11 Minute 58 Second 59 AM

Helpful Hints...

Good timekeeping is important for accurate logs and scheduled firewall rules.

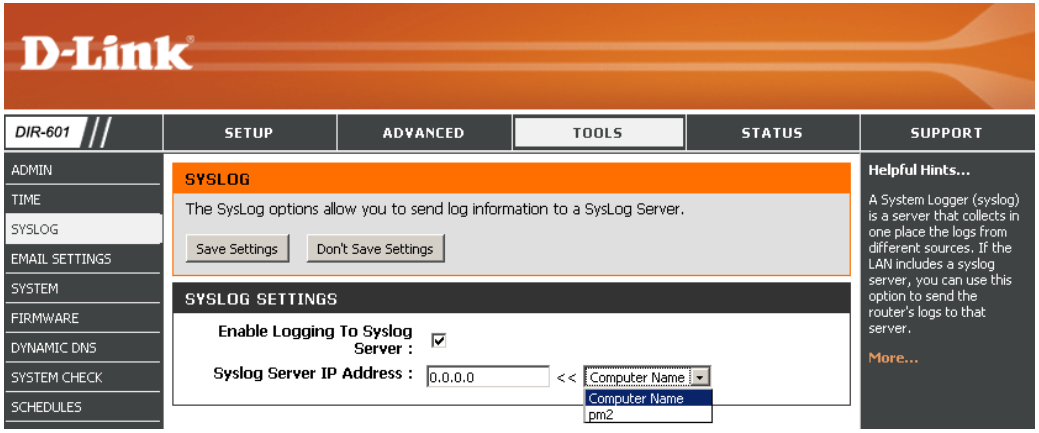
More...

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 : 0.0.0.0 << 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.

More...

E-mail Settings

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

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

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

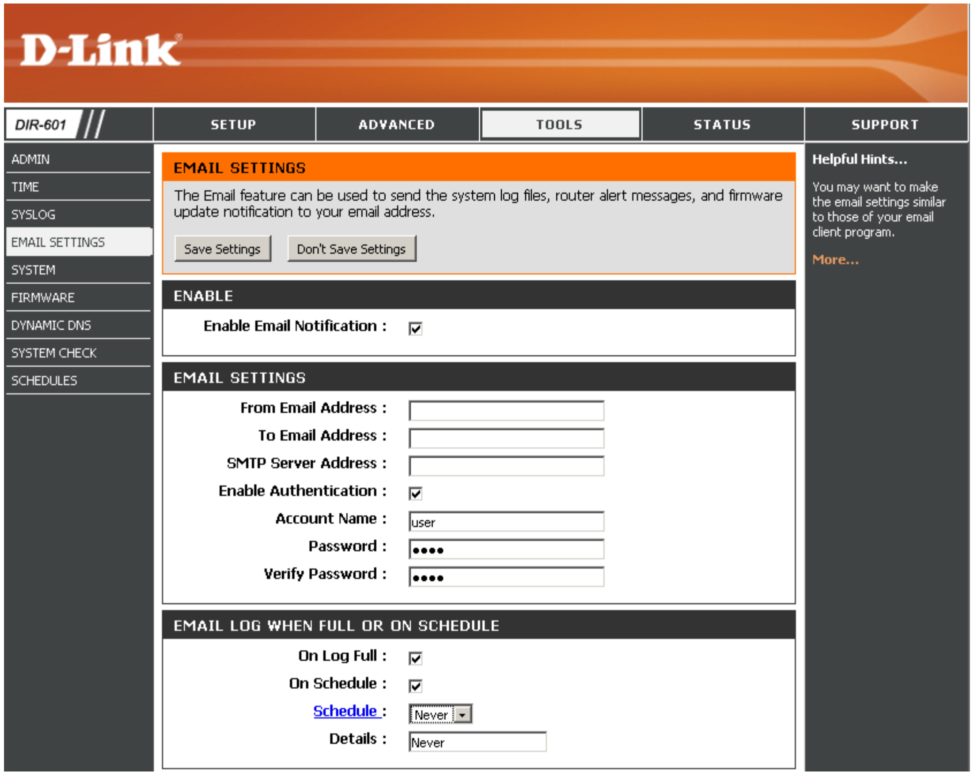
To Email Address: Enter the e-mail address where you want the e-mail sent.

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

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

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

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



EMAIL SETTINGS

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

ENABLE

Enable Email Notification : ☑

EMAIL SETTINGS

From Email Address :
To Email Address :
SMTP Server Address :
Enable Authentication : ☑
Account Name : user
Password : ••••
Verify Password : ••••

EMAIL LOG WHEN FULL OR ON SCHEDULE

On Log Full : ☑
On Schedule : ☑
Schedule : Never
Details : Never

Helpful Hints...

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

More...

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

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

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

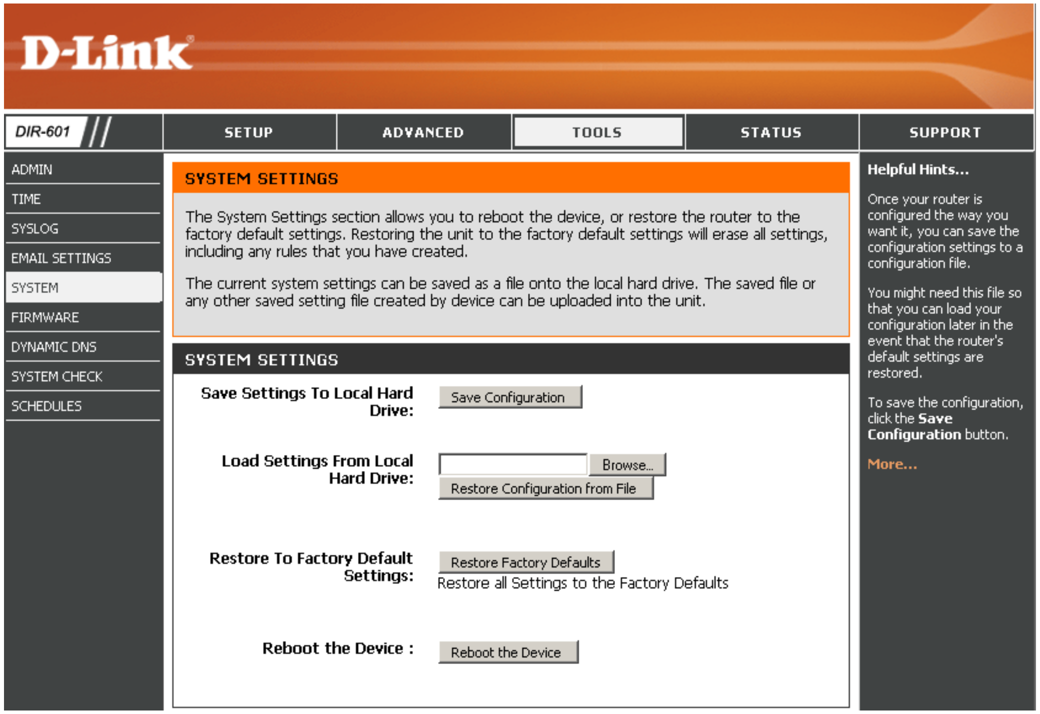
System Settings

Save 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. You will then see a file dialog, where you can 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 control to find a previously save file of configuration settings. Then, click the **Load** button to transfer those settings to the router.

Restore to Factory Default 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.



SYSTEM SETTINGS

The System Settings section allows you to reboot the device, or 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 have created.

The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by device can be uploaded into the unit.

SYSTEM 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
Restore all Settings to the Factory Defaults

Reboot the Device : Reboot the Device

Helpful Hints...

Once your router is configured the way you want it, you can save the configuration settings to a configuration file.

You might need this file so that you can load your configuration later in the event that the router's default settings are restored.

To save the configuration, click the **Save Configuration** button.

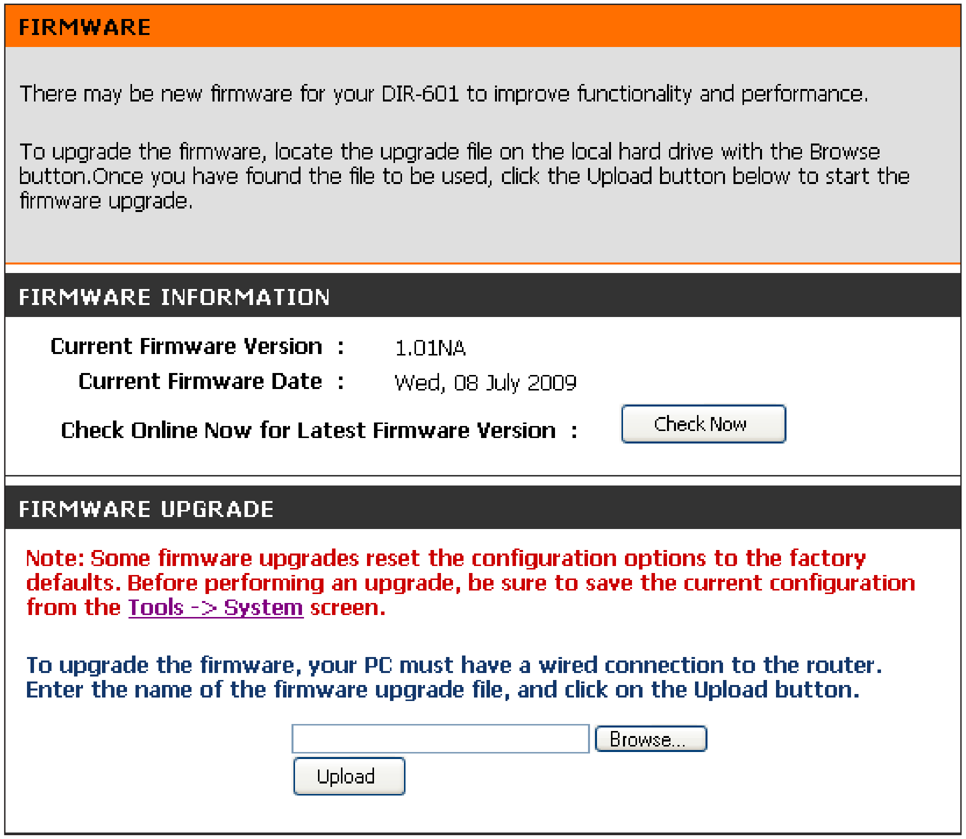
More...

Update Firmware

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

Check Now: Click on **Check Now** 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.



FIRMWARE

There may be new firmware for your DIR-601 to improve functionality and performance.

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 below to start the firmware upgrade.

FIRMWARE INFORMATION

Current Firmware Version : 1.01NA

Current Firmware Date : Wed, 08 July 2009

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 from the Tools -> System screen.

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.

DDNS

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

Enable DDNS: Check to enable DDNS.

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

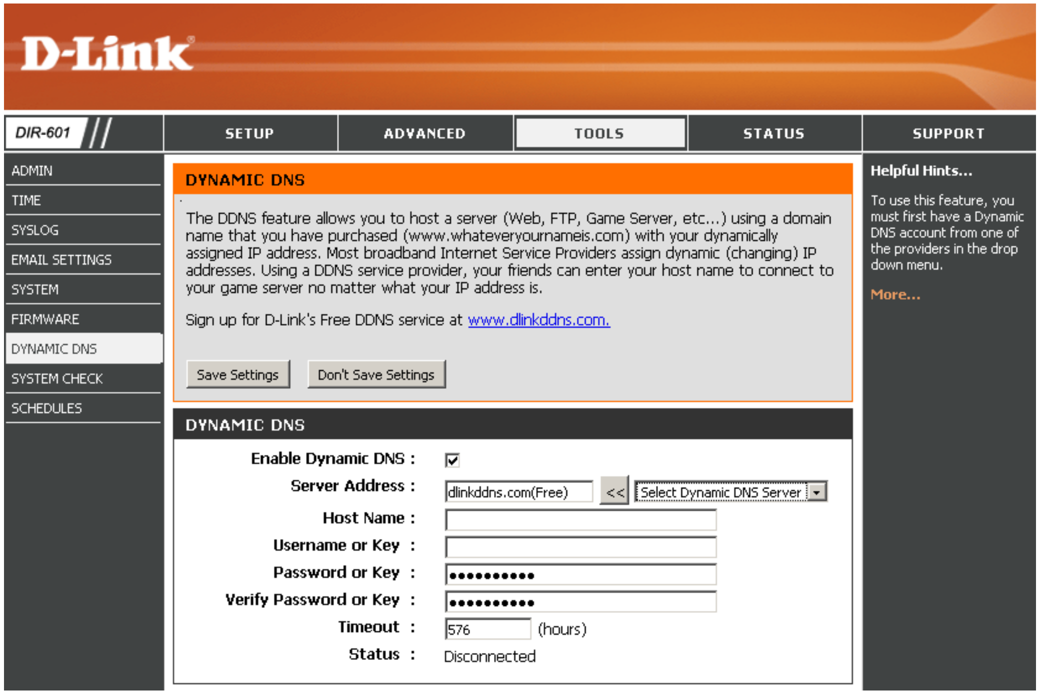
Host Name: Enter the Host Name that you registered with your DDNS service provider.

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

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

Timeout: Enter a time (in hours).

Status: Displays the current connection status to your DDNS server.



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 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.

Save Settings | Don't Save Settings

DYNAMIC DNS

Enable Dynamic DNS : ☑
Server Address : dlinkddns.com(Free) << Select Dynamic DNS Server
Host Name :
Username or Key :
Password or Key : ••••••••••
Verify Password or Key : ••••••••••
Timeout : 576 (hours)
Status : Disconnected

Helpful Hints...

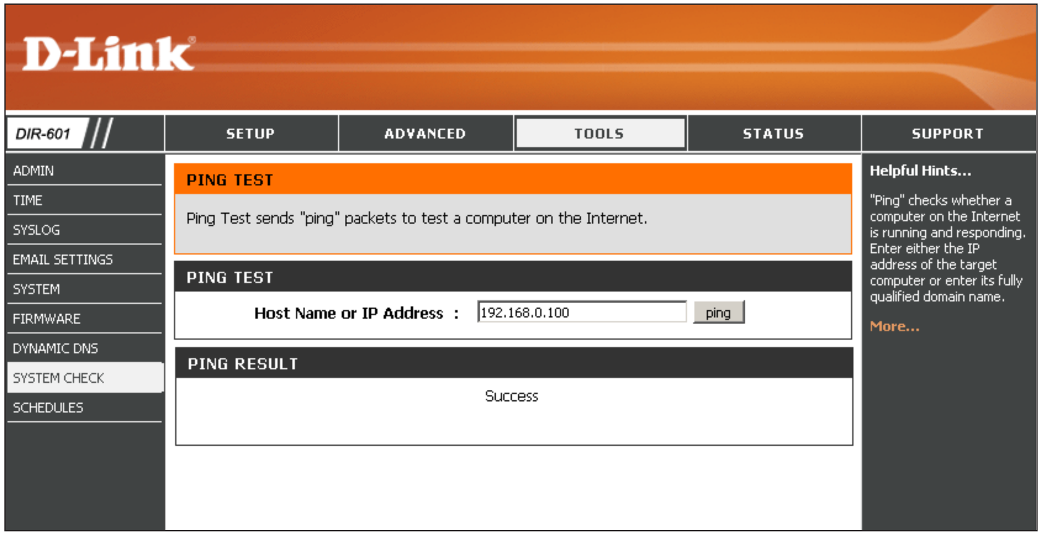
To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu.

More...

System Check

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

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



PING TEST

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

PING TEST

Host Name or IP Address : 192.168.0.100

PING RESULT

Success

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

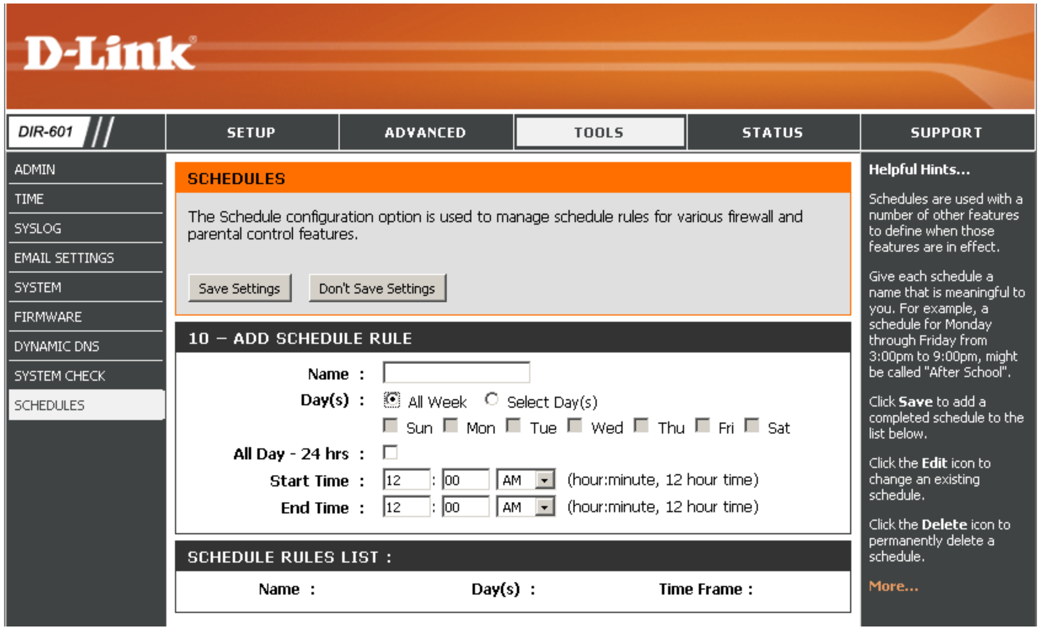
Name: Enter a name for your new schedule.

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

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

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

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



SCHEDULES

The Schedule configuration option is used to manage schedule rules for various firewall and parental control features.

10 – ADD SCHEDULE RULE

Name :	
Day(s) :	● All Week ○ Select Day(s) □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
All Day - 24 hrs :	□
Start Time :	12 : 00 AM (hour:minute, 12 hour time)
End Time :	12 : 00 AM (hour:minute, 12 hour time)

SCHEDULE RULES LIST :

Name :	Day(s) :	Time Frame :

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 **Save** to add a completed schedule to the list below.

Click the **Edit** icon to change an existing schedule.

Click the **Delete** icon to permanently delete a schedule.

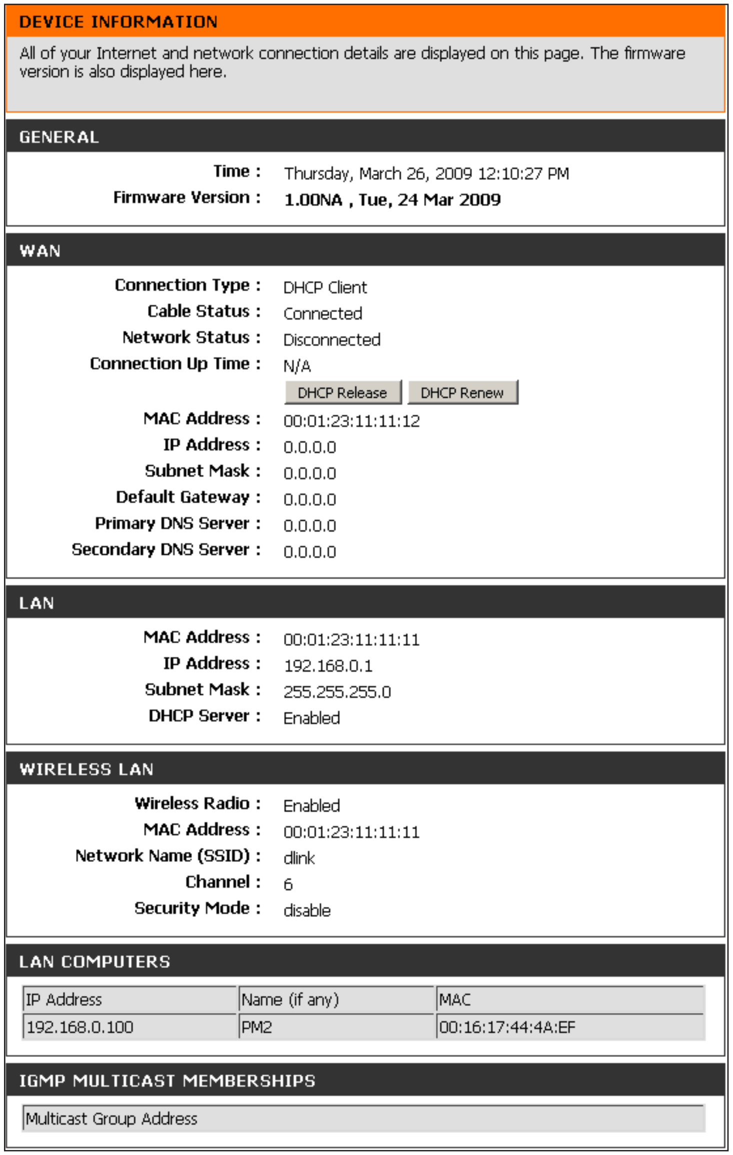
Device Information

This page displays the current information for the DIR-601. 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.

See the following page for more information.



DEVICE INFORMATION

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

GENERAL

Time : Thursday, March 26, 2009 12:10:27 PM
Firmware Version : 1.00NA , Tue, 24 Mar 2009

WAN

Connection Type : DHCP Client
Cable Status : Connected
Network Status : Disconnected
Connection Up Time : N/A
DHCP Release DHCP Renew
MAC Address : 00:01:23:11:11:12
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0

LAN

MAC Address : 00:01:23:11:11:11
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

Wireless Radio : Enabled
MAC Address : 00:01:23:11:11:11
Network Name (SSID) : dlink
Channel : 6
Security Mode : disable

LAN COMPUTERS

IP Address	Name (if any)	MAC
192.168.0.100	PM2	00:16:17:44:4A:EF

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address

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

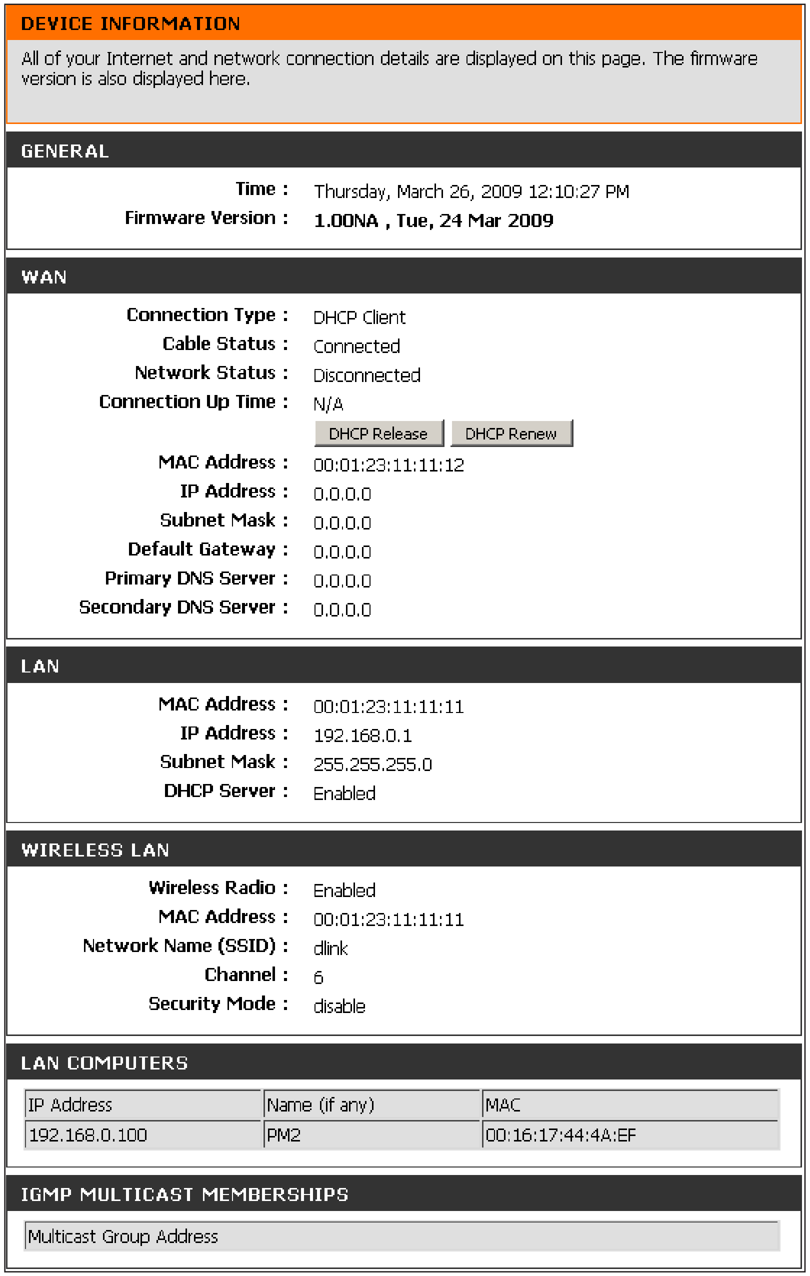
WAN: Displays the MAC address and the public IP settings for the router.

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

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

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

IGMP Multicast Memberships: Displays the Multicast Group IP Address.



DEVICE INFORMATION

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

GENERAL

Time : Thursday, March 26, 2009 12:10:27 PM
Firmware Version : 1.00NA , Tue, 24 Mar 2009

WAN

Connection Type : DHCP Client
Cable Status : Connected
Network Status : Disconnected
Connection Up Time : N/A

MAC Address : 00:01:23:11:11:12
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0
Secondary DNS Server : 0.0.0.0

LAN

MAC Address : 00:01:23:11:11:11
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WIRELESS LAN

Wireless Radio : Enabled
MAC Address : 00:01:23:11:11:11
Network Name (SSID) : dlink
Channel : 6
Security Mode : disable

LAN COMPUTERS

IP Address	Name (if any)	MAC
192.168.0.100	PM2	00:16:17:44:4A:EF

IGMP MULTICAST MEMBERSHIPS

Multicast Group Address

Log

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.

Log Options: You can select the types of messages that you want to display from the log.

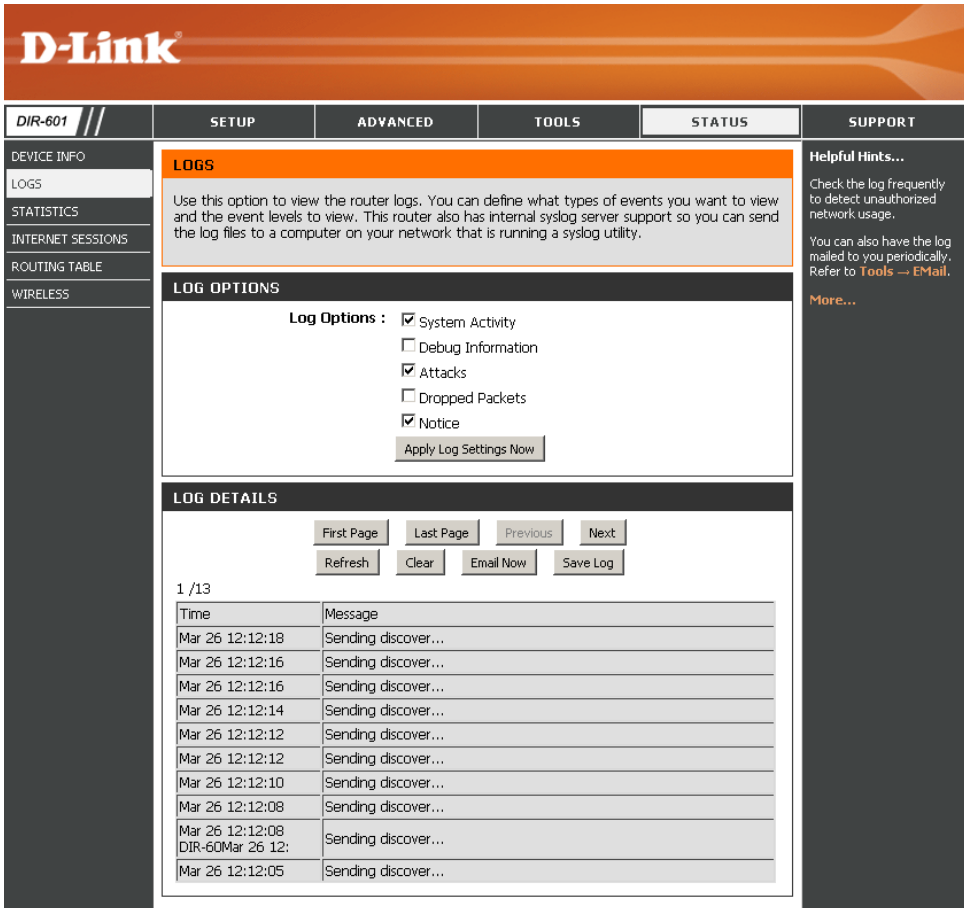
Apply Log Settings: Will filter the log results so that only the selected options appear.

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

Clear: Clears all of the log contents.

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

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



LOGS

Use this option to view the router logs. You can define what types of events you want to view and the event levels to view. This router also has internal syslog server support so you can send the log files to a computer on your network that is running a syslog utility.

LOG OPTIONS

Log Options : ☑ System Activity
□ Debug Information
☑ Attacks
□ Dropped Packets
☑ Notice

Apply Log Settings Now

LOG DETAILS

First Page | Last Page | Previous | Next
Refresh | Clear | Email Now | Save Log

1 /13

Time	Message
Mar 26 12:12:18	Sending discover...
Mar 26 12:12:16	Sending discover...
Mar 26 12:12:16	Sending discover...
Mar 26 12:12:14	Sending discover...
Mar 26 12:12:12	Sending discover...
Mar 26 12:12:12	Sending discover...
Mar 26 12:12:10	Sending discover...
Mar 26 12:12:08	Sending discover...
Mar 26 12:12:08 DIR-60Mar 26 12:	Sending discover...
Mar 26 12:12:05	Sending discover...

Helpful Hints...

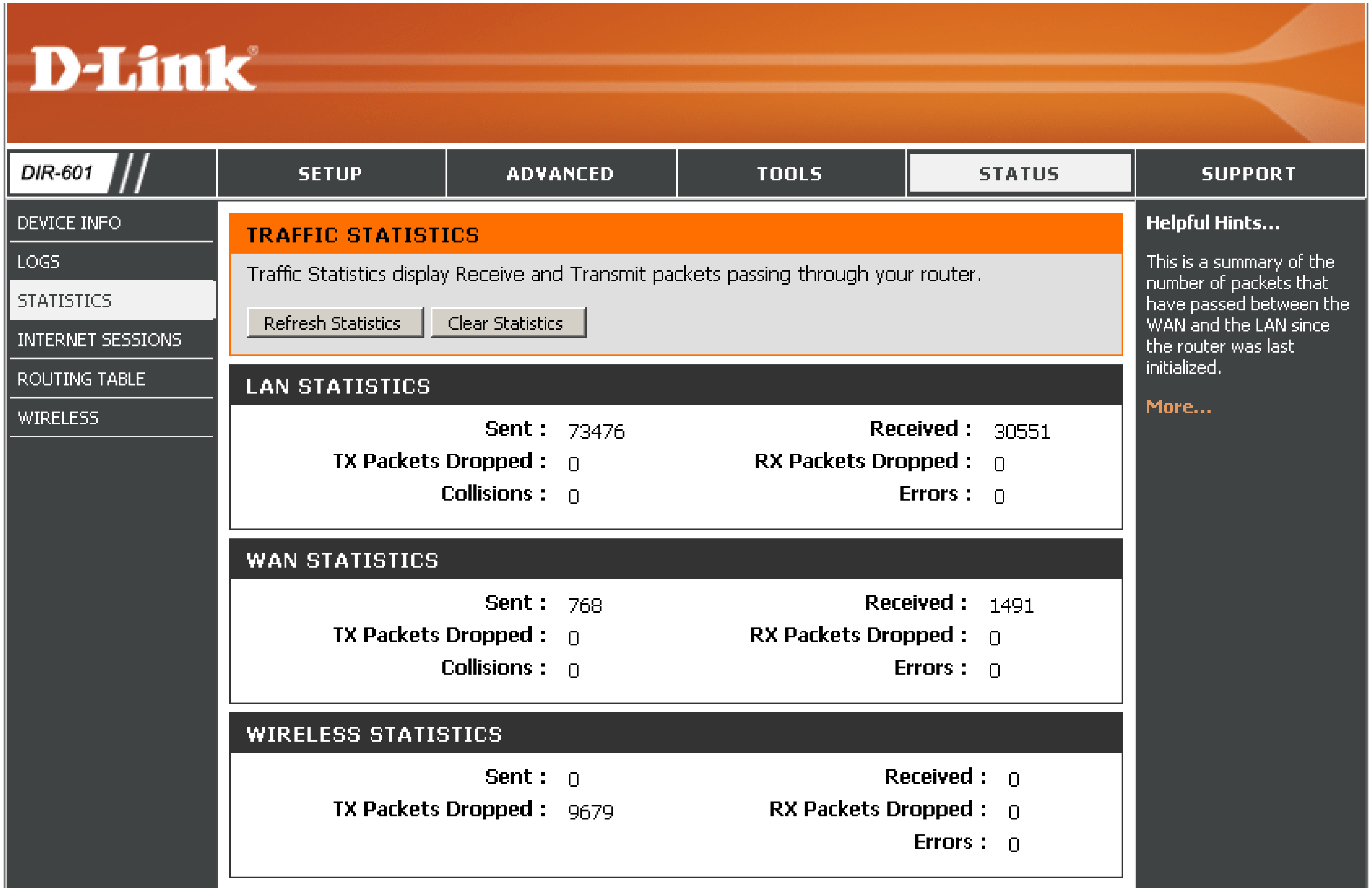
Check the log frequently to detect unauthorized network usage.

You can also have the log mailed to you periodically. Refer to Tools → EMail.

More...

Stats

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-601 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.



TRAFFIC STATISTICS

Traffic Statistics display Receive and Transmit packets passing through your router.

LAN STATISTICS

Sent :	73476	Received :	30551
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

WAN STATISTICS

Sent :	768	Received :	1491
TX Packets Dropped :	0	RX Packets Dropped :	0
Collisions :	0	Errors :	0

WIRELESS STATISTICS

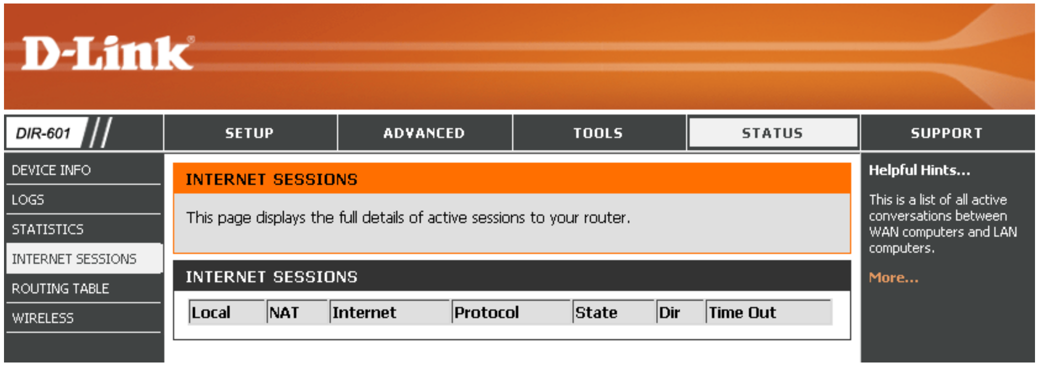
Sent :	0	Received :	0
TX Packets Dropped :	9679	RX Packets Dropped :	0
		Errors :	0

Helpful Hints...

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

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 the full details of active sessions to your router.

INTERNET SESSIONS

Local	NAT	Internet	Protocol	State	Dir	Time Out

Helpful Hints...

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

More...

Local: The IP address and, where appropriate, port number of the local application.

NAT: The port number of the LAN-side application as viewed by the WAN-side application.

Internet: The IP address and, where appropriate, port number of the application on the Internet.

Protocol: The communications protocol used for the conversation.

State: State for sessions that use the TCP protocol:

NO: None -- This entry is used as a placeholder for a future connection that may occur.
SS: SYN Sent -- One of the systems is attempting to start a connection.
EST: Established -- the connection is passing data.
FW: FIN Wait -- The client system has requested that the connection be stopped.
CW: Close Wait -- The server system has requested that the connection be stopped.
TW: Time Wait -- Waiting for a short time while a connection that was in FIN Wait is fully closed.
LA: Last ACK -- Waiting for a short time while a connection that was in Close Wait is fully closed.
CL: Closed -- The connection is no longer active but the session is being tracked in case there are any retransmitted packets still pending.

Dir: The direction of initiation of the conversation:

Priority: **Out** - Initiated from LAN to WAN.
In - Initiated from WAN to LAN.
The preference given to outbound packets of this conversation by the QoS Engine logic. Smaller numbers represent higher priority.

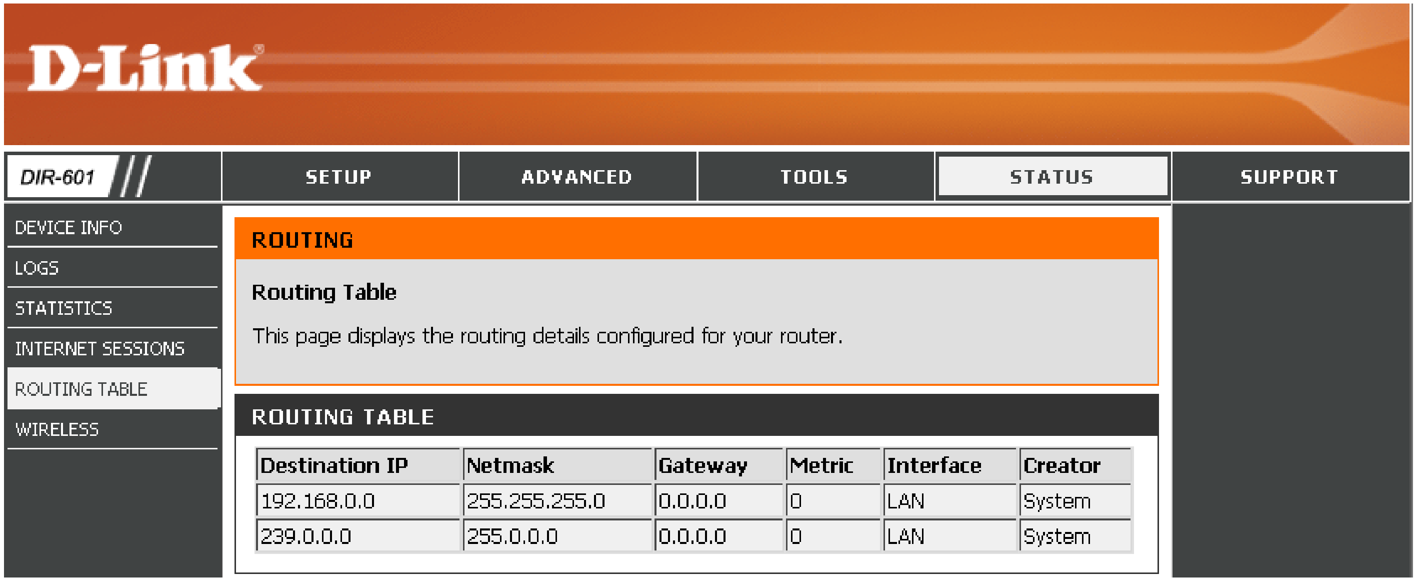
Time Out: The number of seconds of idle time until the router considers the session terminated. The initial value of Time Out depends on the type and state of the connection.

300 seconds - UDP connections.
240 seconds - Reset or closed TCP connections. The connection does not close instantly so that lingering packets can pass or the connection can be re-established.

7800 seconds - Established or closing TCP connections.

Routing Table

This page displays the routing details configured for your router.



ROUTING

Routing Table

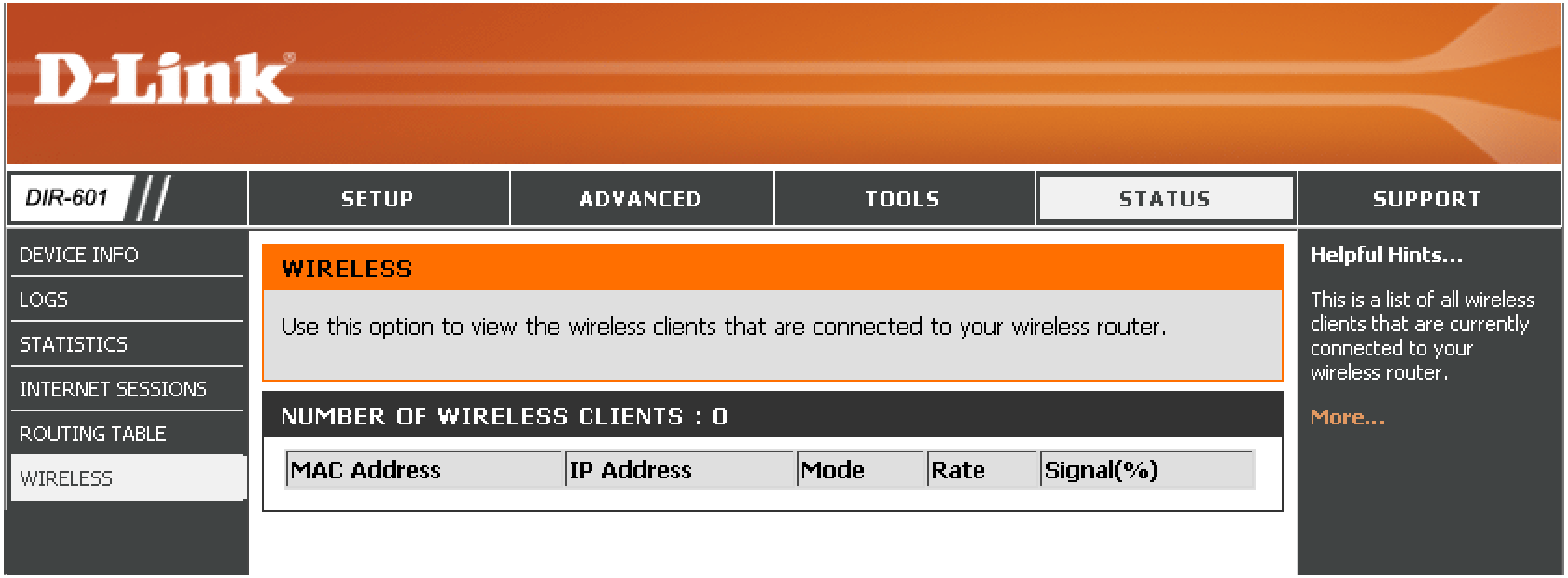
This page displays the routing details configured for your router.

ROUTING TABLE

Destination IP	Netmask	Gateway	Metric	Interface	Creator
192.168.0.0	255.255.255.0	0.0.0.0	0	LAN	System
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN	System

Wireless

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



WIRELESS

Use this option to view the wireless clients that are connected to your wireless router.

NUMBER OF WIRELESS CLIENTS : 0

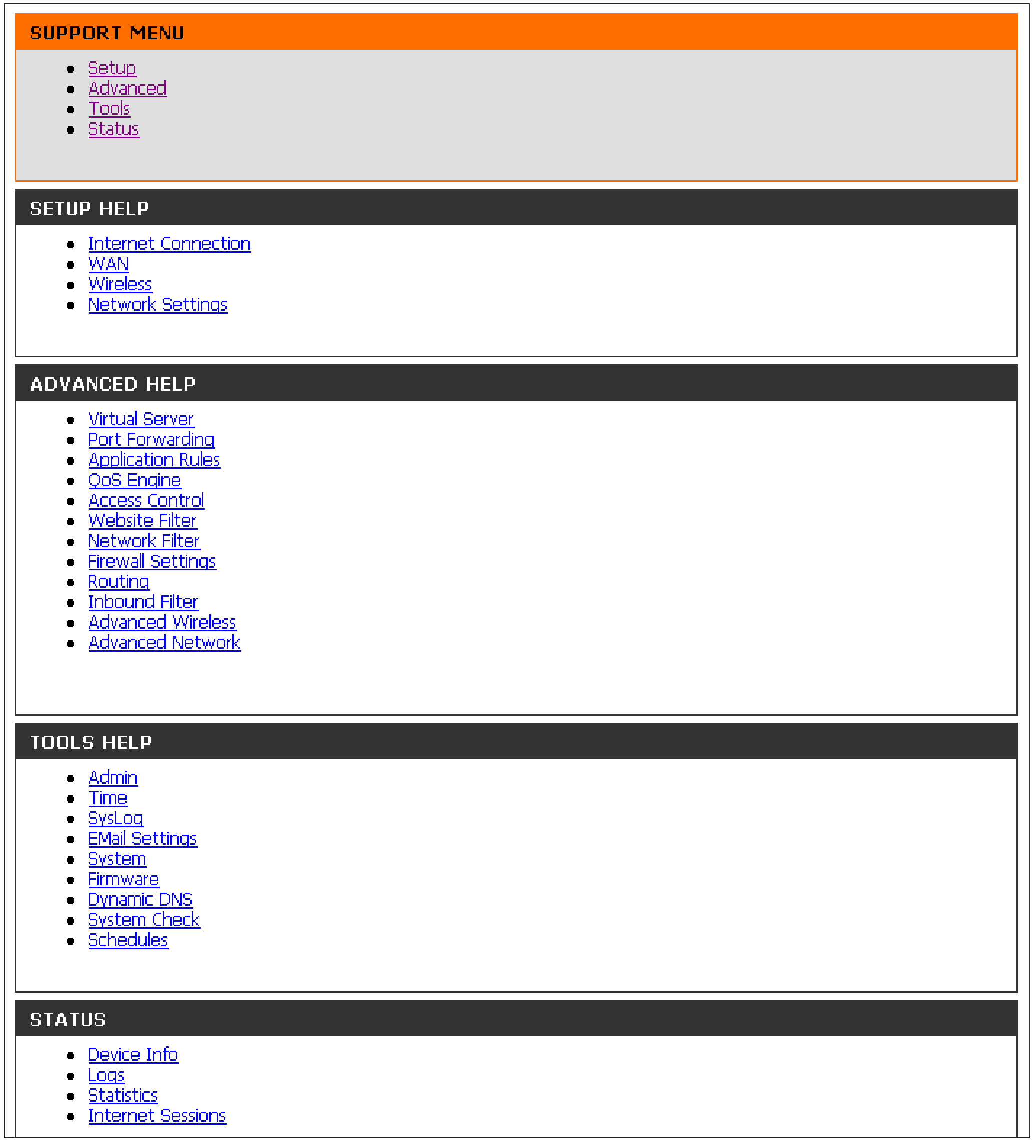
MAC Address	IP Address	Mode	Rate	Signal(%)

Helpful Hints...

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

More...

Support



SUPPORT MENU

- Setup
- Advanced
- Tools
- Status

SETUP HELP

- Internet Connection
- WAN
- Wireless
- Network Settings

ADVANCED HELP

- Virtual Server
- Port Forwarding
- Application Rules
- QoS Engine
- Access Control
- Website Filter
- Network Filter
- Firewall Settings
- Routing
- Inbound Filter
- Advanced Wireless
- Advanced Network

TOOLS HELP

- Admin
- Time
- SysLog
- EMail Settings
- System
- Firmware
- Dynamic DNS
- System Check
- Schedules

STATUS

- Device Info
- Logs
- Statistics
- Internet Sessions

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-601 offers the following types of security:

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

What is WPA?

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

The 2 major improvements over WEP:

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

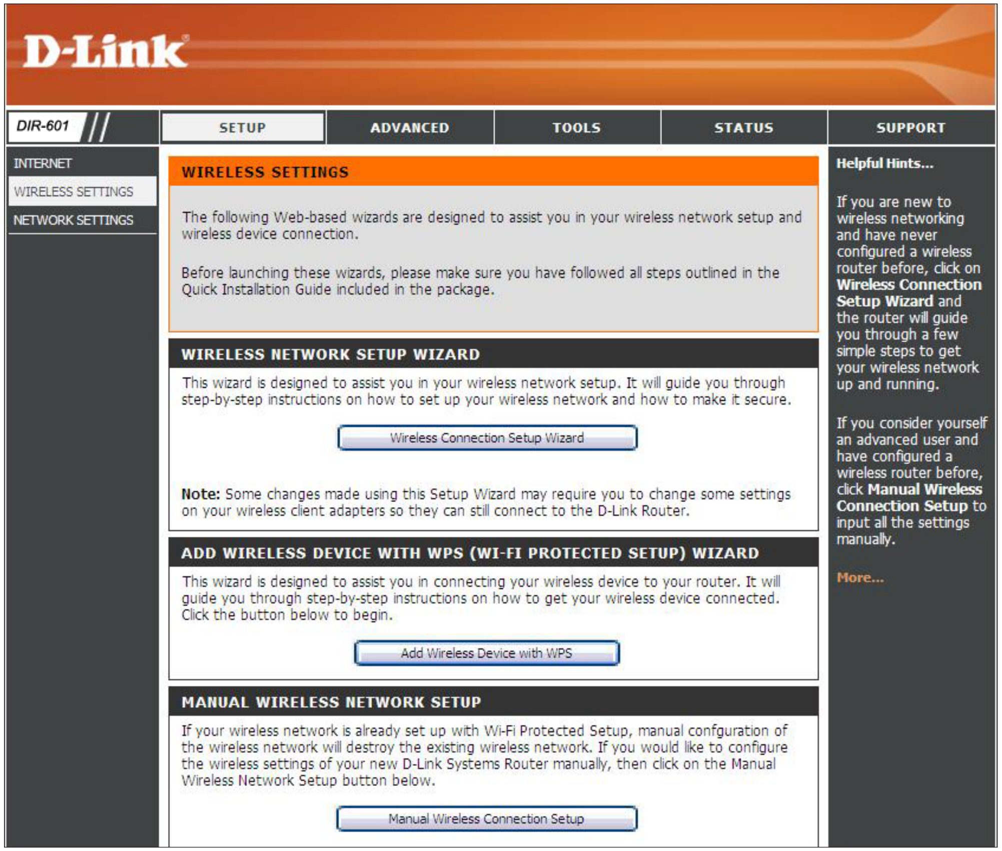
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key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

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

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

Wireless Connection Setup Wizard

To run the security wizard, browse to the Setup page and then click the **Wireless Connection Setup Wizard** button.


D-Link
DIR-601
SETUP
ADVANCED
TOOLS
STATUS
SUPPORT
INTERNET
WIRELESS SETTINGS
NETWORK SETTINGS
Wireless Connection Setup Wizard
Add Wireless Device with WPS
Manual Wireless Connection Setup
More...

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 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

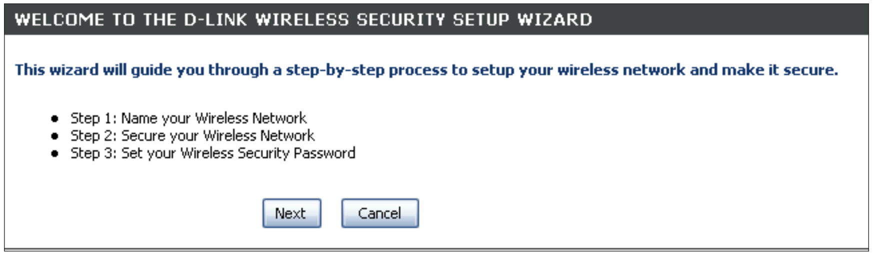
If your wireless network is already set up with Wi-Fi Protected Setup, manual confguration of the wireless network will destroy the existing wireless network. If you would like to configure the wireless settings of your new D-Link Systems Router manually, then click on the Manual Wireless Network Setup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

Helpful Hints...

If you 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.

Click **Next** to continue.



WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

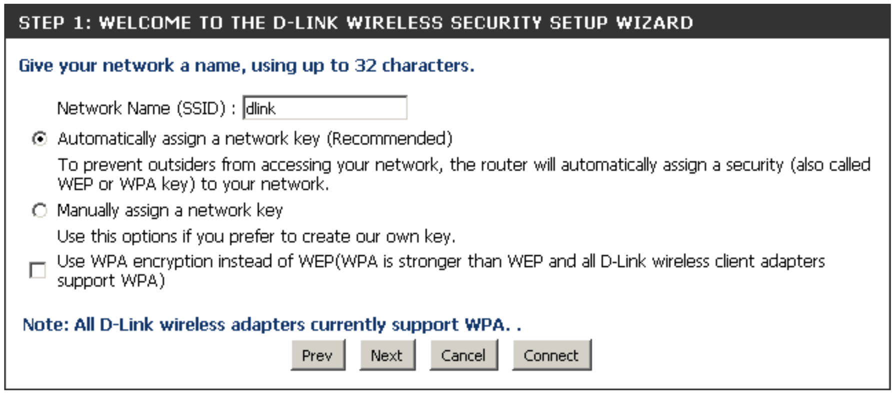
This wizard will guide you through a step-by-step process to setup your wireless network and make it secure.

- Step 1: Name your Wireless Network
- Step 2: Secure your Wireless Network
- Step 3: Set your Wireless Security Password

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

Select **Automatically assign a network key** to have the router create a security key for you or select **Manually assign a network key** if you would like to create your own security key or passphrase.

If you want to use WPA, check the **Use WPA encryption instead of WEP** box.



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

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

Network Name (SSID) : dlink

● 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.

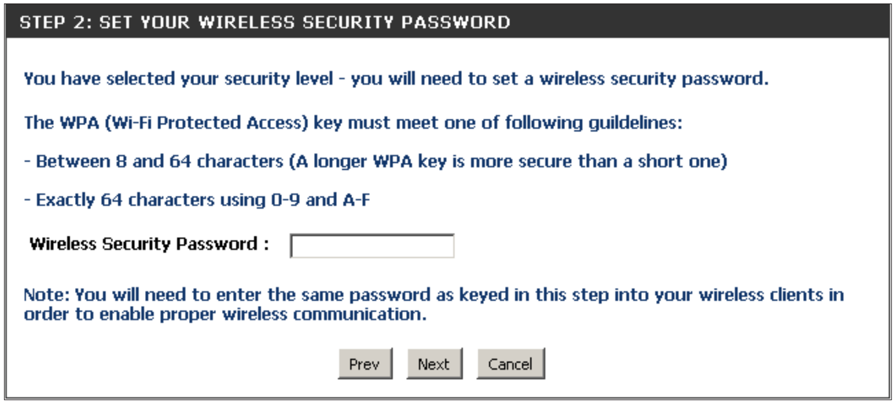
○ Manually assign a network key

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

□ Use WPA encryption instead of WEP(WPA is stronger than WEP and all D-Link wireless client adapters support WPA)

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

If you select **Manually assign a network key**, enter your encryption key in the box and click **Next** to continue. You will need to enter this key on your wireless clients to connect to the router.



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 guildelines:

- Between 8 and 64 characters (A longer WPA key is more secure than a short one)

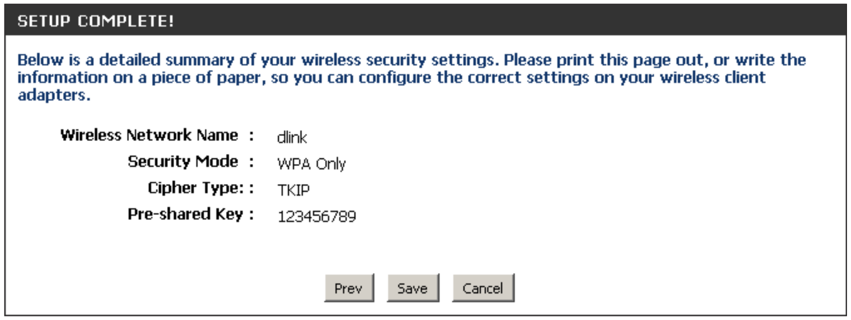
- Exactly 64 characters using 0-9 and A-F

Wireless Security Password :

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

If you selected **Automatically**, the following screen will show you your security key to enter on your wireless clients.

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



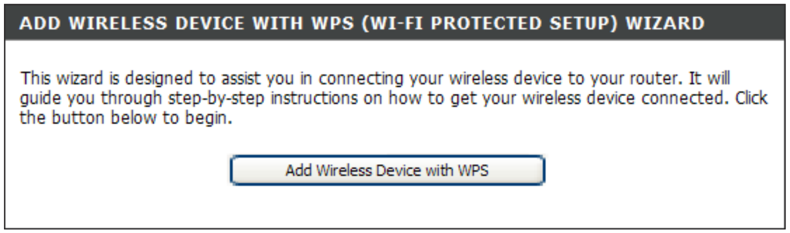
SETUP COMPLETE!

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 Network Name : dlink
Security Mode : WPA Only
Cipher Type: : TKIP
Pre-shared Key : 123456789

Add Wireless Device with WPS Wizard

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

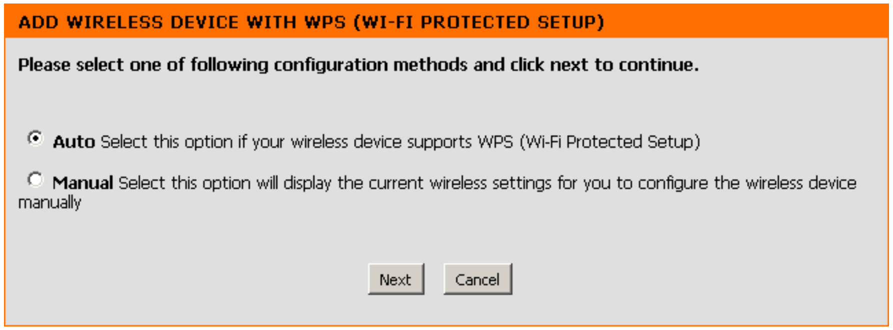


ADD WIRELESS DEVICE WITH WPS (WI-FI PROTECTED SETUP) WIZARD

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

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



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

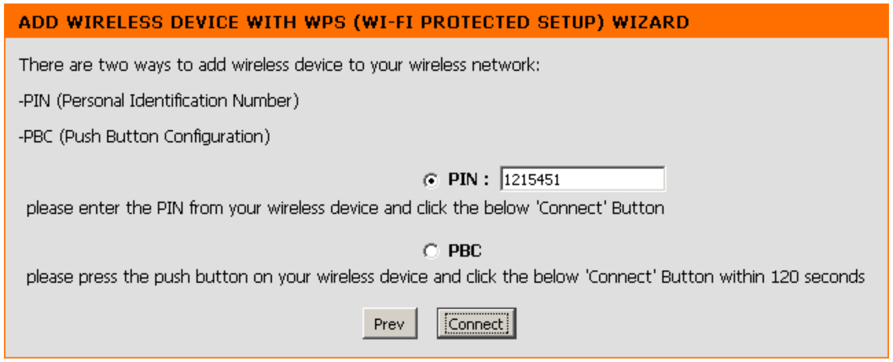
Please select one of following configuration methods and click next to continue.

● **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

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 :** 1215451

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

Configure WPA-Personal (PSK)

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

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. Select the Manual Wireless Connection Setup button.

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

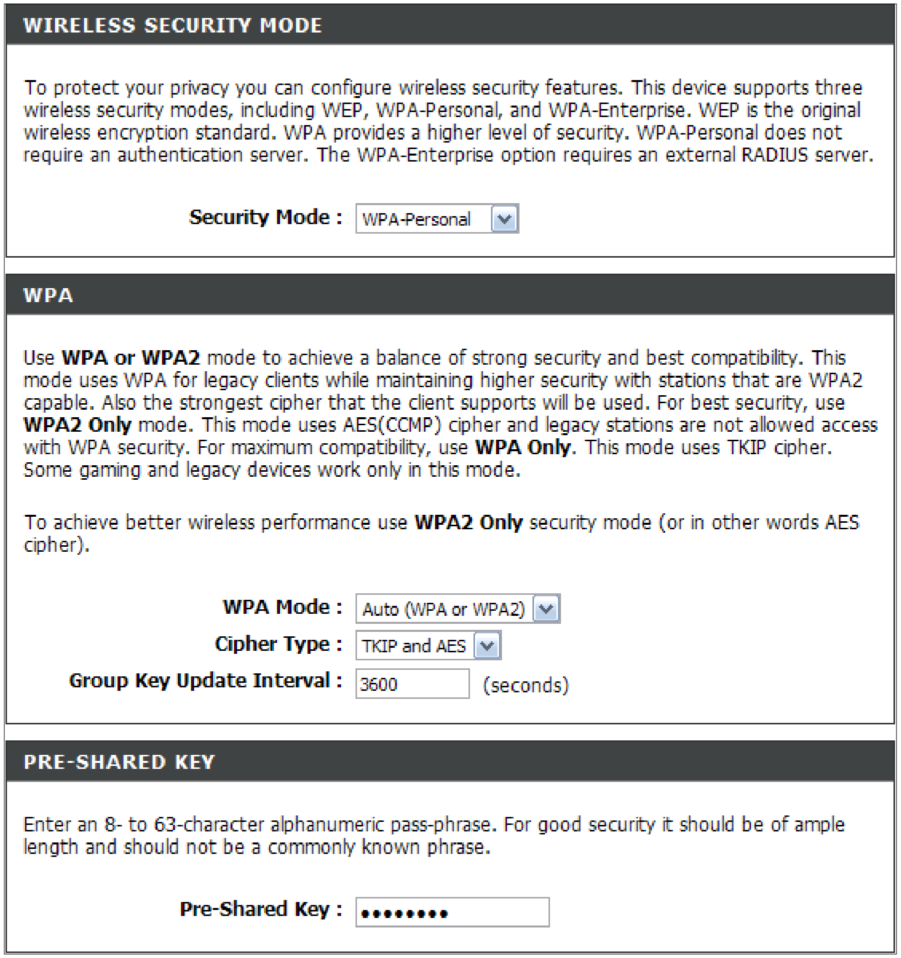
4. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.

5. Next to *Cypher Type*, select **TKIP and AES**, **TKIP**, or **AES**. If you have wireless clients that use both types, use **TKIP and AES**.

6. 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).

7. 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.

8. 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-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. Select the Manual Wireless Connection Setup button.

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

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

5. Next to *Cypher Type*, select **TKIP and AES**, **TKIP**, or **AES**. If you have wireless clients that use both types, use **TKIP and AES**.

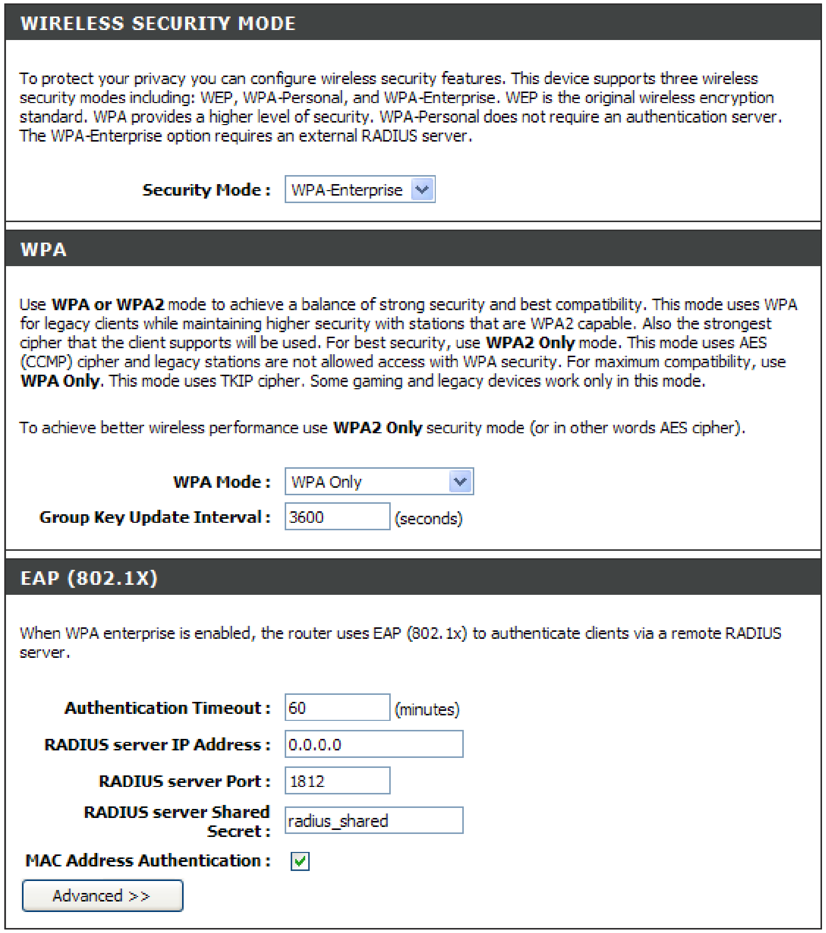
6. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).

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

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

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

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



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-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 : WPA Only

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.

Authentication Timeout : 60 (minutes)

RADIUS server IP Address : 0.0.0.0

RADIUS server Port : 1812

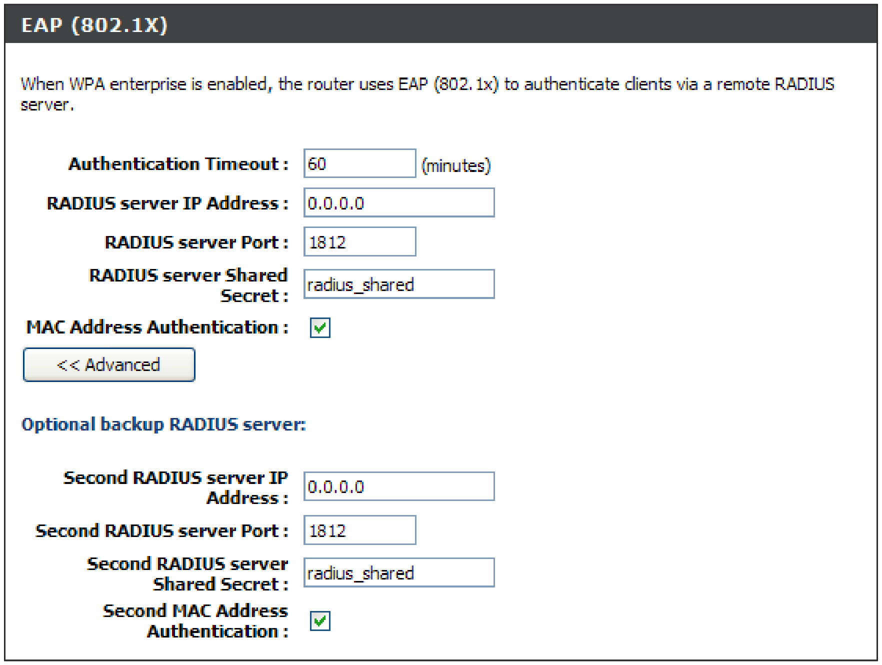
RADIUS server Shared Secret : radius_shared

MAC Address Authentication : ☑

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

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

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



EAP (802.1X)

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

Authentication Timeout : 60 (minutes)

RADIUS server IP Address : 0.0.0.0

RADIUS server Port : 1812

RADIUS server Shared Secret : radius_shared

MAC Address Authentication : ☑

Optional backup RADIUS server:

Second RADIUS server IP Address : 0.0.0.0

Second RADIUS server Port : 1812

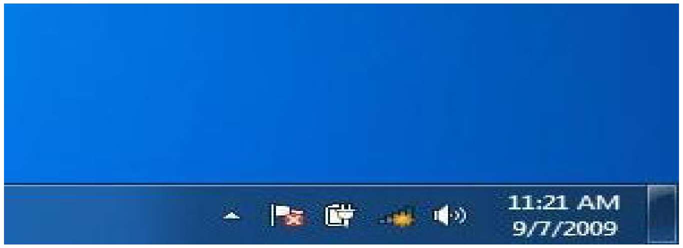
Second RADIUS server Shared Secret : radius_shared

Second MAC Address Authentication : ☑

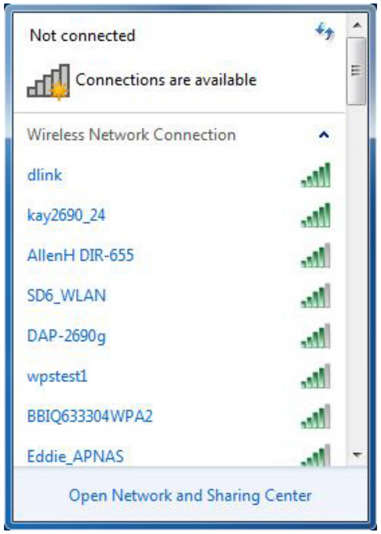
Connect to a Wireless Network
Using Windows® 7

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

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



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



Not connected

Connections are available

Wireless Network Connection

dlink

kay2690_24

AllenH DIR-655

SD6_WLAN

DAP-2690g

wpstest1

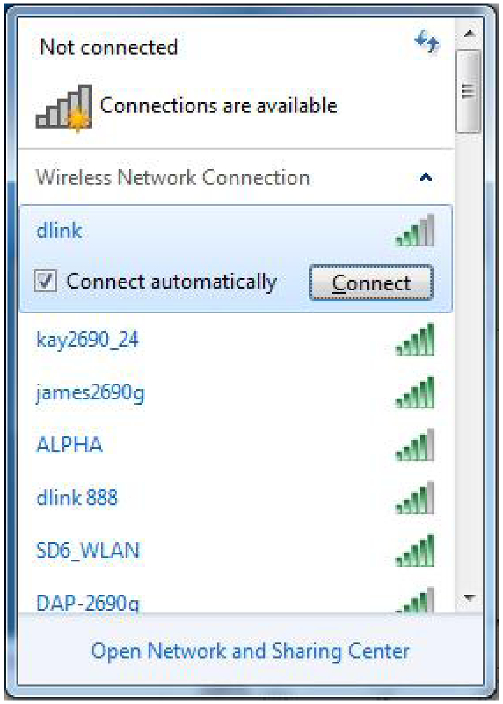
BBIQ633304WPA2

Eddie_APNAS

Open Network and Sharing Center

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

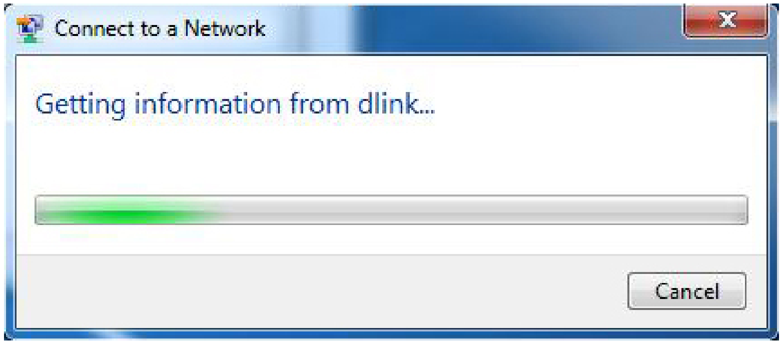
   If you get a good signal but cannot access the Internet, check your TCP/IP settings for your wireless adapter. Refer to the Networking Basics section in this manual for more information.



Not connected

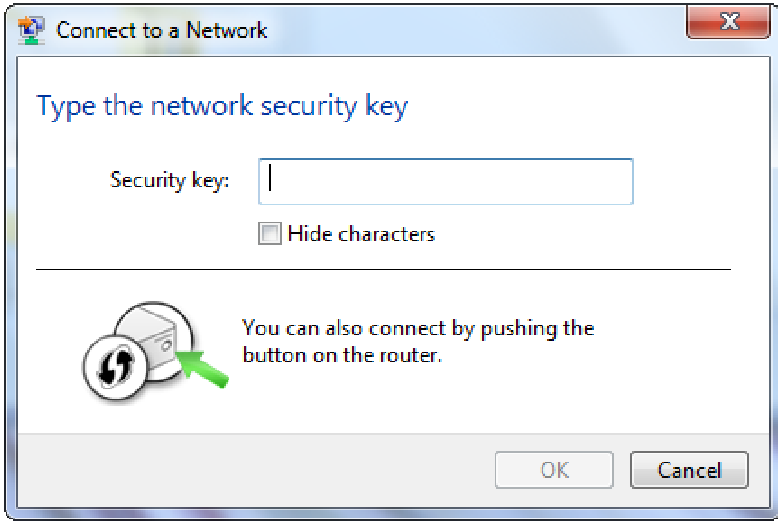
Connections are available

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 Ok.



Connect to a Network

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.

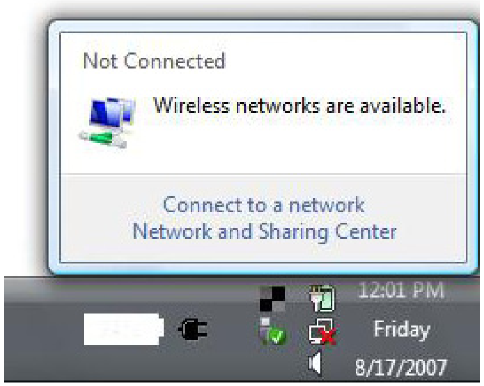
Using Windows Vista®

Windows Vista® users may use the built-in wireless utility. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network. Most utilities will have a "site survey" option similar to the Windows 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**.

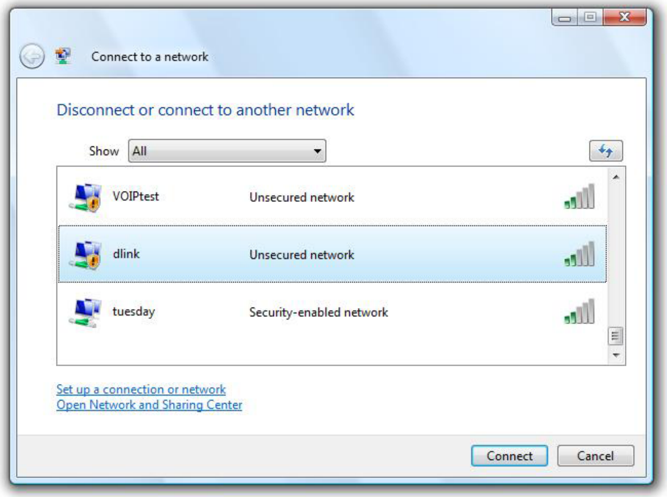


Not Connected

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

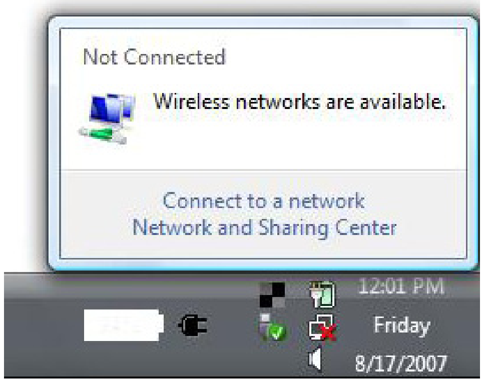
VOIPtest	Unsecured network	
dlink	Unsecured network	
tuesday	Security-enabled network	

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

Configure 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.

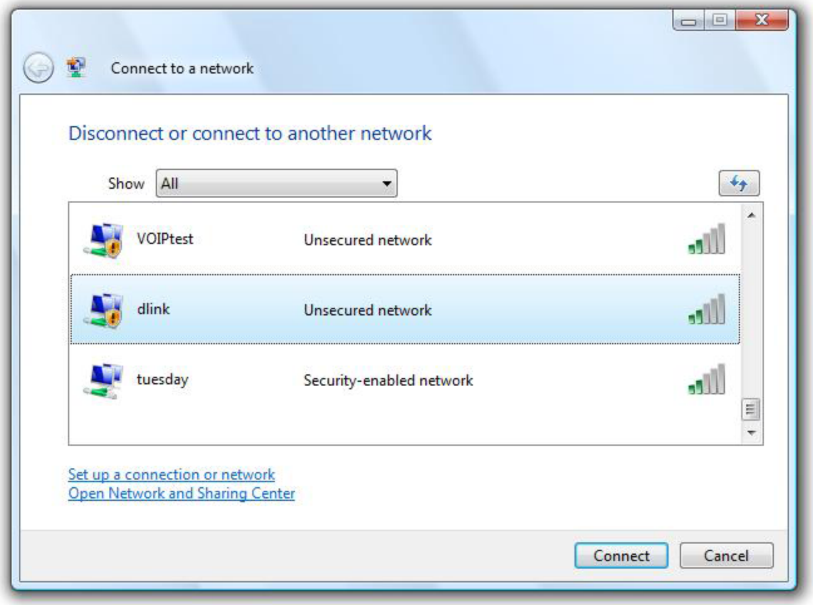
1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.



Not Connected

Wireless networks are available.

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



Connect to a network

Disconnect or connect to another network

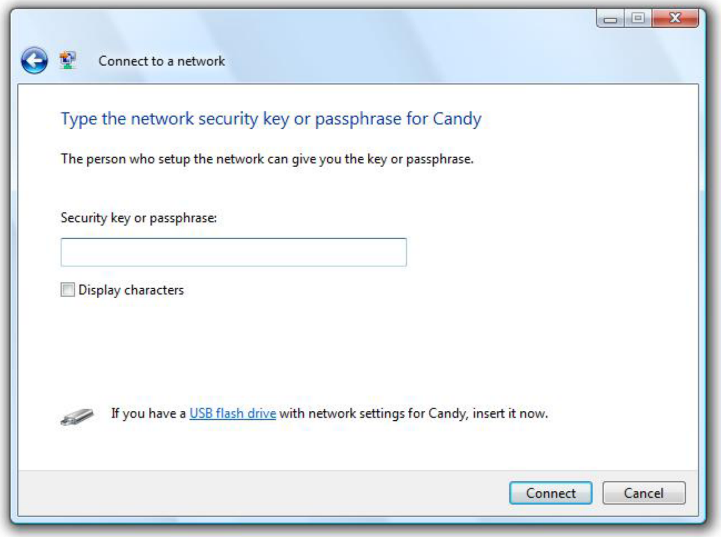
Show: All

VOIPtest	Unsecured network	
dlink	Unsecured network	
tuesday	Security-enabled network	

Set up a connection or network
Open Network and Sharing Center
Connect
Cancel

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.



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

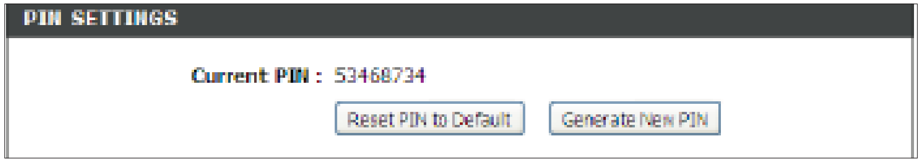
If you have a USB flash drive with network settings for Candy, insert it now.

Connect Using 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.



PIN SETTINGS

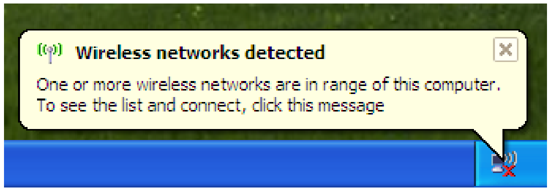
Current PIN : 53468734

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.

Using Windows® XP

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

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

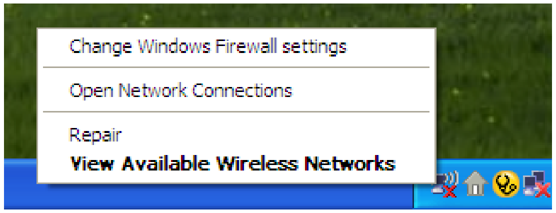


Wireless networks detected

One or more wireless networks are in range of this computer. To see the list and connect, click this message

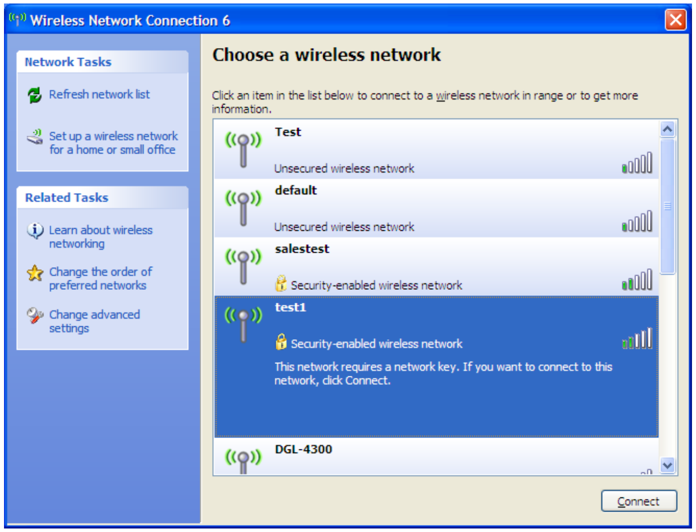
or

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.


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

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

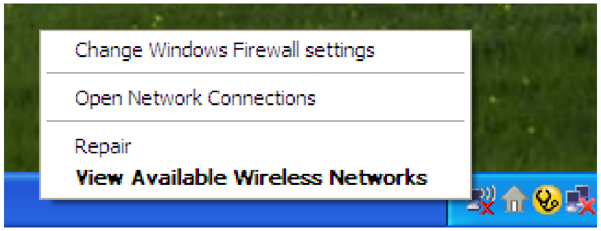
test1
Security-enabled wireless network
This network requires a network key. If you want to connect to this network, click Connect.

DGL-4300

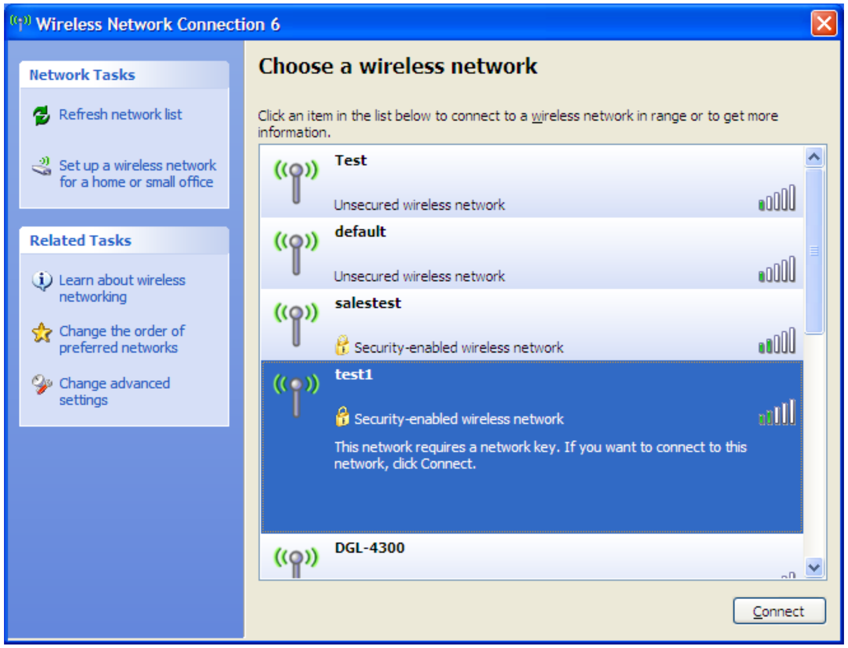
Configure WPA-PSK

It is recommended to enable WEP 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 WEP 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

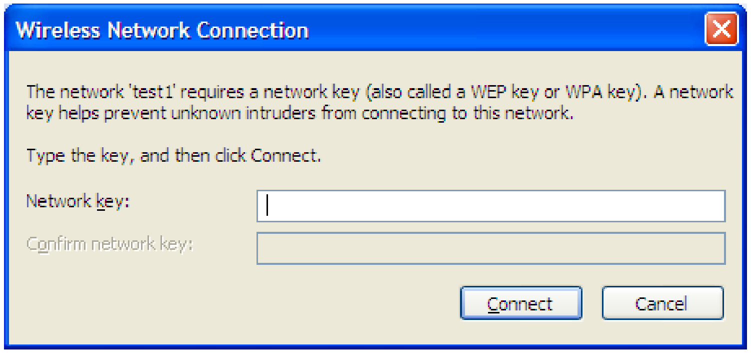
salestest
Security-enabled wireless network

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.


Wireless Network Connection

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-601. 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 screen shots on your computer will look similar to the following examples.)

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

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website on the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

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

    - Microsoft Internet Explorer® 6.0 and higher
    - Mozilla Firefox 3.0 and higher
    - Google™ Chrome 2.0 and higher
    - Apple Safari 3.0 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 the web management.

- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

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

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

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

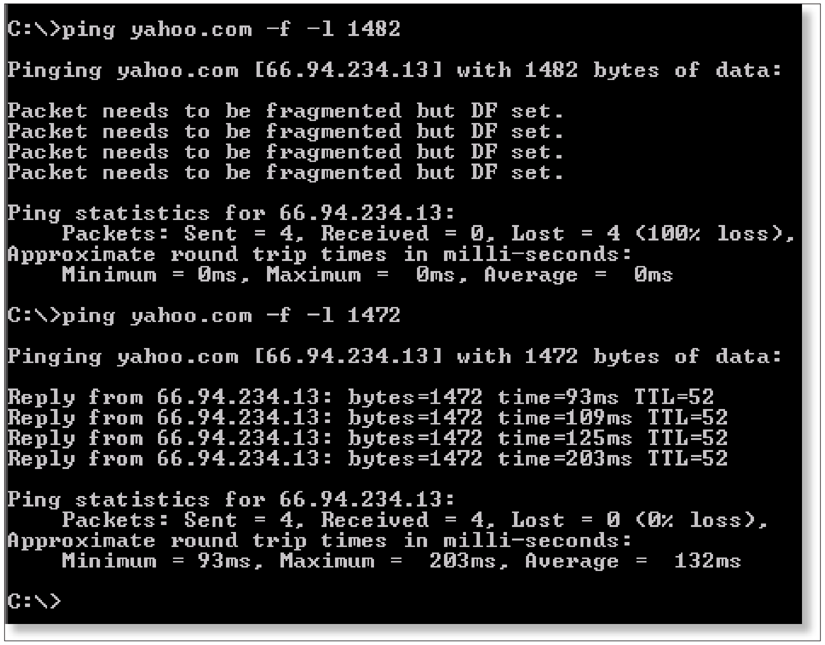
Note: AOL DSL+ users must use MTU of 1400.

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 e-mail. If changing the MTU does not resolve the problem, continue changing the MTU in increments of ten.

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

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

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

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

- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-601 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

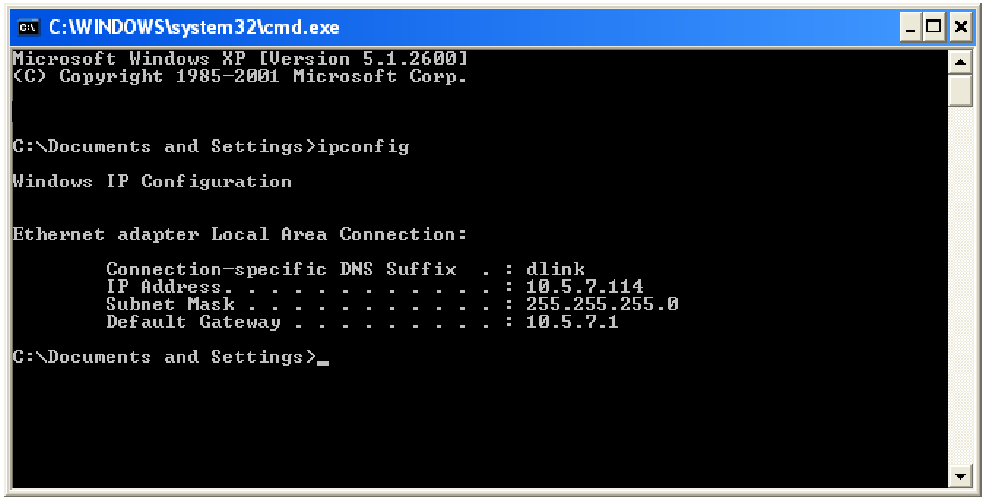
After you install your adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

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

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

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

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



```
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 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

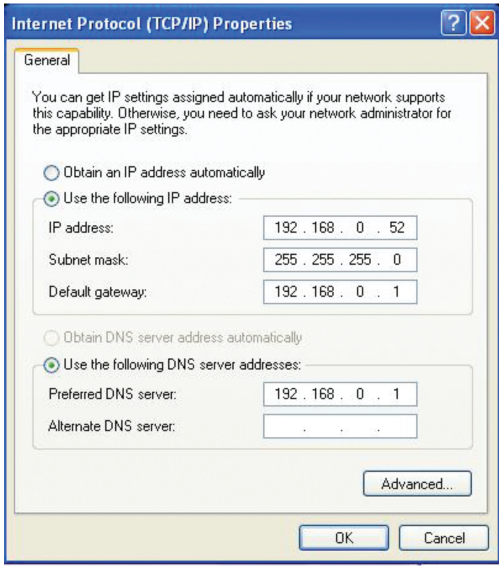
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

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 802.3
- IEEE 802.3u

Security

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

Data Rates*

MSC (0-15)

- 6.5Mbps (13.5)
- 13Mbps (27)
- 19.5Mbps (40.5)
- 26Mbps (54)
- 39Mbps (81)
- 52Mbps (108)
- 58.5Mbps (121.5)
- 65Mbps (135)

- 7.2Mbps (15)
- 14.4Mbps (30)
- 21.7Mbps (45)
- 28.9Mbps (60)
- 43.3Mbps (90)
- 57.8Mbps (120)
- 65Mbps (135)
- 72.2Mbps (150)

Frequency Range

- 2.4GHz to 2.4835GHz

Transmitter Output Power

- 18.7dBm (average)

LEDs

• Power • Internet
• WLAN • LAN (10/100)

Operating Temperature

- 32°F to 104°F (0°C to 40°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- IC

Dimensions

- L = 4.6 inches
- W = 5.75 inches
- H = 1.2 inches

Warranty

- 1 Year Limited

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

Contacting Technical Support

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

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

- Model number of the product (e.g. DIR-601)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev B1))
- Serial Number (s/n number located on the label on the bottom of the router).

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

For customers within the United States:

Phone Support:
(877) 453-5465

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

For customers within Canada:

Phone Support:
(800) 361-5265

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

Warranty

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

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

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

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

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

Limited Software Warranty:
D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Software Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional

specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

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

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

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

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

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

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

What Is Not Covered:

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

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

Disclaimer of Other Warranties:

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

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

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

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

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

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

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.

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

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

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

IMPORTANT NOTE:

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

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.

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

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

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.

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

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

Registration

Register your product online at registration.dlink.com

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 2.1
July 5, 2011