# USER MANUAL

## DIR-627

VERSION 1.0


**Wireless N 300 Open Source Router**
**Wireless N 300 OPEN SOURCE 無線寬頻路由器**

D-Link®

WIRELESS

# Table of Contents

# Package Contents

- D-Link DIR-627 Wireless Router
- Power Adapter
- Ethernet Cable
- Wall Mount Kit
- User Manual on CD
- Open Source Manual on CD
- Warranty Card


**Note:** Using a power supply with a different voltage than the one included with the DIR-627 will cause damage and void the warranty for this product.

**Note:** Always attach the power cord plug to the power supply, before inserting the power cord and connected power supply to the wall outlet.

# System Requirements

- Ethernet-based Cable or DSL Modem
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer 6 or later or Mozilla Firefox 2.0 or later (for configuration)

# Features

- **Faster Wireless Networking** - The DIR-627 provides up to 300Mbps* wireless connection with other 802.11n wireless clients. This capability allows users to participate in real-time activities online, such as video streaming, online gaming, and real-time audio.

- **Compatible with 802.11b and 802.11g Devices** - The DIR-627 is still fully compatible with the IEEE 802.11b and IEEE 802.11g standard, so it can connect with existing 802.11b and IEEE 802.11g PCI, USB and Cardbus adapters.

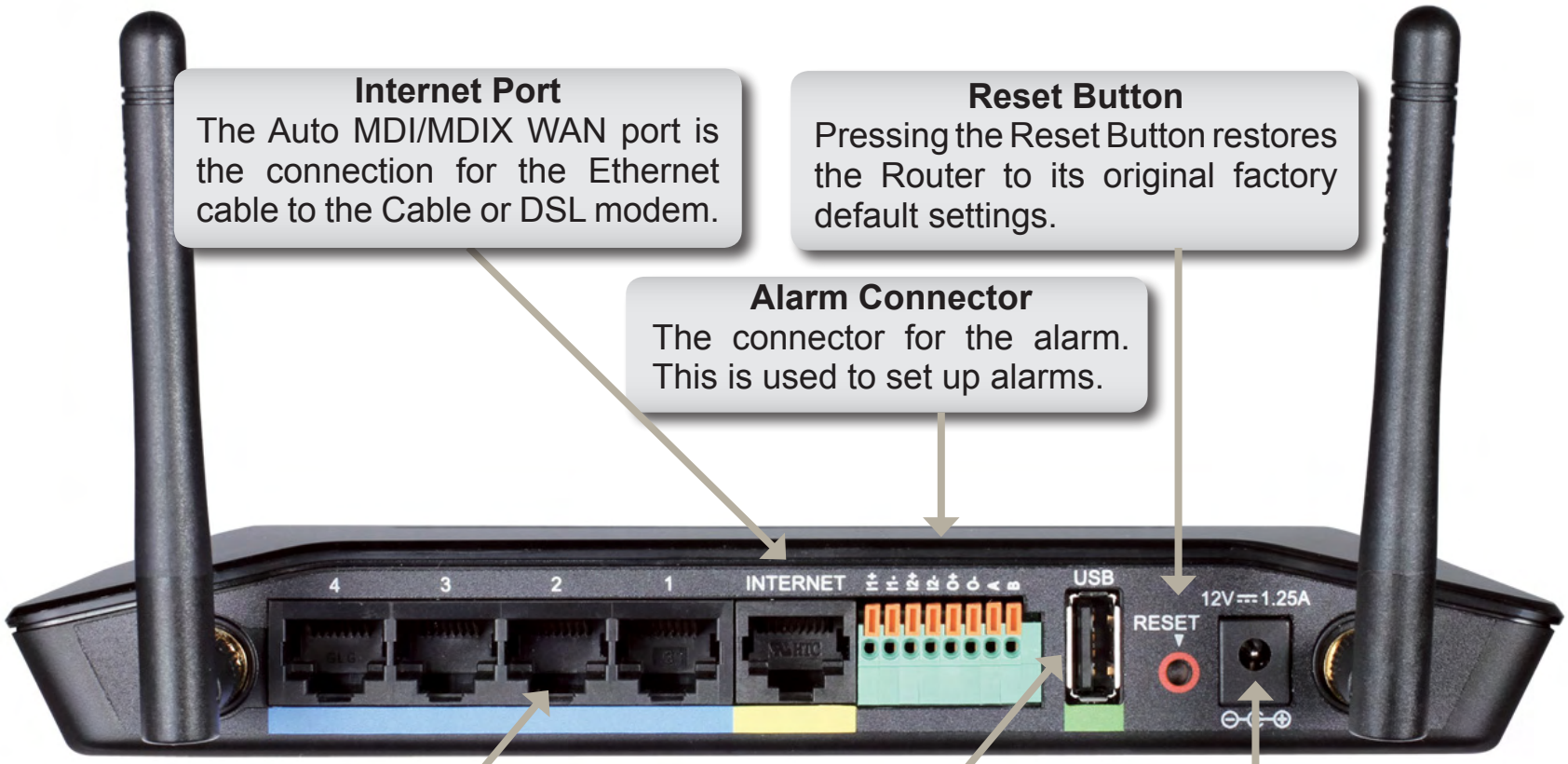
- **Supports four 10/100M Ethernet** ports - The DIR-627 has four LAN ports.

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

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

* Maximum wireless signal rate derived from IEEE Standard 802.11g and Draft 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
## Rear Panel Connections




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

**Reset Button**
Pressing the Reset Button restores the Router to its original factory default settings.

**Alarm Connector**
The connector for the alarm. This is used to set up alarms.

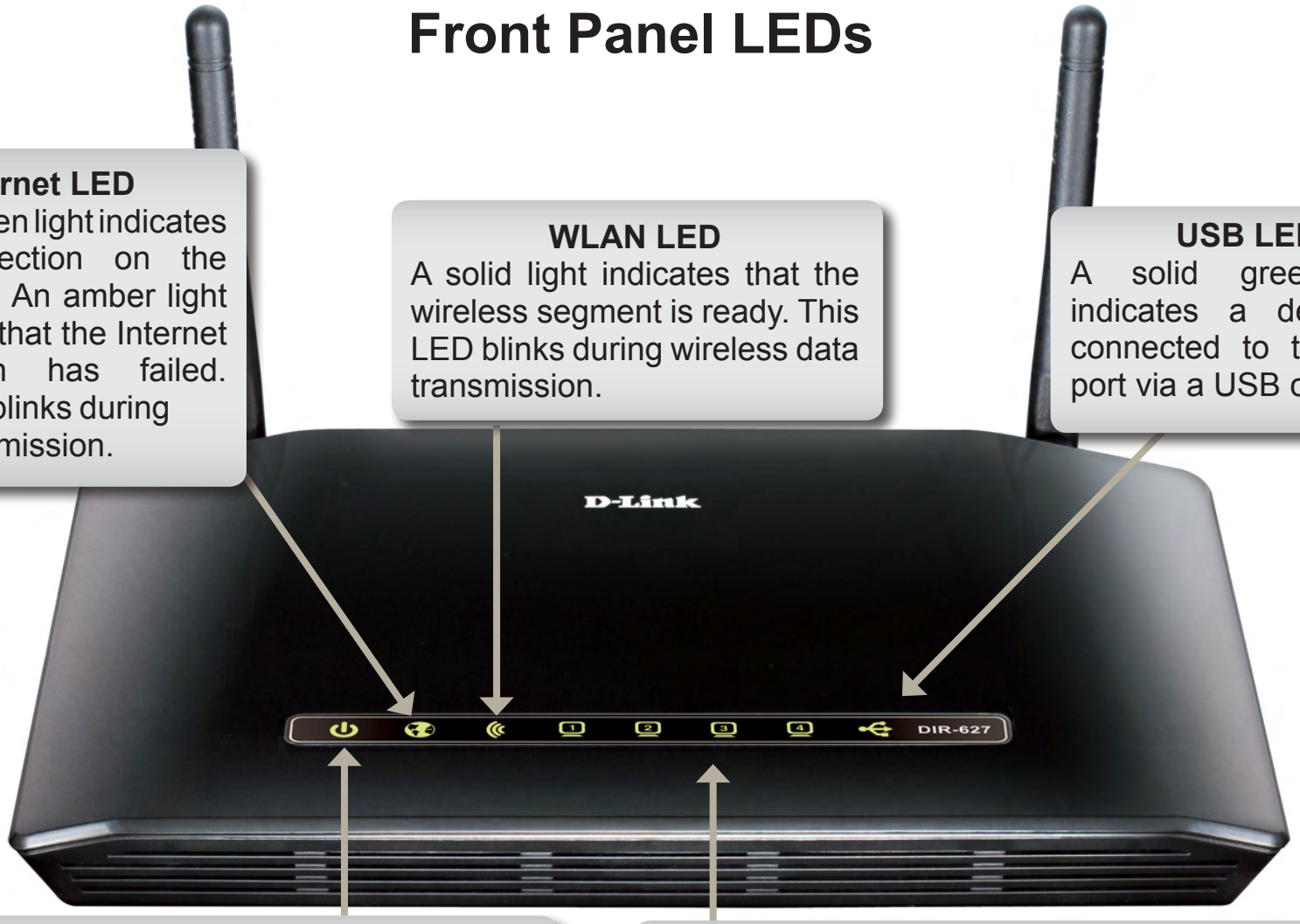
**LAN Ports**
Connect Ethernet devices such as computers, switches, and hubs.

**USB Port**
This USB port supports the D-Link SharePort function. Connect a multi-function printer, scanner, or USB storage device to the port and share the device through the network.

**Power Receptor**
The receptor for the supplied Power Adapter.

# Hardware Overview

## Front Panel LEDs




**Internet LED**
A solid green light indicates the connection on the WAN port. An amber light indicates that the Internet connection has failed. This LED blinks during data transmission.

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

**USB LED**
A solid green light indicates a device is connected to the USB port via a USB cable.

**Power LED**
A solid green light indicates a proper connection to the power supply. A blinking amber light indicates the device is booting up.

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

# Hardware Overview
## Right Side Panel LED

**WPS Button LED**
Use the WPS button on the right side panel of the Router to establish a secure connection to wireless clients that support WPS (Wi-Fi Protected Setup).

# Installation

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

# Before you Begin

Please configure the Router with the computer that was last connected directly to your modem. Also, you can only use the Ethernet port on your modem. If you were using the USB connection before using the Router, then you must turn off your modem, disconnect the USB cable and connect an Ethernet cable to the WAN port on the Router, and then turn the modem back on. In some cases, you may need to call your ISP to change connection types (USB to Ethernet).

If you have DSL and are connecting via PPPoE, make sure you disable or uninstall any PPPoE software such as WinPoet, Broadjump, or Ethernet 300 from your computer or you will not be able to connect to the Internet.

# Wireless Installation Considerations

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

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

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

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

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

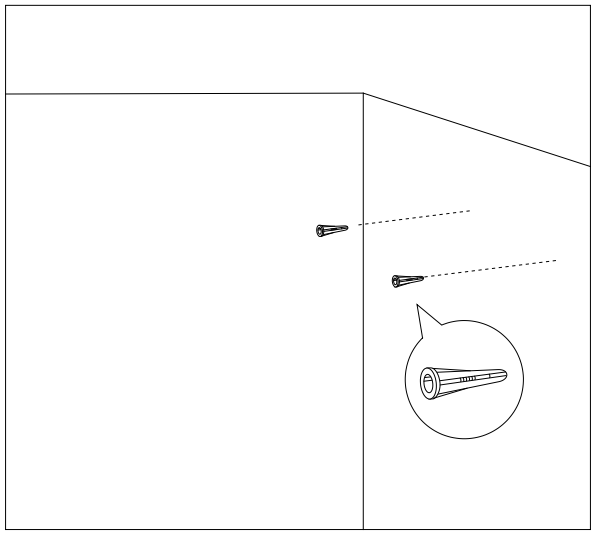
5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits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

# Wall Mounting Your Device

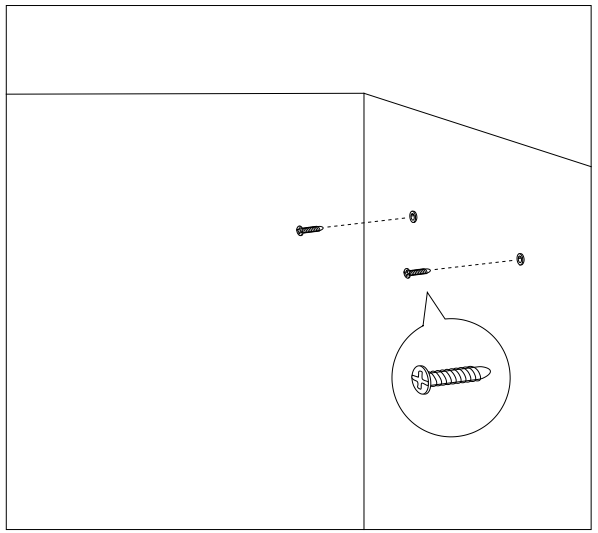
You can mount the Router to a wall or a partition for easy and convenient placement of your device.

To wall mount your device,

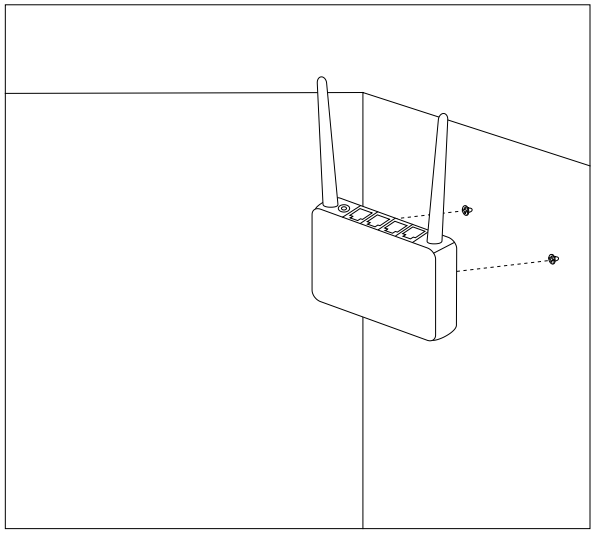
A. Place the two provided screw anchors about 15 centimeters (~6 inches) apart in the wall or partition where the device is to be placed.



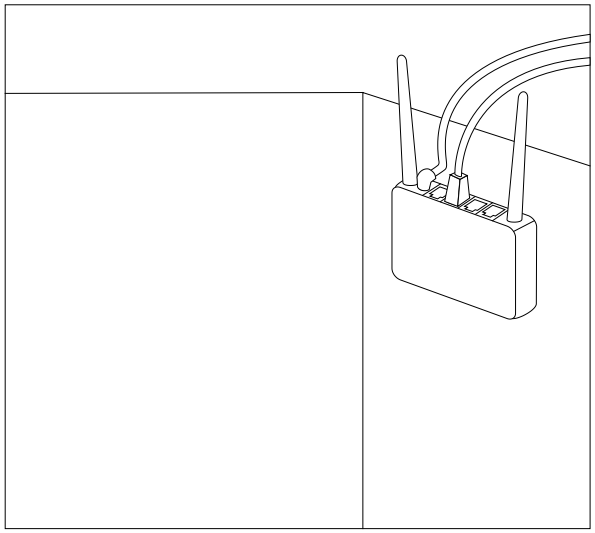
B. Drive the two provided screws into the screw anchors in the wall or partition where the device is to be placed.



C. Place the mounting holes on the bottom of the device over the screws to mount it to the wall or partition.



D. Connect your cables to the device.



# Connect to Cable/DSL/Satellite Modem

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

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

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

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

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

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

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

**7.** Turn on your computer.

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

**9.** Skip to page page 13 to configure your Router.

# Connect to Another Router

If you are connecting the Router to another router to use as a wireless access point and/or switch, you will have to do the following before connecting the router to your network:

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

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

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

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

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

4. Click **Setup** and then click **Network Settings**. Untick the Enable DHCP Server server check box. Click **Save Settings** to continue.

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

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

**7.** Connect an Ethernet cable in one of the LAN ports of the Router and connect it to your other router. Do not plug anything into the WAN port of the 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** and **Wireless Security** sections for more information on setting up your wireless network.

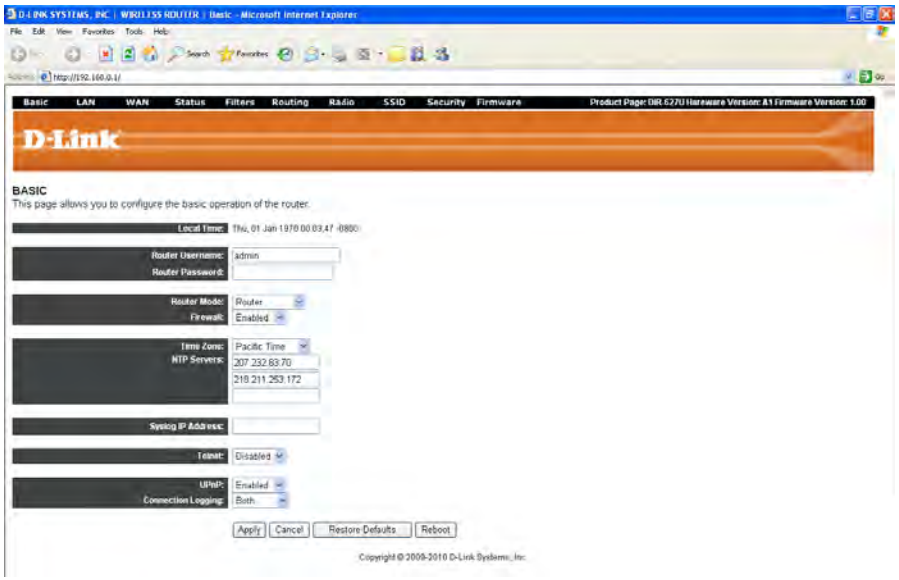
# Configuration

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

## Web-based Configuration Utility

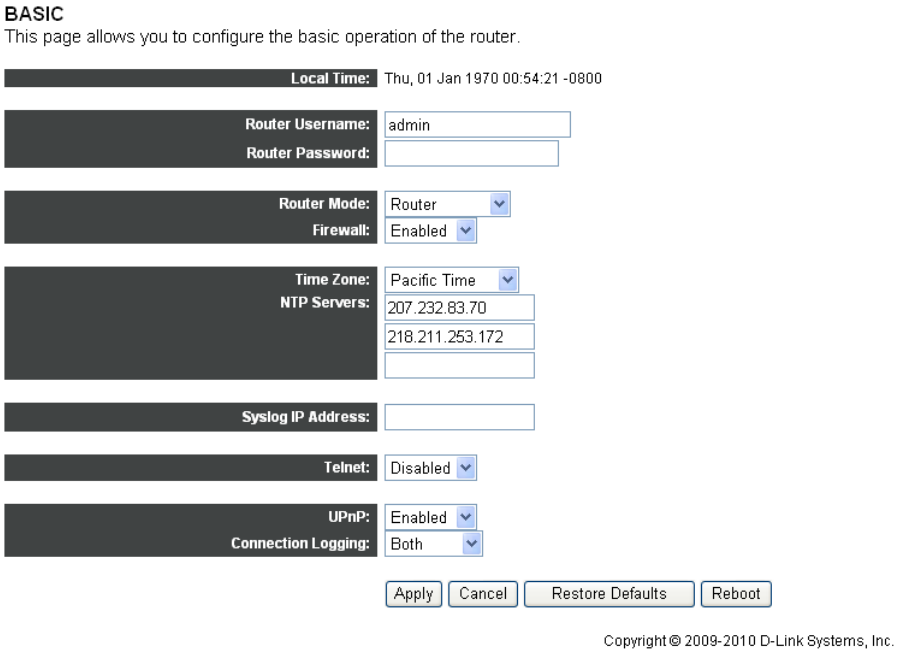
To access the configuration utility, open a Web-browser such as Mozilla Firefox or Internet Explorer and enter the IP address of the Router (192.168.0.1).


The opening Router page appears.



# Basic

The Basic page allows users to configure the basic operations of the Router.




**Local Time:** Displays the Local TIme maintained by the Router.

**Router User Name:** Set the router user name for access to the Router's Web interface. The initial router user name is *admin*. Once this is set up, users can leave this field and the router password field blank to disable the authentication login process.

**Router Password:** Set the router password for access to the Router's Web interface. Once this is set up, users can leave this field and the router user name field blank to disable the authentication login process.

**Router Mode:** Choose either *Router* or *Access Point*. When the mode is *Access Point*, the LAN DHCP server, LAN Spanning Tree Protocol, and WAN protocol are disabled.

**Firewall:** Choose either *Enabled* or *Disabled*. The firewall default state is *Enabled*. Connections from the WAN are still allowed when the firewall is *Disabled*.

**Time Zone:** Select the correct time zone for the Router's location: *Pacific Time*, *Mountain Time*, *Central Time*, or *Eastern Time*.

**NTP Servers:** Enter the NTP server IP addresses to use for time synchronization.

**Syslog IP Address:** Enter the system log IP address where system log messages will be sent.

.

**Telnet:** Choose either *Enabled* or *Disabled*. Telnet is *Disabled* by default.

**UPnP:** Choose either *Enabled* or *Disabled*. Universal Plug and Play is *Enabled* by default.

**Connection Logging:** Choose *Disabled*, *Denied*, *Accepted,* or *Both* to set which connections the Router should log. *Denied* enables logging of denied connections, *Accepted* enables logging of accepted connections, and *Both* enables logging of both denied and accepted connections. The default setting is *Both*.

# LAN

The LAN page allows users to configure the LAN of the Router.

**MAC Address:** Displays the MAC address of the LAN interface. This is also referred to as the Ethernet address.

**IP Address:** Set the IP address of the LAN interface.

**Subnet Mask:** Set the IP netmask of the LAN interface.

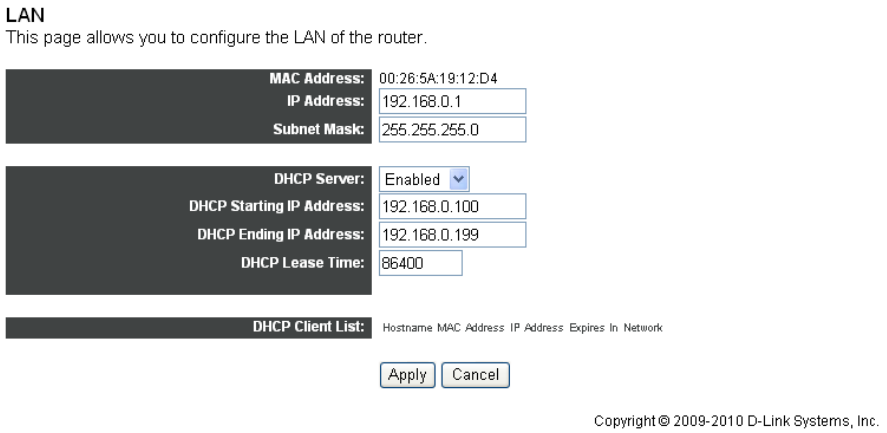
**DHCP Server:** Choose either *Enabled* or *Disabled*. This controls DHCP server functionality on the LAN.

**DHCP Starting IP Address:** Set the start of the IP address range that the DHCP server will use.

**DHCP Ending IP Address:** Set the end of the IP address range that the DHCP server will use.

**DHCP Lease Time:** Set the number of seconds a DHCP lease should be valid for.

**DHCP Client List:** This displays active DHCP leases since the last reboot.



# WAN

The WAN page allows users to configure the WAN connections of the Router.

**Protocol:** Set the method to obtain an IP address for the connection: *DHCP*, *Static*, or *PPPoE*.

**Host Name:** Set a host name. Some ISPs require a host name be provided when requesting an IP address using DHCP. The default host name is *DIR-627*.

**Domain Name:** Set the domain name provided to LAN clients who request an IP address through DHCP.

**MAC Address:** Some ISPs require users to enter a specific MAC address. This MAC cloning feature allows users to set the MAC address of the WAN interface. The MAC address format is: XX:XX:XX:XX:XX:XX.

**IP Address:** Set the IP address of the connection.

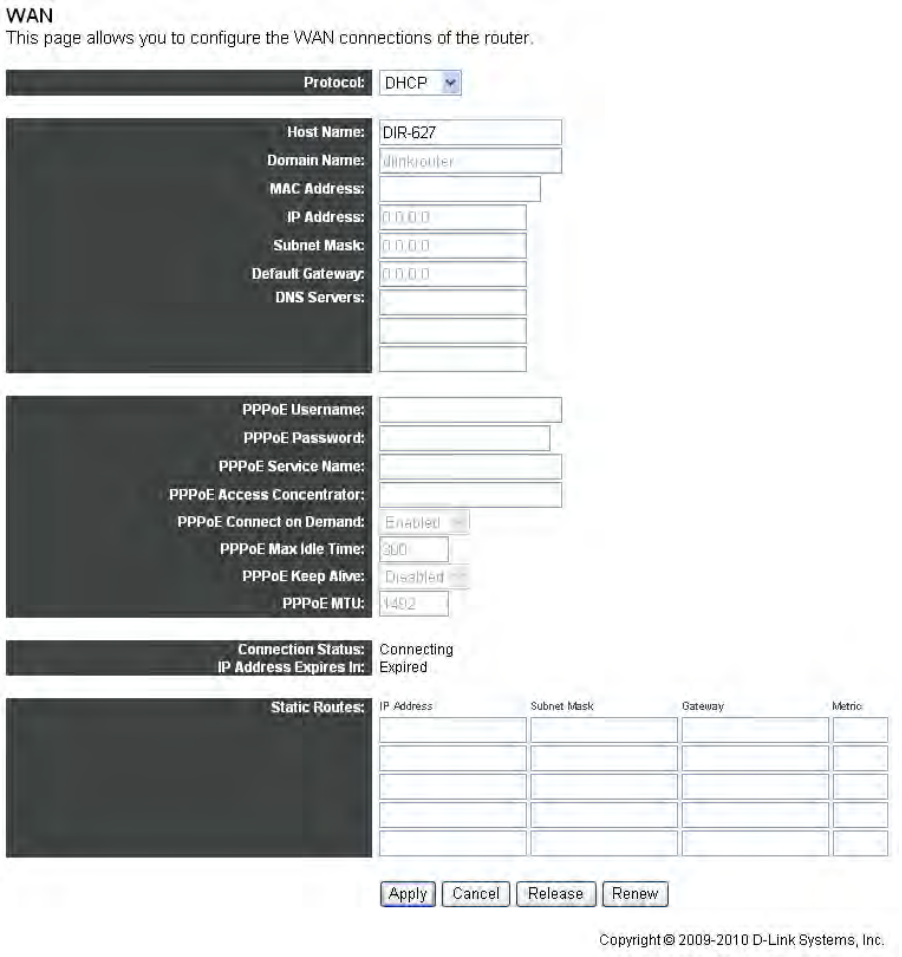
**Subnet Mask:** Set the IP netmask of the connection.

**Default Gateway:** Set the IP address of the default gateway of the connection.

**DNS Servers:** Set the primary and secondary IP addresses of the DNS servers used for resolving host names.

**PPPoE User Name:** Set the user name for authentication with a PPPoE server.

**PPPoE Password:** Set the password for authentication with a PPPoE server.



**PPPoE Service Name:** Set the PPPoE service name. This is required by some ISPs.

**PPPoE Access Concentrator:** Set the PPPoE access concentrator. This is required by some ISPs.

**PPPoE Connect On Demand:** Choose either *Enabled* or *Disabled*. This determines whether the PPPoE link should be automatically disconnected if no traffic has been observed for the period specifies by the PPPoE Max Idle Time.

**PPPoE Max Idle Time:** Set the number of seconds to wait before disconnecting the PPPoE link if PPPoE Connect on Demand is *Enabled*. The default is *300* seconds.

**PPPoE Keep Alive:** Choose either *Enabled* or *Disabled*. This determines whether the PPPoE link should be automatically restored if it is lost. This setting has no effect if PPPoE Connect on Demand is *Enabled*.

**PPPoE MTU:** Set the maximum number of bytes that the PPPoE interface will transmit in a single Ethernet frame.

**Connection Status:** This displays the connection state.

**IP Address Expires In:** This displays IP address lease information.

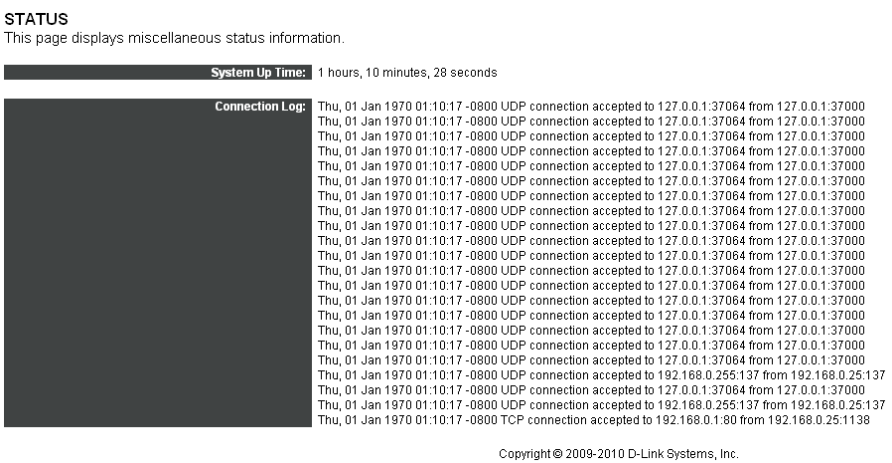
**Static Routes:** Set up static routes in this section.

# Status

The Status page displays miscellaneous status information.

**System Up Time:** Displays the system up time since the Router was last booted up.

**Connection Log:** Displays a log of recent connection attempts.



# Filters

The Filters page allows users to configure LAN filters for the Router. The LAN machines affected by the filters will not be able to communicate through the WAN but will be able to communicate with each other and with the Router itself.

**LAN MAC Filter Mode:** Set whether clients with the specified MAC address are denied or allowed access to the Router and the WAN. The options are: *Disabled*, *Allow*, or *Deny*.

**LAN MAC Filters:** The Router filters packets from LAN machines with specified MAC addresses. The MAC address format is: XX:XX:XX:XX:XX:XX.

**LAN Client Filters** The Router filters packets from IP addresses destined to certain port ranges during the specified times.

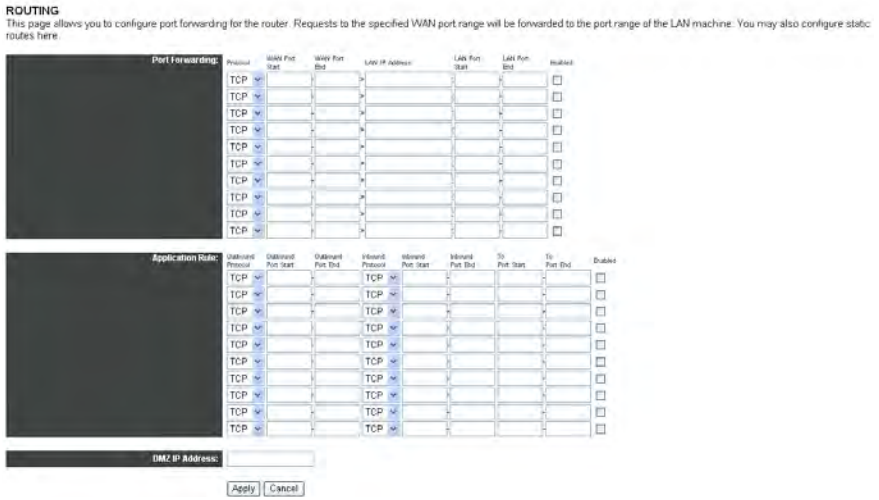
# Routing

The Routing page allows users to configure port forwarding for the Router. Requests to the specified WAN port range will be forwarded to the port range of the LAN machine. Users may also configure static routes here.

**Port Forwarding:** The Router allows users to forward packets destined in the first range to the LAN machine with the specified IP address. In addition, users may specify a second range (please note that the ranges must not overlap and they must be the same size).

**Application Rule:** Enter the appropriate information to automatically forward connections.

**DMZ IP Address** This allows users to forward all other incoming WAN packets to the LAN machine with the specified IP address.



# Radio

The Radio page allows users to configure the physical wireless interfaces.

**Interface:** Choose either *Enabled* or *Disabled*. This enables or disables the wireless interface.

**Control Channel:** Set the channel on which to operate on: *Auto*, *1*, *2*, *3*, *4*, *5*, *6*, *7*, *8*, *9*, *10*, or *11*.

**802.11n Mode:** Choose either *Auto* or *Off* to enable or disable 802.11n support.

**Bandwidth:** Choose the channel bandwith, either *20 MHz in Both Bands* or *40 MHz in Both Bands*.

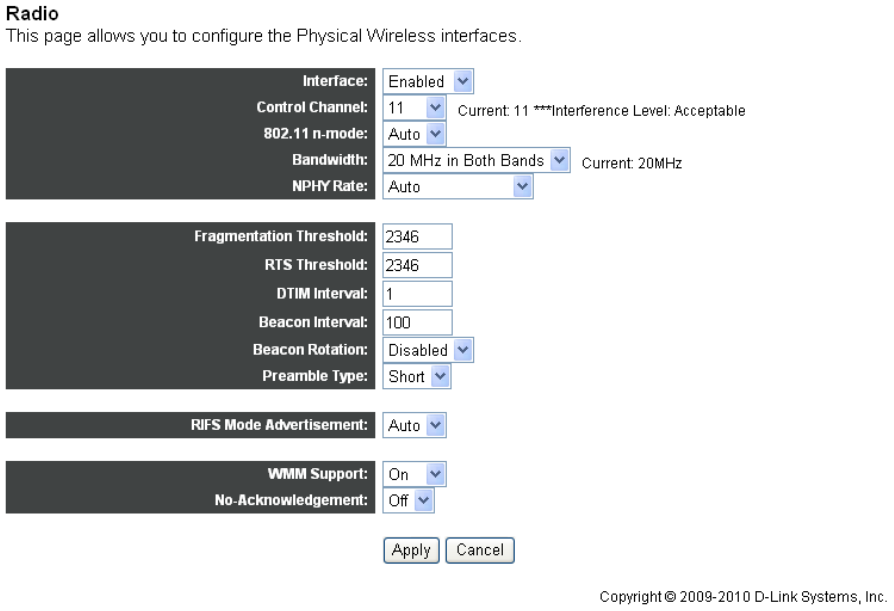
**NPHY Rate:** Set the NPHY Rate (MCS Index): *Auto*, *Use Legacy Rate*, *0: 6.5 Mbps*, *1: 13 Mbps*, *2: 19.5 Mbps*, *3: 26 Mbps*, *4: 39 Mbps*, *5: 52 Mbps*, *6: 58.5 Mbps*, *7: 65 Mbps*, *8: 13 Mbps*, *9: 26 Mbps*, *10: 39 Mbps*, *11: 52 Mbps*, *12: 78 Mbps*, *13: 104 Mbps*, *14: 117 Mbps*, or *15: 130 Mbps.*

**Fragmentation Threshold:** Set the fragmentation threshold. The default is *2346*.

**RTS Threshold:** Set the Request to Send (RTS) threshold. The default is *2346*.

**DTIM Interval:** Set the Delivery Traffic Indication Message (DTIM) value. This is the wakeup interval for clients in power save mode. The default is *1*.

**Beacon Interval:** Set the beacon interval for the access point. The default is *100*.



**Beacon Rotation:** Choose either *Enabled* or *Disabled*. This enables or disables the rotation of the beacon order when running in Multi BSS mode.

**Preamble Type:** Choose either *Short* or *Long*. This sets whether short or long preambles are used. Short preambles improve throughput but all clients in the wireless network must support this capability if selected.

**RIFS Mode Advertisement:** Choose either *Auto* or *Off*. Reduced Interframe Spacing (RIFS) mode is used to advertise in beacons and probe responses.

**WMM Support:** Choose *Auto*, *Off*, or *On* to set Wi-Fi Multimedia (WMM) support.

**No Acknowledgement:** Choose either *Off* or *On* to enable or disable Wi-Fi Multimedia (WMM) non-acknowledgement.

# SSID

The SSID page allows users to configure virtual interfaces for each physical interface.

**Enable Wireless:** Choose either *Enabled* or *Disabled*. This enables or disables the wireless interface.

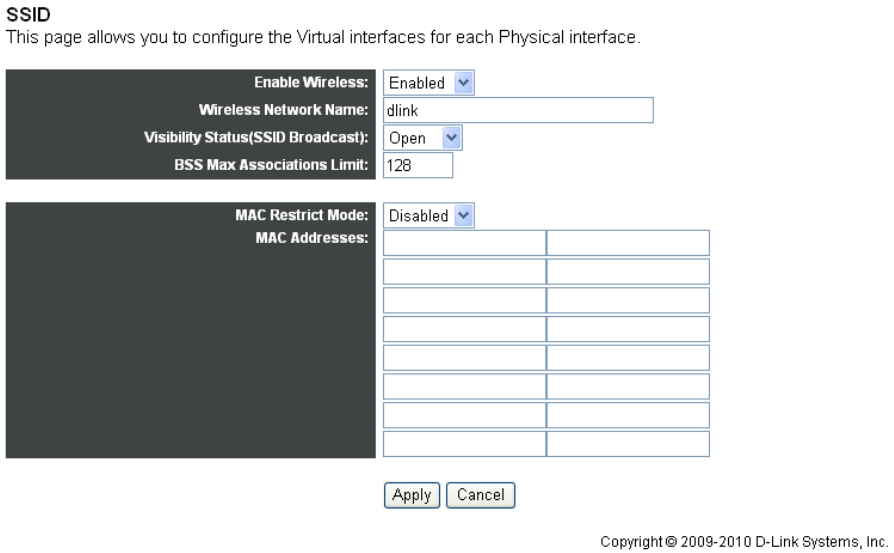
**Wireless Network Name:** Set the service set identifier (SSID), otherwise known as the network name, of this network.

**Visibility Status (SSID Broadcast):** Choose either *Open* or *Closed. Open* reveals the network to active scans while *Closed* hides the network from active scans.

**BSS Max Associations Limit:** Set the maximum associations for this basic service set (BSS). The default is *128*.

**MAC Restrict Mode:** Choose *Enabled*, *Allow*, or *Deny* to determine whether clients with the specified MAC address are allowed or denied wireless access*:*

**MAC Addresses:** Enter the MAC address(es) of clients that are either allowed or denied wireless acess. The MAC address format is XX:XX:XX:XX:XX:XX.



# Security

The Security page allows users to configure security for the wireless interfaces.

**WPS Configuration:** Choose either *Enabled* or *Disabled* to enable or disable Wi-Fi Protected Setup (WPS) simple configuration mode.

**Device Name:** Enter a mnemonic name that can be used to identify the Router.

**Device WPS UUID:** This displays the Wi-Fi Protected Setup (WPS) UUID number of the Router.

**Device PIN:** Click the **Generate** button to create a PIN number for the Router.

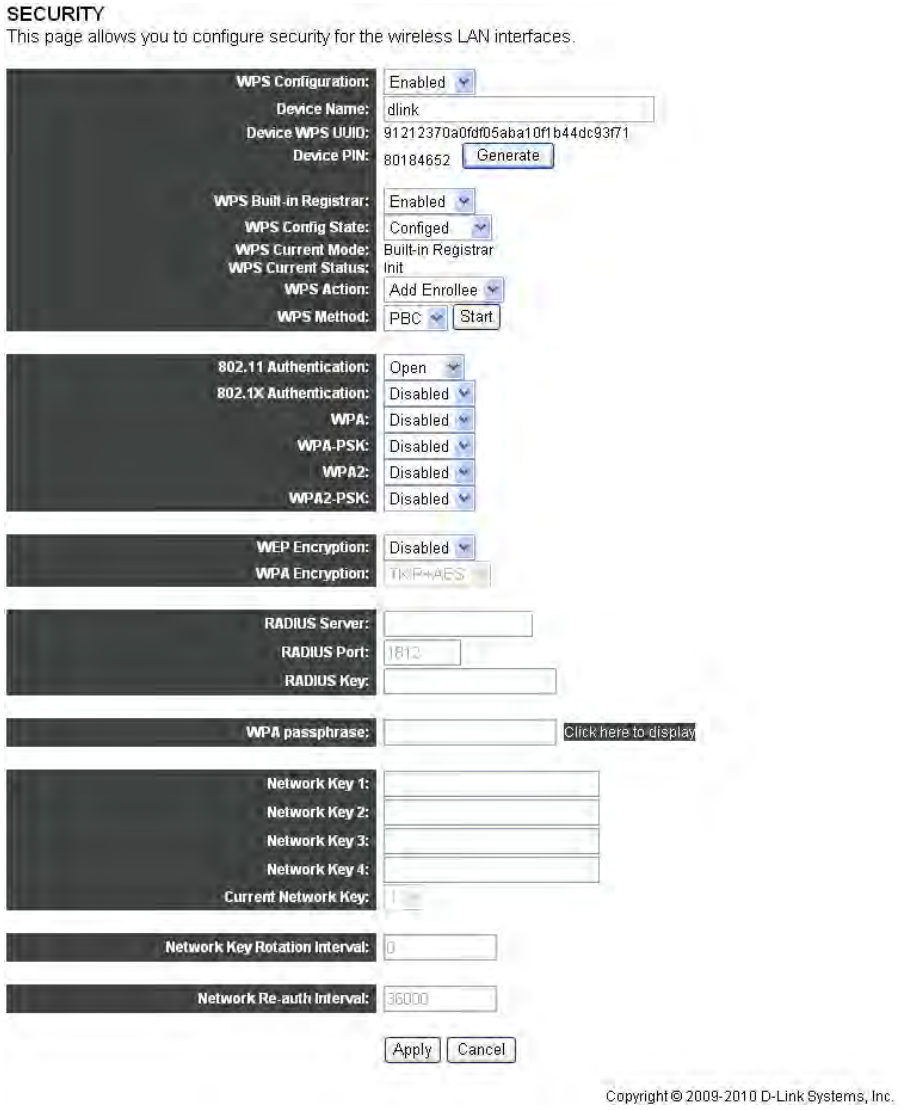
**WPS Built-in Registrar:** Choose either *Enabled* or *Disabled* to enable or disable the Router's built-in registrar feature.

**WPS Config State:** Set the Wi-Fi Protected Setup (WPS) configuration state to *Config(ur)ed* or *Unconfig(ur)ed*.

**WPS Current Mode:** Displays the current Wi-Fi Protected Setup (WPS) mode.

**WPS Current Status:** Displays the Wi-Fi Protected Setup (WPS) processing status.

**WPS Action:** Choose the desired Wi-Fi Protected Setup (WPS) action, *Add Enrollee* or *Config AP*.



**WPS Method:** Click the **Start** button to use the Push Button Configuration (PBC) Wi-Fi Protected Setup (WPS) method.

**802.11 Authentication:** Choose the 802.11 authentication method, either *Open* or *Shared*.

**802.1X Authentication:** Once the user has decided on the network authentication type, choose either *Enabled* or *Disabled* to enable or disable network authentication.

**WPA:** Choose either *Enabled* or *Disabled* to enable or disable Wi-Fi Protected Access (WPA).

**WPA-PSK:** Choose either *Enabled* or *Disabled* to enable or disable Wi-Fi Protected Access Pre-Shared Key (WPA-PSK).

**WPA2:** Choose either *Enabled* or *Disabled* to enable or disable Wi-Fi Protected Access 2 (WPA2).

**WPA2-PSK:** Choose either *Enabled* or *Disabled* to enable or disable Wi-Fi Protected Access 2 Pre-Shared Key (WPA2-PSK).

**WEP Encryption:** Choose either *Enabled* or *Disabled* to enable or disable Wired Equivalent Privacy (WEP) encryption.

**WPA Encryption:** First enable WPA above and then choose the WPA data encryption algorithm, *AES* or *TKIP+AES*.

**RADIUS Server:** Set the IP address of the RADIUS server used for authentication and dynamic key derivation.

**RADIUS Port:** Set the UDP port number of the RADIUS server. The port number is usually *1812* or *1645*, depending on the server. The default RADIUS port number is *1812*.

**RADIUS Key:** Set the shared secret for the RADIUS connection.

**WPA Passphrase:** Set the WPA passphrase. Use the **Click here to display** button to display the WPA passphrase.

**Network Key 1-4:** Enter five ASCII characters or ten hexadecimal digits for a 64-bit key. Enter 13 ASCII characters or 26 hexadecimal digits for a 128-bit key.

**Current Network Key:** Select which network key is used for encrypting outbound data and/or authenticating clients.

**Network Key Rotation Interval:** Set the network key rotation interval, in seconds. Leave blank or set to zero to disable the rotation.

**Network Re-auth Interval:** Set the network re-authentication interval, in seconds. Leave blank or set to zero to disable periodic network authentication.

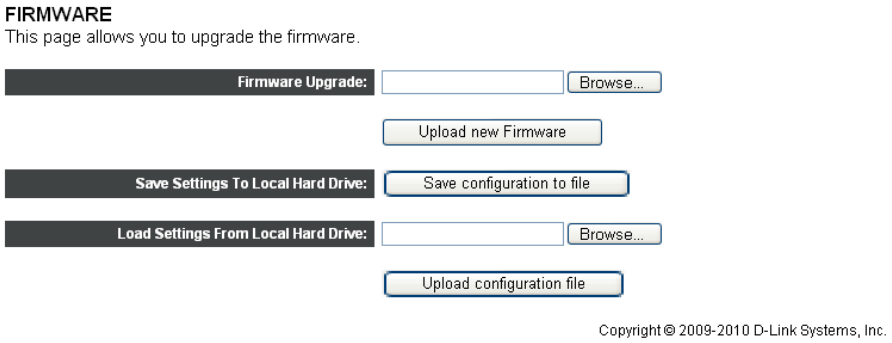
# Firmware

The Firmware page allows users to upgrade the Router firmware.

**Firmware Upgrade:** Enter the new firmware to upload to the Router or click **Browse** to locate the firmware on the user's computer. Click **Upload new Firmware** to initiate the firmware upgrade.

**Save Settings To Local Hard Drive:** Click **Save configuration to file** to save NV-RAM variables to file.

**Load Settings From Local Hard Drive:** Enter the filename of the saved NV-RAM file here or click **Browse** to locate the file on the user's computer. Click **Upload configuration file** to initiate the configuration file upload.



# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-627 offers the following types of security:

- WPA2 (Wi-Fi Protected Access 2)
- WPA (Wi-Fi Protected Access)
- WEP (Wired Equivalent Privacy)
- WPA2-PSK (Pre-Shared Key)
- WPA-PSK (Pre-Shared Key)

# What is WEP?

WEP stands for Wired Equivalent Privacy. It is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. WEP provides security by encrypting data over your wireless network so that it is protected as it is transmitted from one wireless device to another.

To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily.

# Configure WEP

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

1. Log into the Web-based configuration by opening a Web browser and entering the IP address of the Router (192.168.0.1). Click **Security** at the top of the window.

2. Go to **WEP Encryption** and toggle *Disabled* to *Enabled*.

3. Go to **802.11 Authentication** and select either *Shared* or *Open*. *Shared* is recommended as it provides greater security when WEP is enabled.

4. Go to **Network Key 1** and enter a WEP key (passphrase) that you create. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using hexadecimal or ASCII. Hexadecimal is recommended (letters A-F and numbers 0-9 are valid). In ASCII all numbers and letters are valid.

5. Go to **Current Network Key** and select which network key to use for encrypting outbound data and/or authenticating clients.

6. Click **Apply** to save your settings. If you are configuring the Router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the Router.

# What is WPA?

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

The two 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.

# Configure WPA-PSK

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

1. Log into the Web-based configuration by opening a Web browser and entering the IP address of the router (192.168.0.1). Click **Security** at the top of the window.

2. Go to **802.11 Authentication** and select *Open*.

3. Go to **WPA-PSK** and toggle *Disabled* to *Enabled*.

4. Go to **WPA Encryption** and select *AES* or *TKIP+AES*.

5. Go to **WPA Passphrase** and enter the WPA Passphrase that is being used on your wireless network.

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

# Configure WPA2-PSK

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

1. Log into the Web-based configuration by opening a Web browser and entering the IP address of the router (192.168.0.1). Click **Security** at the top of the window.

2. Go to **802.11 Authentication** and select *Open*.

3. Go to **WPA2-PSK** and toggle *Disabled* to *Enabled*.

4. Go to **WPA Encryption** and select *AES* or *TKIP+AES*.

5. Go to **WPA Passphrase** and enter the WPA Passphrase that is being used on your wireless network.

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

# Configure WPA

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

If you are using a RADIUS server for wireless authentication that is using WPA encryption, carry out the following:

1. Log into the Web-based configuration by opening a Web browser and entering the IP address of the Router (192.168.0.1). Click **Security** at the top of the window.

2. Go to **802.11 Authentication** and select *Open*.

3. Go to **WPA** and toggle *Disabled* to *Enabled*.

4. Go to **WPA Encryption** and select *AES* or *TKIP+AE*.

5. Go to **RADIUS Server** and enter the IP address of your RADIUS server.

6. Go to **RADIUS Port** and enter the port number that is being used by your RADIUS server. *1812* is the default port.

7. Go to **RADIUS Key** and enter the security key that is being used by your RADIUS server.

8. Go to **Network Key Rotation Interval** and enter a value, in seconds, for the interval for cycling through the network keys entered above. If this field is left blank, this feature is disabled.

9. Go to **Network Re-auth Interval** and enter a value, in seconds, for the interval for periodic network re-authentication. If this field is left blank, this feature is disabled.

10. Click **Apply** to save your settings. If you are configuring the Router with a wireless adapter, you will lose connectivity until you enable WPA on your adapter and enter the same passphrase as you did on the Router.

# Configure WPA2

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

If you are using a RADIUS server for wireless authentication that is using WPA2 encryption, carry out the following:

1. Log into the Web-based configuration by opening a Web browser and entering the IP address of the Router (192.168.0.1). Click **Security** at the top of the window.

2. Go to **802.11 Authentication** and select *Open*.

3. Go to **WPA2** and toggle *Disabled* to *Enabled*.

4. Go to **RADIUS Server** and enter the IP address of your RADIUS server.

5. Go to **RADIUS Port** and enter the port number that is being used by your RADIUS server. *1812* is the default port.

6. Go to **RADIUS Key** and enter the security key that is being used by your RADIUS server.

7. Go to **WPA Encryption** and select *AES* or *TKIP+AE*.

8. Go to **Network Key Rotation Interval** and enter a value, in seconds, for the interval for cycling through the network keys entered above. If this field is left blank, this feature is disabled.

9. Go to **Network Re-auth Interval** and enter a value, in seconds, for the interval for periodic network re-authentication. If this field is left blank, this feature is disabled.

10. Click **Apply** to save your settings. If you are configuring the Router with a wireless adapter, you will lose connectivity until you enable WPA2 on your adapter and enter the same passphrase as you did on the Router.

# Configure WPA (RADIUS)

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

1. Log into the Web-based configuration by opening a Web browser and entering the IP address of the Router (192.168.0.1). Click **Security** at the top of the window.

2. Go to **802.11 Authentication** and select *Open*.

3. Go to **WPA** and toggle *Disabled* to *Enabled*.

4. Go to **WPA Encryption** and select *AES* or *TKIP+AE*.

5. Go to **RADIUS Server** and enter the IP Address of your RADIUS server.

6. Go to **RADIUS Port** and enter the port you are using with your RADIUS server. *1812* is the default port.

7. Go to **RADIUS Key** and enter the security key.

8. Click **Apply** to save your settings.

# Configure and WPA2 (RADIUS)

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

1. Log into the Web-based configuration by opening a Web browser and entering the IP address of the Router (192.168.0.1). Click **Security** at the top of the window.

2. Go to **802.11 Authentication** and select *Open*.

3. Go to **WPA2** and toggle *Disabled* to *Enabled*.

4. Go to **WPA Encryption** and select *AES* or *TKIP+AE*.

5. Go to **RADIUS Server** and enter the IP Address of your RADIUS server.

6. Go to **RADIUS Port** and enter the port you are using with your RADIUS server. *1812* is the default port.

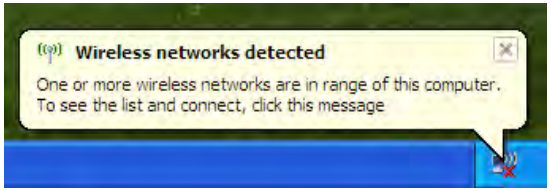
7. Go to **RADIUS Key** and enter the security key.

8. Click **Apply** to save your settings.

# Connect to a Wireless Network Using Windows® XP

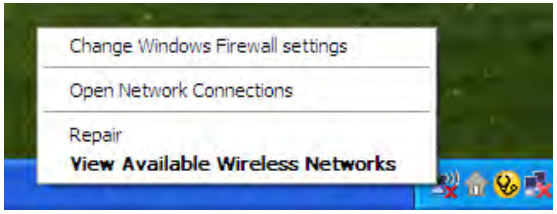
Windows® XP users may use the built-in wireless utility (Zero Configuration Utility). The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help with connecting to a wireless network.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

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



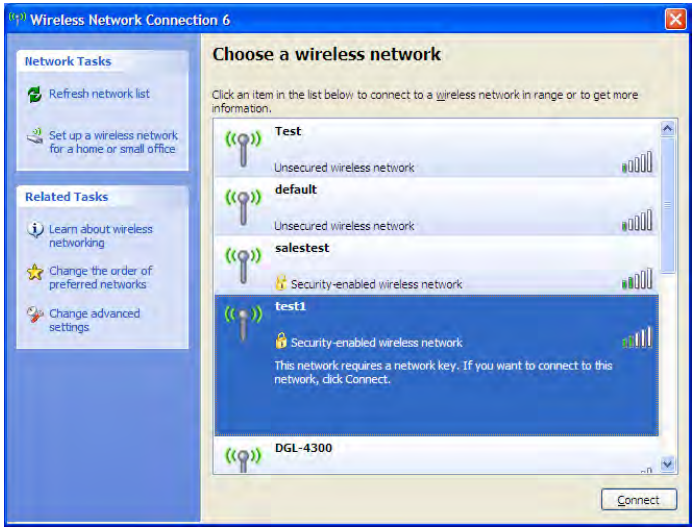

or

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.

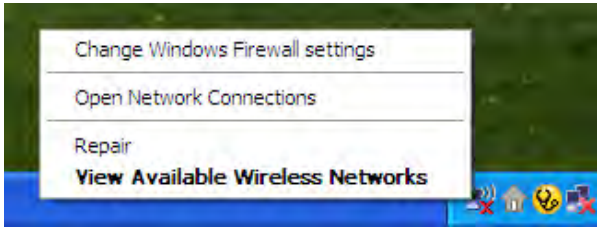
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



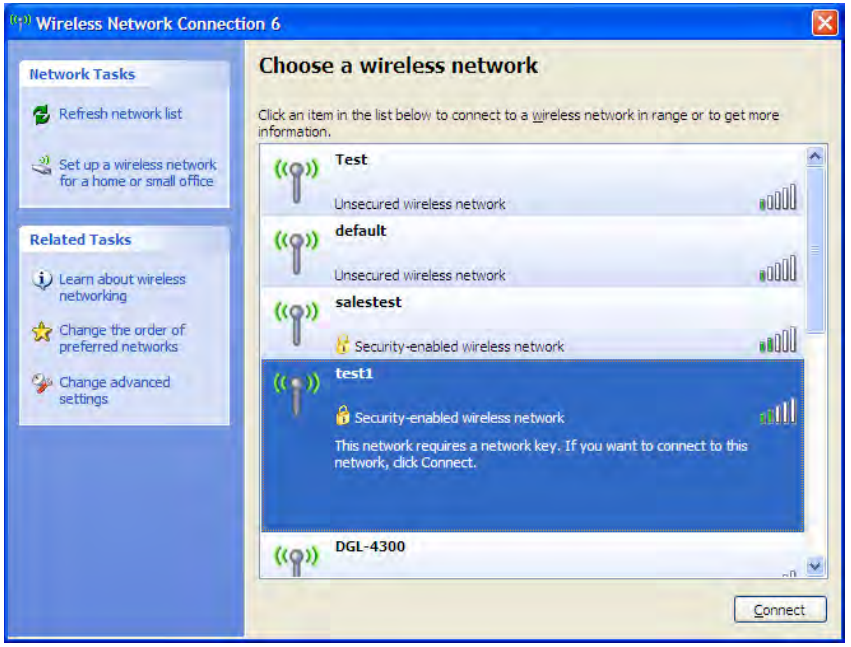
# Configure WEP

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

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

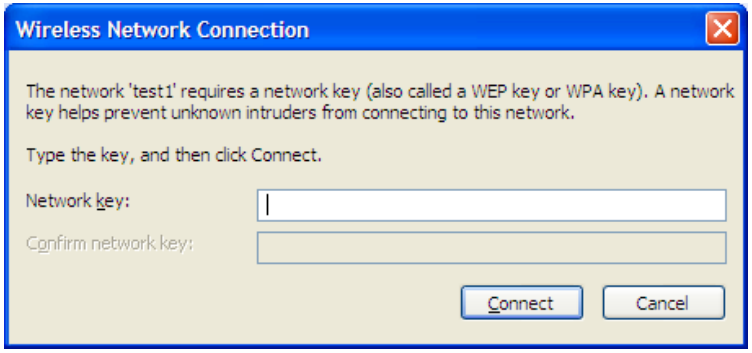



2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



3. The **Wireless Network Connection** box will appear. Enter the same WEP key that is on your Router and click **Connect**.

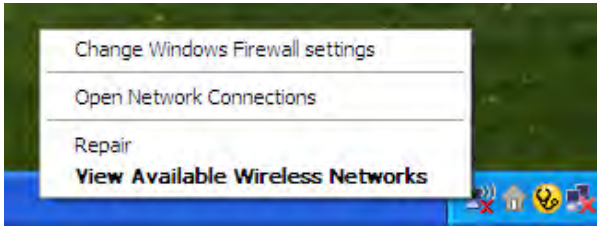
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



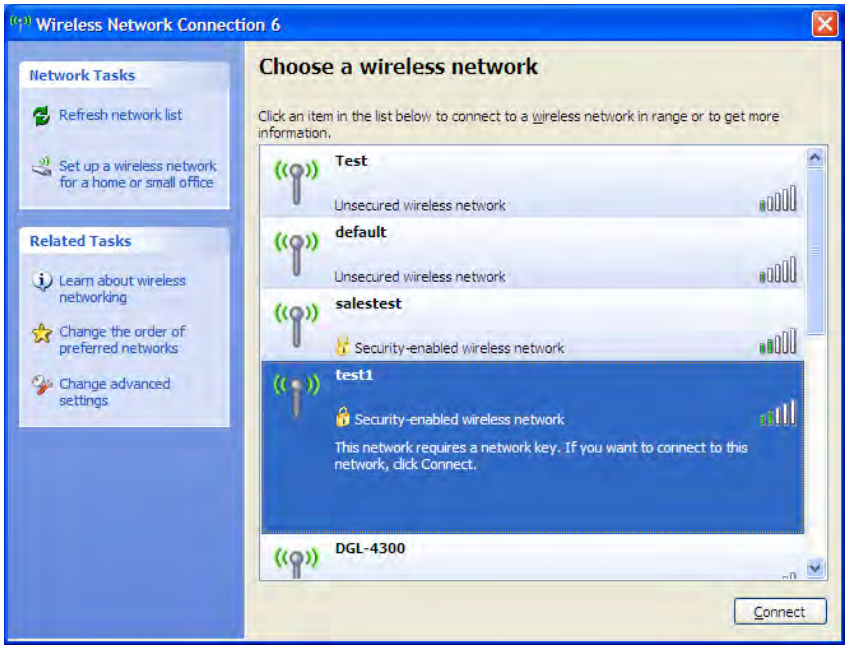
# Configure WPA-PSK

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

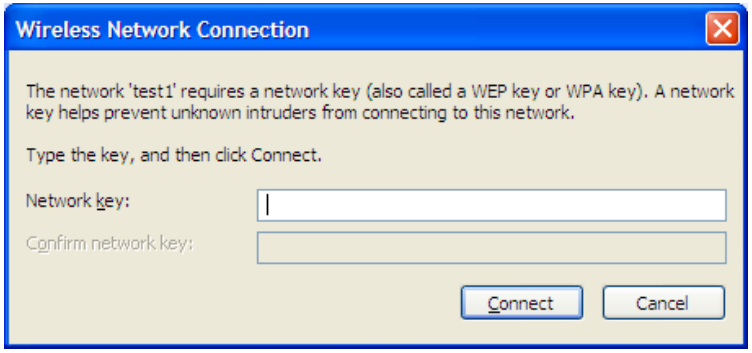
1. Open the Windows® XP Wireless Utility by right-clicking on the wireless computer icon in your system tray (lower-right corner of screen). Select **View Available Wireless Networks**.




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.

# Setting Up Wi-Fi Protection (WCN 2.0 in Windows Vista)

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

## Initial Router Configuration for Wi-Fi Protection

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 use the traditional Ethernet approach.

If you are running Windows Vista, use the WPS Configuration drop-down menu on the **Security** window to select *Enabled*. Use the Current PIN that is displayed on the **Security** window or choose to click the Device PIN **Generate** 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.

# Setting Up a Configured Router

Once the Router has been configured, you can use the push button on the Router or third party software to invite a newcomer to join your Wi-Fi protected network. For maximum security, the software method is recommended. However, the push button method is ideal if there is no access to a GUI.

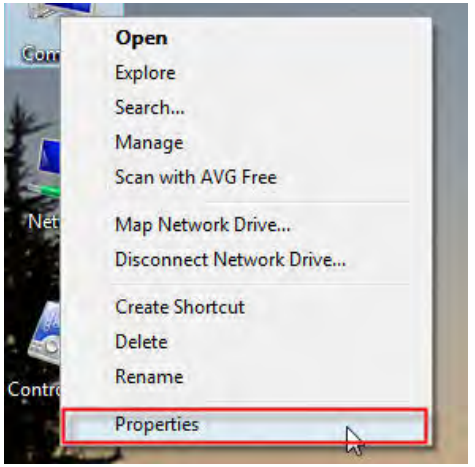
If you are using the Router's Wi-Fi Security push button option, simultaneously depress the push button located on the side of the Router and the button on the client (or virtual button on the client's GUI). Next click **Finish**. The Client's software will then allow a newcomer to join your secure, Wi-Fi protected network.

If you are using third party software, run the appropriate Wi-Fi Protected System utility. You will be asked to either use the push button method or to manually enter the PIN. Follow the on-screen instructions.

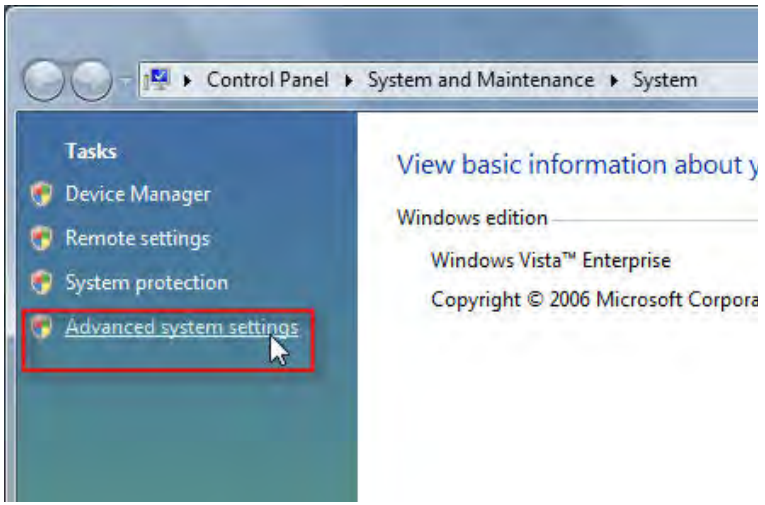
# Changing the Computer Name and Joining a Workgroup

The following are step-by-step directions to change the computer name and join a workgroup.

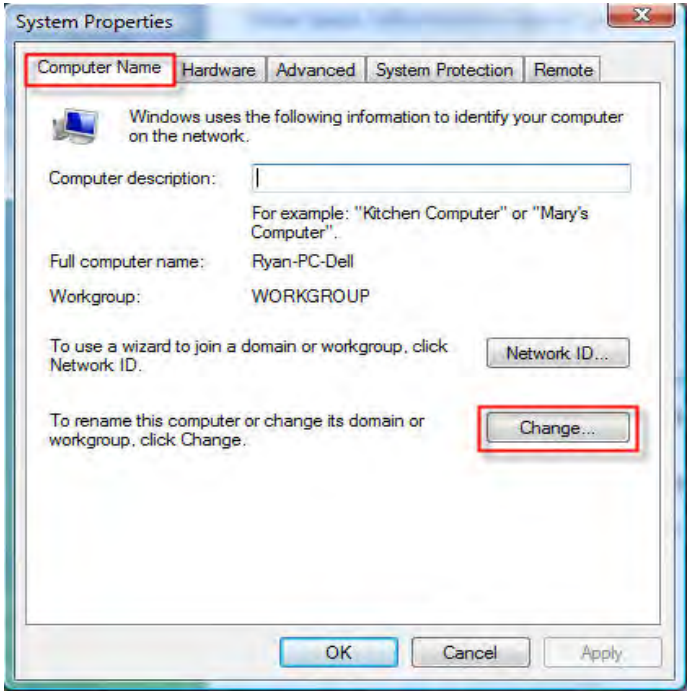
1. Click on **Properties**.



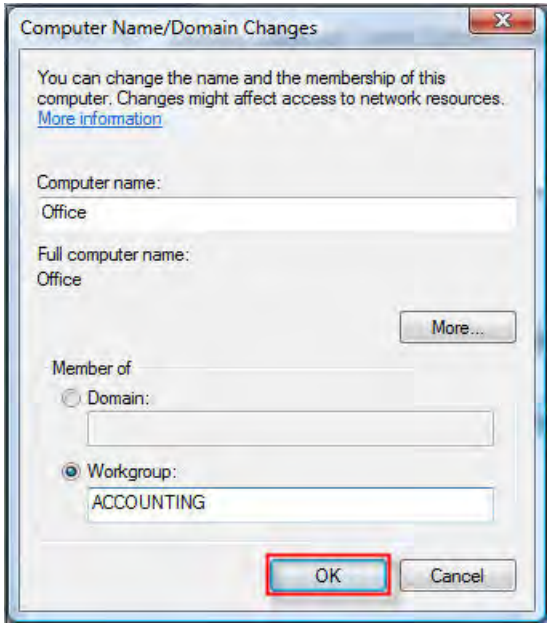

2. Click on the **Advanced system settings** link.



3. Click the **Computer Name** tab in the **System Properties** window and enter a description of your computer in the textbox. When you are finished, click the **Change** button.



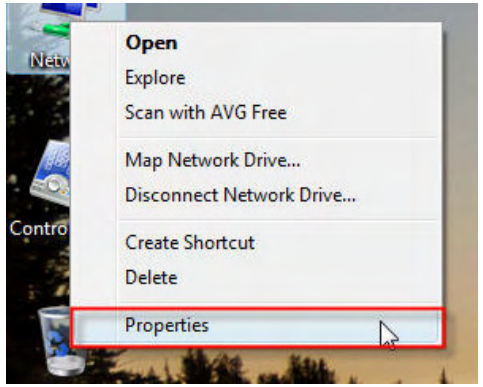

4. Go to the **Computer Name/Domain Changes** window and click the radio button next to the Workgroup you want to join. When you are finished, click the **OK** button.



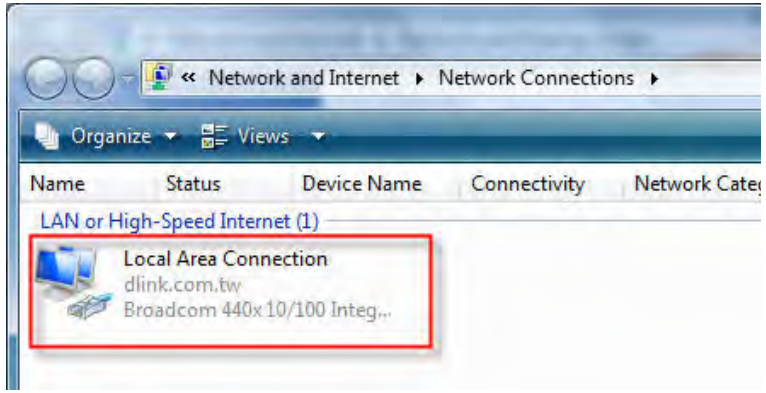
# Configuring the IP Address in Vista

The following are step-by-step directions to configure the IP address in Windows Vista.

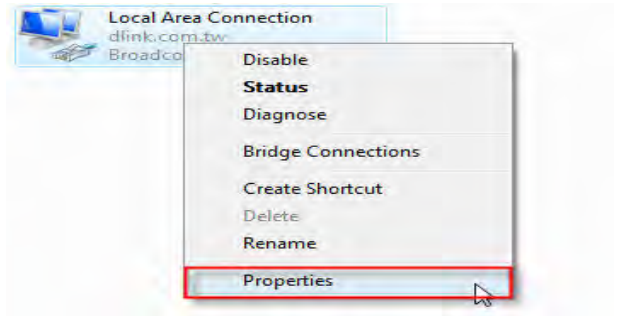
1. Click on **Properties**.



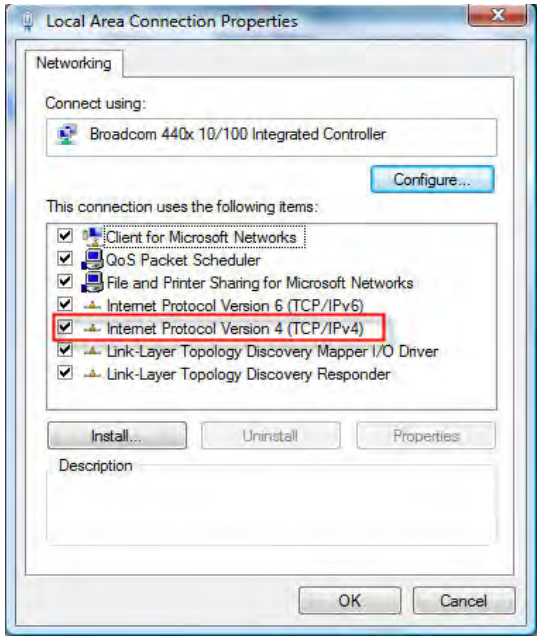

2. Go to the **Network and Internet** window and click the appropriate **Local Area Connection** icon.



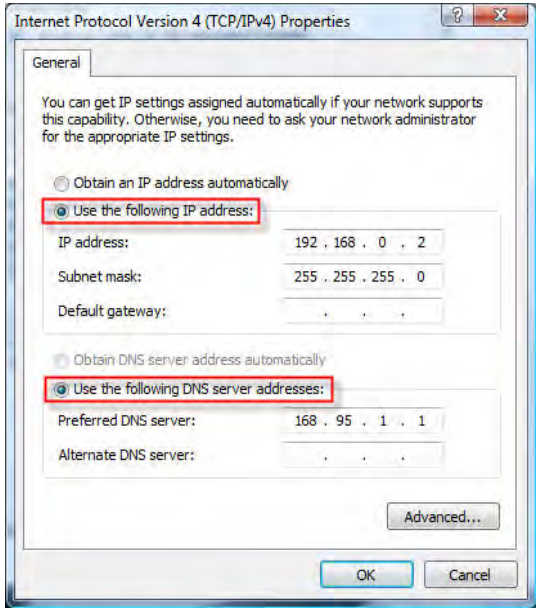

3. Right-click the **Local Area Connection** icon and then select **Properties** from the drop-down menu.



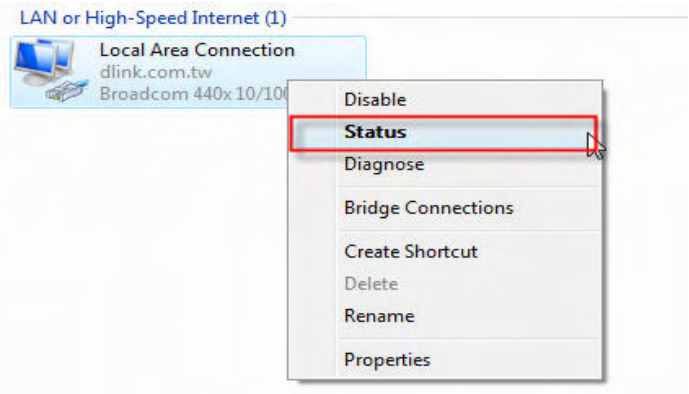
4. Tick the **Internet Protocol Version 4 (TCP/IPv4)** check box in the **Networking** tab in the **Local Area Connection Properties** window.



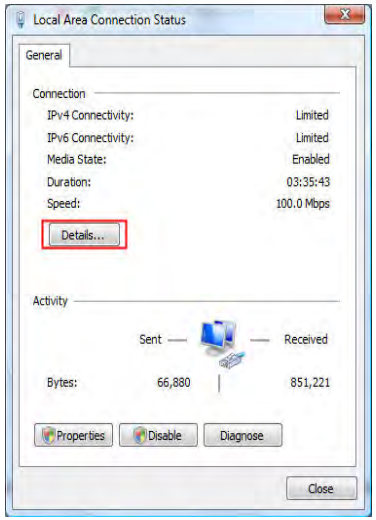

5. Click the “Use the following IP address” option in the **General** tab in the **Local Area Connections Properties** window and enter the desired IP address in the space offered. Then click the “Use the following DNS server adresses” option on the same tab and enter the desired DNS server information.



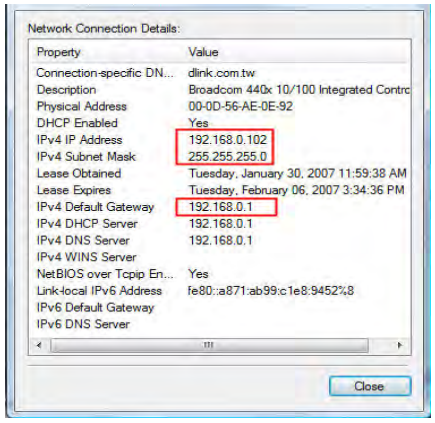
6. Right-click the **Local Area Connection** icon and then select **Status** from the drop-down menu.




7. Go to the **Local Area Connection Status** window and click the **Details** button.



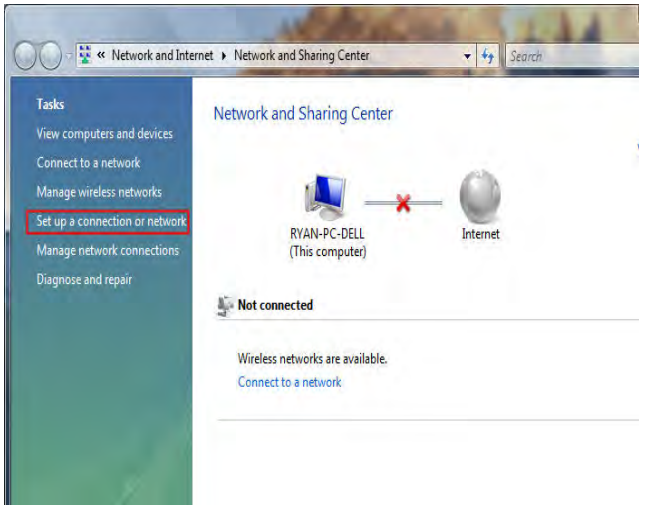

8. Confirm your new settings on the **Network Connection Status** window. When you are finished, click the **Done** button.



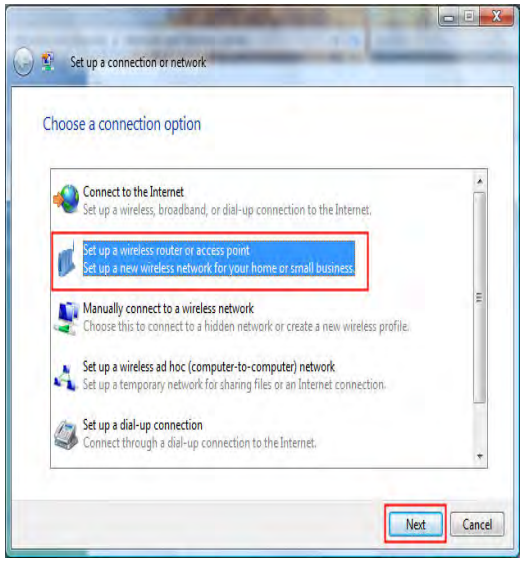
# Setting Up a Connection or Network Wirelessly

The following are step-by-step directions to set up a wireless connection.

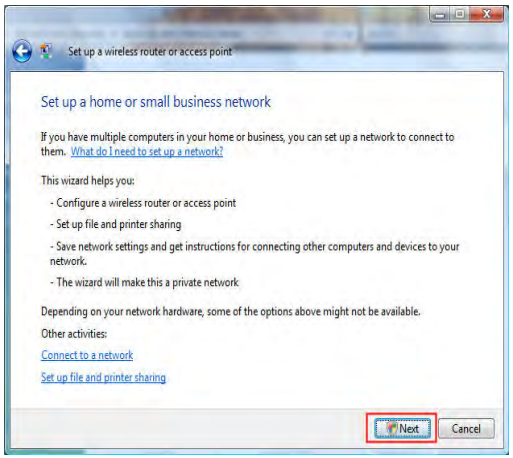
1. Click on **Set up a connection or network in the Network and Sharing Center** section.



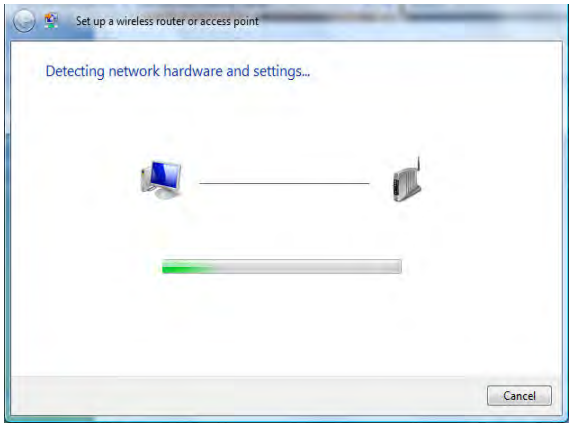

2. Go to the **Set up a connection or network** window and choose the **Set up a wireless router or access point Set up a new wireless network for your home or business** option. Click the **Next** button.



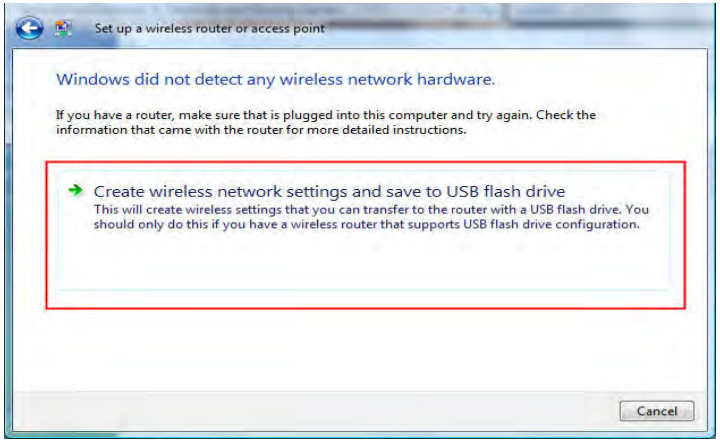
3. Click the **Next** button on the **Set up a wireless router or access point** window.



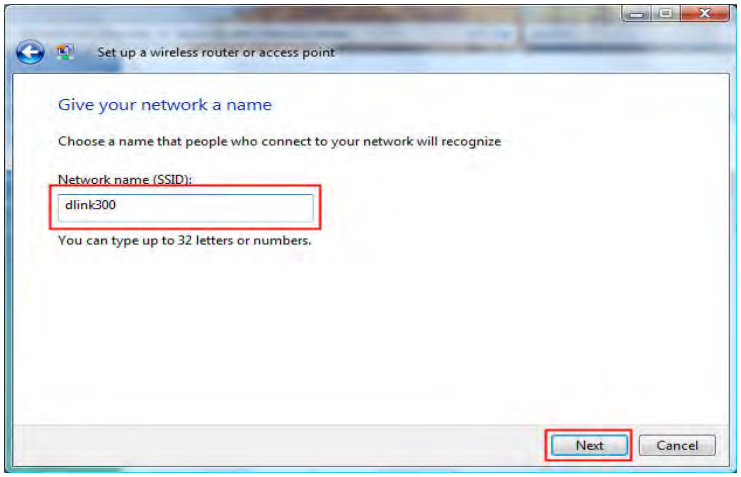

4. The following window displays the system progress.



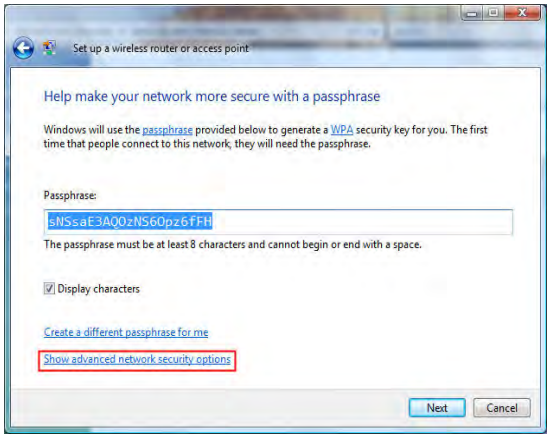

5. This window confirms that you want to create wireless network settings that are savable to a USB flash drive.



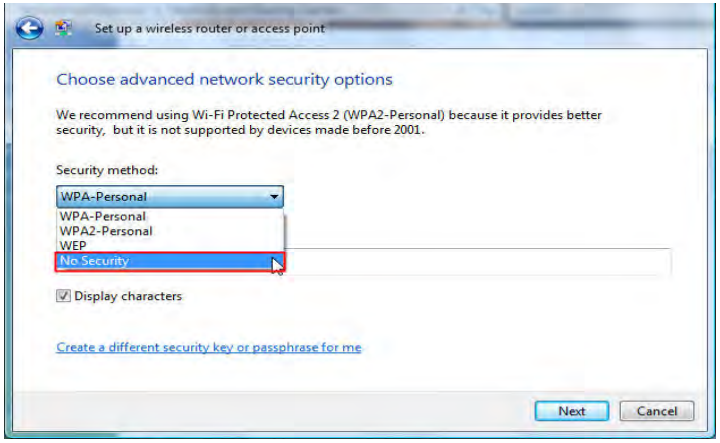
6. Enter a network name on the **Give your network a name** window in the **Set up a wireless router or access point** wizard. Click the **Next** button.



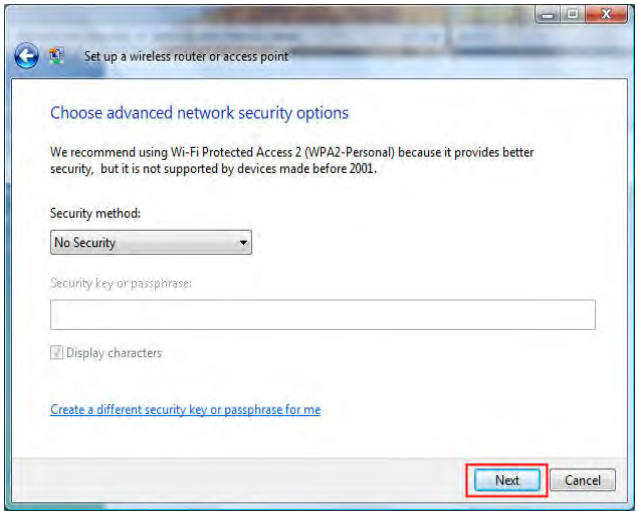

7. Enter a passphrase on the **Help make your network more secure with a passphrase** window in the **Set up a wireless router or access point** wizard. Click the **Show advanced network security options** link.



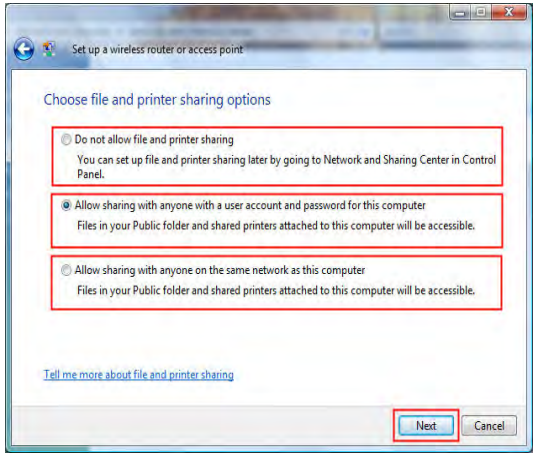

8. Select security method on the **Choose advanced network security options** window in the **Set up a wireless router or access point** wizard. Click the **Next** button.



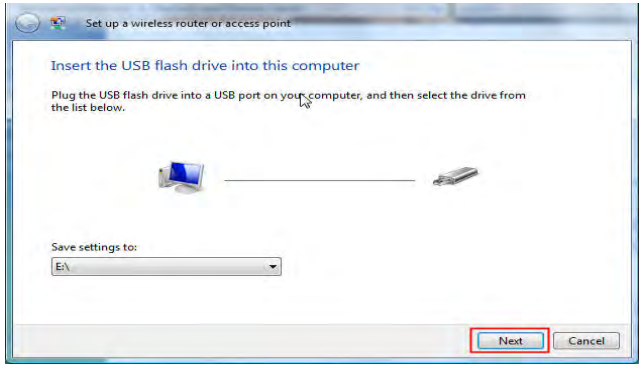
9. Once you have selected the desired security method on the **Choose advanced network security options** window in the **Set up a wireless router or access point** wizard, click the **Next** button.



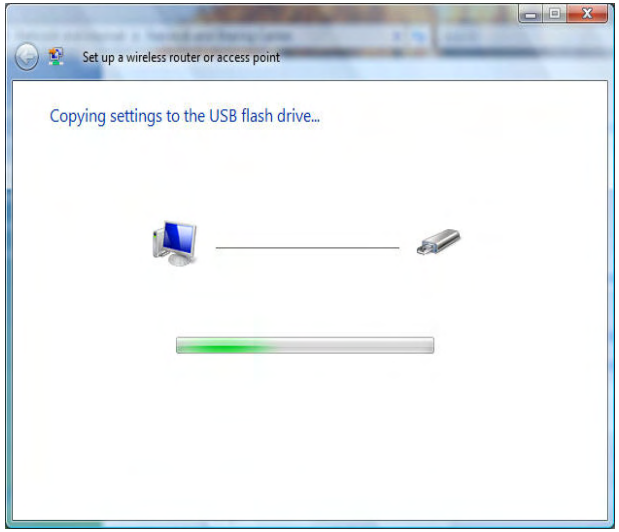

10. Select the desired file and printer sharing option on the **Choose file and printer sharing options** window in the **Set up a wireless router or access point** wizard. Click the **Next** button.




11. Once you have saved your network settings to USB, use the pull-down menu on the **Insert the USB flash drive into this computer** window in the **Set up a wireless router or access point** wizard to select a destination for your network settings. Click the **Next** button.



12. Once you have saved your network settings to USB, the **Copying settings to the USB drive** window in the **Set up a wireless router or access point** wizard opens to indicate the system progress.

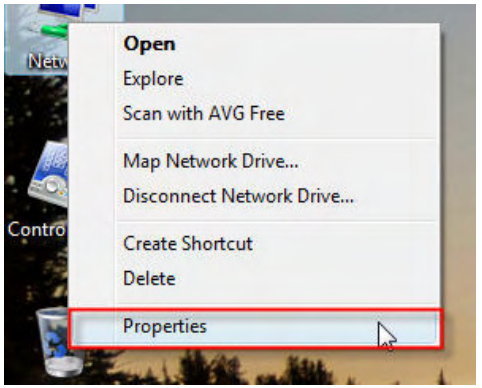



13. Once you are finished, the **To add a device or computer, follow these instructions** window in the **Set up a wireless router or access point** wizard opens. When you are finished, click the **Close** button.

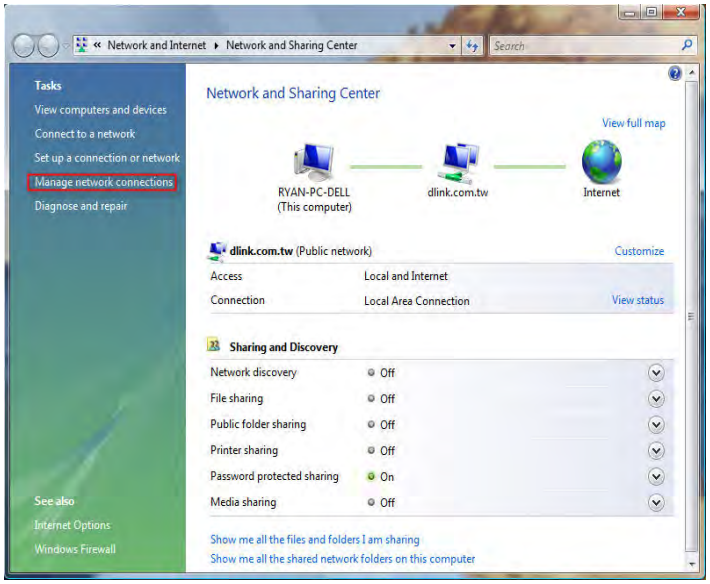
# Connecting to a Secured Wireless Network (WEP, WPA-PSK & WPA2-PSK)

The following are step-by-step directions to set up a wireless connection.

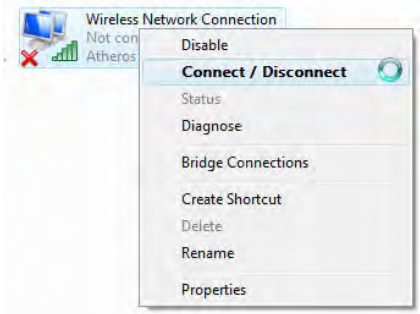
1. Click on **Properties**.



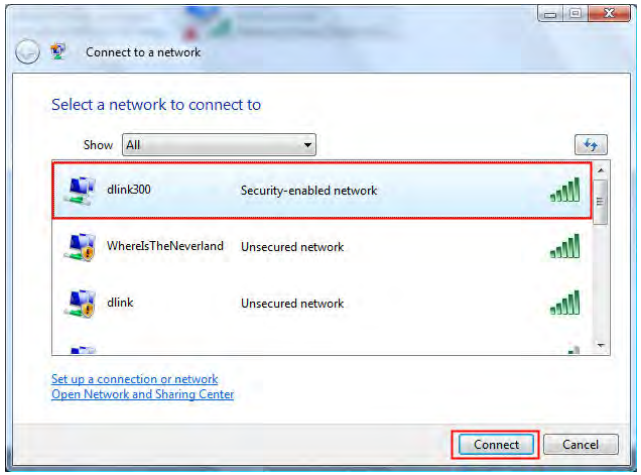

2. Click the **Manage network connections** link in the **Network and Sharing Center** window.



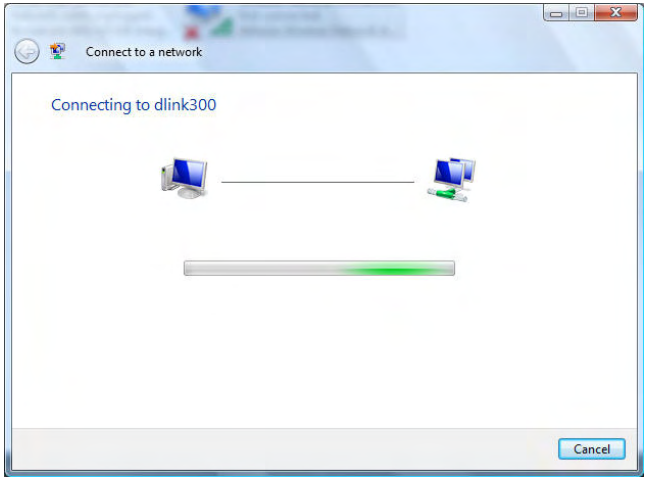
3. Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



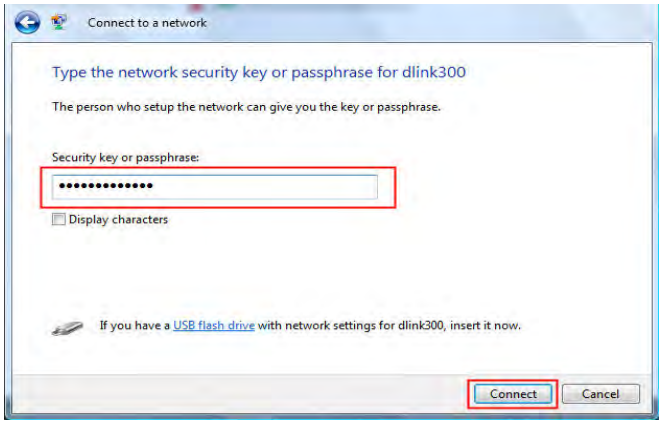

4. Select a network to connect to in the **Select a network to connect to** window in the **Connect to a network** wizard and then click the **Connect** button.



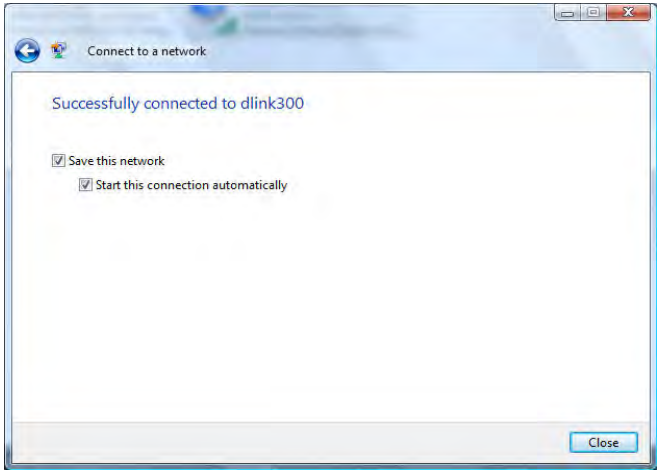

5. The following **Connect to a network** wizard window displays the system progress.



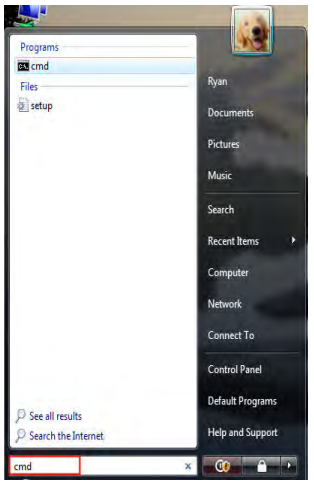
6. Enter the network security key or passphrase for the Router in the textbox provided in the **Type the network security key or passphrase for dlink300** window in the **Connect a network** wizard. When you are finished, click the **Connect** button.



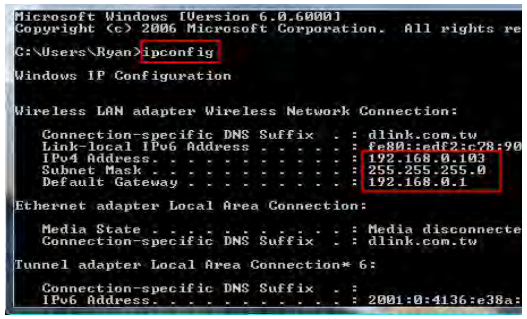

7. The following **Successfully connected to dlink300** window in the **Connect to a network** wizard is displayed. Choose to save to the network and/or start the new connection automatically. When you are finished, click the **Close** button.



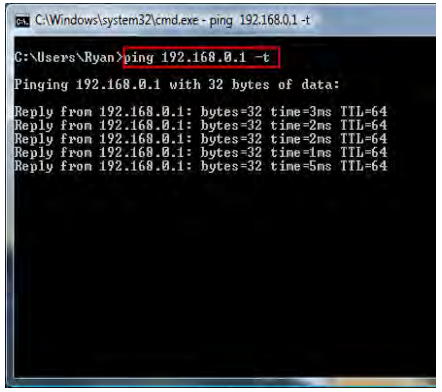

8. The successful connection is displayed at the bottom of the Windows start up menu.



9. Confirm your new settings by calling up the command prompt and then entering the ipconfig command.



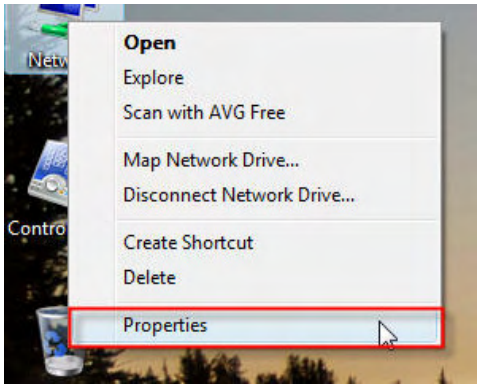

10. To test the new IP address, use the Ping feature of the command prompt.



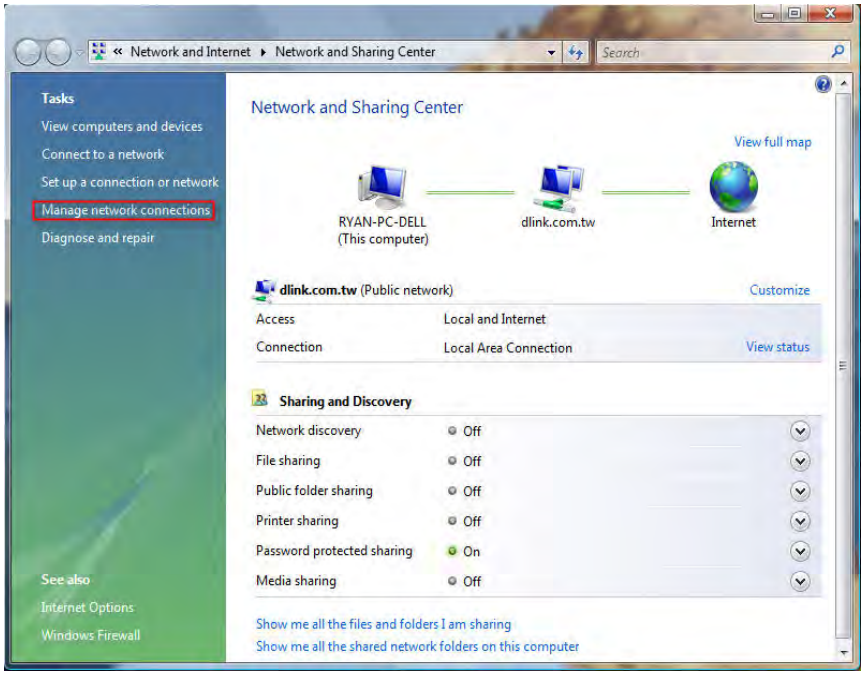
# Connecting to an Unsecured Wireless Network

The following are step-by-step directions to set up an unsecured wireless connection.

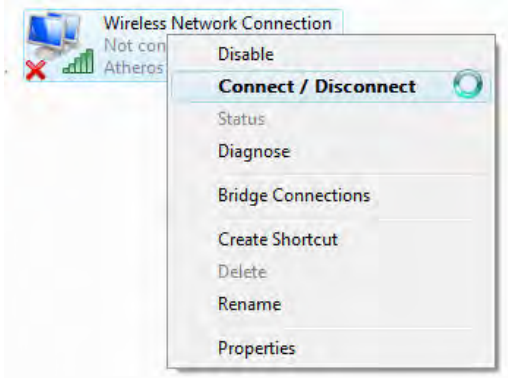
1. Click on **Properties**.



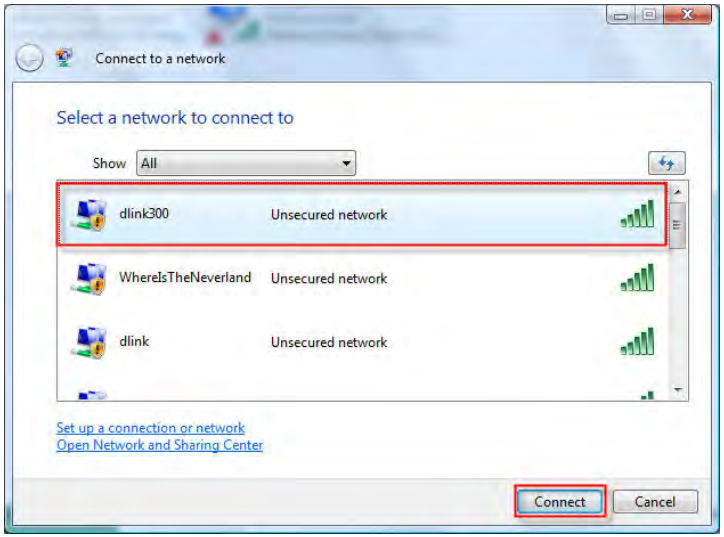

2. Go to the **Network and Sharing Center** window and click the **Manage Network Connections** link.



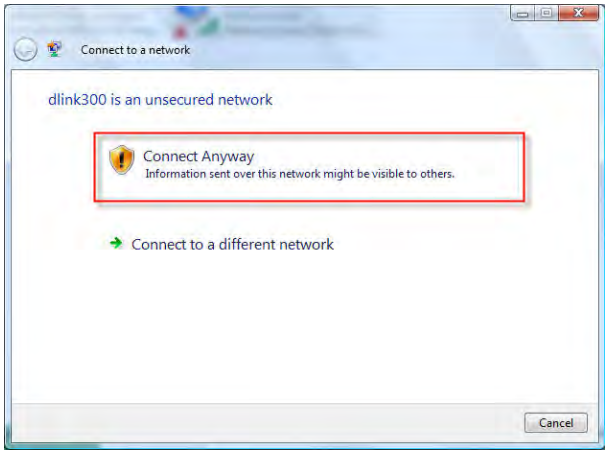
3. Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



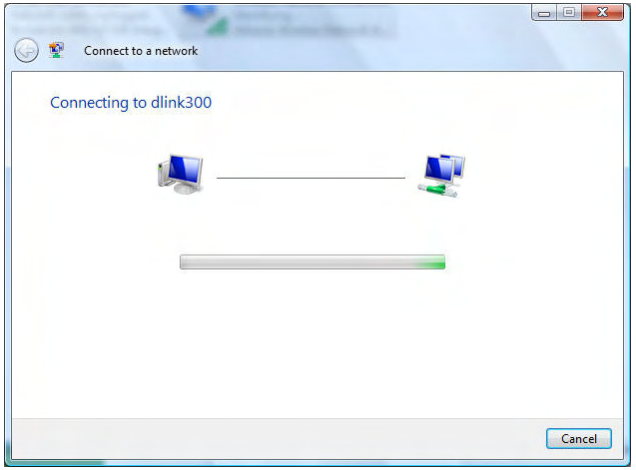

4. Select a network to connect to in the **Select a network to connect to** window in the **Connect to a network** wizard and then click the **Connect** button.



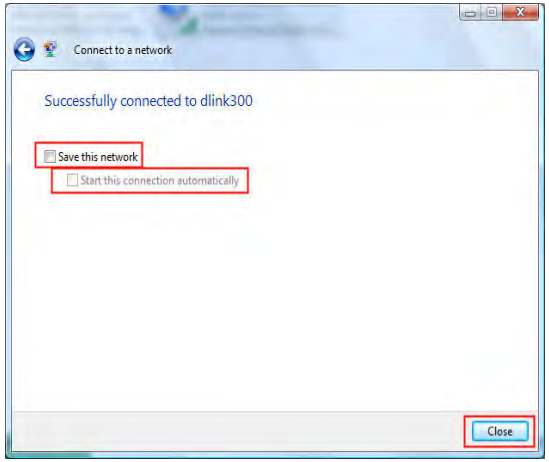

5. Confirm your desire to connect anyway on the following **Network Connection Status** window.



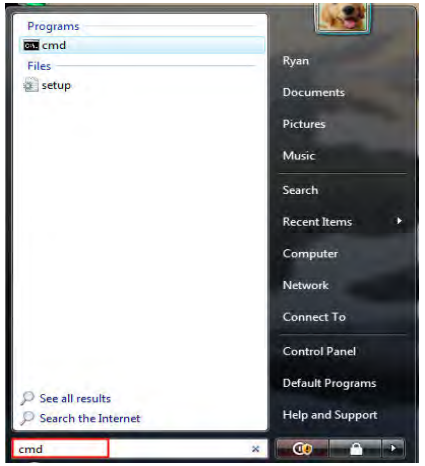
6. The following **Connect to a network** wizard window displays the system progress.



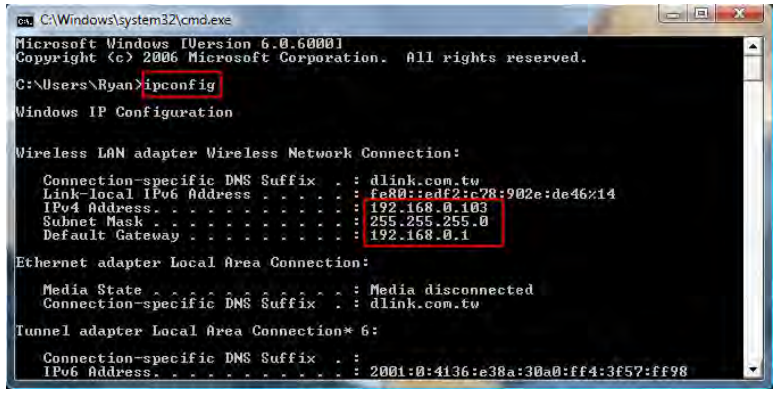

7. The following **Successfully connected to dlink300** window in the **Connect to a network** wizard is displayed. Choose to save to the network and/or start the new connection automatically. When you are finished, click the **Close** button.



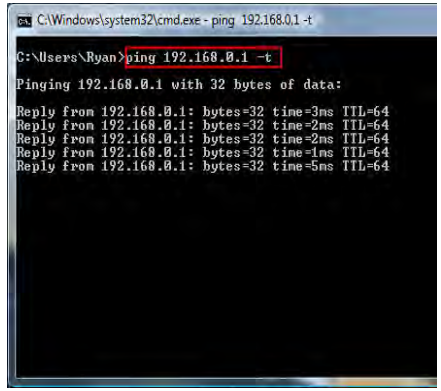

8. The successful connection is displayed at the bottom of the Windows start up menu.



9. Confirm your new settings by calling up the command prompt and then entering the ipconfig command.




10. To test the new IP address, use the Ping feature of the command prompt.

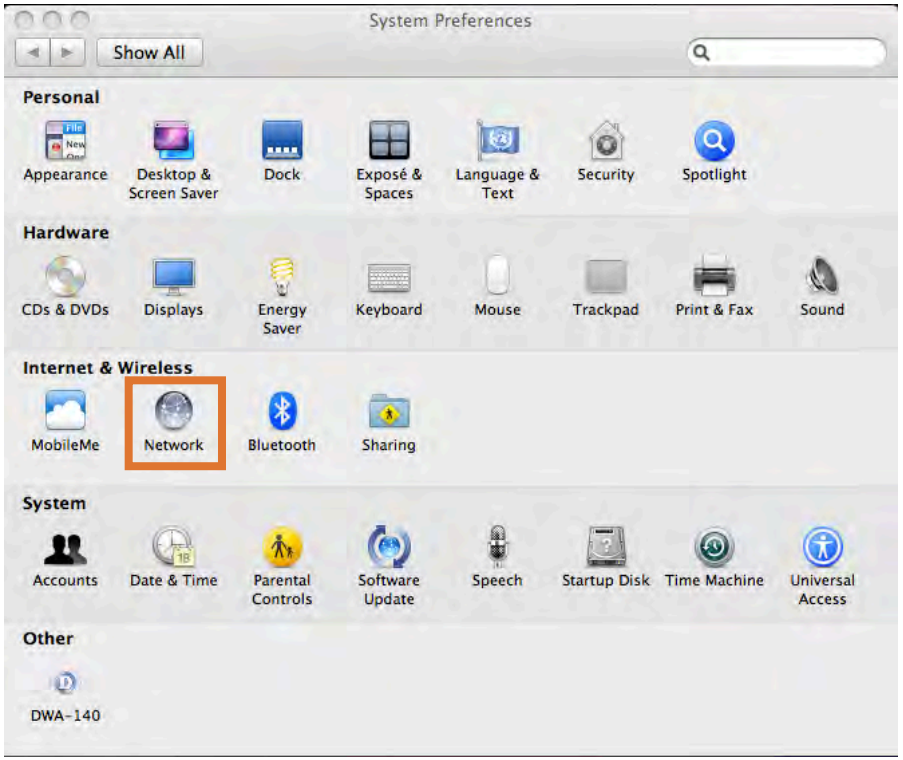


# Configuring the Network in MAC OS X Snow Leopard (10.6)

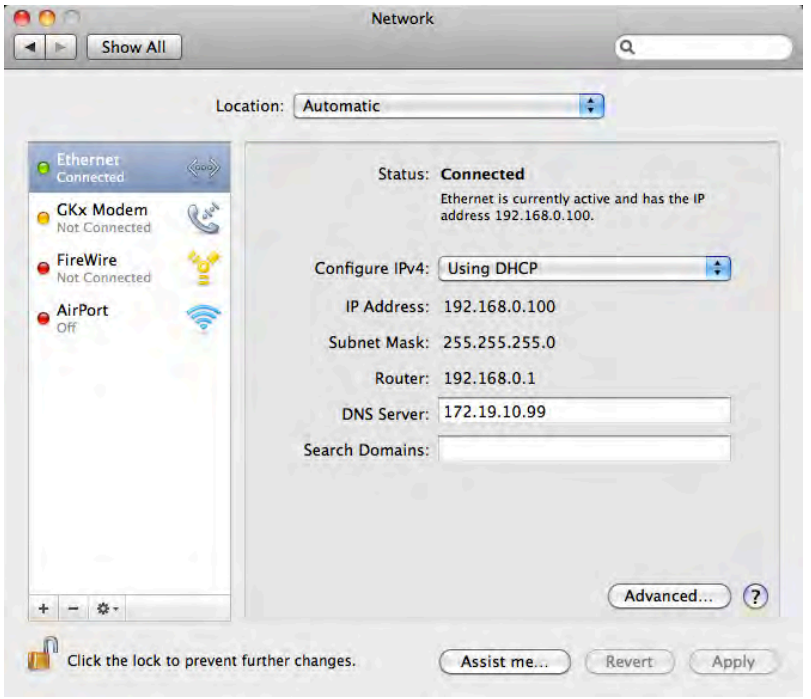
The following are step-by-step directions to configure the network in MAC OS X Snow Leopard (10.6).

1. Click the  icon in your Dock to open your System Preferences window.

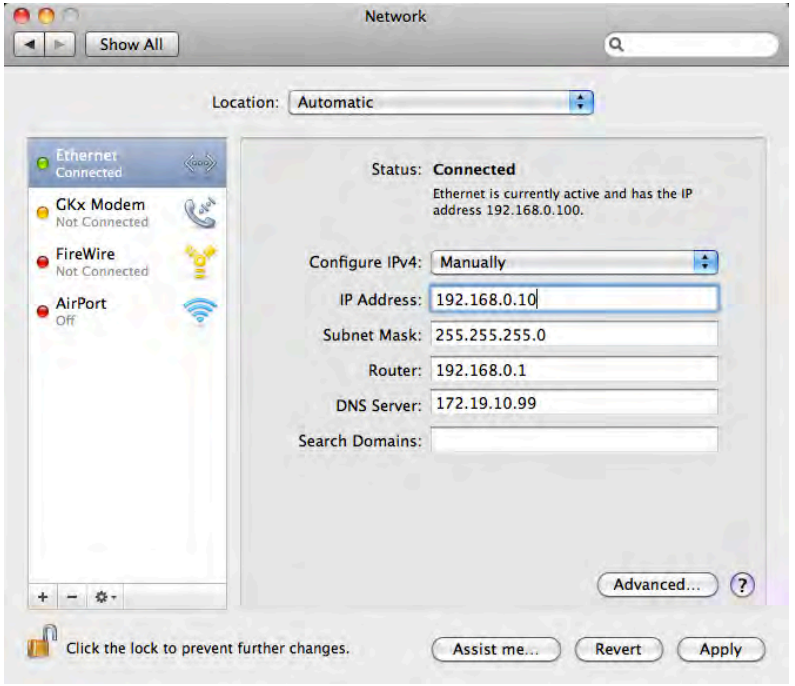
2. Click the **Network** icon in System Preferences menu to view the Network menu.



3. Click **Ethernet** on the left to see the local network settings. TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. The IP address, its subnet mask and the router's IP address displays when selecting **Using DHCP** from the **Configure IPv4** drop-down menu.




If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, select **Manually** from the **Configure IPv4** drop-down menu to manually enter the IP address and it's subnet mask.



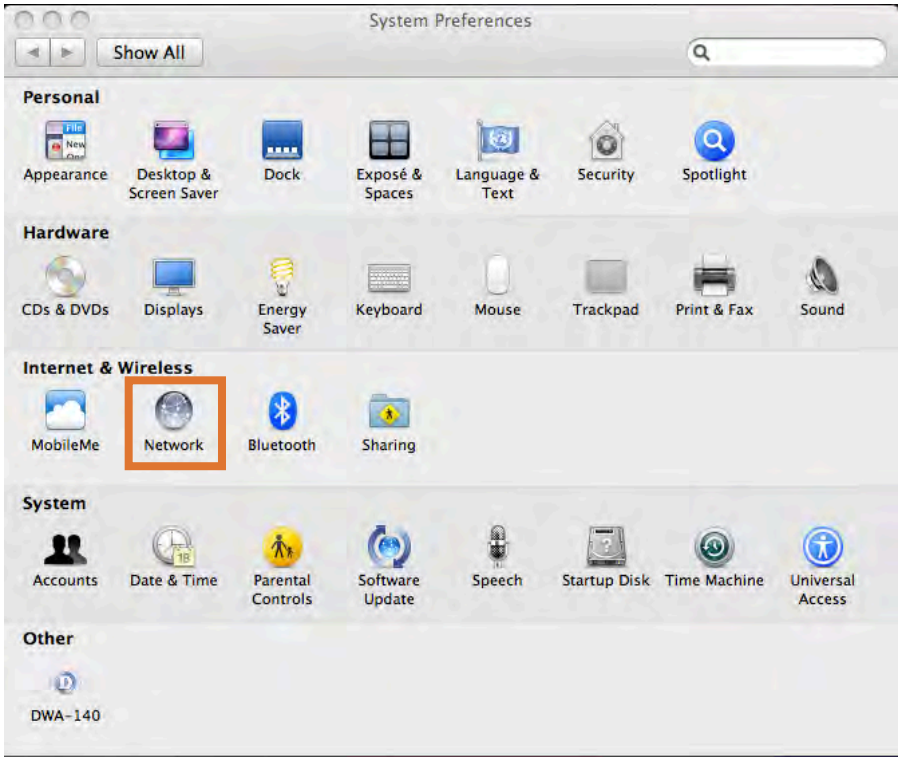

4. Click the **Apply** button to save the settings.

# Configuring the Wireless Network in MAC OS X Snow Leopard (10.6)

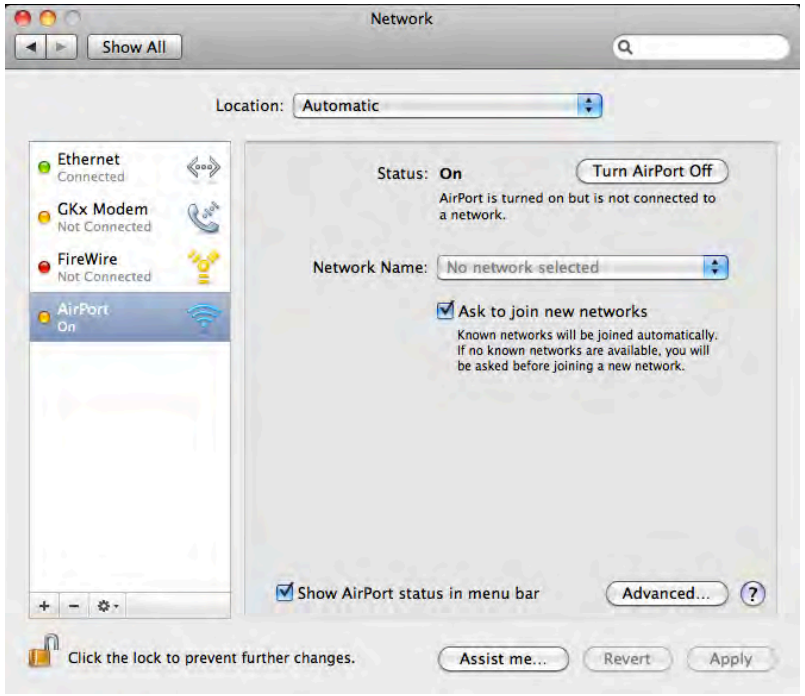
The following are step-by-step directions to configure the Wireless in MAC OS X Snow Leopard (10.6).

1. Click the  icon in your Dock to open your System Preferences window.

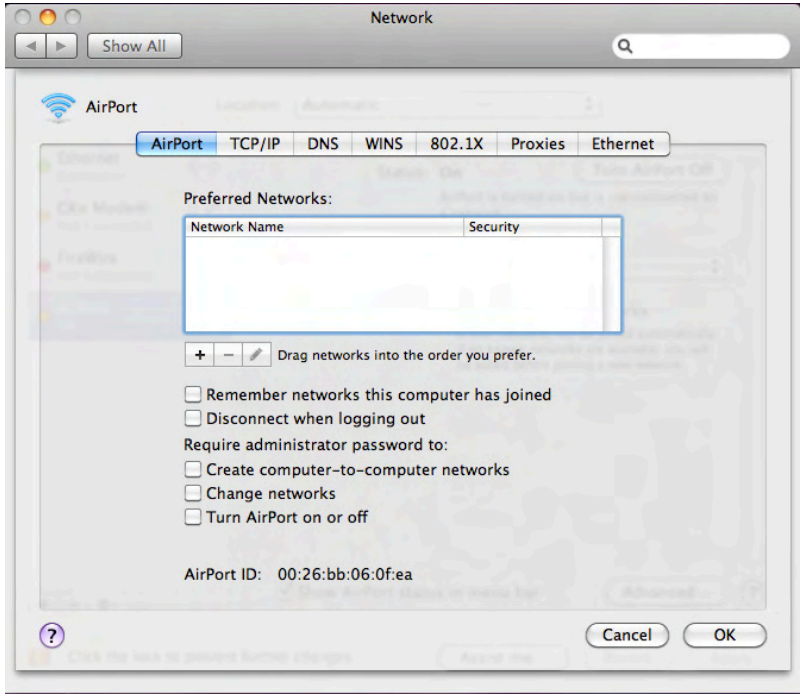
2. Click the **Network** icon in System Preferences menu to view the Network menu.



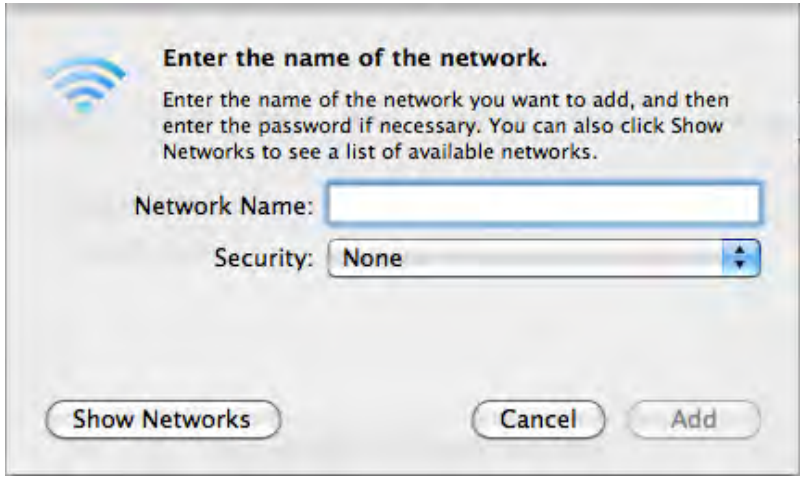
3. Click AirPort on the left to configure the wireless network.
4. Make sure the **Status** is **On**. If the Status is Off, click the **Turn AirPort On** button to enable AirPort.



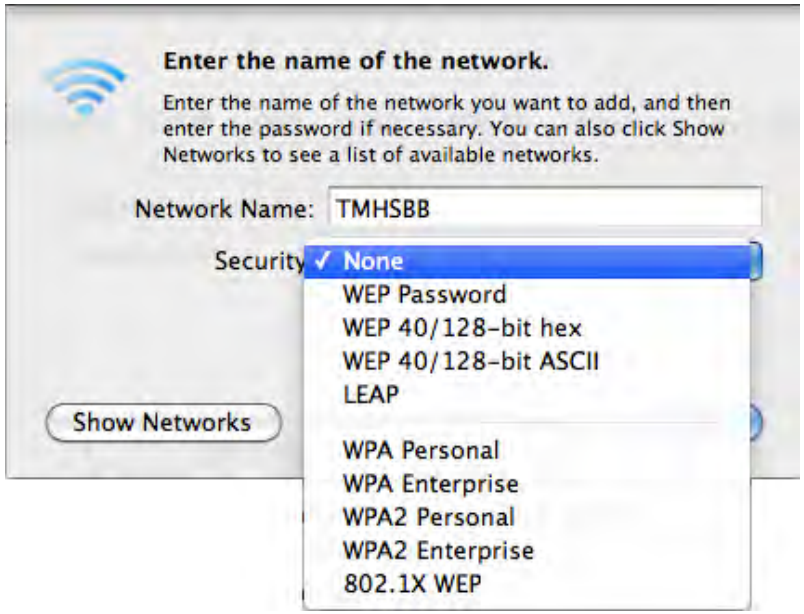

5. Click the **Advanced** button to see the window.
6. Click the **+** button to see the window in the next page.



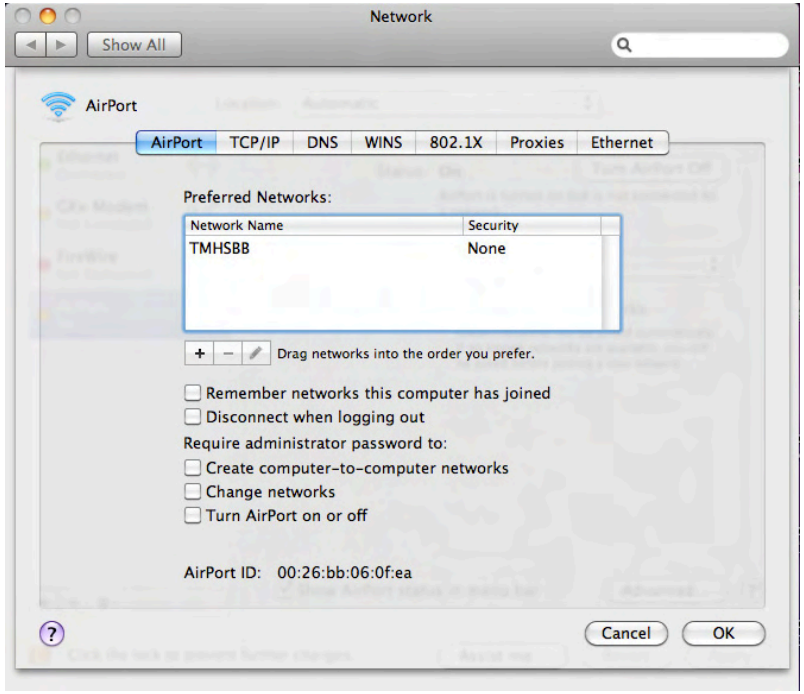
7. Enter the Network Name (SSID) of the Router.



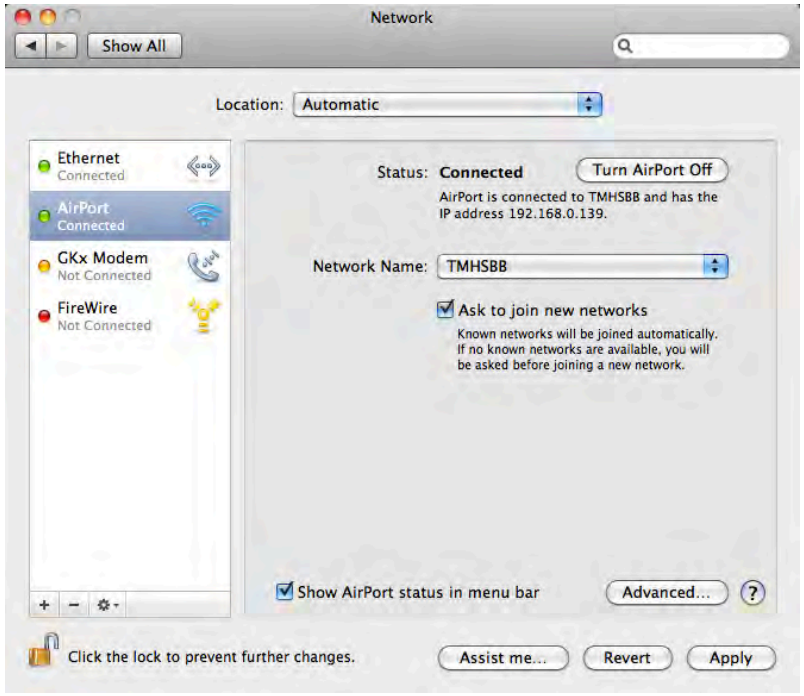

8. Select the Security type of the network from the drop-down list, and security related information below.
   Click the **Add** button to add the wireless network in the Preferred Network list.



9. Click **OK** to proceed.




10. Select the **Network Name** from the drop-down menu.
11. Click the **Apply** button to save the settings.



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-627. Read the following descriptions if you are having problems. (The examples below are illustrated in Windows® XP. If you have a different operating system, the screenshots on your computer will look similar to the following examples.)

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

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

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

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

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

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

• Configure your Internet settings:

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

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

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

  • Close your Web browser (if open) and open it.

• Access the Web management. Open your Web browser and enter the IP address of your D-Link router in the address bar. This should open the login page for your the Web management.

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

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

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

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

**3. Why can't I connect to certain sites or send and receive emails when connecting through my router?**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C:\>
```

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

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

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

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

# Wireless Basics

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

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

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

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

## What is Wireless?

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

## Why D-Link Wireless?

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

## How does wireless work?

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

## Why is the speed of my Wireless N device limited to 54mbps?

This is likely to be the result of the wireless settings. Go to **Advanced** -> **Advanced Wireless** to see if the Wireless Mode is configured as 802.11n only. As the Wi-Fi Alliance restricts the maximum speed to 54Mbps when WPA or WPA2 wireless security is configured with TKIP Cipher Type, go to **Setup** -> **Wireless Setup** to make sure the Cipher Type is configured as AES.

### Wireless Local Area Network (WLAN)

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

### Wireless Personal Area Network (WPAN)

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

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

## Who uses wireless?

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

**Home**

- Gives everyone at home broadband access
- Surf the Web, check e-mail, instant message, 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.
For the wireless repeater, there are two types of repeater in D-Link for user to select:

- Universal repeater: It acts as an AP and a wireless STA at the same time. It can support all AP and wireless STA if they work in the same wireless channel.
- AP-repeater (AP with WDS): only repeat same model or limited models which base on the same proprietary protocol.

Please choose a universal repeater to boost the signal to extend the range.

# Wireless Modes

**Eliminate Interference**

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

**Security**

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

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 WNA-2330 wireless network Cardbus adapters.

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

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

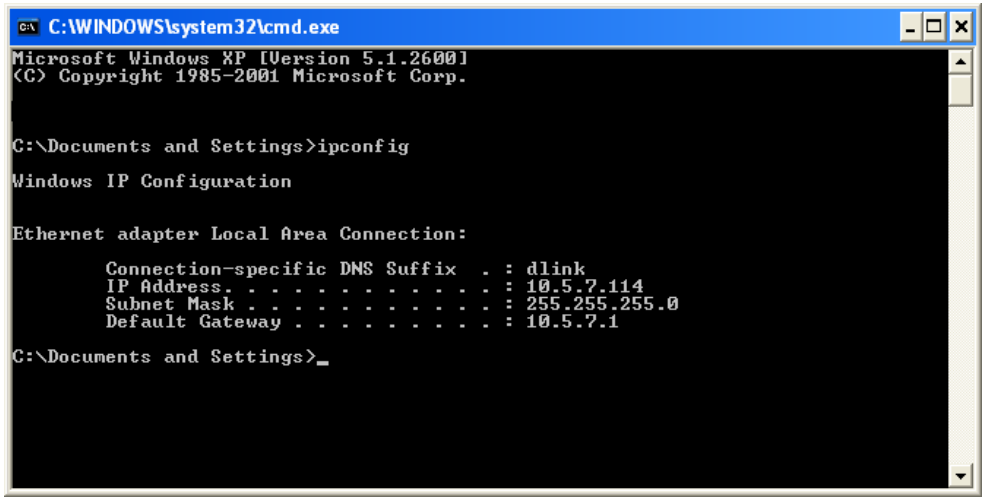
# Networking Basics

## Check your IP address

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

Click on **Start** > **Run**. In the run box type `cmd` and click **OK**.

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




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

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

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

# Statically assign an IP address

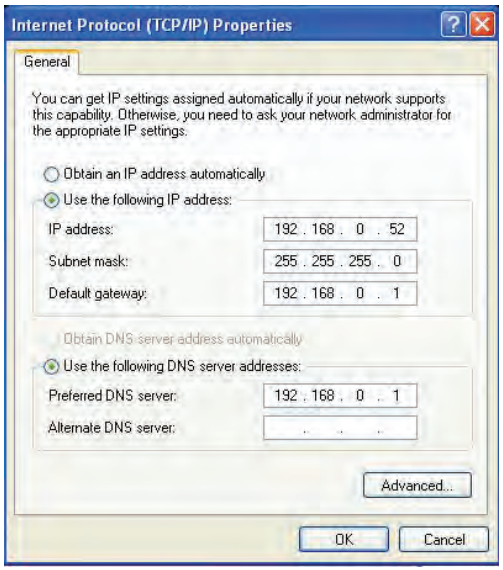
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

**Step 1**
Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

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

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

**Step 4**
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.




Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

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

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

# Technical Specifications

**Standards**

- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.11n draft 2.0
- IEEE 802.3
- IEEE 802.3u

**Wireless Signal Rates***

- 300Mbps
- 54Mbps
- 48Mbps
- 36Mbps
- 24Mbps
- 18Mbps
- 12Mbps
- 11Mbps
- 9Mbps
- 6Mbps
- 5.5Mbps
- 2Mbps
- 1Mbps

**Security**

- WPA - Wi-Fi Protected Access (TKIP, MIC, IV Expansion, Shared Key Authentication)
- 802.1x
- 64/128-bit WEP
- PIN/PBC WPS

**Modulation Technology**

802.11 b: DSSS / DBPSK / DQPSK / CCK
802.11 g: 16QAM / 64QAM / BPSK / QPSK with OFDM
802.11 n: 16QAM / 64QAM / BPSK / QPSK with OFDM

**Receiver Sensitivity**

802.11n

HT20

- 300Mbps OFDM, 10% PER, –68dBm

HT40

- 300Mbps OFDM, 10% PER, –64dBm

802.11b and 802.11g

- 54Mbps OFDM, 10% PER,-70dBm
- 48Mbps OFDM, 10% PER,-72dBm
- 36Mbps OFDM, 10% PER,-76dBm
- 24Mbps OFDM, 10% PER,-78dBm
- 18Mbps OFDM, 10% PER,-80dBm
- 12Mbps OFDM, 10% PER,-83dBm
- 11Mbps CCK, 8% PER,-85dBm
- 9Mbps OFDM, 10% PER,-85dBm
- 6Mbps OFDM, 10% PER,-88dBm
- 5.5Mbps CCK, 8% PER,-87dBm
- 2Mbps DQPSK, 8% PER,-89dBm
- 1Mbps DBPSK, 8% PER,-90dBm

**Device Management**

- Web-based Internet Explorer v6 or later; Netscape Navigator v6 or later; or other Java-enabled browsers
- DHCP Server and Client

**Wireless Frequency Range**

2.4GHz to 2.4835GHz

**Wireless Operating Range2**

- Indoors - up to 328 ft. (100 meters)
- Outdoors- up to 1312 ft. (400 meters)

**Wireless Transmit Power (AVG Power)**

11b:17dBm(Max)  11g:16dBm(Max)  11n:13dBm(Max)

**External Antenna Type**

Two fixed reverse SMA external antennas

**Operating Temperature**

32°F to 129 °F (0°C to 40°C)

**Humidity**

95% maximum (non-condensing)

**Safety and Emissions**

FCC Part 15B/ 15C/ MPE
IC RSS-210
NCC LP0002

**LEDs**

- Power
- Internet
- WLAN (Wireless Connection)
- Ethernet
- USB
- WPS

**Dimensions**

- L = 197.82mm
- W = 133.18mm
- H = 28.91mm

**Weight**

0.273kg

* Maximum wireless signal rate derived from IEEE Standard 802.11b, 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.

**Federal Communication Commission Interference Statement**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

**IMPORTANT NOTE:**

**FCC Radiation Exposure Statement:**

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

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

以下**警語適用台灣地區**

經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。