



User Manual

Gaming Router AC1300

DGL-5500

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	August 14, 2013	• Initial release for Revision A1 (based on Firmware v1.01 B5)

Trademarks

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

Copyright © 2013 by D-Link Systems, Inc.

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

Table of Contents

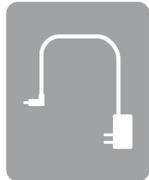
Preface	i	Internet Connection Setup Wizard.....	27
Manual Revisions.....	i	Wireless Settings.....	31
Trademarks	i	802.11n/g (2.4GHz).....	31
Product Overview	1	802.11ac/n/a (5GHz)	32
Package Contents.....	1	Wireless Security	33
System Requirements.....	2	What is WPA?	33
Introduction	3	WPA/WPA2-Personal (PSK)	34
Hardware Overview.....	4	Configure WPA/WPA2-Enterprise (RADIUS)....	35
Connections	4	Network Settings	36
LEDs	5	Router Settings	36
Installation	6	DHCP Server Settings	37
Before you Begin.....	6	DHCP Reservation.....	39
Wireless Installation Considerations.....	7	StreamBoost	40
Connect to your Network.....	8	Advanced.....	41
Connect to an Existing Router	11	Server	41
Configuration	13	Virtual Server	42
Quick Setup Wizard.....	14	Port Forwarding.....	43
Web-based Configuration Utility	19	Firewall Settings.....	44
My Network	20	Filter	45
Active Devices.....	20	Access Control.....	45
Priorities	22	Access Control Wizard	45
Setup	23	Inbound Filter.....	48
Static (assigned by ISP)	24	MAC Filtering Rules	49
Dynamic (Cable).....	25	Web Filtering Rules.....	50
PPPoE (DSL).....	26	DMZ	51
		Schedules	52

Maintenance.....	53	Wireless Basics	82
Admin.....	53	What is Wireless?.....	83
Time	54	Tips.....	85
System	55	Wireless Modes.....	86
Firmware Upgrade.....	55	Networking Basics	87
Status	56	Check your IP address.....	87
Device Info	56	Windows® 8 Users.....	87
Logs.....	57	Windows® 7/Vista® Users.....	87
Statistics	58	Windows® XP Users.....	87
Usage in Time	58	Statically Assign an IP Address	88
Usage by Data	59	Windows® 8 Users	88
Activity Tracker.....	60	Windows® 7/ Vista® Users	89
Connect a Wireless Client to your Router	61	Windows® XP Users.....	90
WPS Button.....	61	Technical Specifications	91
Windows® 8.....	62	Contacting Technical Support	92
Windows® 7.....	64	GPL Code Statement.....	93
WPA/WPA2	64	Warranty.....	105
WPS.....	67	Registration	112
Windows Vista®	71		
WPA/WPA2	72		
WPS/WCN 2.0	74		
Windows® XP	75		
WPA/WPA2	76		
Troubleshooting	78		
Reset Router/Forgot Password	79		

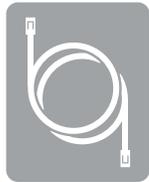
Package Contents



DGL-5500 Gaming Router



Power Adapter



Ethernet Cable



Wi-Fi Configuration Card



Quick Install Guide

If any of the above items are missing, please contact your reseller.

Note: Using a power supply with a different voltage rating than the one included with the DGL-5500 will cause damage and void the warranty for this product.

System Requirements

Network Requirements	<ul style="list-style-type: none">• An Ethernet-based broadband modem
Web-based Configuration Utility Requirements	<p>Computer with the following:</p> <ul style="list-style-type: none">• Windows®, Macintosh, or Linux-based operating system• An installed Ethernet adapter or wireless adapter <p>Supported Browsers:</p> <ul style="list-style-type: none">• Internet Explorer 7 or higher• Firefox• Safari 4 or higher• Chrome <p>Windows® Users: Make sure you have the latest version of Java installed. Visit www.java.com to download the latest version.</p>

Introduction

The DGL-5500 Wireless AC1300 Gaming Router provides revolutionary Gigabit 802.11ac wireless speed - up to 1300Mbps – for flawless HD video streaming to multiple devices.

The integrated StreamBoost QoS engine intelligently prioritizes bandwidth to make lag and buffering a thing of the past. StreamBoost manages your connection automatically, and gives you the power to manually route more bandwidth to a specific activity – or even to a specific device -- intuitively creating optimal allocation. That means lag free gaming, crystal clear FaceTime® calls, and ultra smooth HD streaming.

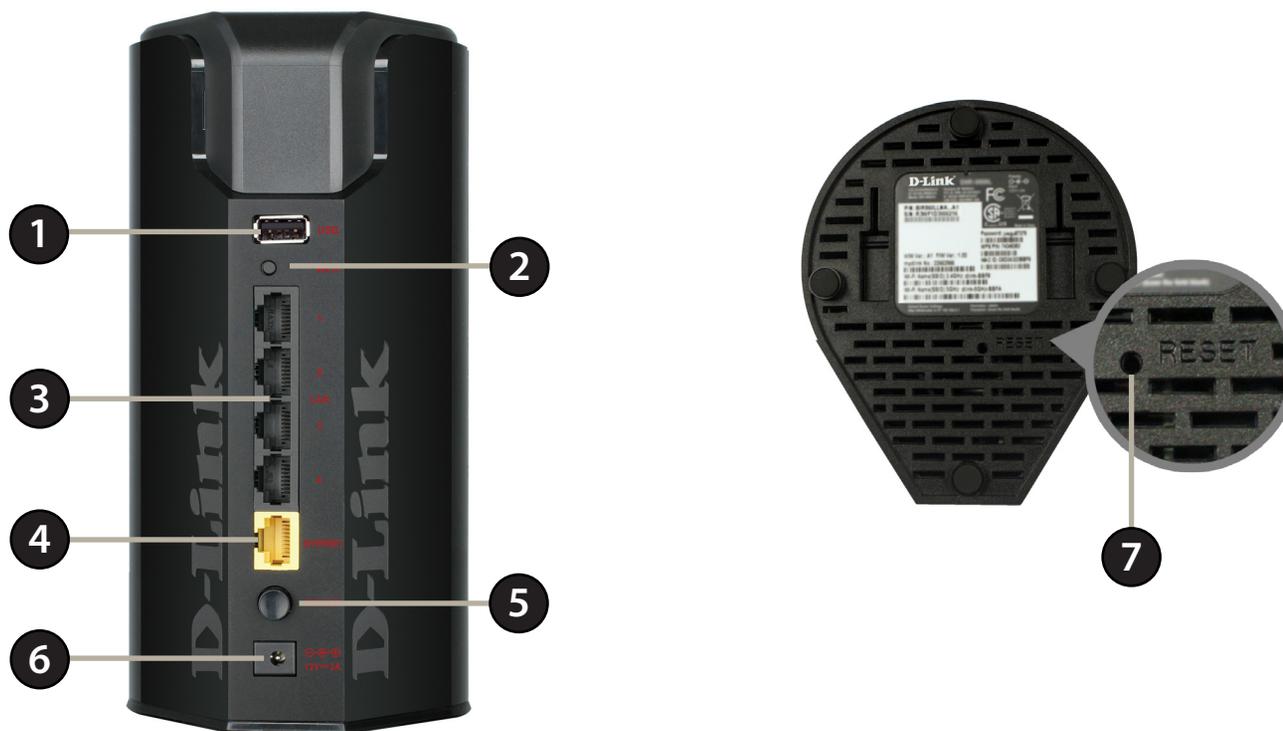
What does Wireless AC mean for your home network? Flawless HD video streaming, faster gaming, and lag-free Skype™ and Facetime® calls, all with less Wi-Fi interference for smooth, lightning-fast performance. And while your home gains all the cutting-edge benefits of AC, the Wireless AC1300 Dual Band Gigabit Cloud Router is also compatible with all of your current Wireless N products. And with four Gigabit ports, you can give your media players and gaming consoles more speed than you dreamed possible.

The DDGL-5500 router delivers Dual Band Technology for intelligent, versatile, interference-free bandwidth. Check your email and surf the Internet on the 2.4GHz band; or game, make Skype™ calls and stream HD movies to multiple devices using the cleaner, interference-free 5GHz band. Whatever you like to do online, Dual Band has you covered.

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

Hardware Overview

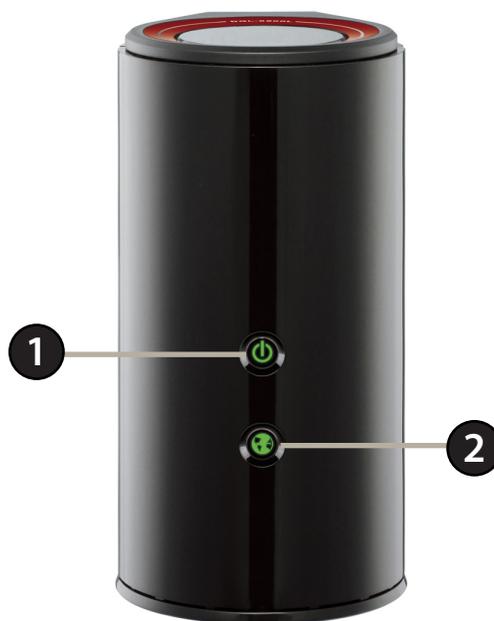
Connections



1	USB Port	Connect a USB printer to share on your network.
2	WPS Button	Press to start the WPS process. The Power LED will start to blink.
3	LAN Ports (1-4)	Connect Ethernet devices such as computers, switches, and game consoles.
4	Internet Port	Connect your broadband modem to this port using an Ethernet cable.
5	Power Button	Press to power the router on and off.
6	Power Port	Connect the supplied power adapter.
7	Reset Button	Press and hold the reset button with a paper clip for six seconds to reset the router to the factory default settings.

Hardware Overview

LEDs



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

Installation

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

Before you Begin

- **Users with DSL providers** - If you are using a PPPoE connection, you will need your PPPoE user name and password. If you do not have this information, contact your Internet provider. Do not proceed until you have this information.
- **Users with Cable providers** - Make sure you unplug the power to your modem. In some cases, you may need to turn it off for up to 5 minutes.
- **Advanced Users** - If your ISP provided you with a modem/router combo, you will need to set it to “bridge” mode so the DGL-5500 router can work properly. Please contact your ISP or refer to the user manual for your modem/router device.

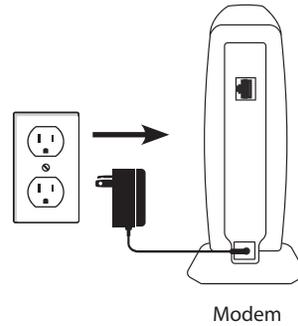
Wireless Installation Considerations

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:

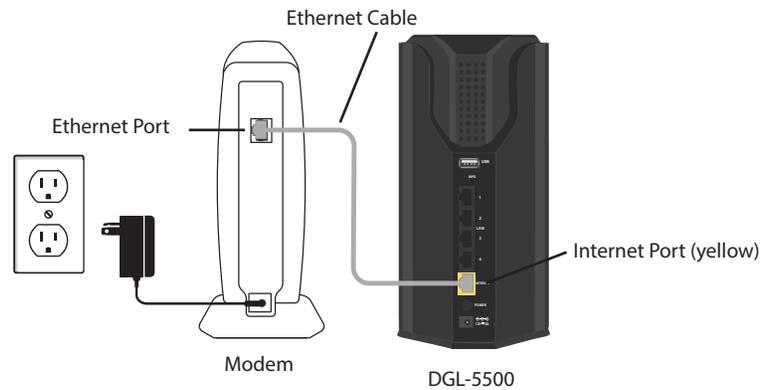
1. Keep the number of walls and ceilings between the D-Link router and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between 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 is not in use.

Connect to your Network

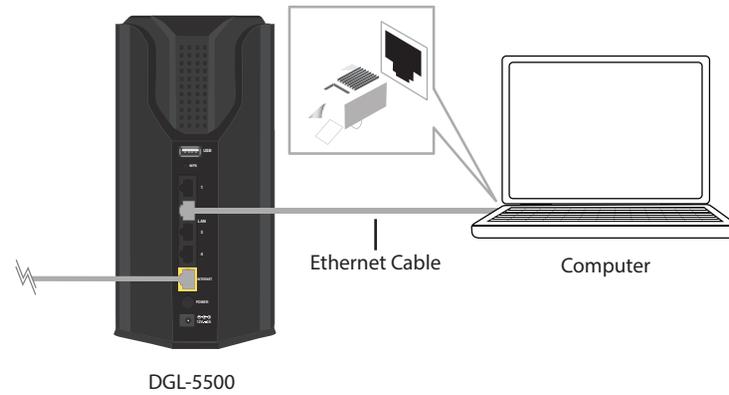
1. Turn off and unplug your DSL or Cable modem. This is required.



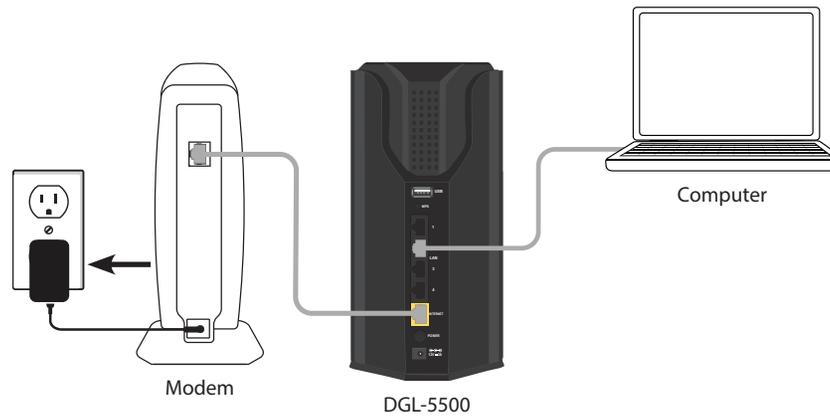
2. Connect an Ethernet cable from the Internet port of the router to the Ethernet port on your DSL or Cable modem.



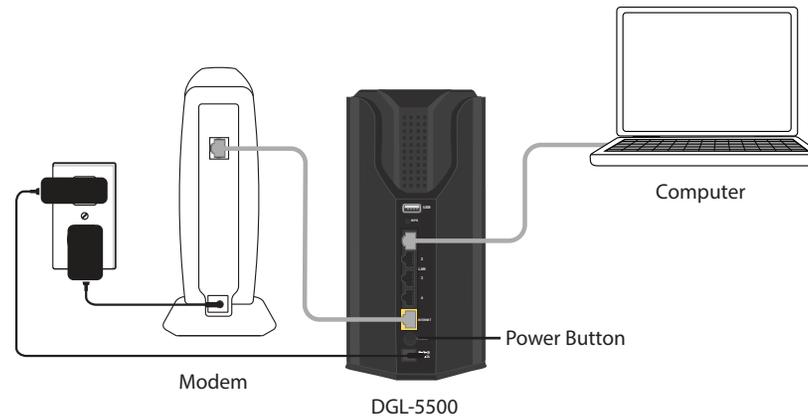
3. Connect another Ethernet cable from the Ethernet port on your computer to one of the LAN ports on the router.



4. Plug the power back into your DSL or Cable modem. Please wait about one minute before continuing.



5. Plug the power adapter into your router and connect to an available power outlet or surge protector. If the Power LED does not light up, press the Power button on the back of the router.



6. After the router has powered up, verify that the power (green) and Internet (orange or green) LEDs are both lit. Please skip to page 18 to configure your router and use the manual setup procedure to configure your network and wireless settings. If you did not connect to the Internet, use the D-Link Setup Wizard (refer to page 14).

Connect to an Existing Router

Note: It is strongly recommended to replace your existing router with the DGL-5500 instead of using both. If your modem is a combo router, you may want to contact your ISP or refer to the manufacturer's user guide to put the router into Bridge mode, which will 'turn off' the router (NAT) functions.

If you are connecting the DGL-5500 router to an existing router to use as a wireless access point and/or switch, you will have to do the following to the DGL-5500 before connecting it to your network:

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

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

1. Plug the power into the router. Connect one of your computers to the router (LAN port) using an Ethernet cable. Make sure your IP address on the computer is 192.168.0.xxx (where xxx is between 2 and 254). Please see the **Networking Basics** section for more information. If you need to change the settings, write down your existing settings before making any changes. In most cases, your computer should be set to receive an IP address automatically in which case you will not have to do anything to your computer.
2. Open a web browser, enter **http://192.168.0.1** (or **http://dlinkrouter.local./**) 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 **Firewall Settings**. Uncheck the **Enable UPnP** checkbox. Click **Save Settings** to continue and then click **Restart Later**.
4. Click **Setup** and then click **Network Settings**. Uncheck the **Enable DHCP Server** checkbox. Click **Save Settings** to continue.

5. Under *Router Settings*, enter an available IP address and the subnet mask of your network. Click **Save Settings** to save your settings and then click **Restart Now**. You will need to use this new IP address to access the configuration utility of the router in the future. Close the browser and change your computer's IP settings back to the original values as in Step 1.
6. Disconnect the Ethernet cable from the router and reconnect your computer to your network.
7. Connect an Ethernet cable in one of the **LAN** ports of the router and connect it to your other router. Do not plug anything into the Internet (WAN) port of the D-Link router.
8. You may now use the other three 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** section for more information on setting up your wireless network.

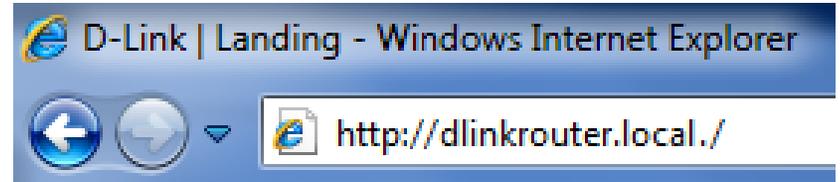
Configuration

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

- **D-Link Setup Wizard** - This wizard will launch when you log into the router for the first time. Refer to the next page.
- **Manual Setup** - Log into the router and manually configure your router (advanced users only). Refer to page 19.

Quick Setup Wizard

If this is your first time installing the router, launch your web browser (e.g., Internet Explorer, Firefox, Safari, and Chrome), and enter **http://dlinkrouter.local/** or the router's IP address (default is 192.168.0.1).



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

Note: *If you are directed to the login screen, you have a dynamic connection, and the Internet LED is green, you should be connected to the Internet and do not need to continue.*

Click **Next** to continue.



Please wait while your router detects your internet connection type. If the router detects your Internet connection, you may need to enter your ISP information such as username and password. (See instructions on page 16 for PPPoE and Static IP).

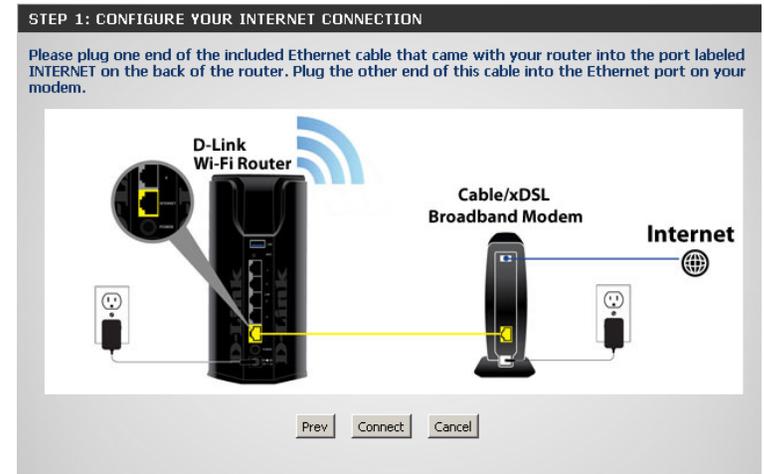


If the router does not detect a valid Ethernet connection from the Internet port, this screen will appear. Connect your broadband modem to the Internet port and then click **Connect**.

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

Select your Internet connection type. You can select **Username / Password Connection (PPPoE)** if you are using a PPPoE connection (common with DSL), or select **Static IP Address Connection** if your IP settings are supplied to you by your ISP.

Click **Next** to continue.



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

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

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

Click either **I want automatic StreamBoost updates** or **I decline automatic StreamBoost updates**. Click **Next** to continue.

SET USERNAME AND PASSWORD CONNECTION (PPPOE)

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

User Name :

Password :

Prev Next Cancel

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 :

Subnet Mask :

Gateway Address :

DNS SETTINGS

Primary DNS Address :

Secondary DNS Address :

Prev Next Cancel

STEP 2: STREAMBOOST AUTO UPDATES

Maximize your online experience by keeping StreamBoost up to date.

Check below to enable your router to receive automatic StreamBoost updates during your initial 3-year manufacturer service term. The 3-year service term will start on the day the router is purchased but in no event will be valid beyond April 1st, 2017. (After the 3-year period, further updates may be made available from the manufacturer via firmware updates.) StreamBoost updates may help improve your router's Internet traffic management capabilities through better traffic identification and bandwidth management techniques. In exchange, your StreamBoost enabled router will send Qualcomm Atheros, Inc. anonymous information from your router. If you decline, you can find updates through software or firmware postings from your router's manufacturer.

[Learn More.](#)

Would you like to receive StreamBoost auto updates?

Yes, I want StreamBoost updates. I opt-in to data analysis and updates.

No, I do not wish to receive updates.

Prev Next

You can keep the **Enable Auto Bandwidth Estimation** box checked to auto-detect your bandwidth or uncheck it to manually enter your download and upload speeds. Click the **Test Bandwidth** button first so the router can detect your speeds. After processing is completed, click **Next** to continue.

STEP 3: STREAMBOOST SETTINGS

Enable StreamBoost Bandwidth Control :

Enable Auto Bandwidth Estimation :

Download Speed(Mbps) :

Upload Speed(Mbps) :

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

STEP 4: 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 :

Enter a Wi-Fi Network Name (SSID) and Wi-Fi Password for both the 2.4GHz and 5GHz bands. Click **Next** to continue.

STEP 5: CONFIGURE YOUR WI-FI SECURITY

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

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

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

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

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

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

Click **Connect** to finish your router setup.

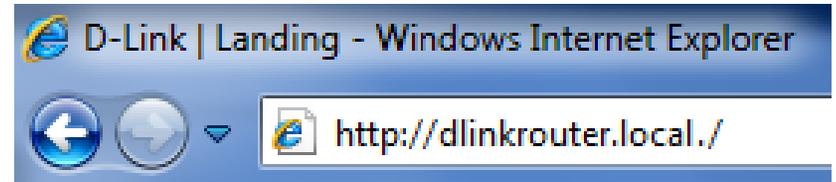


If you want to create a bookmark to the router, click **OK**. Click **Cancel** if you do not want to create a bookmark.



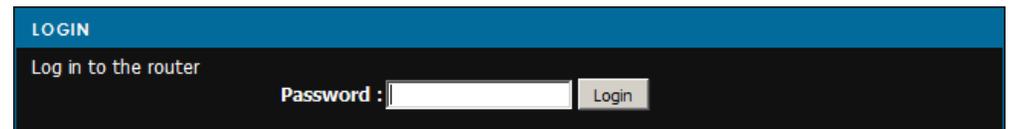
Web-based Configuration Utility

Open a web browser (e.g., Internet Explorer, Chrome, Firefox, or Safari) and enter **http://dlinkrouter.local/** or **http://192.168.0.1**.



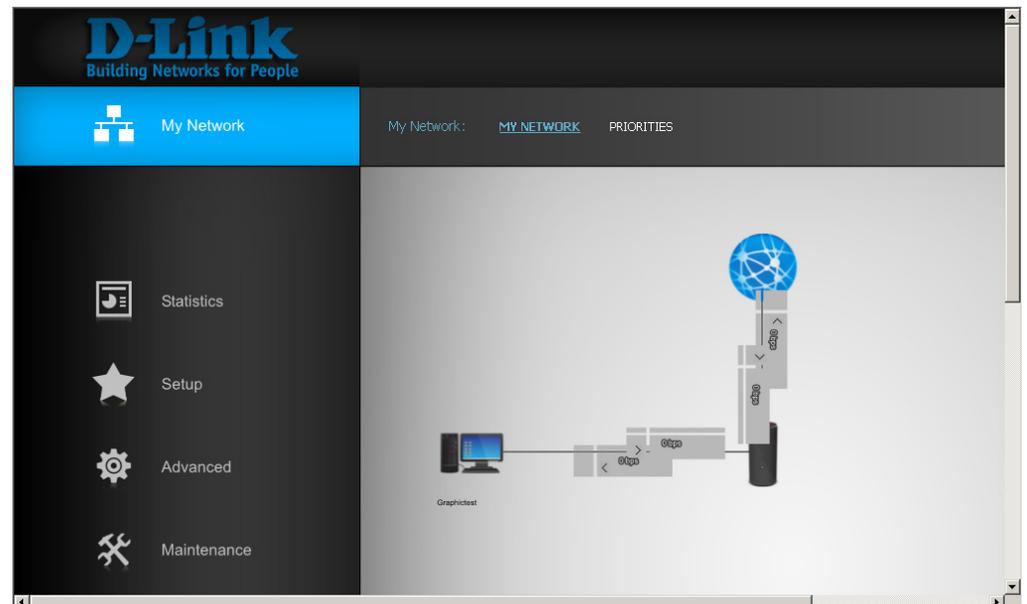
Enter your password and click **Login**.

Note: If you did not create a password with the Setup Wizard, leave the password blank by default.



The My Network page will have a graphical layout of your network. Note that devices connected to the router must be transmitting/receiving data to show up. You can click on any of the devices for more information such as IP address, MAC address, and data statistics.

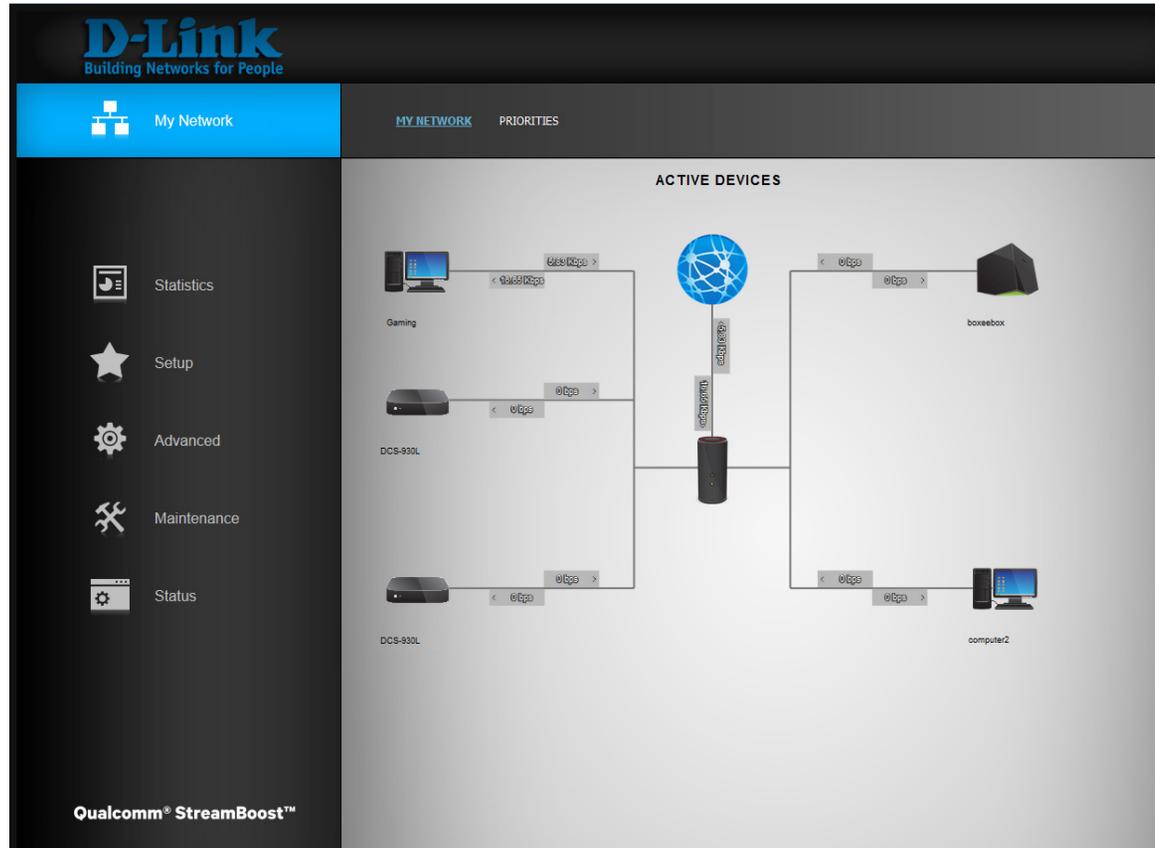
Note: You cannot edit the names or icon images.



My Network

Active Devices

The My Network page will display a graphical diagram of your local network. You can click on the device icon to display more information (refer to the next page). Note that devices may not show up until they transmit data.



When you click on a device more information will appear. Below is an example of the 'Gaming' computer shown in the diagram on the previous page.



Priorities

You can select the priority of each device on your local network. Click the up arrow to move the item higher in the priority list or the down arrow to lower the priority.

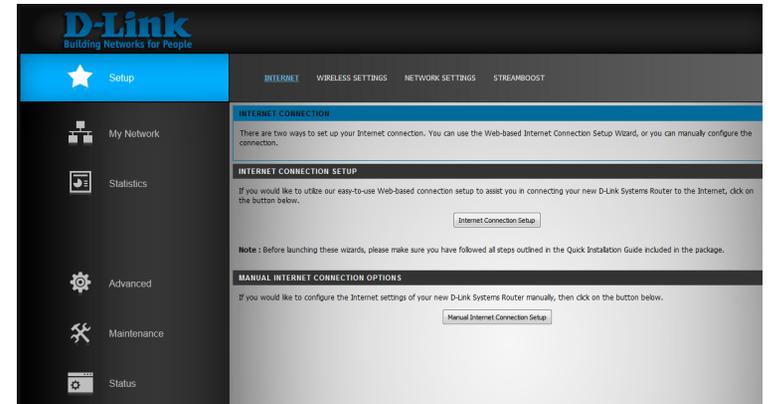
The screenshot shows the D-Link web interface for configuring network priorities. The interface includes a navigation menu on the left with options like Statistics, Setup, Advanced, Maintenance, and Status. The main content area is titled 'PRIORITIES' and contains a list of devices with their priority levels and associated OS or device type. The devices are listed as follows:

Priority	Device Name	OS/Device Type
1	Gaming	Windows
2	computer2	Windows
3	boxeebox	Boxee
4	boxeebox	Boxee
5	f0:b4:79:...	Unknown
6	annas-ipad	iPad
7	192.168.0.20	Unknown

Setup

If you want to configure your router to connect to the Internet using the wizard, click **Internet Connection Setup**. Please refer to page 27.

Click **Manual Internet Connection Setup** to configure your connection manually. (Instructions for manual setup begin below.)



The next few pages will explain each of the ISP connection types. You can select the type from the **My Internet Connection is** drop-down menu.

Manual Internet Setup

Static (assigned by ISP)

Select **Static IP** 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.

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

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

The screenshot shows the WAN configuration page. At the top, there's a 'WAN' header. Below it, a note says: 'Use this section to configure your Internet Connection type. There are several connection types to choose from Static IP, DHCP, PPPoE. If you are unsure of your connection method, please contact your Internet Service Provider.' A sub-note states: 'Note: If using the PPPoE option, you will need to remove or disable any PPPoE client software on your computers.' There are three buttons: 'Save Settings', 'Don't Save Settings', and 'Restart Now'. Below this is the 'INTERNET CONNECTION TYPE' section, which says 'Choose the router mode to connect to the Internet.' and has a dropdown menu set to 'Static IP'. The next section is 'STATIC IP ADDRESS INTERNET CONNECTION TYPE', which says 'Enter the static address information provided by your Internet Service Provider (ISP)'. It contains several input fields: 'IP Address' (10.10.10.22), 'Subnet Mask' (255.0.0.0), 'Default Gateway' (10.10.10.1), 'Primary DNS Server' (10.10.10.1), 'Secondary DNS Server' (4.2.2.2), 'MTU' (1500), and 'MAC Address'. A 'Copy Your PC's MAC Address' button is located below the MAC Address field.

Internet Setup Dynamic (Cable)

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

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

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

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

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

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

The screenshot shows the WAN configuration interface. At the top, there's a 'WAN' header. Below it, a text block explains the purpose of the section and lists connection types: Static IP, DHCP, and PPPoE. A note mentions that PPPoE requires disabling client software. Three buttons are present: 'Save Settings', 'Don't Save Settings', and 'Reboot Now'. The 'INTERNET CONNECTION TYPE' section has a dropdown menu set to 'Dynamic IP (DHCP)'. Below this, the 'DYNAMIC IP (DHCP) INTERNET CONNECTION TYPE' section provides fields for 'Host Name' (containing 'DGL-5500A1'), 'Use Unicasting' (checked), 'Primary DNS Server', 'Secondary DNS Server', 'MTU' (set to 1500), and 'MAC Address'. A 'Copy Your PC's MAC Address' button is located at the bottom of the MAC Address field.

Internet Setup

PPPoE (DSL)

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

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

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

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

Username: Enter your PPPoE user name.

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

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

Reconnect Mode: 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, set the *Reconnect Mode* to **Always-on**.

DNS Servers: Enter the Primary and secondary DNS server IP addresses assigned by your ISP. These addresses are usually obtained automatically from your ISP. Leave blank if you did not specifically receive these from your ISP.

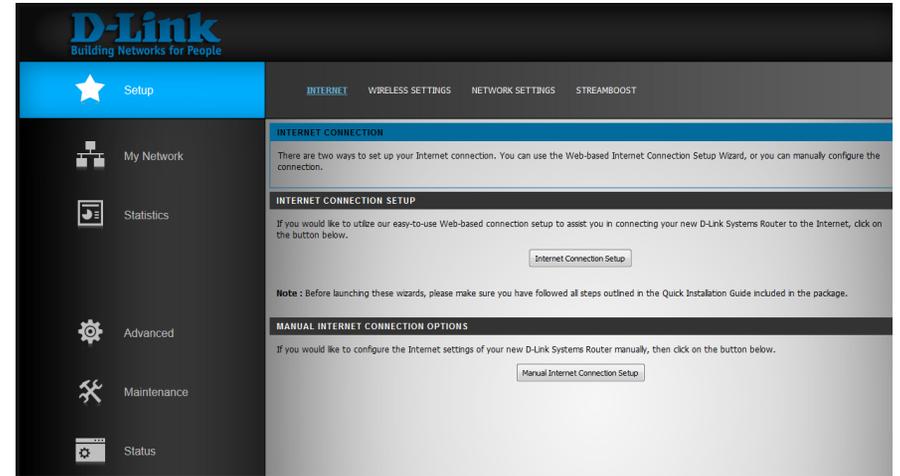
MTU: Maximum Transmission Unit - you may need to change the MTU for optimal performance with your specific ISP. 1492 is the default MTU.

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

The screenshot shows the WAN configuration interface. At the top, it says 'WAN' and provides instructions on how to choose a connection type. Below that, there are three buttons: 'Save Settings', 'Don't Save Settings', and 'Restart Now'. The main section is titled 'INTERNET CONNECTION TYPE' and asks the user to choose the router mode to connect to the Internet. The selected mode is 'PPPoE (Username / Password)'. Below this, there is a section for 'PPPOE INTERNET CONNECTION TYPE' which asks for information provided by the ISP. The fields include: Address Mode (Dynamic IP selected), IP Address (0.0.0.0), Username, Password, Verify Password, Service Name (Optional), Reconnect Mode (Always on selected), Maximum Idle Time (5 minutes), Primary DNS Address (10.10.10.1 Optional), Secondary DNS Address (4.2.2.2 Optional), MTU (1492 bytes), and MAC Address. There is a button labeled 'Clone Your PC's MAC Address'.

Internet Connection Setup Wizard

If you did not initially choose to install your router with the *Quick Setup Wizard*, you can click on **Internet Connection Setup** from the **Setup > Internet** page.



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

Click **Next** to continue.

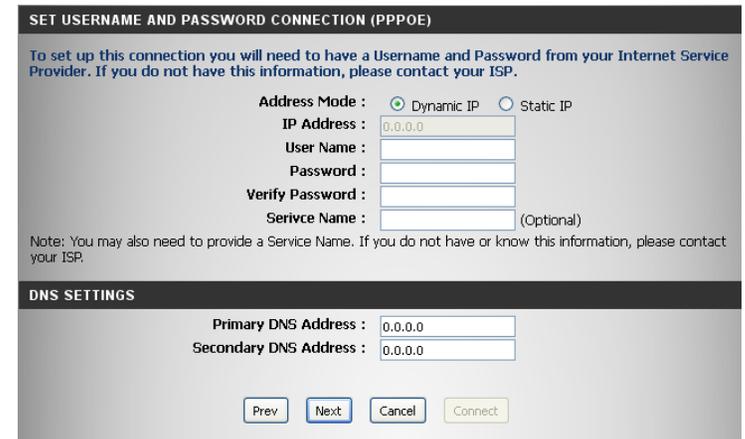


The router will scan for your Internet type. If it does not detect what type, the following screens will appear.

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

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

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



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

SET STATIC IP ADDRESS CONNECTION

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

IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Gateway Address : 0.0.0.0

DNS SETTINGS

Primary DNS Address : 0.0.0.0
Secondary DNS Address : 0.0.0.0

Prev Next Cancel Connect

Click either **I want automatic StreamBoost updates** or **I decline automatic StreamBoost updates**. Click **Next** to continue.

STEP 3: STREAMBOOST AUTO UPDATES

Maximize your online experience by keeping StreamBoost up to date.

Check below to enable your router to receive automatic StreamBoost updates during your initial 3-year manufacturer service term. The 3-year service term will start on the day the router is purchased but in no event will be valid beyond April 1st, 2017. (After the 3-year period, further updates may be made available from the manufacturer via firmware updates.) StreamBoost updates may help improve your router's Internet traffic management capabilities through better traffic identification and bandwidth management techniques. In exchange, your StreamBoost enabled router will send Qualcomm Atheros, Inc. anonymous information from your router. If you decline, you can find updates through software or firmware postings from your router's manufacturer.

[Learn More.](#)

Would you like to receive StreamBoost auto updates?

Yes, I want StreamBoost updates. I opt-in to data analysis and updates.
 No, I do not wish to receive updates.

Prev Next Cancel

You can keep the **Enable Auto Bandwidth Estimation** box checked to auto-detect your bandwidth or uncheck it to manually enter your download and upload speeds. Click the **Test Bandwidth** button first so the router can detect your speeds. After processing is completed, click **Next** to continue.

STEP 4: STREAMBOOST SETTINGS

Enable StreamBoost Bandwidth Control :

Enable Auto Bandwidth Estimation :

Download Speed(Mbps) :

Upload Speed(Mbps) :

Prev Next Cancel Test Bandwidth

When the setup process is completed, you will see this screen. Click on **Connect** to save your settings.

SETUP COMPLETE!

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

Prev Next Cancel Connect

Wireless Settings

802.11n/g (2.4GHz)

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

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

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

802.11 Mode: Select one of the following:

- 802.11b Only** - Select only if all of your wireless clients are 802.11b.
- 802.11g Only** - Select only if all of your wireless clients are 802.11g.
- 802.11n Only** - Select only if all of your wireless clients are 802.11n.
- Mixed 802.11g and 802.11b** - Select if you are using both 802.11g and 802.11b wireless clients.
- Mixed 802.11n and 802.11g** - Select if you are using both 802.11n and 802.11g wireless clients.
- Mixed 802.11n, 11g, and 11b** - Select if you are using a mix of 802.11n, 802.11g, and 802.11b wireless clients.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DGL-5500 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DGL-5500. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you check **Enable Auto Channel Scan**, this option will be greyed out.

Channel Width: Select the Channel Width:

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

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DGL-5500. If Invisible is selected, the SSID of the DGL-5500 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DGL-5500 in order to connect to it.

Wireless Security: Refer to page 33 for more information regarding wireless security.

WIRELESS NETWORK SETTINGS : 2.4GHZ BAND

Enable Wireless : Always

Wireless Network Name : yournetwork (Also called the SSID)

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

Enable Auto Channel Scan :

Wireless Channel : 2.437 GHz - CH 6

Channel Width : Auto 20/40 MHz

Visibility Status : Visible Invisible

WI-FI PROTECTED SETUP

Enable :

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 :

Show Password

802.11ac/n/a (5GHz)

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

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

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

802.11 Mode: Select one of the following:

- 802.11n Only** - Select if all of your wireless clients are 802.11n.
- 802.11ac Only** - Select only if all of your wireless clients are 802.11ac.
- Mixed 802.11a and 802.11n** - Select if you are using both 802.11n and 802.11a wireless clients.
- Mixed 802.11ac and 802.11n** - Select if you are using both 802.11n and 802.11ac wireless clients.
- Mixed 802.11ac, 802.11n and 802.11a** - Select if you are using 802.11ac, 802.11n, and 802.11a wireless clients.

Enable Auto Channel Scan: The **Auto Channel Scan** setting can be selected to allow the DGL-5500 to choose the channel with the least amount of interference.

Wireless Channel: Indicates the channel setting for the DGL-5500. The Channel can be changed to fit the channel setting for an existing wireless network or to customize the wireless network. If you check **Enable Auto Channel Scan**, this option will be greyed out.

Channel Width: Select the Channel Width:

- 20MHz** - Select if you are not using any 802.11n wireless clients.
- 20/40MHz(Auto)** - This is the default setting. Select if you are using both 802.11n and non-802.11n wireless devices.
- 20/40/80MHz(Auto)** - Select if you are using 802.11ac, 802.11n and non-802.11n wireless devices. This option is only available when the 802.11 Mode is set to Mixed 802.11ac.

Visibility Status: Select **Invisible** if you do not want the SSID of your wireless network to be broadcasted by the DGL-5500. If Invisible is selected, the SSID of the DGL-5500 will not be seen by Site Survey utilities so your wireless clients will have to know the SSID of your DGL-5500 in order to connect to it.

Wireless Security: Refer to the next page for wireless security.

WIRELESS NETWORK SETTINGS : 5GHZ BAND

Enable Wireless : Always

Wireless Network Name : yournetworks (Also called the SSID)

802.11 Mode : Mixed 802.11ac, 802.11n and 802.11a

Enable Auto Channel Scan :

Wireless Channel : 5.200 GHz - CH 40

Channel Width : Auto 20/40/80 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 : 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 :

Show Password

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DGL-5500 offers the following types of security:

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

What is WPA?

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

The 2 major improvements over WEP:

- Improved data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. WPA2 is based on 802.11i and uses Advanced Encryption Standard (AES) instead of TKIP.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.

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

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

WPA/WPA2-Personal (PSK)

It is recommended to enable wireless security on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption.

1. Log in to the web-based configuration by opening a web browser and entering **http://dlinkrouter.local/**. Click on **Setup** and then click **Wireless Settings** on the top.
2. Next to *Security Mode*, select **WPA-Personal**.
3. Next to *WPA Mode*, select **Auto(WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Cypher Type*, select **TKIP and AES**, **TKIP**, or **AES**.
5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
6. Next to *Pre-Shared Key*, enter a Wi-Fi password (key/passphrase). The password must be between 8-63 characters.
7. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you re-connect using the new Wi-Fi password.

The screenshot shows the 'WIRELESS SECURITY MODE' configuration page. At the top, it says '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.' Below this, the 'Security Mode' is set to 'WPA-Personal'. The 'WPA' section explains that WPA or WPA2 mode achieves a balance of security and compatibility, using WPA for legacy clients and WPA2 for higher security. It notes that WPA2 Only mode uses AES(CCMP) cipher and legacy stations are not allowed. WPA Only mode uses TKIP cipher. To achieve better performance, WPA2 Only mode (or AES cipher) is recommended. The 'WPA Mode' is set to 'Auto (WPA or WPA2)', 'Cipher Type' is 'TKIP and AES', and 'Group Key Update Interval' is '3600 (seconds)'. The 'PRE-SHARED KEY' section prompts the user to enter an 8 to 63 character alphanumeric pass-phrase. The 'Pre-Shared Key' field contains 'mywifi@password' and the 'Show Password' checkbox is checked.

Configure WPA/WPA2-Enterprise (RADIUS)

It is recommended to enable wireless security on your wireless router before your wireless network adapters. Please establish wireless connectivity before enabling encryption.

1. Log in to the web-based configuration by opening a web browser and entering **http://dlinkrouter.local/**. Click on **Setup** and then click **Wireless Settings** on the top.
2. Next to *Security Mode*, select **WPA-Enterprise**.
3. Next to *WPA Mode*, select **Auto(WPA or WPA2)**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Cypher Type*, select **TKIP and AES**, **TKIP**, or **AES**.
5. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
6. Next to *RADIUS Server IP Address* enter the IP Address of your RADIUS server.
7. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
8. Next to *RADIUS Server Shared Secret*, enter the security key.
9. Click **Advanced** to enter settings for a secondary RADIUS Server.
10. Click **Save Settings** to save your settings.

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(128) 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)

EAP (802.1X)

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

Authentication Timeout : **60** (minutes)

RADIUS server IP Address : **0.0.0.0**

RADIUS server Port : **1812**

RADIUS server Shared Secret : *******

Second MAC Address Authentication :

[Advanced >>](#)

Network Settings

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

Router Settings

Router IP Address: Enter the IP address of the router. The default IP address is 192.168.0.1. If you statically assign your network clients, make sure to use the new IP address as the Default Gateway address.

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

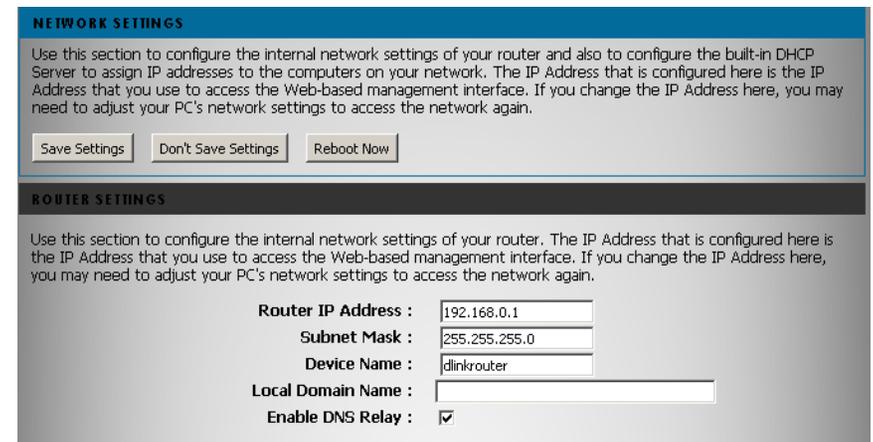
Default Subnet Mask: Enter the Subnet Mask. The default subnet mask is 255.255.255.0.

Device Name: Enter a name for the router. Note that if you change the name, you must use it the next time you want to log in to the router (i.e., `http://dlinkrouter.local/`).

For example, if you change the router name to **myrouter**, to log in, you must enter **`http://myrouter.local/`**.

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

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



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.

Save Settings Don't Save Settings Reboot Now

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 :

Subnet Mask :

Device Name :

Local Domain Name :

Enable DNS Relay :

DHCP Server Settings

DHCP stands for Dynamic Host Control Protocol. The DGL-5500 has a built-in DHCP server which will automatically assign an IP address to computers/devices on your 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 DGL-5500. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

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

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

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

DHCP Lease Time: The length of time for the IP address lease. Enter the Lease time in minutes. The default is 1440.

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

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

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

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

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

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

DHCP Reservation

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

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

Enable: Check this box to enable the reservation.

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

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

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

Copy Your PC's MAC Address: You can use the **Copy Your PC's MAC Address** button to insert the MAC address of the computer you are working from in the MAC address box.

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

DHCP Reservations List

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

Enable: Check to enable the reservation.

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

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

ADD DHCP RESERVATION

Enable :

Computer Name : << Computer Name ▾

IP Address :

MAC Address :

[Copy Your PC's MAC Address](#)

DHCP RESERVATIONS LIST

Enable	Host Name	MAC Address	IP Address		
NUMBER OF DYNAMIC DHCP CLIENTS : 3					
	MAC Address	Assigned IP	Hostname	Expires	
	00:15:e9:2e:26:3c	192.168.0.100	Graphicstest	Sat May 11 08:12:15 2013	Revoke Reserve
	58:94:6b:9a:c2:c4	192.168.1.87	160-TLUU	Fri May 10 14:22:38 2013	Revoke Reserve
	cc:b2:55:cc:8b:ba	192.168.0.101	dlinkap	Fri May 10 14:23:22 2013	Revoke Reserve

DHCP RESERVATIONS LIST

Enable	Host Name	IP Address	MAC Address		
<input checked="" type="checkbox"/>	Graphicstest	192.168.0.105	00:15:e9:2e:26:3c		

NUMBER OF DYNAMIC DHCP CLIENTS

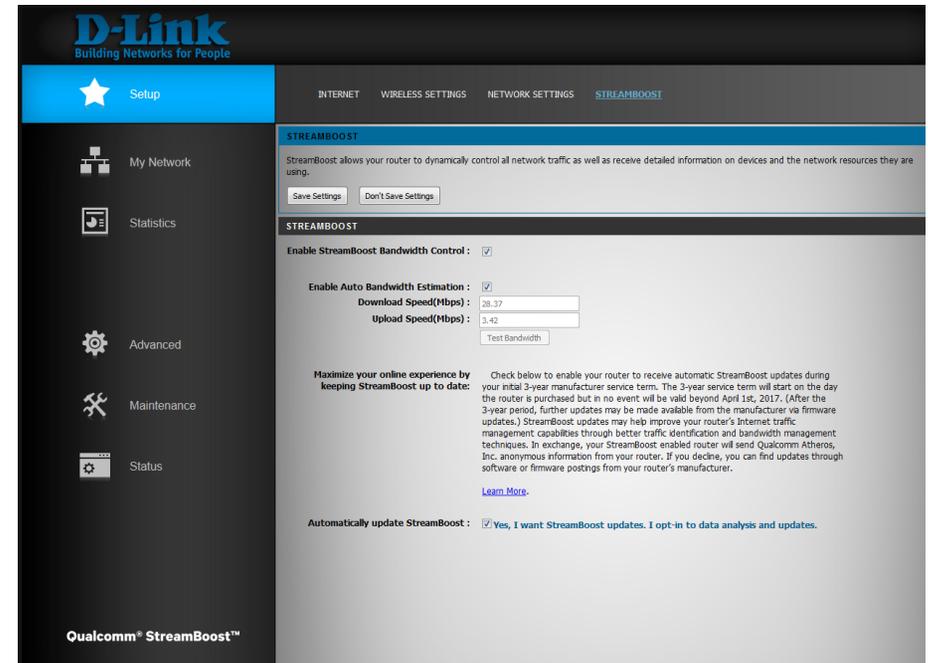
Host Name	IP Address	MAC Address	Expired Time
Graphicstest	192.168.0.105	00:15:e9:2e:26:3c	6 Days 2 Hours 52 Minutes

StreamBoost

Enable Auto Bandwidth Control: Check this box to allow the router to use StreamBoost and optimize your Internet traffic.

Enable Auto Bandwidth Estimation: Check to have the router automatically estimate your bandwidth speeds. If you uncheck this box, you can manually enter your bandwidth or click the Test Bandwidth button (recommended).

Automatically update StreamBoost: Read the information on the screen and check the box if you agree to the terms.



Advanced Server

Enable Media Check this box to enable the Media Server function.

Server: This will allow you to share data from a USB thumb drive attached to your router.

Media Server Enter a name for the media server.

Name:

SERVER

Media Server allows you to share a USB storage device when connected to the USB port of the DGL-5500.

The Virtual Server option allows you to identify 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 Restart Now

MEDIA SERVER

Enable Media Server :

Media Server Name :

Virtual Server

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

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

IP Address: Enter the IP address of the computer on your local network that you want to allow the incoming service to. If your computer is receiving an IP address automatically from the router (DHCP), your 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.

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 **Advanced > Schedules** section.

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

24 -- VIRTUAL SERVERS LIST				
		Port	Traffic Type	
<input type="checkbox"/>	Name Application Name	Public Port 0	Protocol TCP	Schedule Always
<input type="checkbox"/>	IP Address 0.0.0.0 Computer Name	Private Port 0	6	Inbound Filter Allow All
<input type="checkbox"/>	Name Application Name	Public Port 0	Protocol TCP	Schedule Always
<input type="checkbox"/>	IP Address 0.0.0.0 Computer Name	Private Port 0	6	Inbound Filter Allow All
<input type="checkbox"/>	Name Application Name	Public Port 0	Protocol TCP	Schedule Always
<input type="checkbox"/>	IP Address 0.0.0.0 Computer Name	Private Port 0	6	Inbound Filter Allow All

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), your computer will be listed in the "Computer Name" drop-down menu. Select your computer and click <<.

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

Example: 24,1009,3000-4000

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

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

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 Mxed (1020-5000, 689).

Save Settings Don't Save Settings

24 -- PORT FORWARDING RULES

		Ports to Open		Schedule
<input type="checkbox"/>	Name [] << Application Name	TCP	0	Always
<input type="checkbox"/>	IP Address 0.0.0.0 << Computer Name	UDP	0	Inbound Filter Allow All
<input type="checkbox"/>	Name [] << Application Name	TCP	0	Always
<input type="checkbox"/>	IP Address 0.0.0.0 << Computer Name	UDP	0	Inbound Filter Allow All
<input type="checkbox"/>	Name [] << Application Name	TCP	0	Always
<input type="checkbox"/>	IP Address 0.0.0.0 << Computer Name	UDP	0	Inbound Filter Allow All
<input type="checkbox"/>	Name [] << Application Name	TCP	0	Always
<input type="checkbox"/>	IP Address 0.0.0.0 << Computer Name	UDP	0	Inbound Filter Allow All
<input type="checkbox"/>	Name [] << Application Name	TCP	0	Always

Firewall Settings

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

Anti-Spoof Checking: Enable this feature to protect your network from certain kinds of “spoofing” attacks.

UPnP: Check the enable UPnP box to allow the router to be detected by devices with UPnP enabled. From your Windows computer the router will be displayed in your network settings. Double-click the icon to access the web-based configuration utility.

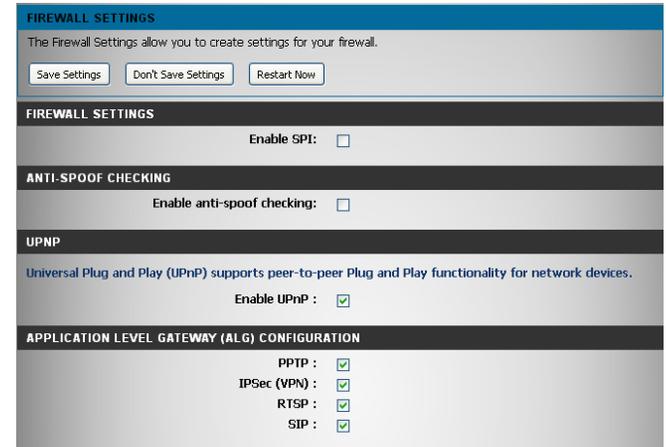
This feature also will allow clients on your network to automatically open ports on the router so you do not have to manually open them (i.e., virtual server/port forwarding). If you disable UPnP, you may have to manually open ports for certain applications and games in the Virtual Server or Port Forwarding sections. Please refer to the application manufacturer for a list of ports needed.

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

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

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

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



Filter 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.

Enable Access Check the **Enable Access Control** box, and then
Control: click on **Add Policy** to start the Wizard.



Access Control Wizard

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



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



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



Enter the following information:

- **Address Type** - Select **IP**, **MAC**, or **Other Machines**.
- **IP Address** - Enter the IP address of the computer you want to apply the rule to.
- **Machine Address** - Enter the PC MAC address or click on **Clone Your PC's MAC Address**.



Click **Add** and then click **Next** to continue.

Select the filtering method.

If you select the option to **Block Some Access**, check **Apply Web Filter** and/or **Apply Advanced Port Filters**.



Click **Next** to continue.

Add Port Filter Rules:

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.

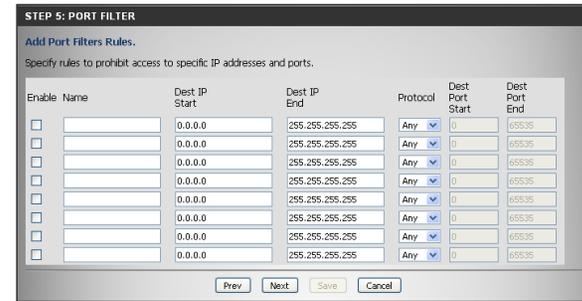
Dest Port End - Enter the ending port number.

Click **Next**.

To enable **Web Access Logging**, click **Enabled**.

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

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



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 with Virtual Server, Port Forwarding, or Remote Administration features.

Name: Enter a name for the inbound filter rule.

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

Enable: Check to enable rule.

Remote IP Start: Enter the starting IP address.

Remote IP End: Enter the ending IP address.

Add: Click the **Add** button to apply your settings.

Inbound Filter This section will list any rules that are created. You may click

Rules List: the Edit icon to change the settings or enable/disable the rule, or click the Delete icon to remove the rule.

ADD INBOUND FILTER RULE

Configure inbound data filtering rules based on IP Address range.

Name :

Action : Allow ▼

Remote IP Range :	Enable	Remote IP Start	Remote IP End
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>
<input type="checkbox"/>	<input type="checkbox"/>	<input style="width: 60px;" type="text" value="0.0.0.0"/>	<input style="width: 60px;" type="text" value="255.255.255.255"/>

INBOUND FILTER RULES LIST

Name	Action	Remote IP Range	

MAC Filtering Rules

Use MAC Filters to allow or deny local computers/devices by their MAC addresses from accessing the network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the router.

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

MAC Address: Enter the MAC address of the computer or device you would like to filter.

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

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

Save: Click **Save** to save your entry.

Clear: Click **Clear** to erase your current entry.

MAC Filter List: This section will list your current entries.

Note: If you enable filtering and create an "allow" list, you must add the computer or device you are currently using to the list or you will be blocked when the router reboots.

The screenshot shows the 'MAC FILTERING RULES' configuration page. At the top, it says 'Allow or deny network access using the computer's MAC address.' Below this, there is a section 'Configure MAC Filtering below:' with a dropdown menu set to 'Turn MAC Filtering ON and ALLOW computers listed to access the network'. Underneath, there are two columns: 'MAC Address' and 'DHCP Client List'. The 'MAC Address' field contains '00:00:00:00:00:00' and a '<<' button. The 'DHCP Client List' field contains 'Computer Name' and a dropdown arrow. Below these fields are 'Save' and 'Clear' buttons. At the bottom, there is a section titled 'MAC FILTER LIST' with a table header 'MAC Address' and two empty columns.

Web Filtering Rules

Website Filters are used to allow you to set up a list of Web sites that can be viewed by multiple users through the network. To use this feature select to Allow or Deny, enter the domain or website and click Save Settings.

Configure Select either **DENY computers access to ONLY these sites** or **Website Filter: ALLOW computers access to ONLY these sites**.

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

When completed, click **Save Settings** to restart your router and activate your new settings.



Website URL/Domain		
www.ablockedwebsite.net		

DMZ

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

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

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

The screenshot shows the 'DMZ HOST' configuration page. At the top, there is a blue header with the text 'DMZ HOST'. Below the header, a grey box contains the following text: '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.' Below this text is a 'Note' in italics: '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.' Under the note are three buttons: 'Save Settings', 'Don't Save Settings', and 'Restart Now'. Below the buttons is another grey box with the title 'DMZ HOST' in bold. It contains two settings: 'Enable DMZ Host : ' and 'DMZ IP Address : 192.168.0.100 << dlinktestpc (192.168.0.100) >>'. The IP address is shown in a text box, followed by a '<<' button, the host name 'dlinktestpc (192.168.0.100)', and a '>>' button.

Schedules

Name: Enter a name for your new schedule.

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

All Day - 24 Hrs: Uncheck this box to enter a start and end time for your schedule or check it to select 24 hours.

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

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

Once you create a schedule, click **Save Settings**.

The screenshot shows the D-Link Advanced Schedules configuration page. The page has a dark sidebar on the left with navigation options: My Network, Statistics, Setup, Maintenance, and Status. The main content area is titled 'SCHEDULES' and includes a 'Save Settings' button and a 'Don't Save Settings' button. Below this is the 'ADD SCHEDULE RULE' form with the following fields:

- Name: example
- Day(s): All Week Select Day(s)
- Sun Mon Tue Wed Thu Fri Sat
- All Day - 24 hrs:
- Time Format: 12-hour
- Start Time: 08 : 00 AM (hour:minute)
- End Time: 07 : 00 PM (hour:minute)

At the bottom of the page is a 'SCHEDULE RULES LIST' table with the following data:

Name	Day(s)	Schedule Rules List		
example	Tue Wed Thu	08:00 AM-07:00 PM		

Maintenance

Admin

This page will allow you to change the Administrator password, system name, remote management, and time settings.

Admin Password: Enter a new password for the Admin login name. Enter again to verify password.

Gateway Name: Enter a name for your router.

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

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

Enable Remote Management: Remote management allows the DGL-5500 to be configured from the Internet by a web browser. A username/password is still required to access the Web Management interface.

Remote Admin Port: The port number used to access the DGL-5500 is used in the URL. Example: **http://x.x.x.x:8080** whereas x.x.x.x is the Internet IP address of the DGL-5500 and 8080 is the port used for the Web Management interface.

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

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

The screenshot displays the 'ADMINISTRATOR SETTINGS' page. It includes a header section with a blue bar, followed by an explanatory text block about the 'admin' account. Below this are three buttons: 'Save Settings', 'Don't Save Settings', and 'Restart Now'. The 'ADMIN PASSWORD' section contains two input fields for 'Password' and 'Verify Password' with a confirmation instruction. The 'SYSTEM NAME' section has a 'Gateway Name' field with the value 'DGL-5500A1'. The 'ADMINISTRATION' section contains several checkboxes for 'Enable Graphical Authentication', 'Enable HTTPS Server', and 'Enable Remote Management'. It also features a 'Remote Admin Port' field set to '8080', a 'Use HTTPS' checkbox, and an 'Inbound Filter' dropdown menu set to 'Allow All' with a 'Details' field below it.

Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock.

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

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

Enable Daylight Saving: Check to enable manual entry of daylight saving time.

Daylight Saving Dates: Enter a start date, an end date, including day of the week, and time for daylight saving time.

The screenshot shows the 'TIME CONFIGURATION' page. At the top, it displays the current time: 'Wednesday, May 29, 2013 1:41:31 PM'. Below this is a 'Time Zone' dropdown menu set to '(GMT-08:00) Pacific Time (US/Canada), Tijuana'. There is an unchecked checkbox for 'Enable Daylight Saving'. Under 'Daylight Saving Dates', there are two rows of dropdown menus. The first row is for 'DST Start' with values: Mar, 3rd, Sun, 1:00 AM. The second row is for 'DST End' with values: Nov, 2nd, Sun, 1:00 AM.

System

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

Firmware Upgrade

Check Now: Click to see if there is an update available. If there is you must download the firmware file to your computer.

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

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

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

Restart the Device: Click to reboot the router.

Save Configuration: 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 Configuration** button. A file dialog will appear, allowing you to select a location and file name for the settings.

Upload Configuration: Use this option to load previously saved router configuration settings. First, use the **Choose File** option to find a previously saved file of configuration settings. Then, click the **Restore Configuration from File** button to transfer those settings to the router.

The screenshot displays the 'SYSTEM SETTINGS' page. It includes a header section with instructions on restarting the device or restoring factory defaults. Below this are several functional sections: 'FIRMWARE INFORMATION' showing the current version (1.00) and date (27 May 2013), with a 'Check Now' button; 'FIRMWARE UPGRADE' featuring a note about configuration resets, a file selection field with a 'Browse...' button, and an 'Upload' button; 'RESTORE TO FACTORY DEFAULT SETTINGS' with a 'Restore Factory Defaults' button; 'RESTART THE DEVICE' with a 'Restart The Device' button; 'SAVE CONFIGURATION' with a 'Save Configuration' button; and 'UPLOAD CONFIGURATION' with a file selection field, a 'Browse...' button, and a 'Restore Configuration from File' button.

Status

Device Info

This page displays the current information for the DGL-5500. It will display the LAN, WAN (Internet), and Wireless information. If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

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

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

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

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

Wi-Fi Network (2.4GHz): Displays the 2.4GHz wireless MAC address and your wireless settings such as SSID, channel, and security settings.

Wi-Fi Network (5GHz): Displays the 5GHz wireless MAC address and your wireless settings such as SSID, channel, and security settings.

DEVICE INFORMATION

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

GENERAL

Time : Wednesday, May 29, 2013 1:51:06 PM
Firmware Version : 1.00 , 27, May, 2013
StreamBoost Build Version :

WAN

Connection Type : DHCP Client
Cable Status : Connected
Network Status : Established
Connection Up Time : 0 Day, 0:55:40

MAC Address : 00:18:E7:95:82:5A
IP Address : 10.10.10.100
Subnet Mask : 255.255.255.0
Default Gateway : 10.10.10.1
Primary DNS Server : 10.10.10.1
Secondary DNS Server : 0.0.0.0

LAN

MAC Address : 00:18:E7:95:82:59
IP Address : 192.168.0.1
Subnet Mask : 255.255.255.0
DHCP Server : Enabled

WI-FI NETWORK : 2.4GHZ BAND

Wireless Radio : Enabled
802.11 Mode : Mixed 802.11n, 802.11g and 802.11b
Channel Width : Auto 20/40 MHz
Channel : 6
Wi-Fi Protected Setup : Enabled/Configured
SSID List :

Wi-Fi Network Name (SSID)	Guest	MAC Address	Security Mode
dlink-8259	No	00:18:E7:95:82:59	AUTO (WPA or WPA2) - PSK

WI-FI NETWORK : 5GHZ BAND

Wireless Radio : Enabled
802.11 Mode : Mixed 802.11a and 802.11n
Channel Width : Auto 20/40 MHz
Channel : 36
Wi-Fi Protected Setup : Enabled/Configured
SSID List :

Wi-Fi Network Name (SSID)	Guest	MAC Address/	Security Mode
dlink_meida-8258	No	00:18:E7:95:82:5B	AUTO (WPA or WPA2) - PSK

Logs

The router automatically logs (records) events of possible interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs and select what types of events you want to view.

Log Type: You can select the type you would like to keep track of.

Apply Log Settings Click to save your log settings.
Now:

First Page: Click to go to the first page.

Last Page: Click to go to the last page.

Previous: Click to go back one page.

Next: Click to go to the next page.

Refresh: Updates the log details.

Clear: Clears all of the log contents.

Save Log: Click **Save** to save log file to local hard drive.

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 Type : System Activity
 Debug Information
 Attacks
 Dropped Packets
 Notice

Apply Log Settings Now

LOG DETAILS

1/12

Time	Message
May 29 13:36:06	UDHCPD Inform: add_lease 192.168.0.100
May 29 13:08:16	ath0: STA 00:26:5e:25:7d:ed IEEE 802.11: disassociated
May 29 13:08:11	ath0: STA 00:26:5e:25:7d:ed IEEE 802.11: associated
May 29 13:00:01	USER root pid 1598 cmd cull_incoming_pcaps
May 29 12:55:57	HTTP listening on port 65530
May 29 12:55:47	Current local time and date: Wed May 29 12:55:47 2013
May 27 16:09:38 d.	Service D-Link HNAP Service (/var/etc/avahi/services/dhnap.service) successfully established.
May 27 16:09:38	Service D-Link DGL-5500A1 Configuration Utility (/var/etc/avahi/services/http.service) successfully established.

Statistics

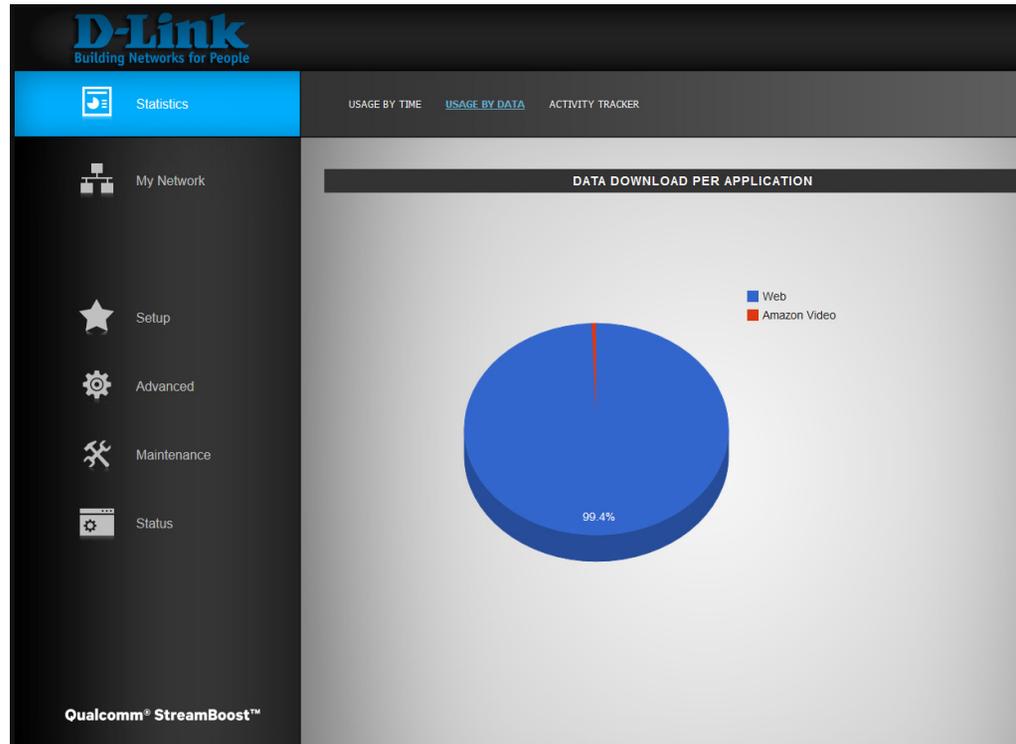
Usage in Time

The screen below displays the **Usage in Time**. Here you can view the amount of traffic that pass through the DGL-5500 and what applications are being used.



Usage by Data

The screen below displays the **Usage by Data**.



Activity Tracker

The screen below displays application activity and status.

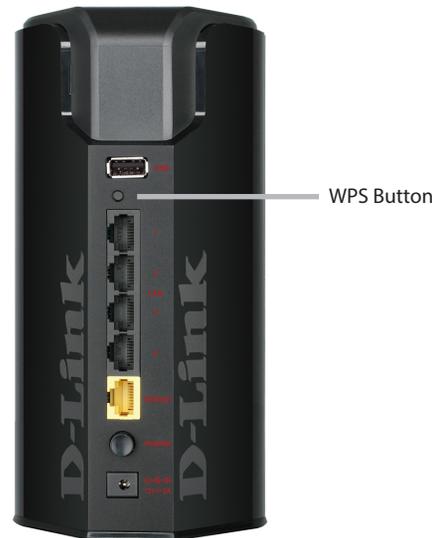


Connect a Wireless Client to your Router

WPS Button

The easiest and most secure way to connect your wireless devices to the router is WPS (Wi-Fi Protected Setup). Most wireless devices such as wireless adapters, media players, Blu-ray DVD players, wireless printers and cameras will have a WPS button (or a software utility with WPS) that you can press to connect to the DGL-5500 router. Please refer to your user manual for the wireless device you want to connect to make sure you understand how to enable WPS. Once you know, follow the steps below:

Step 1 - Press the WPS button on the DGL-5500 for about one second. The Internet LED on the front will start to blink.



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

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

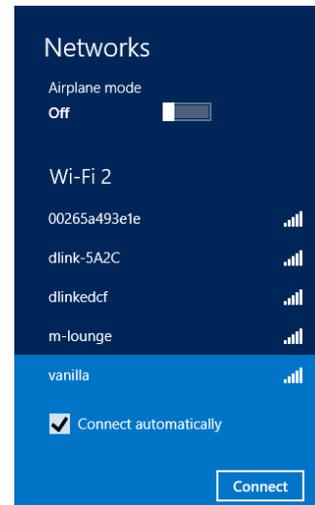
Windows® 8

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

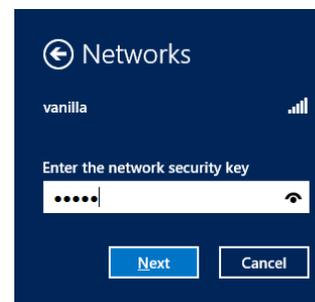
2. A list of available wireless networks will appear.



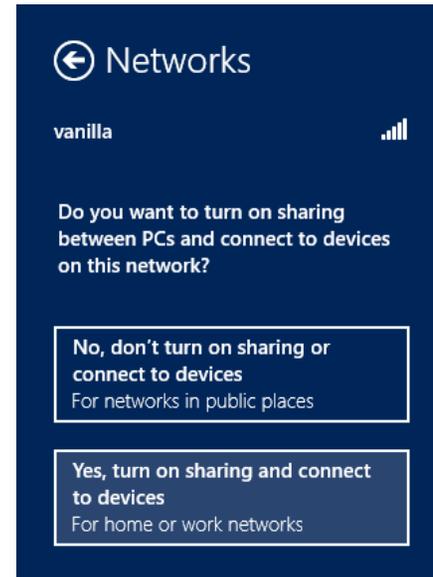
3. Click the wireless network (SSID) you want to connect to and then click **Connect**.



4. If the network is secure/encrypted, enter the Wi-Fi password (security key) and click **Next**.



5. Click either to enable or disable file sharing.
6. You will now be connected to your wireless network.



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

Windows® 7

WPA/WPA2

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

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



Wireless Icon

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

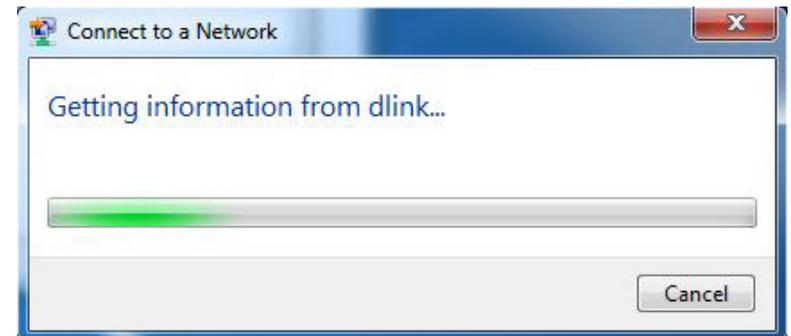


3. Highlight the wireless network (SSID) you would like to connect to and click the **Connect** button.

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.



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



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

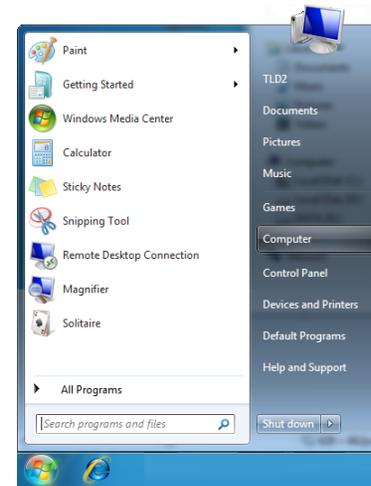
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the security settings are correct. The key or passphrase must be exactly the same as on the wireless router.



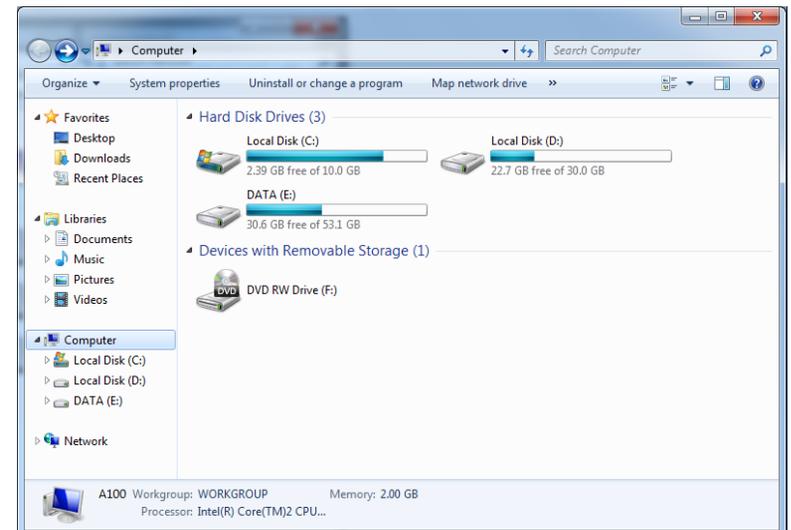
WPS

The WPS feature of the DGL-5500 can be configured using Windows® 7. Carry out the following steps to use Windows® 7 to configure the WPS feature:

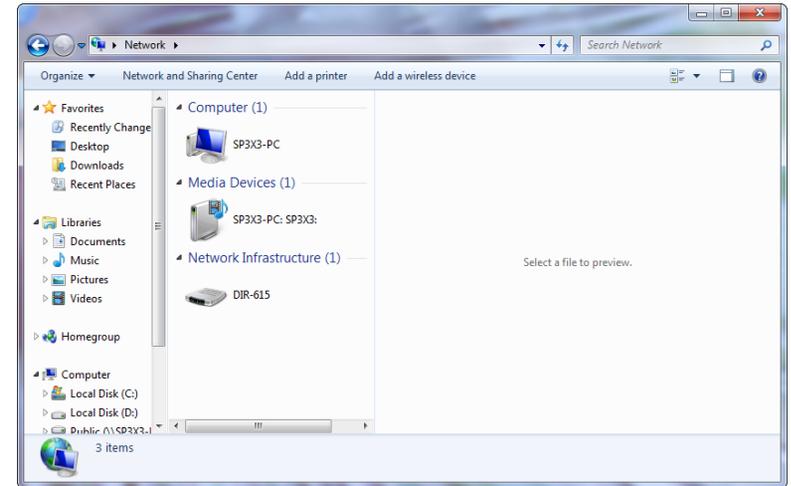
1. Click the **Start** button and select **Computer** from the Start menu.



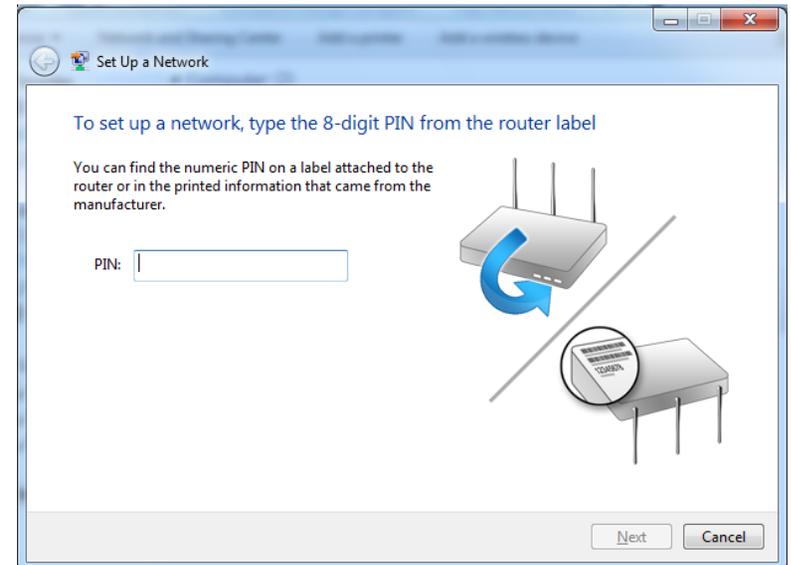
2. Click **Network** on the left side.



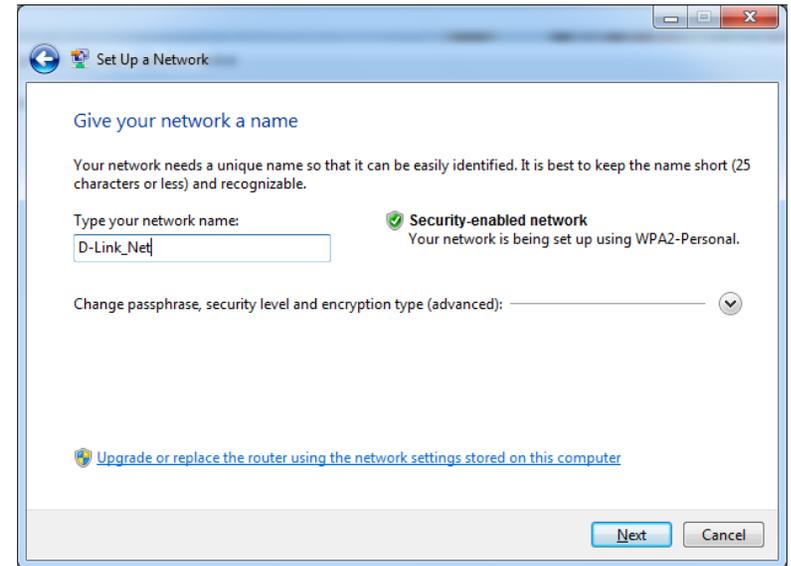
3. Double-click the DGL-5500.



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

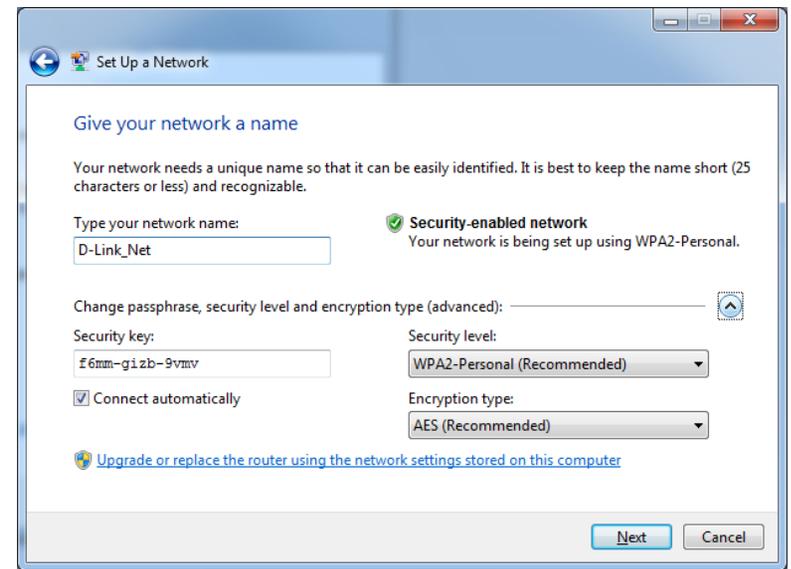


5. Type a name to identify the network.



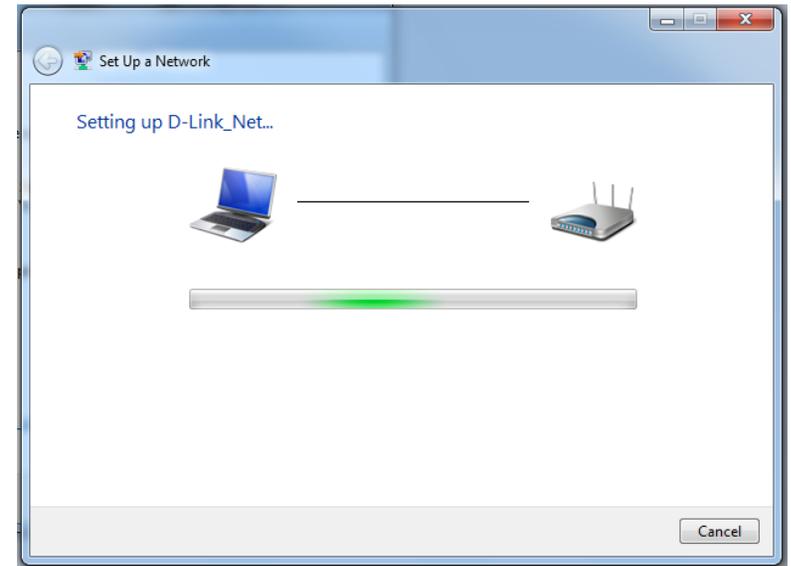
6. To configure advanced settings, click the  icon.

Click **Next** to continue.



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

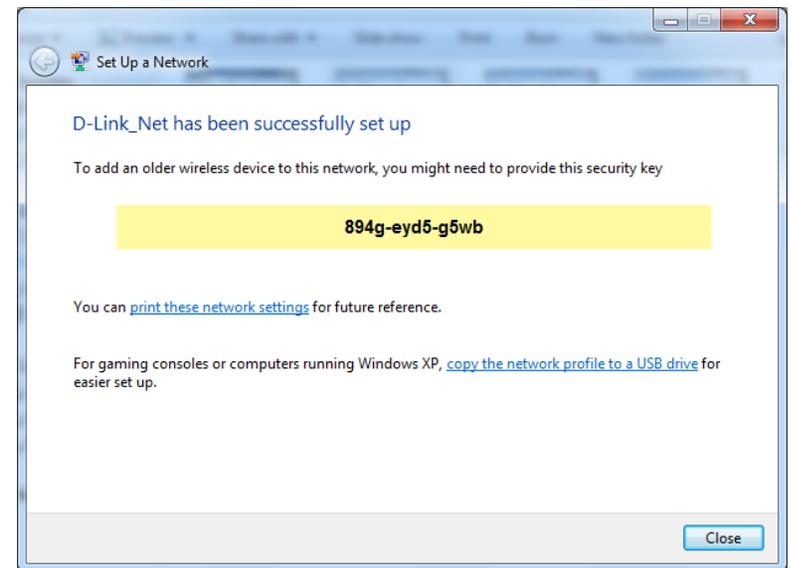
Wait for the configuration to complete.



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

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

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



Windows Vista®

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

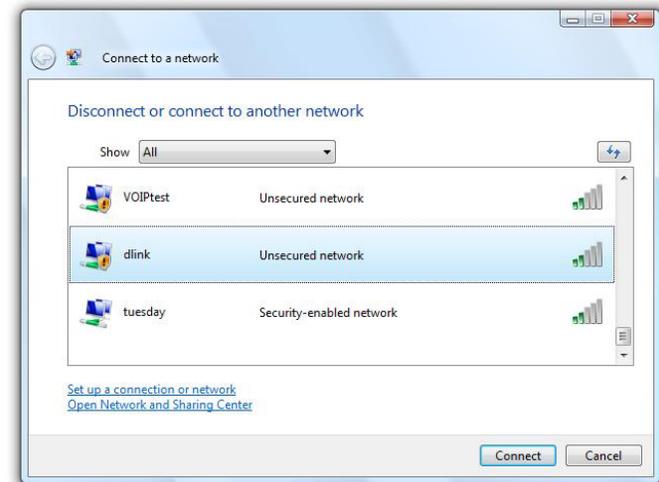
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

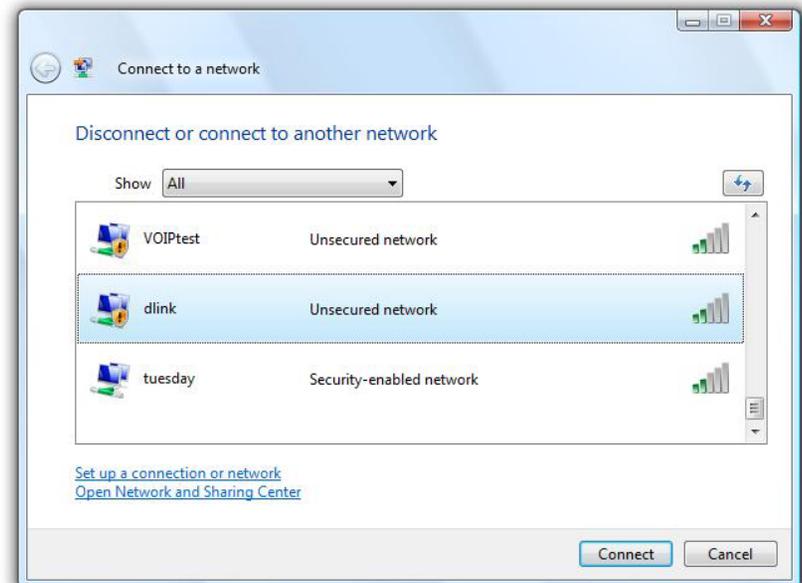
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



WPA/WPA2

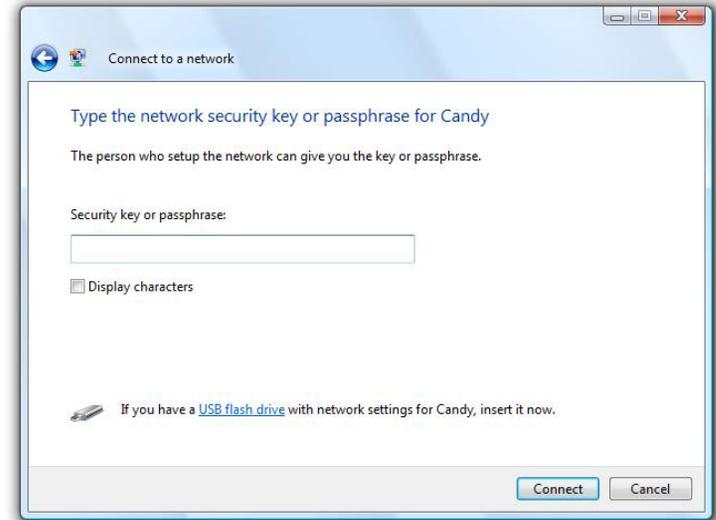
It is recommended to enable wireless security (WPA/WPA2) on your wireless router or access point before configuring your wireless adapter. If you are joining an existing network, you will need to know the security key or passphrase being used.

1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower right corner of screen). Select **Connect to a network**.
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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.



WPS/WCN 2.0

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

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

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



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

Windows® XP

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

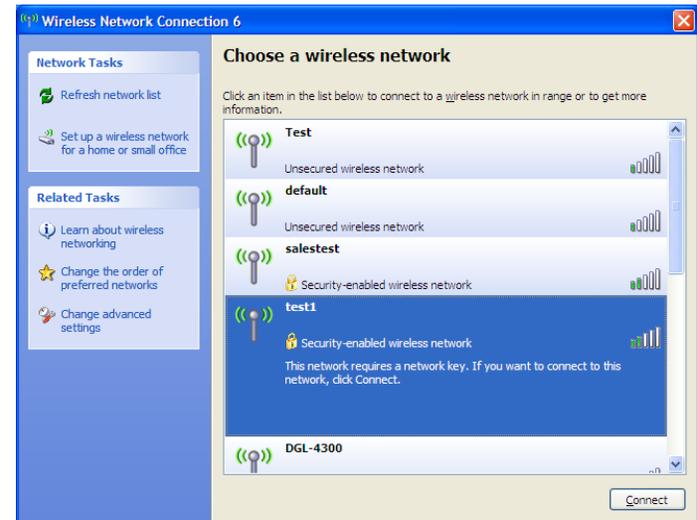
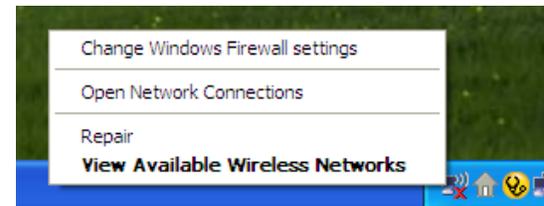
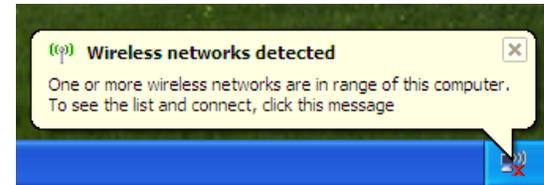
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

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

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

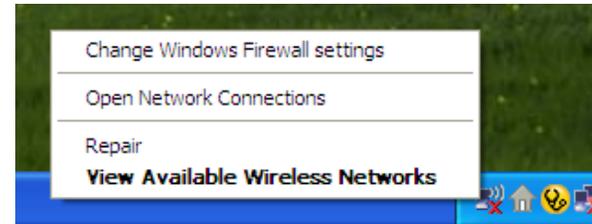
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



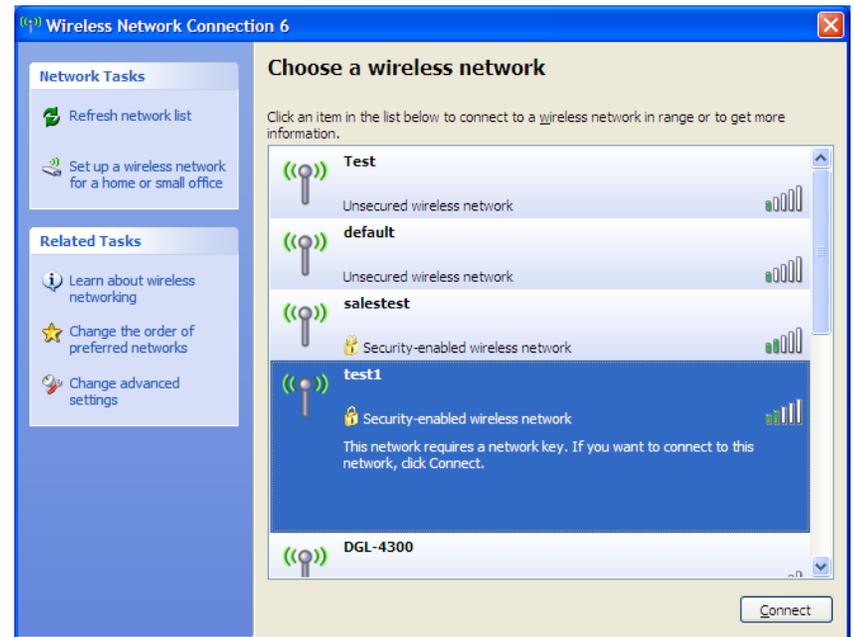
WPA/WPA2

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

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

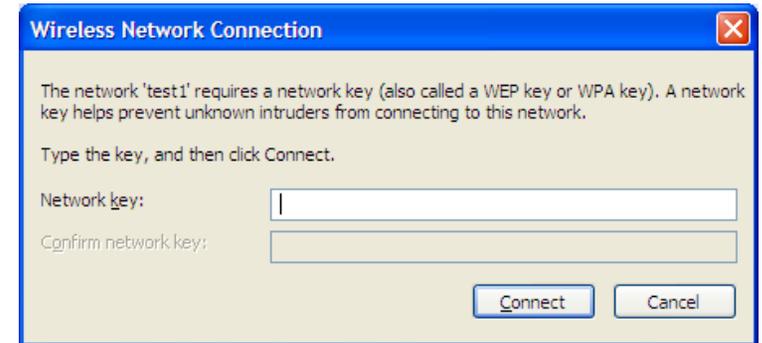


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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.



Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DGL-5500. Read the following descriptions if you are having problems. The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.

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

When entering the IP address of the D-Link router (192.168.0.1 for example), you are not connecting to a website nor do you have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

- Make sure you have an updated Java-enabled web browser. We recommend the following:
 - Microsoft Internet Explorer® 7 and higher
 - Mozilla Firefox 3.5 and higher
 - Google™ Chrome 8 and higher
 - Apple Safari 4 and higher
- Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.
- Disable any Internet security software running on the computer. Software firewalls such as Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, and Windows® XP firewall may block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

- Configure your Internet settings:
 - Go to **Start > Settings > Control Panel**. Double-click the **Internet Options** icon. From the **Security** tab, click the button to restore the settings to their defaults.
 - Click the **Connection** tab and set the dial-up option to Never Dial a Connection. Click the LAN Settings button. Make sure nothing is checked. Click **OK**.
 - Go to the **Advanced** tab and click the button to restore these settings to their defaults. Click **OK** three times.
 - Close your web browser (if open) and open it.
- Access the web management. Open your web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your web management.
- If you still cannot access the configuration, unplug the power to the router for 10 seconds and plug back in. Wait about 30 seconds and try accessing the configuration. If you have multiple computers, try connecting using a different computer.

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

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

To reset the router, locate the reset button (hole) on the bottom 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. To re-configure the router, refer to page 13.



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).

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

- Click on **Start** and then click **Run**.
- Windows® 95, 98, and Me users type in **command** (Windows® NT, 2000, XP, Vista®, and 7 users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

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

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

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
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, let's 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 phones 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, 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 has become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

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

Small Office and Home Office

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

Where is wireless used?

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

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

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

Tips

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

Centralize your router or Access Point

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

Eliminate Interference

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

Security

Don't let your 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 DGL-5500 wireless network Cardbus adapters.

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

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

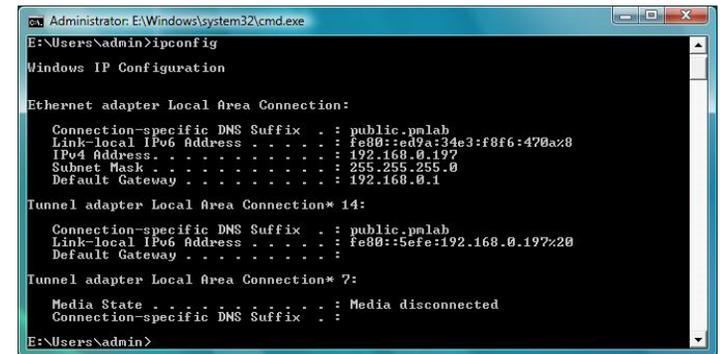
Networking Basics

Check your IP address

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

Windows® 8 Users

- Press the **Windows key** and **R** together. Type **cmd** in the box and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.



```
Administrator: E:\Windows\system32\cmd.exe
E:\Users\Admin>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : public.pmlab
    Link-local IPv6 Address . . . . . : fe80::ed9a:34e3:f8f6:470a%8
    IPv4 Address. . . . . : 192.168.0.197
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Tunnel adapter Local Area Connection* 14:

    Connection-specific DNS Suffix  . : public.pmlab
    Link-local IPv6 Address . . . . . : fe80::5efe:192.168.0.197%20
    Default Gateway . . . . . :

Tunnel adapter Local Area Connection* 7:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

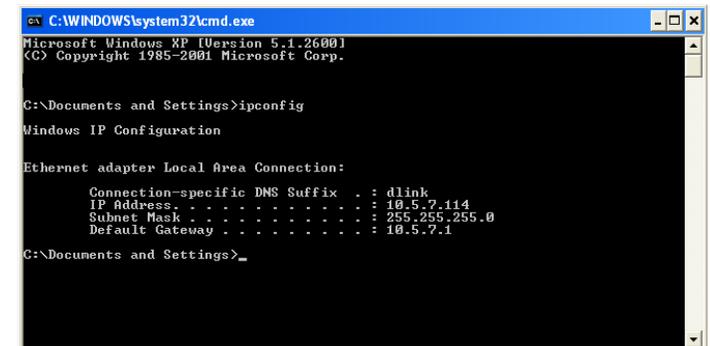
E:\Users\Admin>
```

Windows® 7/Vista® Users

- Click **Start**, type **cmd** in the search box and then click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and default gateway of your adapter.

Windows® XP Users

- Click on **Start > Run**. In the run box type **cmd** and click **OK**.
- At the prompt, type **ipconfig** and press **Enter**.
- This will display the IP address, subnet mask, and the default gateway of your adapter.



```
C:\WINDOWS\system32\cmd.exe
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>_
```

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.

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:

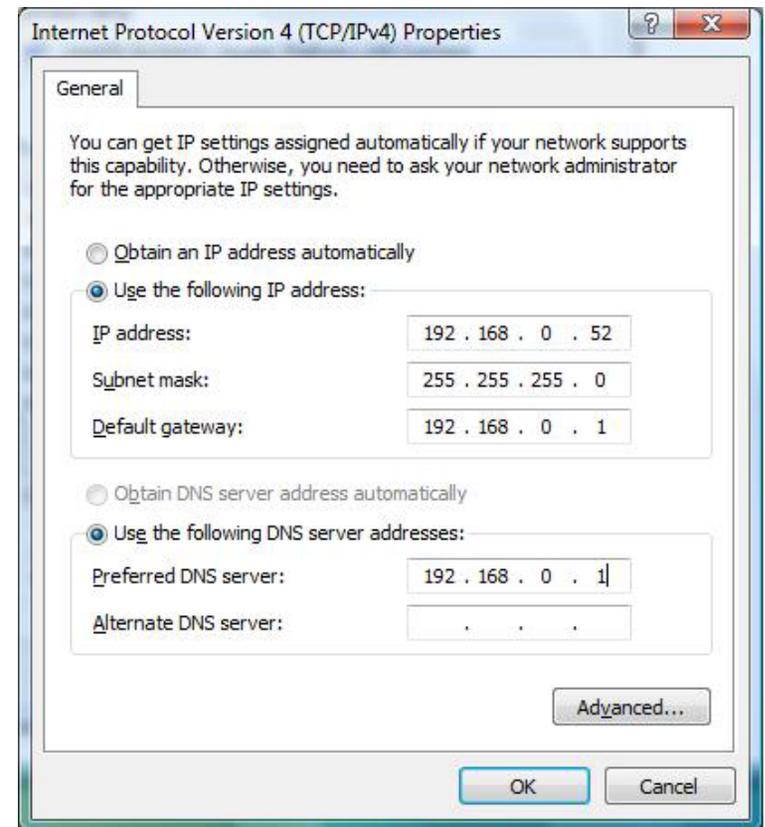
Windows® 8 Users

- Press the **Windows** key and then type **IP**. Click **Settings** on the right side and then click **View Network Connections**.
- Right-click on the adapter which represents your D-Link wireless network adapter.
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.

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

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 or gateway.
- Set **Primary DNS** the same as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.



Windows® 7/ Vista® Users

- Click on **Start > Control Panel** (make sure you are in Classic View). Double-click on the **Network and Sharing Center** icon. If you are using Windows Vista, click on **Manage network connections** along the left panel in the window. For Windows® 7, click on **Change adapter settings**.

- Right-click on the **Local Area Connection** which represents your D-Link wireless network adapter which will be connected to your network.

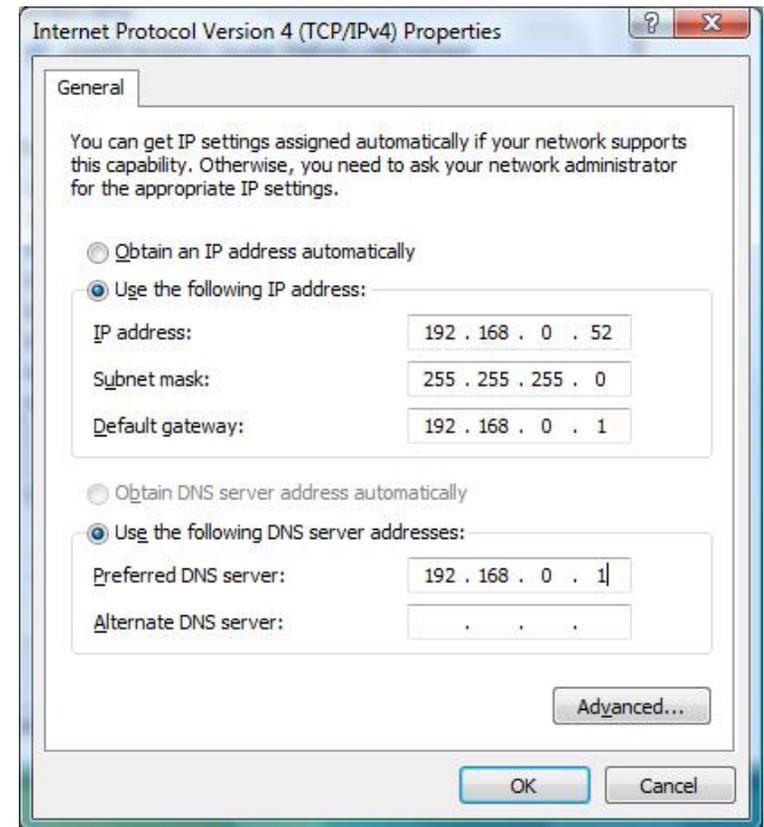
- Highlight **Internet Protocol Version 4 (TCP /IPv4)** and click **Properties**.

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

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 or gateway.
- Set **Primary DNS** the same as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).

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

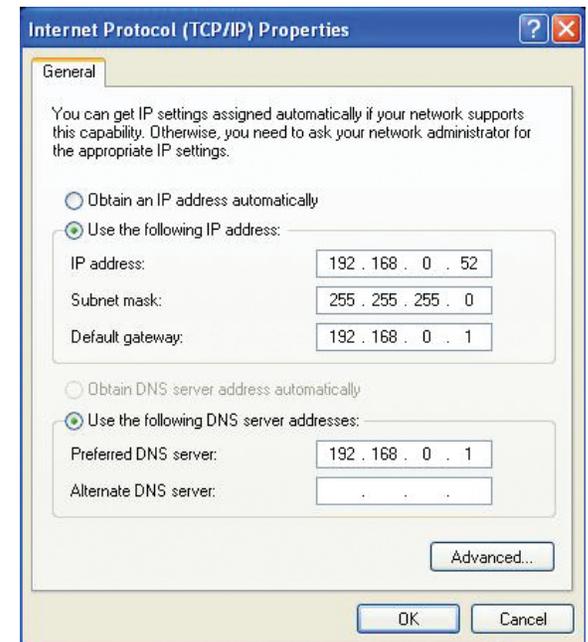


Windows® XP Users

- Click on **Start > Control Panel**. Make sure you are in Classic View. Double-click on the Network Connections icon.
- Right-click on the **Local Area Connection** which represents your D-Link wireless network adapter (or other adapter) which will be connected to your router.
- Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
- Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or 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 or gateway.
- Set **Primary DNS** as the LAN IP address of your router or gateway.
- The **Secondary DNS** is optional (you may enter a DNS server from your ISP).
- Click **OK** to save your settings.



Technical Specifications

Standards

- IEEE 802.11ac (draft)
- IEEE 802.11n
- IEEE 802.11g
- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3ab
- IEEE 802.3x Flow Control support

Physical Interface

- 4 Gigabit Ethernet LAN Ports
- 1 Gigabit Ethernet WAN Port
- 1 WPS Push Button
- Reset Button
- USB 2.0 Port

Security

- Wi-Fi Protected Access (WPA/WPA2)
- WPS™

LEDs

- Power/WPS
- Internet

Power

- DC 12V/2.0A

Operating Temperature

- 30° to 104° F (0° to 40° C)

Operating Humidity

- 10% to 90% non-condensing

Certifications

- CE
- FCC
- IC
- C-Tick
- CSA international

Dimensions

- 4.5" x 3.9" x 7.6"

Weight

- 0.77 lb

Warranty

- 1-Year Limited Warranty

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

² Frequency Range varies depending on country's regulation.

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. DGL-5500)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev A1))
- 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>

GPL Code Statement

This D-Link product includes software code developed by third parties, including software code subject to the GNU General Public License (“GPL”) or GNU Lesser General Public License (“LGPL”). As applicable, the terms of the GPL and LGPL, and information on obtaining access to the GPL code and LGPL code used in this product, are available to you at:

<http://tsd.dlink.com.tw/GPL.asp>

The GPL code and LGPL code used in this product is distributed WITHOUT ANY WARRANTY and is subject to the copyrights of one or more authors. For details, see the GPL code and the LGPL code for this product and the terms of the GPL and LGPL.

WRITTEN OFFER FOR GPL AND LGPL SOURCE CODE

Where such specific license terms entitle you to the source code of such software, D-Link will provide upon written request via email and/or traditional paper mail the applicable GPL and LGPL source code files via CD-ROM for a nominal cost to cover shipping and media charges as allowed under the GPL and LGPL.

Please direct all inquiries to:
Email: GPLCODE@DLink.com
Snail Mail:
Attn: GPLSOURCE REQUEST
D-Link Systems, Inc.
17595 Mt. Herrmann Street
Fountain Valley, CA 92708

GNU GENERAL PUBLIC LICENSE Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <<http://fsf.org/>> Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program—to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps:

(1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

“This License” refers to version 3 of the GNU General Public License.

“Copyright” also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

“The Program” refers to any copyrightable work licensed under this License. Each licensee is addressed as “you”. “Licensees” and “recipients” may be individuals or organizations.

To “modify” a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a “modified version” of the earlier work or a work “based on” the earlier work.

A “covered work” means either the unmodified Program or a work based on the Program.

To “propagate” a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To “convey” a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays “Appropriate Legal Notices” to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The “source code” for a work means the preferred form of the work for making modifications to it. “Object code” means any non-source form of a work.

A “Standard Interface” means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The “System Libraries” of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A “Major Component”, in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The “Corresponding Source” for a work in object code form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work’s System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf, under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

- a) The work must carry prominent notices stating that you modified it, and giving a relevant date.
- b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".
- c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.
- d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an “aggregate” if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation’s users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

- a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.
- b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.
- c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.
- d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.
- e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A “User Product” is either (1) a “consumer product”, which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, “normally used” refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

“Installation Information” for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

“Additional permissions” are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work). You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

- a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or
- b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or
- c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or
- d) Limiting the use for publicity purposes of names of licensors or authors of the material; or
- e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or
- f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered “further restrictions” within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An “entity transaction” is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party’s predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A “contributor” is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor’s “contributor version”.

A contributor’s “essential patent claims” are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, “control” includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor’s essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a “patent license” is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To “grant” such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. “Knowingly relying” means you have actual knowledge that, but for the patent license, your conveying the covered work in a country, or your recipient’s use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is “discriminatory” if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others’ Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License “or any later version” applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation. If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be used, that proxy’s public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an absolute waiver of all civil liability in connection with the Program, unless a warranty or assumption of liability accompanies a copy of the Program in return for a fee.

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
- Power supplies and fans: One (1) year
- 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 (USA):

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 DLink 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.

Submitting A Claim (Canada):

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:

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.
- 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 1-800-361-5265, 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.ca/>.
- 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 be rejected by D-Link. Products shall be fully insured by the customer and shipped to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. 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 Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, 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.
- RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST

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.

Copyright ©2013 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

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.

FCC Caution:

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

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

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

IMPORTANT NOTICE:**FCC Radiation Exposure Statement:**

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

ICC Notice:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes:

- (1) le dispositif ne doit pas produire de brouillage préjudiciable, et
- (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution:

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

Avertissement:

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement:

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

Déclaration d'exposition aux radiations:

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

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 1.0
August 14, 2013