

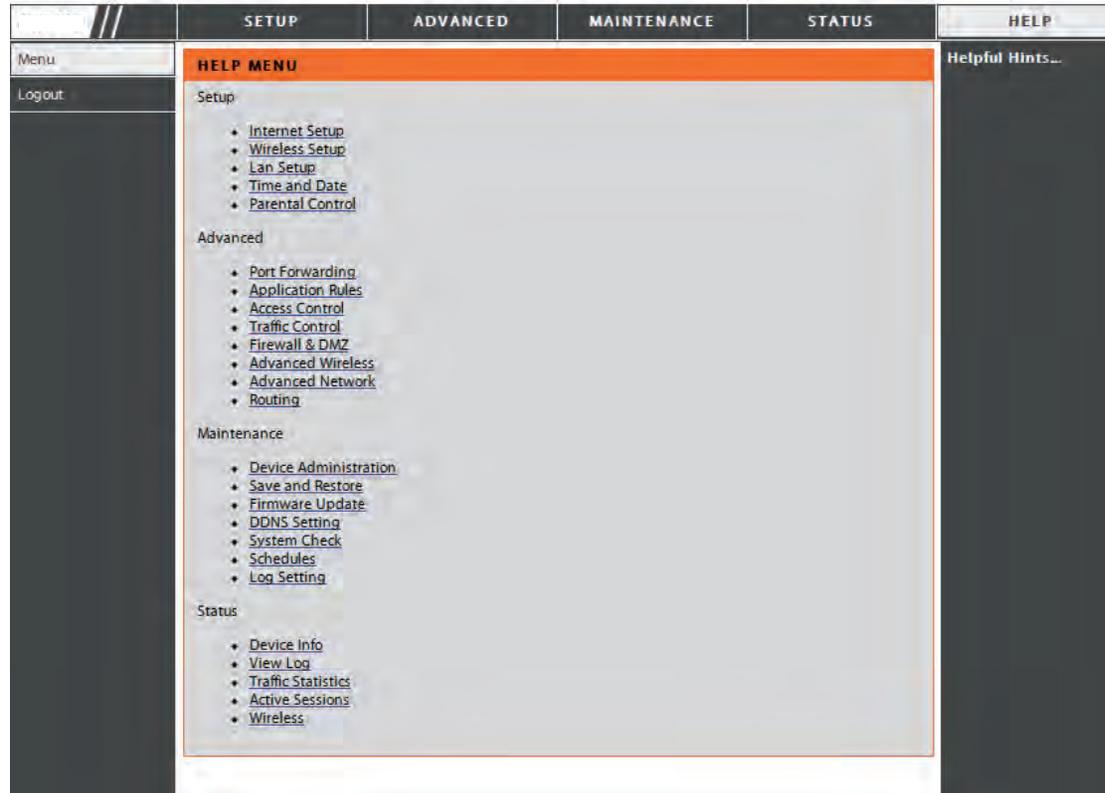
Wireless

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

	SETUP	ADVANCED	MAINTENANCE	STATUS	HELP				
Device Info	WIRELESS				Helpful Hints... This is a list of all wireless clients that are currently connected to your wireless router. More...				
View Log	Use this option to view the wireless clients that are connected to your wireless router.								
Traffic Statistics									
Active Sessions	NUMBER OF WIRELESS CLIENTS : 0								
Wireless	<table border="1"><thead><tr><th>MAC Address</th><th>IP Address</th><th>Mode</th><th>Rate</th><th>Signal (%)</th></tr></thead></table>					MAC Address	IP Address	Mode	Rate
MAC Address	IP Address	Mode	Rate	Signal (%)					
Logout									

Help

Click the desired hyperlink to get more information about how to use the Router.



Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-619L 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 on **Wireless Setup** on the left side.
2. Next to **Security Mode**, select *Enable WEP Wireless Security (basic)*.
3. Next to **Authentication**, select either *Shared Key* or *Open*. *Shared Key* is recommended as it provides greater security when WEP is enabled.
4. Select either *64Bit* or *128Bit* encryption from the drop-down menu next to **WEP Encryption**.
5. Next to **Default Key Type**, select *WEP Key 1* and enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to four different keys either using *Hex* or *ASCII*. *Hex* is recommended (letters A-F and numbers 0-9 are valid). In *ASCII* all numbers and letters are valid.
6. Click **Save Settings** to save your settings. If you are configuring the router with a wireless adapter, you will lose connectivity until you enable WEP on your adapter and enter the same WEP key as you did on the router.

WIRELESS SECURITY MODE

Security Mode :

WEP

WEP is the wireless encryption standard. To use it you must enter the same key(s) into the router and the wireless stations. For 64 bit keys you must enter 10 hex digits into each key box. For 128 bit keys you must enter 26 hex digits into each key box. A hex digit is either a number from 0 to 9 or a letter from A to F. For the most secure use of WEP set the authentication type to "Shared Key" when WEP is enabled.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal key using the ASCII values of the characters. A maximum of 5 text characters can be entered for 64 bit keys, and a maximum of 13 characters for 128 bit keys.

Authentication :

WEP Encryption :

Default WEP Key :

WEP Key : (5 ASCII or 10 HEX)

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 and 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 on **Wireless Setup** on the left side.
2. Next to **Security Mode**, select *Enable WPA Only Wireless Security (enhanced)* or *Enable WPA2 Only Wireless Security (enhanced)*.
3. Next to **Cipher Mode**, select *TKIP*, *AES*, or *Both*.
4. Next to **PSK/EAP**, select *PSK*.
5. Next to **Network Key**, enter a key (passphrase). The key is an alphanumeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. Make sure you enter this key exactly the same on all other wireless clients.
6. Click **Save Settings** to save your settings. If you are configuring the Router with a wireless adapter, you will lose connectivity until you enable WPA-PSK or WPA2-PSK on your adapter and enter the same passphrase as you did on the Router.

WIRELESS SECURITY MODE

Security Mode : Enable WPA Only Wireless Security (enhanced) ▼

WPA ONLY

WPA Only requires stations to use high grade encryption and authentication.

Cipher Type : TKIP ▼

PSK / EAP : PSK ▼

Network Key : (8~63 ASCII or 64 HEX)

WIRELESS SECURITY MODE

Security Mode : Enable WPA2 Only Wireless Security (enhanced) ▼

WPA2 ONLY

WPA2 Only requires stations to use high grade encryption and authentication.

Cipher Type : TKIP ▼

PSK / EAP : PSK ▼

Network Key : (8~63 ASCII or 64 HEX)

Configure WPA/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 on **Wireless Setup** on the left side.
2. Next to **Security Mode**, select *Enable WPA/WPA2 Wireless Security (enhanced)*.
3. Next to **Cipher Mode**, select *TKIP, AES, or Both*.
4. Next to **PSK/EAP**, select *PSK*.
5. Next to **Network Key**, enter a key (passphrase). 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 the same on all other wireless clients.
6. Click **Save Settings** to save your settings. If you are configuring the Router with a wireless adapter, you will lose connectivity until you enable WPA/WPA2-PSK on your adapter and enter the same passphrase as you did on the Router.

The screenshot shows the 'WIRELESS SECURITY MODE' section of a router's web interface. The 'Security Mode' dropdown menu is set to 'Enable WPA/WPA2 Wireless Security (enhanced)'. Below this is the 'WPA/WPA2' section, which includes a note: 'WPA/WPA2 requires stations to use high grade encryption and authentication.' The 'Cipher Type' dropdown is set to 'TKIP', and the 'PSK / EAP' dropdown is set to 'PSK'. The 'Network Key' field is empty, with a note '(8~63 ASCII or 64 HEX)' to its right. At the bottom of the form are two buttons: 'Save Settings' and 'Don't Save Settings'.

Configure WPA, WPA2, and WPA/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 on **Wireless Settings** on the left side.
2. Next to **Security Mode**, select *Enable WPA Only Wireless Security (enhanced)*, *Enable WPA2 Only Wireless Security (enhanced)*, or *Enable WPA/WPA2 Wireless Security (enhanced)*.
3. Next to **Cipher Type**, select *TKIP*, *AES*, or *Auto*.
4. Next to **PSK/EAP**, select *EAP*.
5. Next to **RADIUS Server 1** enter the **IP Address** of your RADIUS server.
6. Next to **Port**, enter the port you are using with your RADIUS server. *1812* is the default port.
7. Next to **Shared Secret**, enter the security key.
8. If you have a secondary RADIUS server, enter its IP address, port, and secret key.
9. Click **Save Settings** to save your settings.

WIRELESS SECURITY MODE

Security Mode : Enable WPA Only Wireless Security (enhanced) ▼

WPA ONLY

WPA Only requires stations to use high grade encryption and authentication.

Cipher Type : TKIP ▼

PSK / EAP : EAP ▼

802.1X

RADIUS Server 1 IP Address :

Port :

Shared Secret :

RADIUS Server 2 IP Address :

Port :

Shared Secret :

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.

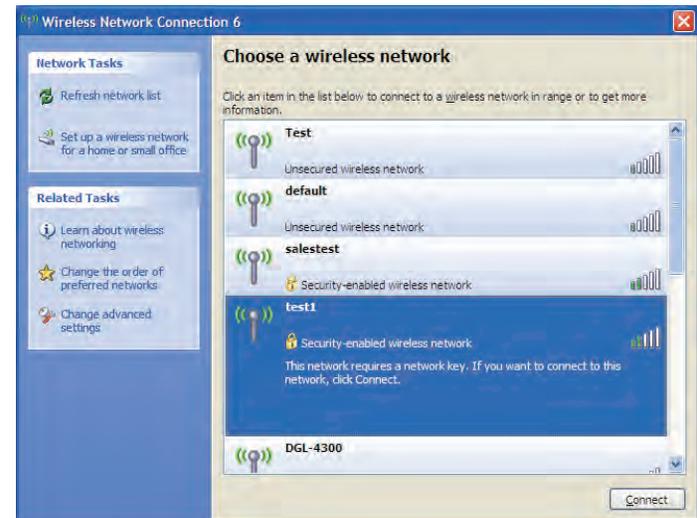
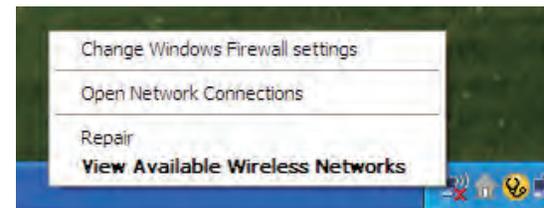
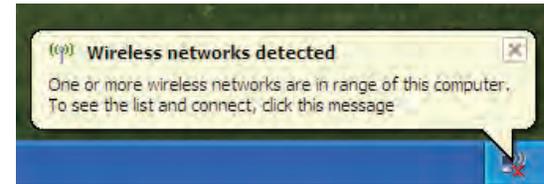
If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

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.

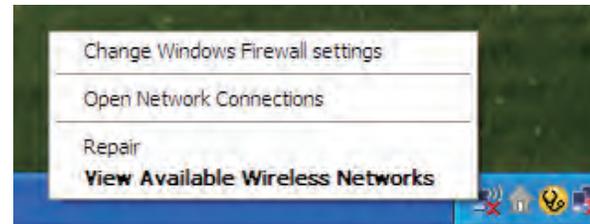
If you get a good signal but cannot access the Internet, check you TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



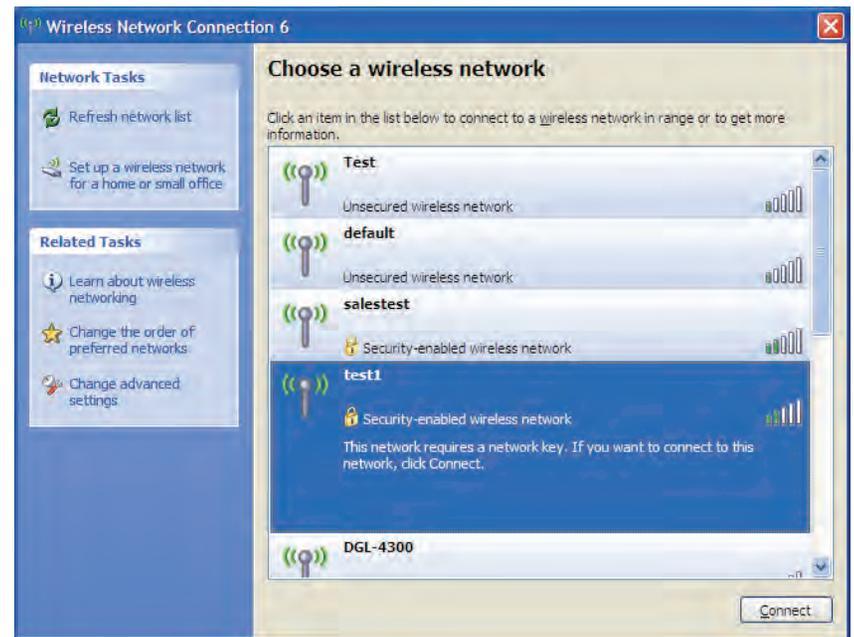
Configure WEP

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**.

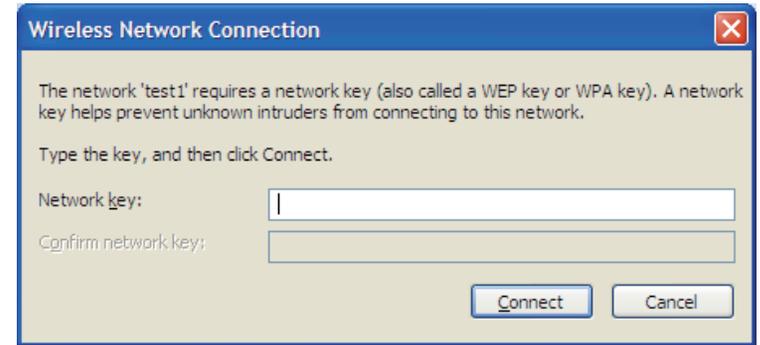


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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

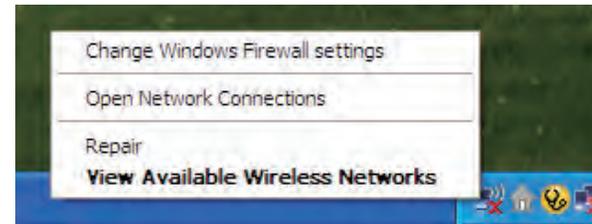
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



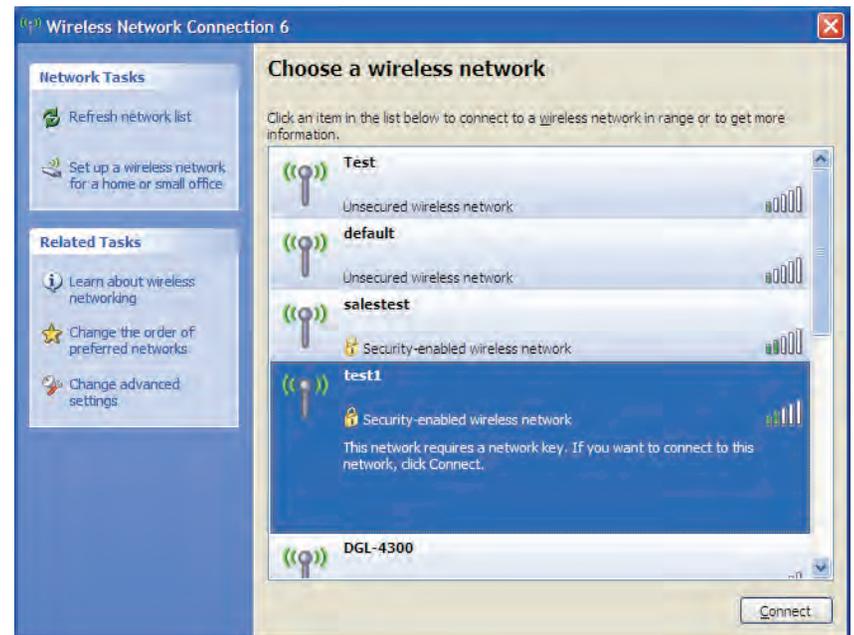
Configure WPA-PSK

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**.

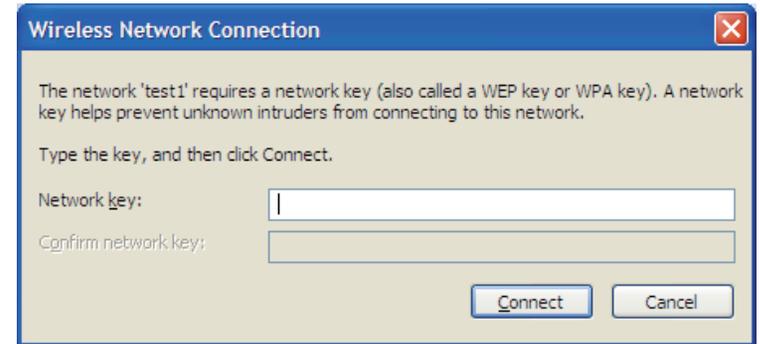


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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 DIR-619L 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, tick the Enable checkbox on the **Wireless Network** window. Use the Current PIN that is displayed on the **Wireless Network** window 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.

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.

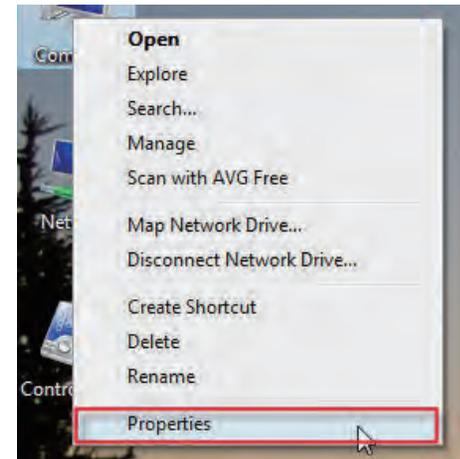
If you are using the Router's Wi-Fi Security push button option, simultaneously depress the push button located on the side of the Router and the button on the client (or virtual button on the client's GUI). Next click **Finish**. The Client's software will then allow a newcomer to join your secure,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

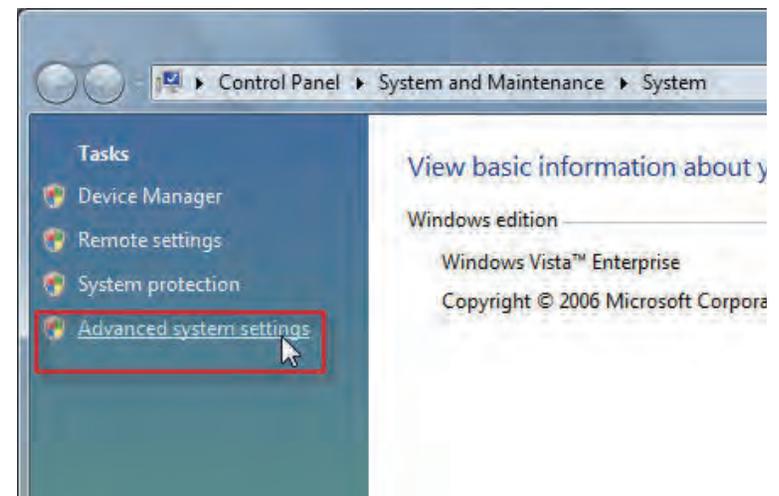
Changing the Computer Name and Joining a Workgroup

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

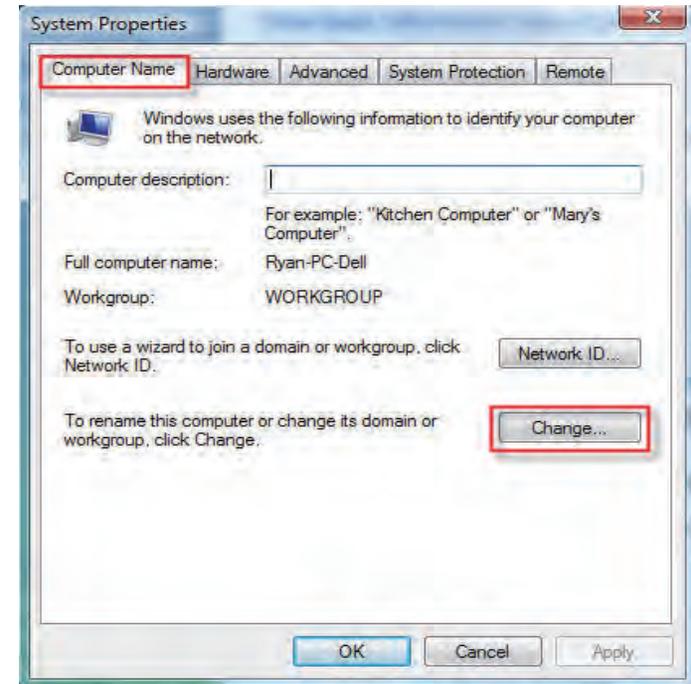
1. Click on **Properties**.



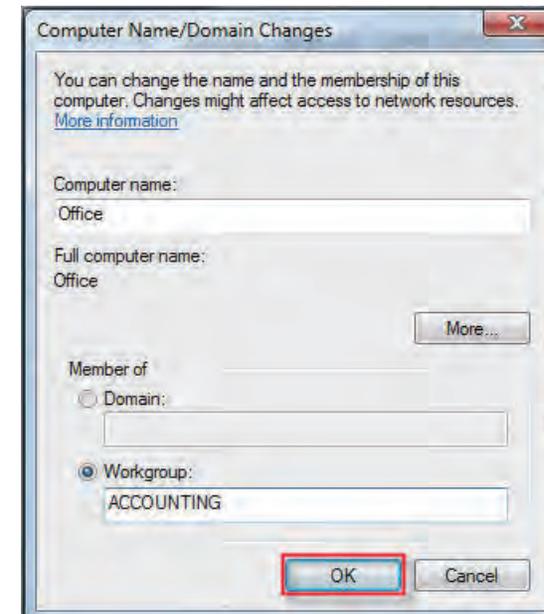
2. Click on the **Advanced system settings** link.



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.



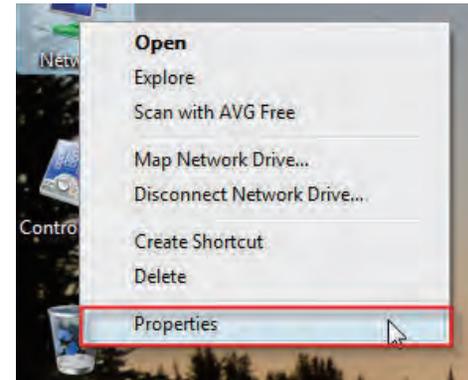
4. Go to the **Computer Name/Domain Changes** window and click the radio button next to the Workgroup you want to join. When you are finished, click the **OK** button.



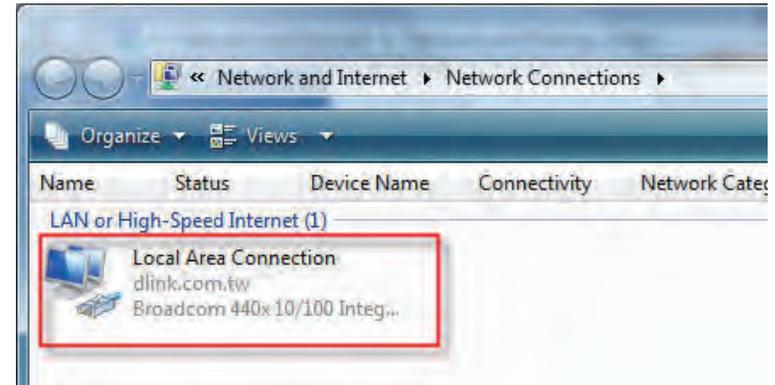
Configuring the IP Address in Vista

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

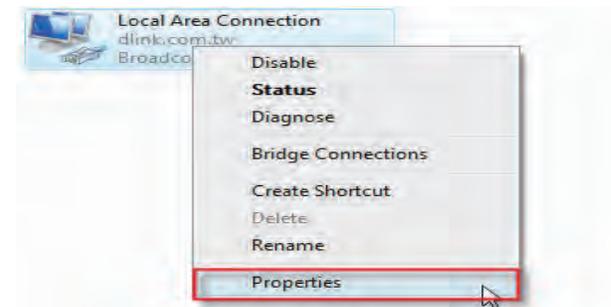
1. Click on **Properties**.



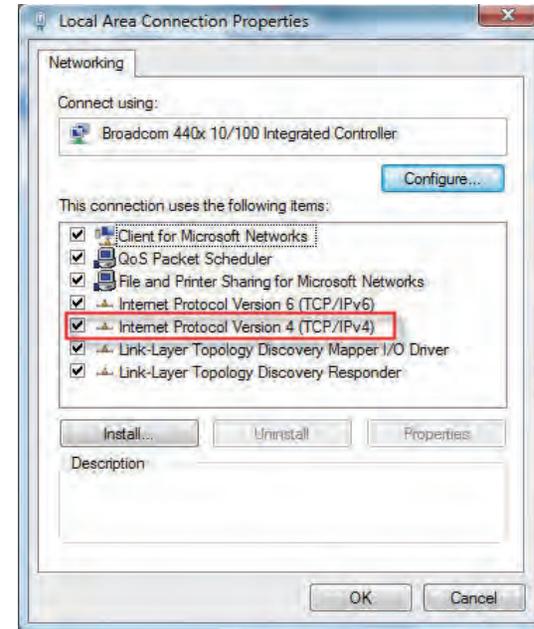
2. Go to the **Network and Internet** window and click the appropriate **Local Area Connection** icon.



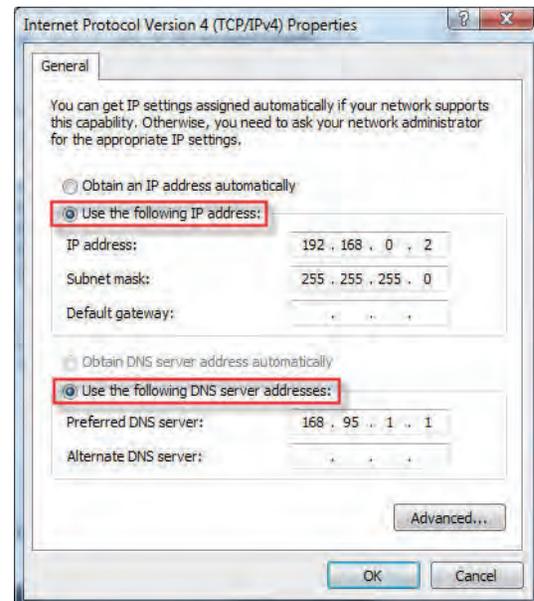
3. Right-click the **Local Area Connection** icon and then select **Properties** from the drop-down menu.



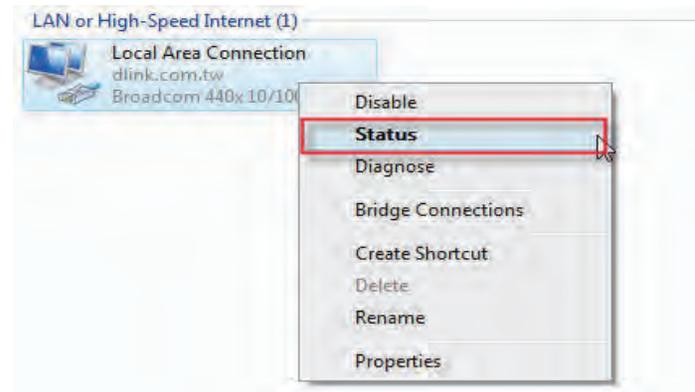
4. Tick the **Internet Protocol Version 4 (TCP/IPv4)** checkbox in the **Networking** tab in the **Local Area Connection Properties** window.



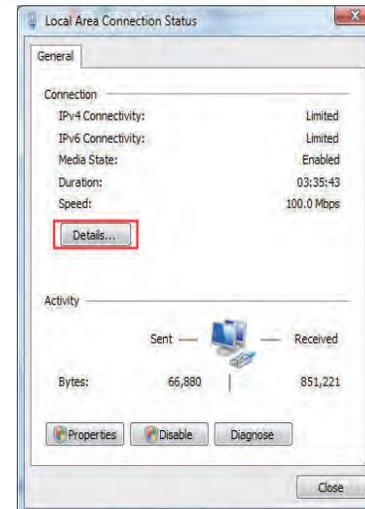
5. Click the “Use the following IP address” option in the **General** tab in the **Local Area Connections Properties** window and enter the desired IP address in the space offered. Then click the “Use the following DNS server addresses” option on the same tab and enter the desired DNS server information.



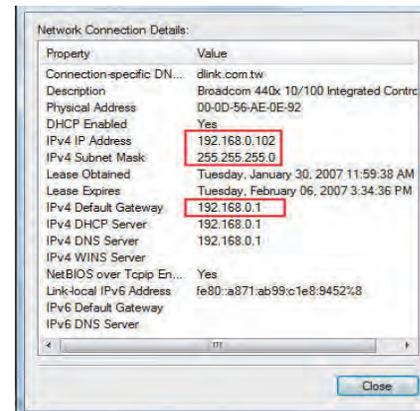
6. Right-click the **Local Area Connection** icon and then select **Status** from the drop-down menu.



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



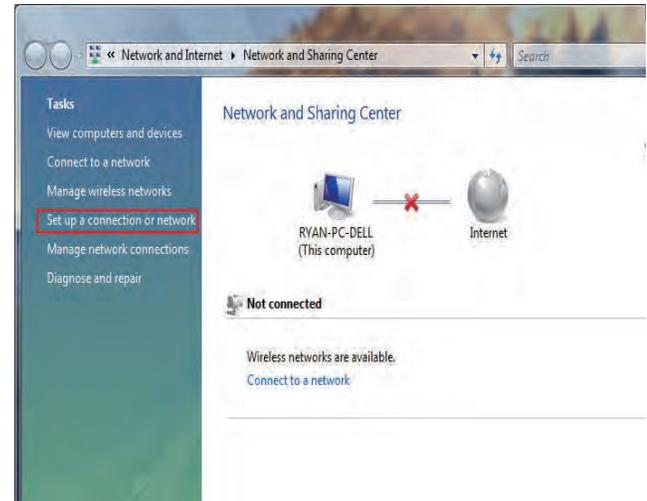
8. Confirm your new settings on the **Network Connection Status** window. When you are finished, click the **Done** button.



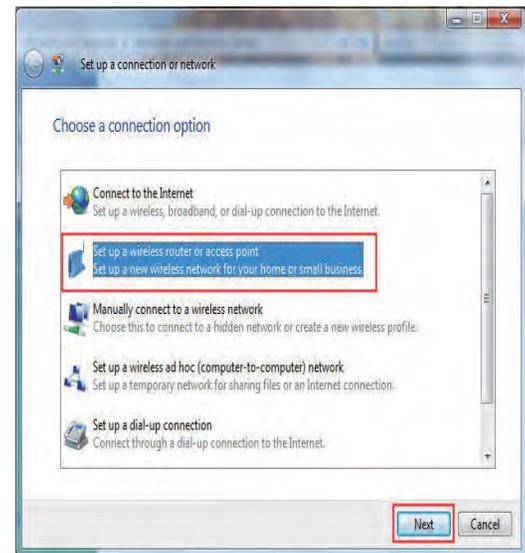
Setting Up a Connection or Network Wirelessly

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

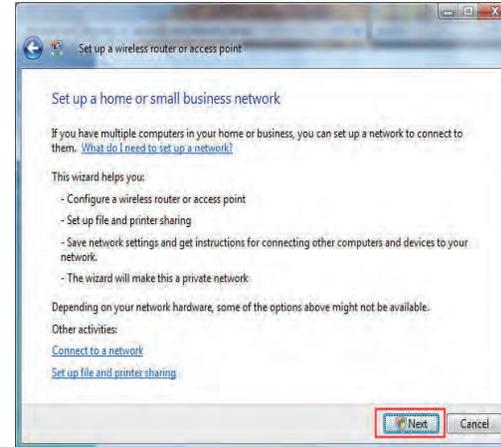
1. Click on **Set up a connection or network** in the **Network and Sharing Center** section.



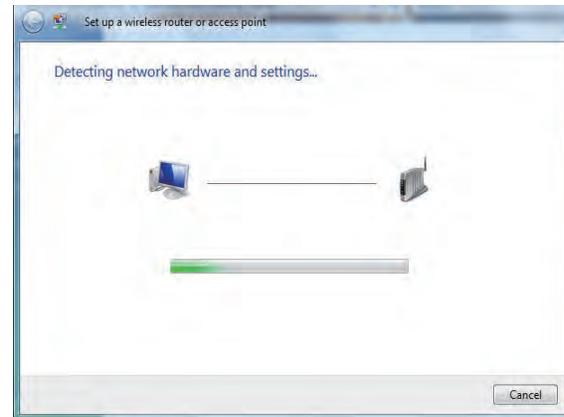
2. Go to the **Set up a connection or network** window and choose the **Set up a wireless router or access point** or **Set up a new wireless network for your home or business** option. Click the **Next** button.



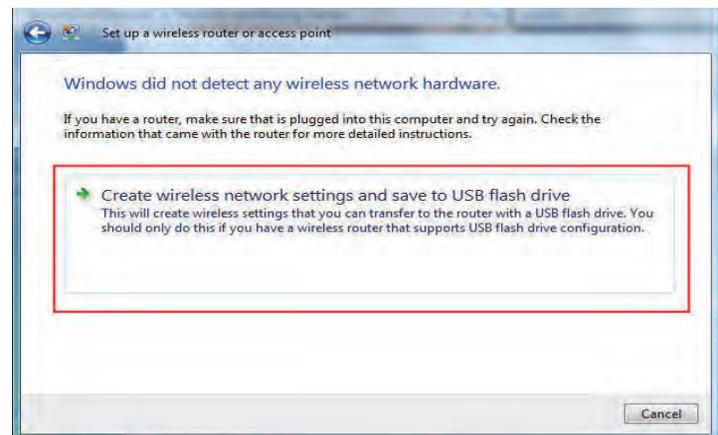
3. Click the **Next** button on the **Set up a wireless router or access point** window.



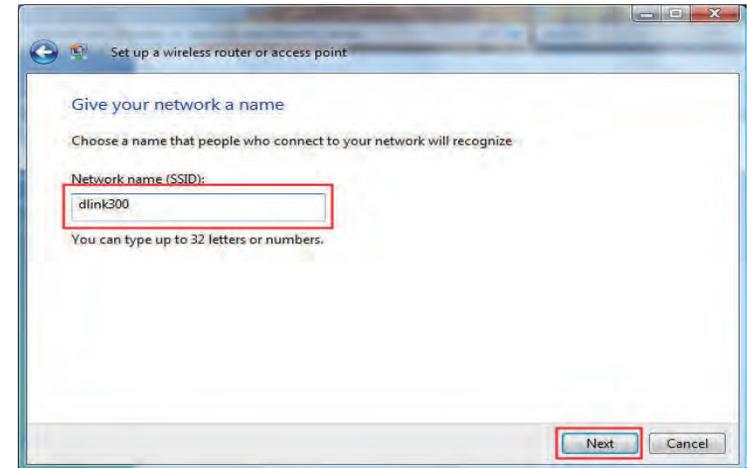
4. The following window displays the system progress.



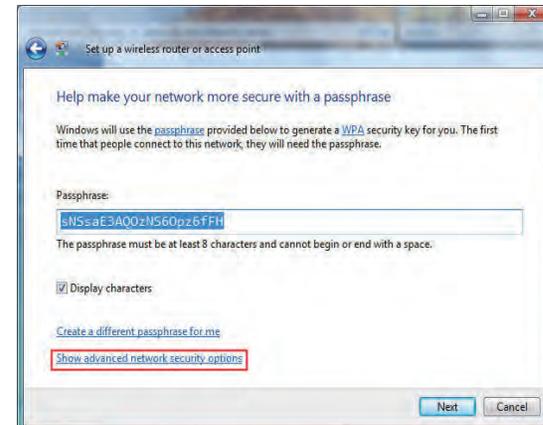
5. This window confirms that you want to create wireless network settings that are savable to a USB flash drive.



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.



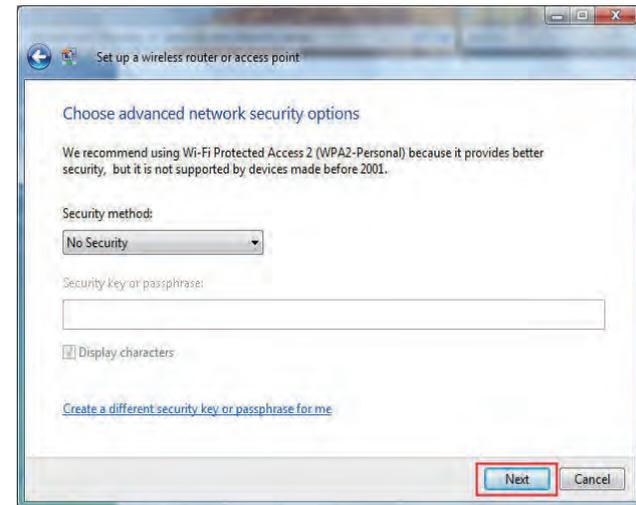
7. Enter a passphrase on the **Help make your network more secure with a passphrase** window in the **Set up a wireless router or access point** wizard. Click the **Show advanced network security options** link.



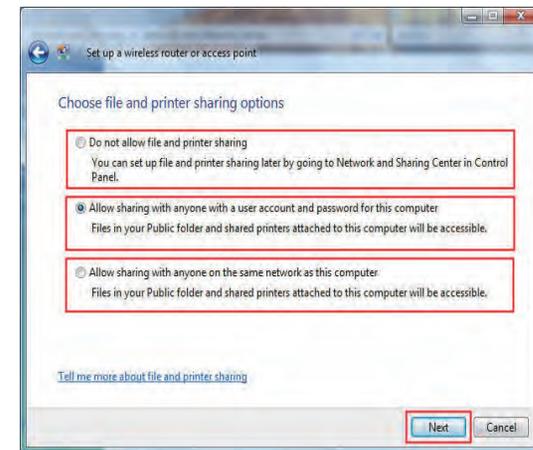
8. Select security method on the **Choose advanced network security options** window in the **Set up a wireless router or access point** wizard. Click the **Next** button.



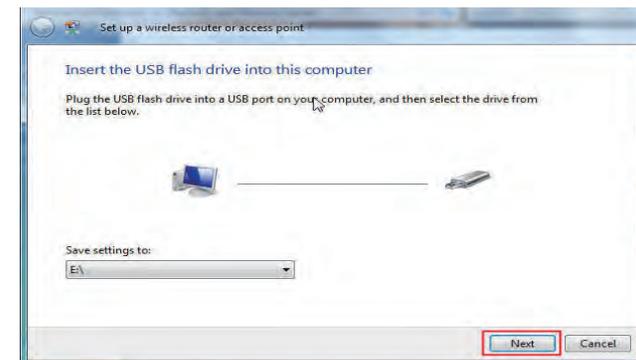
9. Once you have selected the desired security method on the **Choose advanced network security options** window in the **Set up a wireless router or access point** wizard, click the **Next** button.



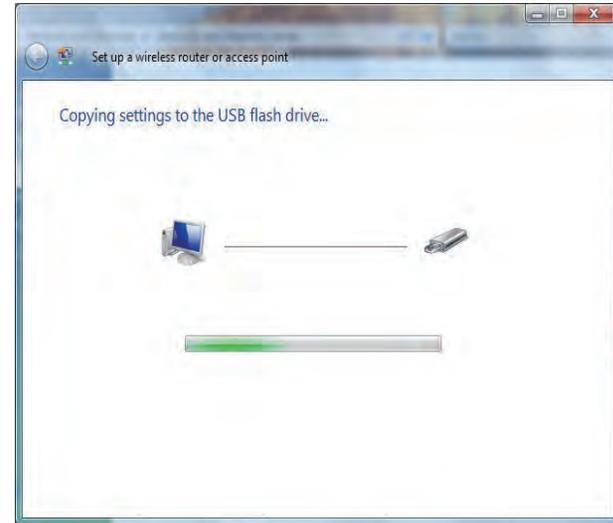
10. Select the desired file and printer sharing option on the **Choose file and printer sharing options** window in the **Set up a wireless router or access point** wizard. Click the **Next** button.



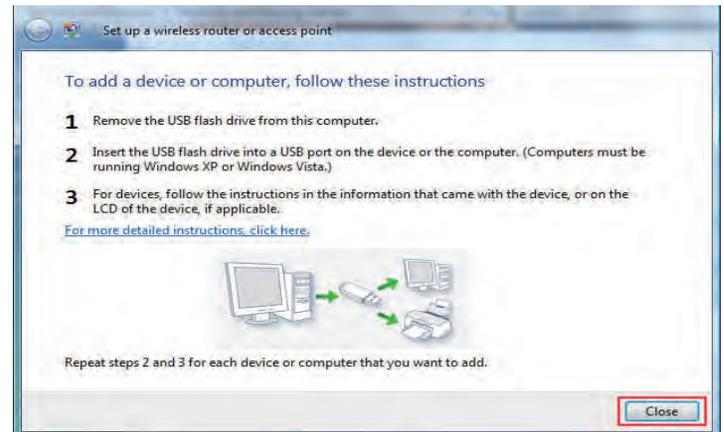
11. Once you have saved your network settings to USB, use the pull-down menu on the **Insert the USB flash drive into this computer** window in the **Set up a wireless router or access point** wizard to select a destination for your network settings. Click the **Next** button.



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.



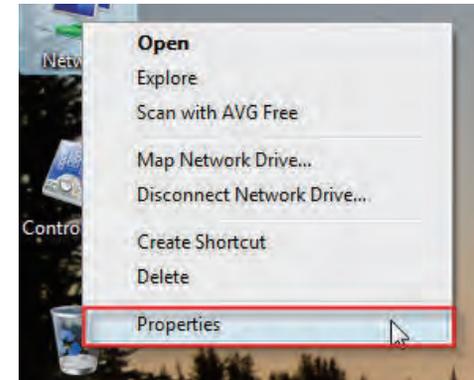
13. Once you are finished, the **To add a device or computer, follow these instructions** window in the **Set up a wireless router or access point wizard** opens. When you are finished, click the **Close** button.



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

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

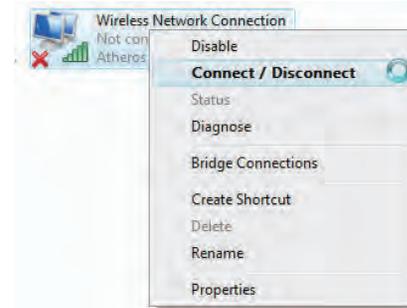
1. Click on **Properties**.



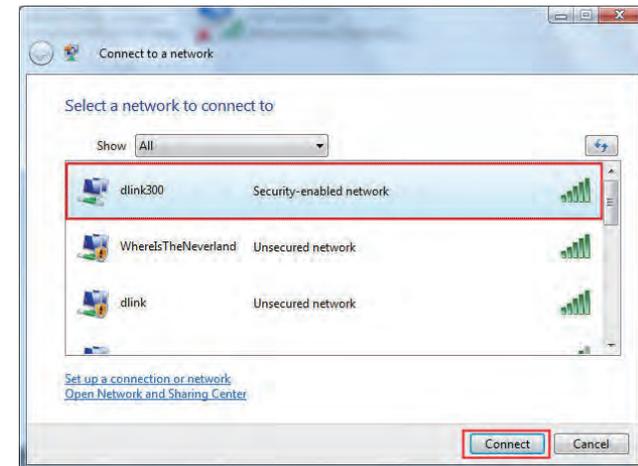
2. Click the **Manage network connections** link in the **Network and Sharing Center** window.



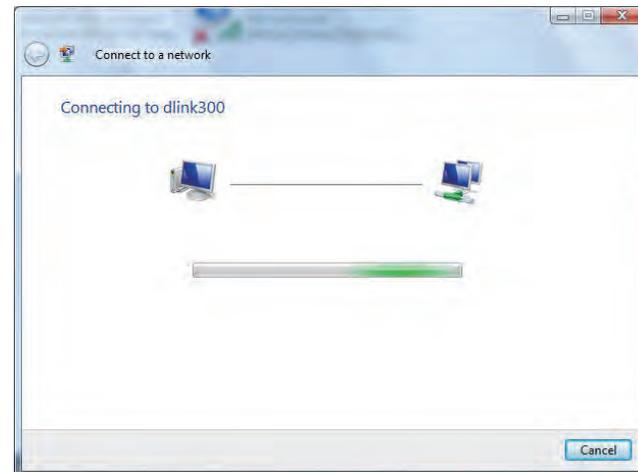
3. Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



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.



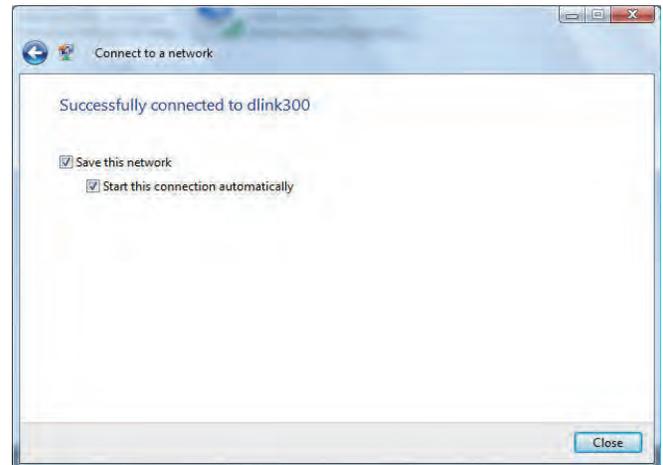
5. The following **Connect to a network** wizard window displays the system progress.



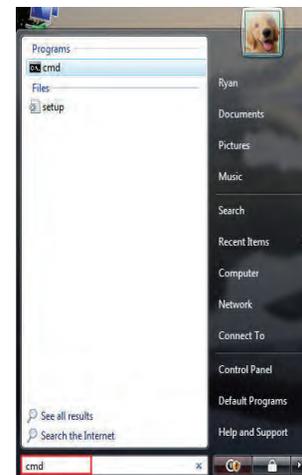
6. Enter the network security key or passphrase for the Router in the textbox provided in the **Type the network security key or passphrase for dlink300** window in the **Connect a network** wizard. When you are finished, click the **Connect** button.



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.

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Ryan>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . . : dlink.com.tw
    Link-local IPv6 Address . . . . . : fe80::adf2:c78:90
    IPv4 Address. . . . . : 192.168.0.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : dlink.com.tw

Tunnel adapter Local Area Connection* 6:

    Connection-specific DNS Suffix . . :
    IPv6 Address. . . . . : 2001:0:4136:e38a:
```

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

```
C:\Windows\system32\cmd.exe - ping 192.168.0.1 -t

C:\Users\Ryan>ping 192.168.0.1 -t

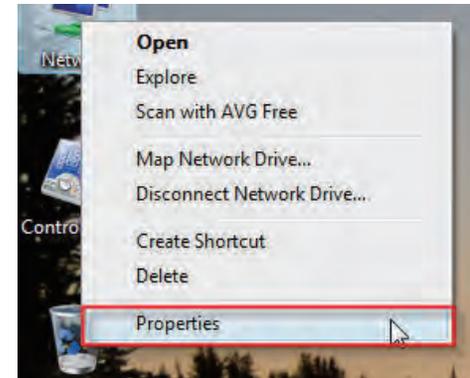
Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64
```

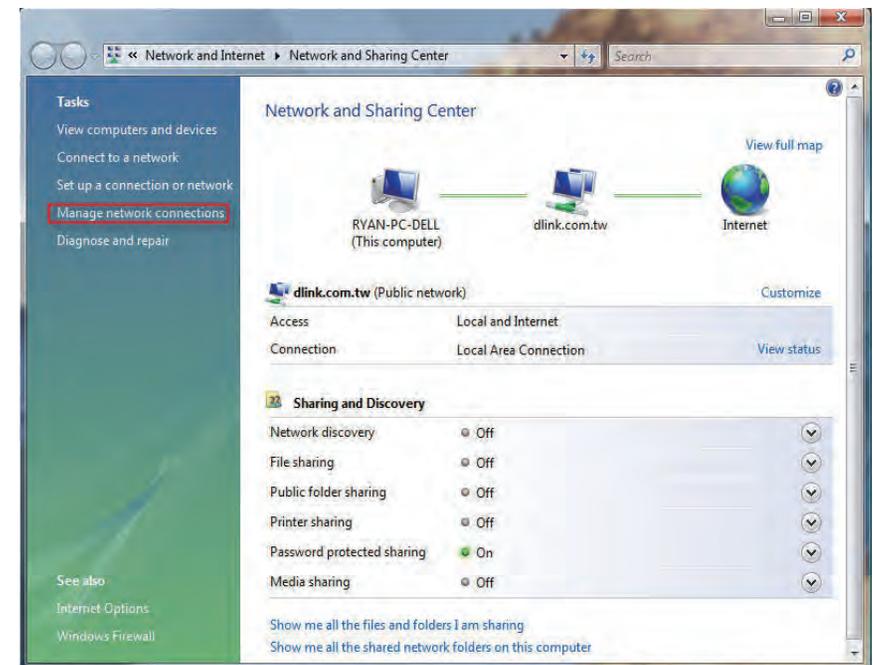
Connecting to an Unsecured Wireless Network

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

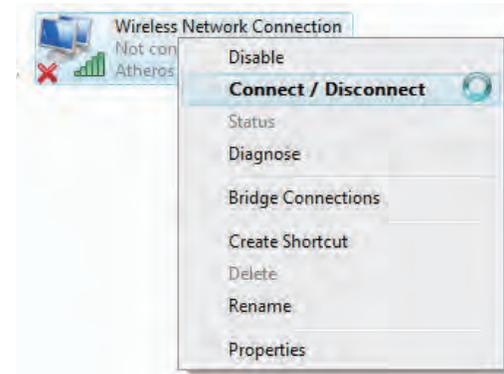
1. Click on **Properties**.



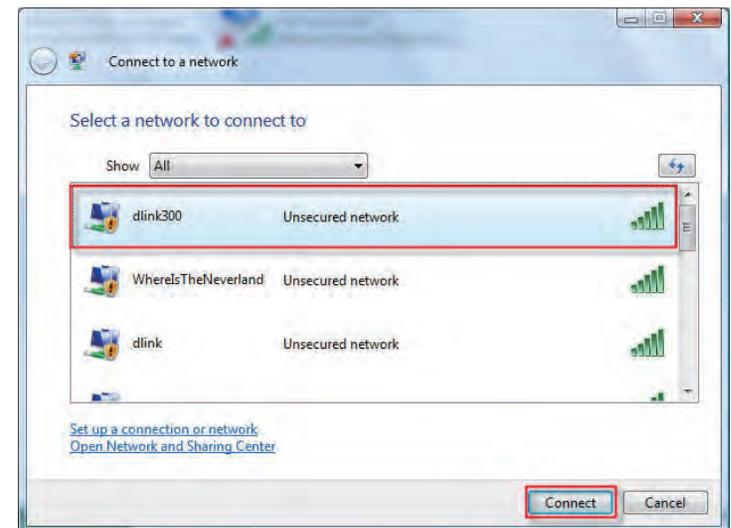
2. Go to the **Network and Sharing Center** window and click the **Manage Network Connections** link.



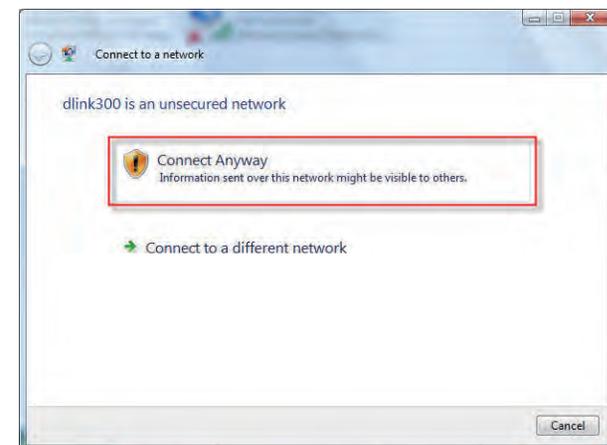
3. Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



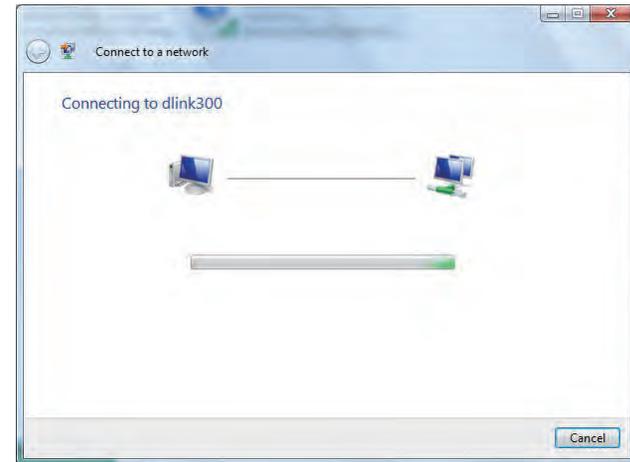
4. Select a network to connect to in the **Select a network to connect to** window in the **Connect to a network** wizard and then click the **Connect** button.



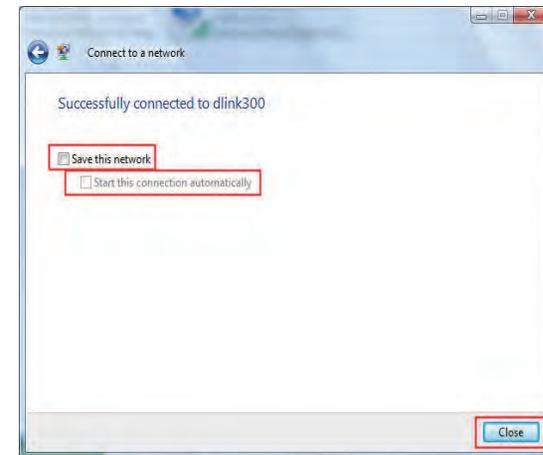
5. Confirm your desire to connect anyway on the following **Network Connection Status** window.



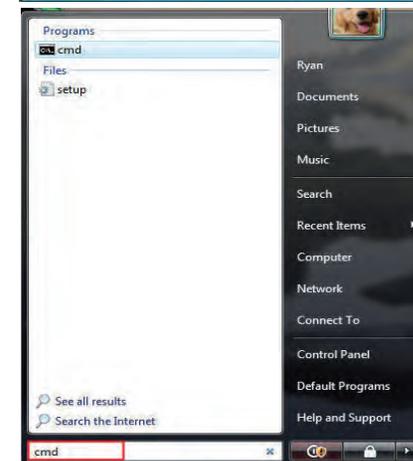
6. The following **Connect to a network** wizard window displays the system progress.



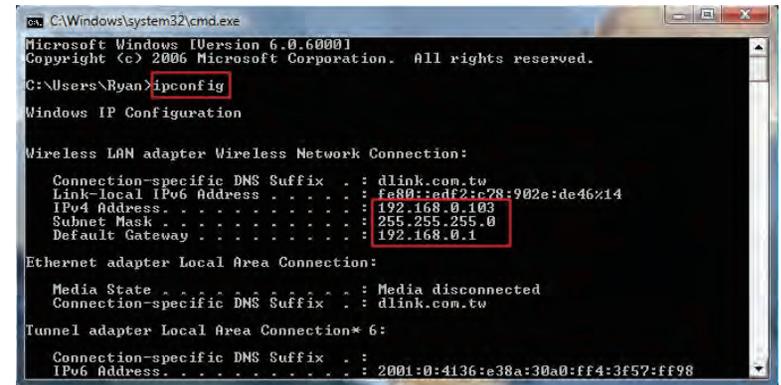
7. The following **Successfully connected to dlink300** window in the **Connect to a network** wizard is displayed. Choose to save to the network and/or start the new connection automatically. When you are finished, click the **Close** button.



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.



```
ca C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6000.1
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Ryan>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . . . : dlink.com.tw
    Link-local IPv6 Address . . . . . : fe80::edf2:c28:902e:de46%14
    IPv4 Address. . . . . : 192.168.0.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : dlink.com.tw

Tunnel adapter Local Area Connection* 6:

    Connection-specific DNS Suffix . . :
    IPv6 Address. . . . . : 2001:0:4136:e38a:30a0:ff4:3f57:ff98
```

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



```
ca C:\Windows\system32\cmd.exe - ping 192.168.0.1 -t

C:\Users\Ryan>ping 192.168.0.1 -t

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time=3ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=2ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=5ms TTL=64
```

Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-619L. 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.

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 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).

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 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, and etc
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

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

Where is wireless used?

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

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like airports, hotels, coffee shops, libraries, restaurants, and convention centers.

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

Tips

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

Centralize your router or Access Point

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

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.

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 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.

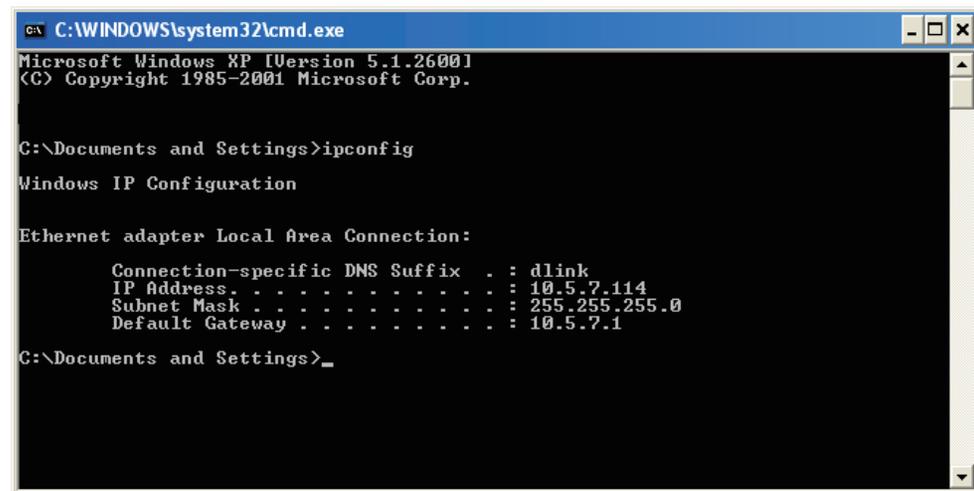
Click on **Start > Run**. In the run box type **cmd** and click **OK**.

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.



```
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>_
```

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

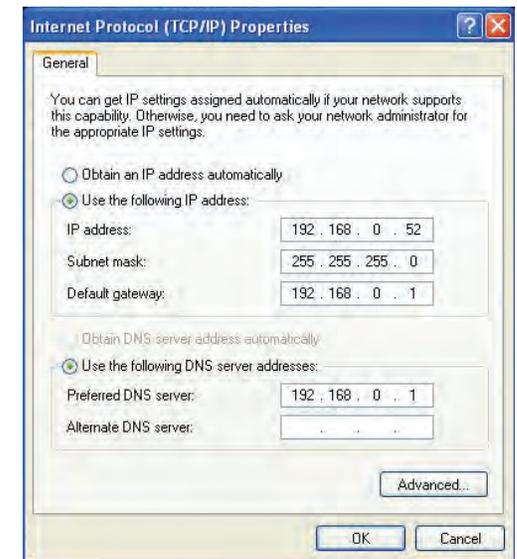
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.

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
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x

Wireless Signal Rates*

- 300Mbps
- 150Mbps
- 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)
- 64/128-bit WEP

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

VPN Pass Through/ Multi-Sessions

- PPTP
- IPSec

Device Management

- Web-based Internet Explorer 8 or later; Netscape Navigator v6 or later; or other Java-enabled browsers
- DHCP Server and Client

Wireless Frequency Range

2.4GHz to 2.497GHz (802.11b)
2.4GHz to 2.4835GHZ (802.11g and 802.11n)

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

Three fixed external antenna

Advanced Firewall Features

- NAT with VPN Pass-through (Network Address Translation)
- MAC Filtering
- IP Filtering
- URL Filtering
- Scheduling

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

CE

C-tick

NCC

CCC

LEDs

- Power
- Status
- Internet
- WLAN (Wireless Connection)
- LAN (10/100)

Dimensions

- L = 135mm
- W = 99.8mm
- H = 31.5mm

Weight

0.246kg

* 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.

CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement:

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

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

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

FCC Caution:

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

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body. To maintain compliance with FCC RF exposure compliance requirements, please avoid direct contact to the transmitting antenna during transmitting.

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.

Radiation Exposure Statement:

The product comply with the FCC portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

ICC Notice:

Operation is subject to the following two conditions:

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

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Règlement d'Industry Canada

Les conditions de fonctionnement sont sujettes à deux conditions:

- (1) Ce périphérique ne doit pas causer d'interférence et.
- (2) Ce périphérique doit accepter toute interférence, y compris les interférences pouvant perturber le bon fonctionnement de ce périphérique.

Industry Canada statement:

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

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.

FOR MOBILE DEVICE USAGE (>20cm/low power)

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.