

# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-605 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.

**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 adapter. For 64Bit encryption, the length of the key(s) will be 40 bits. For 128Bit encryption, the length of the key(s) will be 104 bits. The key(s) must be entered in hexadecimal. For 64Bit encryption, you may enter one key. For 128Bit encryption, you may enter up to four keys. The keys must be entered in hexadecimal. For 64Bit encryption, the length of the key(s) must be 40 bits. For 128Bit encryption, the length of the key(s) must be 104 bits.

You may also enter any text string into a WEP key box, in which case it will be converted into a hexadecimal string. For 64Bit encryption, the length of the key(s) must be 40 bits. For 128Bit encryption, the length of the key(s) must be 104 bits.

Authentication:

WEP Encryption:

Default WEP Key:

WEP Key:

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.

## 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.

WIRELESS SECURITY MODE

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

WPA ONLY

WPA Only requires status to be high grade encryption and authentication

Other Type: **TKIP**

PSK / Cipher: **PSK**

Network Key:

Save Settings    Restore Defaults

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 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.

WIRELESS SECURITY MODE

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

WPA2 ONLY

WPA2 Only requires status to be high grade encryption and authentication

Other Type: **TKIP**

PSK / Cipher: **PSK**

Network Key:

Save Settings    Restore Defaults

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.



# 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.

The screenshot shows the 'WIRELESS SECURITY MODE' configuration page. The 'Security Mode' dropdown is set to 'Enable WPA Only Wireless Security (enhanced)'. Below this, the 'WPA ONLY' section is active, displaying a warning: 'WPA Only requires stations to use high grade encryption and authentication.' The 'Cipher Type' is set to 'TKIP' and 'PSK / EAP' is set to 'EAP'. There are two RADIUS server configuration sections. The first, 'RADIUS Server 1', has 'IP Address' set to '802.IX' and empty fields for 'Port' and 'Shared Secret'. The second, 'RADIUS Server 2', has empty fields for 'IP Address', 'Port', and 'Shared Secret'.

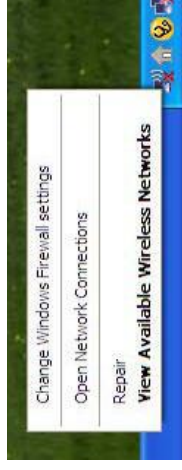
# Connect to a Wireless Network Using Windows® XP

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**.



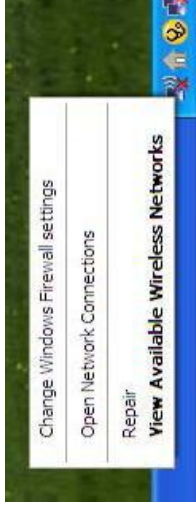
The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

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**.



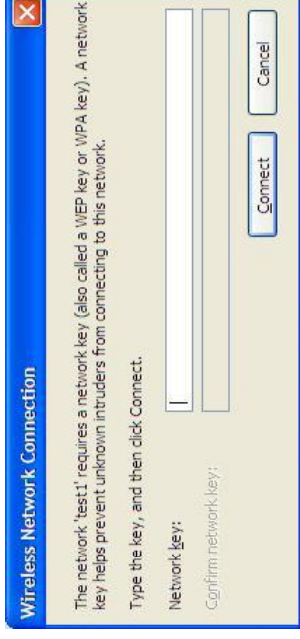
2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.





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

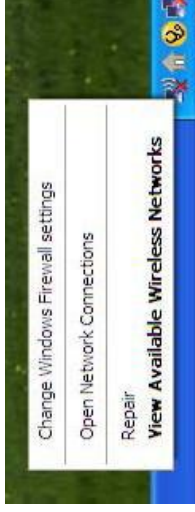
It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP settings are correct. The WEP key must be exactly the same as on the wireless router.



# 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**.

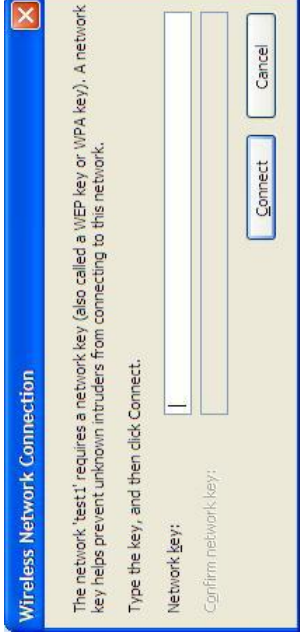


2. Highlight the wireless network (SSID) you would like to connect to and click **Connect**.



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-605 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.

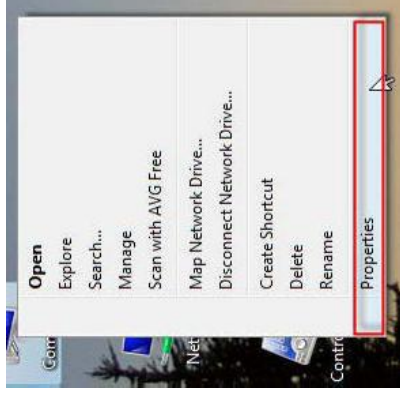
If you are using the Router's Wi-Fi Security push button option, simultaneously depress the push button located on the side of the Router and the button on the client (or virtual button on the client's GUI). Next click **Finish**. The Client's software will then allow a newcomer to join your secure,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

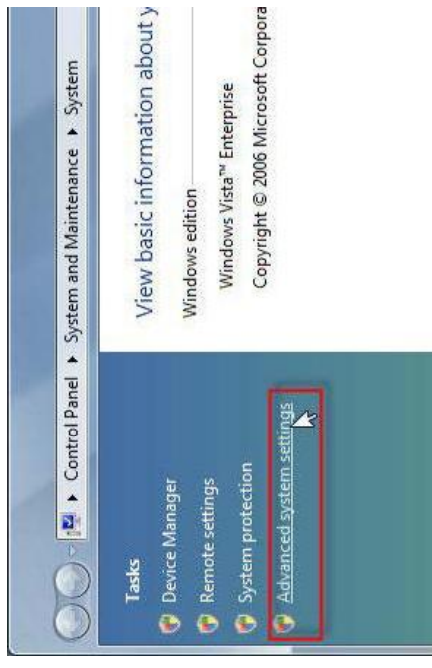
# Changing the Computer Name and Joining a Workgroup

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

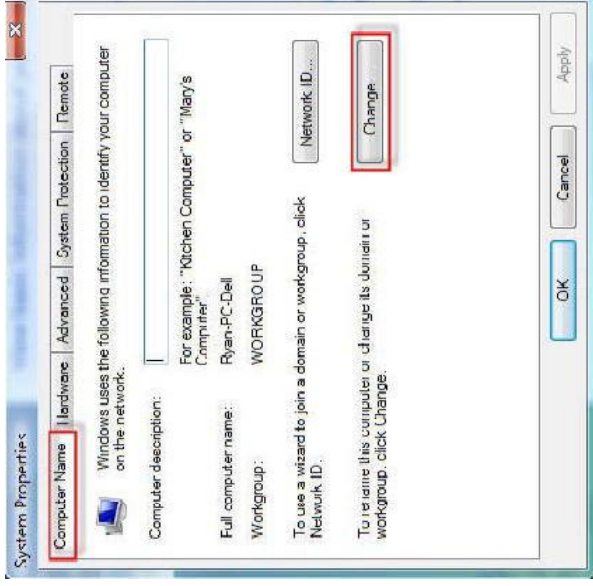
1. Click on **Properties**.



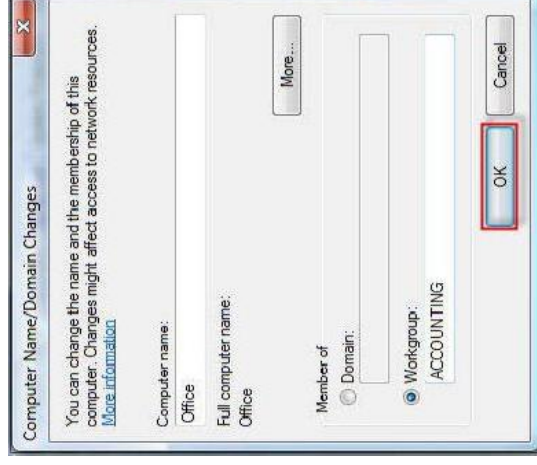
2. Click on the **Advanced system settings** link.



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.



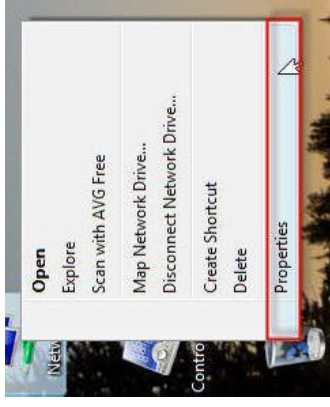
4. Go to the **Computer Name/Domain Changes** window and click the radio button next to the Workgroup you want to join. When you are finished, click the **OK** button.



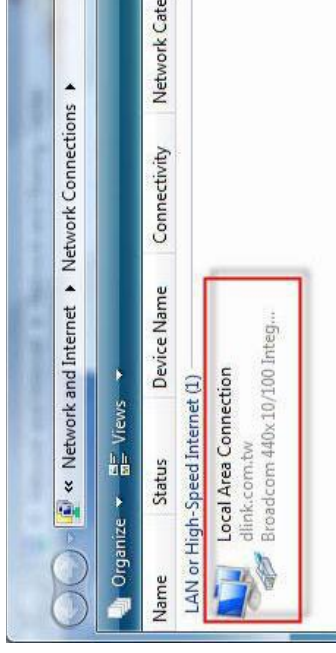
# Configuring the IP Address in Vista

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

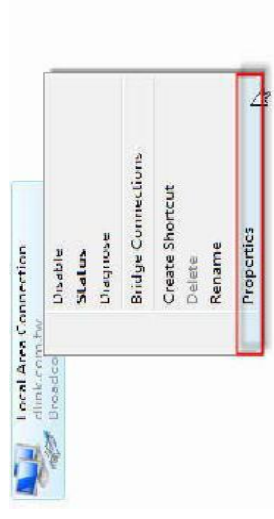
1. Click on **Properties**.



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

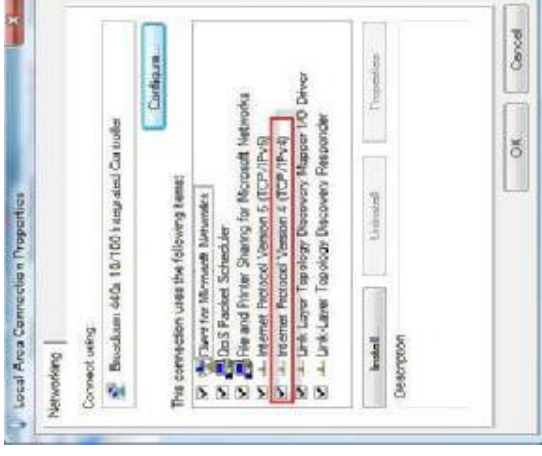


3. Right-click the **Local Area Connection** icon and then select **Properties** from the drop-down menu.

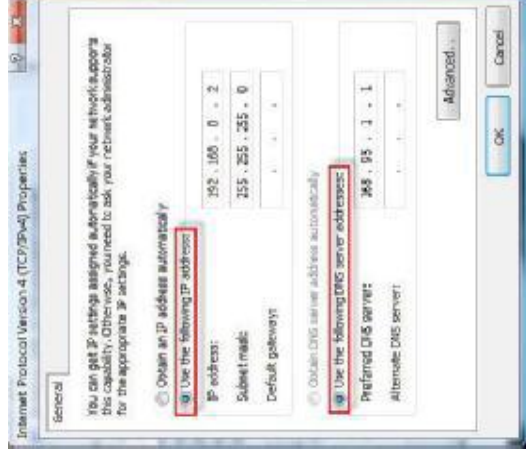




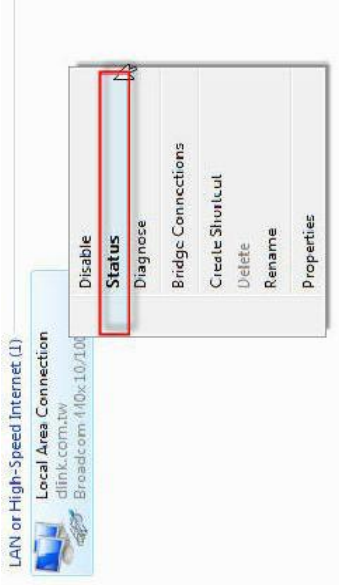
4. Tick the **Internet Protocol Version 4 (TCP/IPv4)** checkbox in the **Networking** tab in the **Local Area Connection Properties** window.



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.



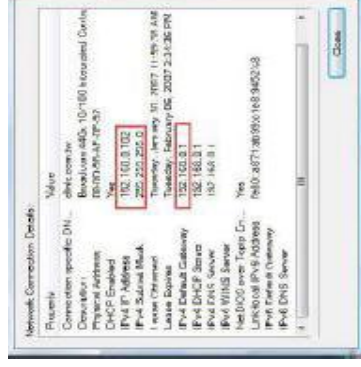
6. Right-click the **Local Area Connection** icon and then select **Status** from the drop-down menu.



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** **Set up a new wireless network for your home or business** option. Click the **Next** button.



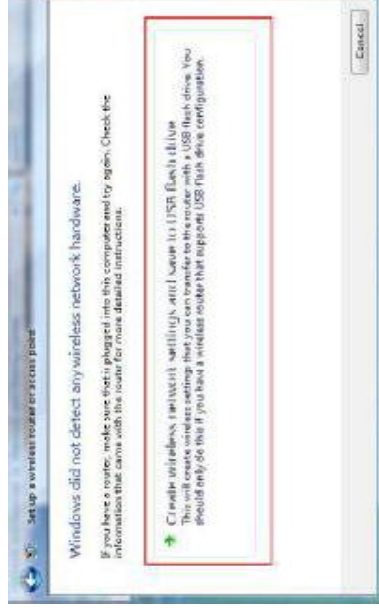
3. Click the **Next** button on the **Set up a wireless router or access point** window.



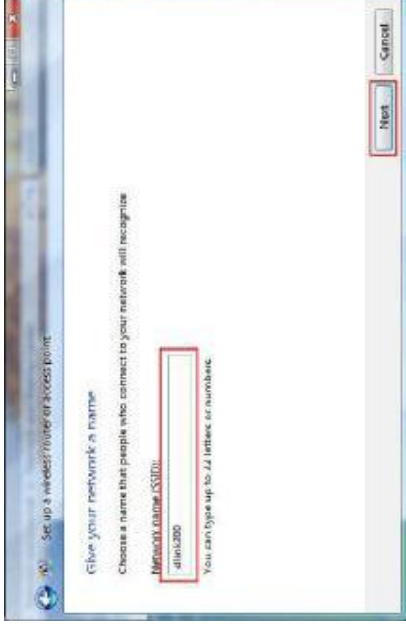
4. The following window displays the system progress.



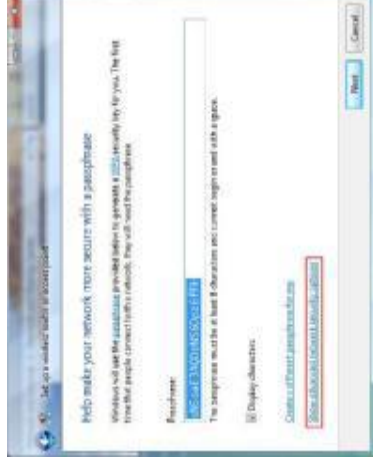
5. This window confirms that you want to create wireless network settings that are saveable to a USB flash drive.



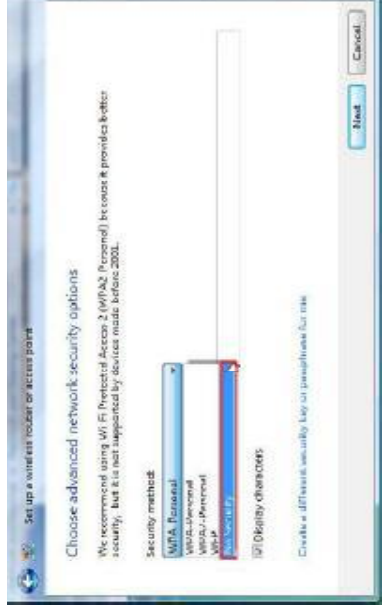
6. Enter a network name on the **Give your network a name** window in the **Set up a wireless router or access point** wizard. Click the **Next** button.



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



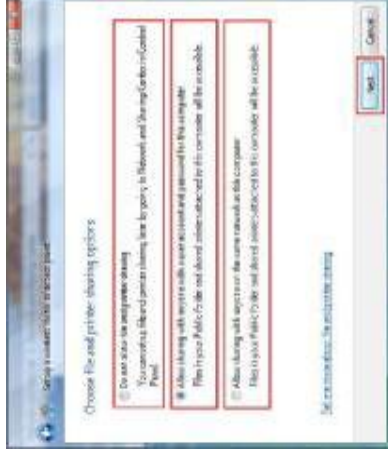
8. Select security method on the **Choose advanced network security options** window in the **Set up a wireless router or access point** wizard. Click the **Next** button.



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 flash drive** window opens. The window shows a progress bar and a USB flash drive icon. The progress bar is filled with green, indicating that the copying process is complete.



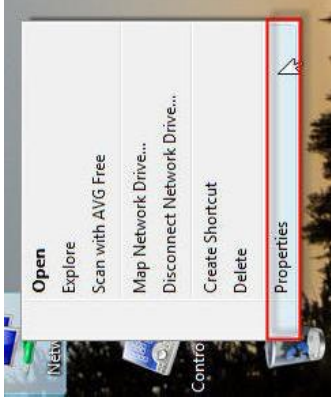
13. Once you are finished, the **To add a device or computer** window opens. The window displays instructions for adding a device or computer to the network. The instructions are: 1. Remove the USB flash drive from this computer. 2. Insert the USB flash drive into a USB port on the device or the computer. (Computer must be running Windows XP or Windows Vista.) 3. For devices, follow the instructions in the information that came with the device, or on the LCD of the device, if applicable. For more detailed instructions, click here. A diagram shows a computer connected to a wireless router, which is then connected to a printer. A 'Close' button is in the bottom right corner.



# 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** and **Sharing Center** window.





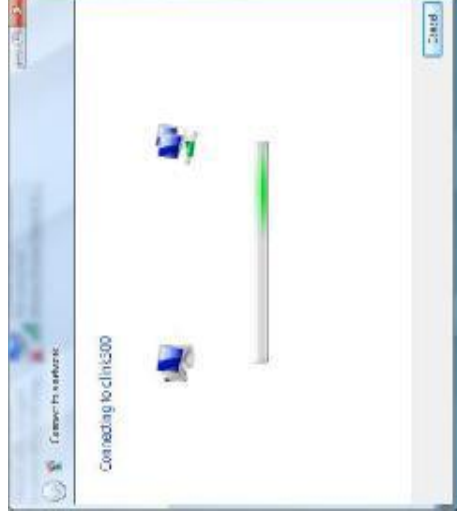
3. Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



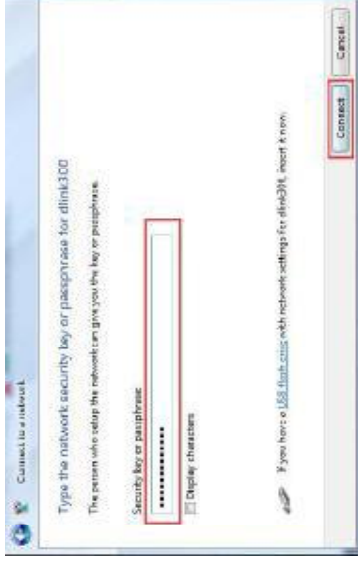
4. Select a network to connect to in the **Select a network to connect to** window in the **Connect to a network** wizard and then click the **Connect** button.



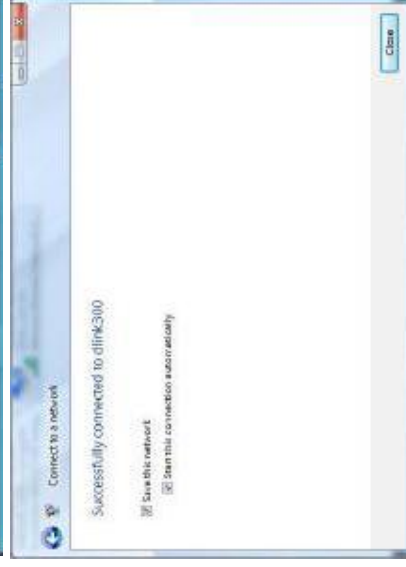
5. The following **Connect to a network** wizard window displays the system progress.



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. 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.

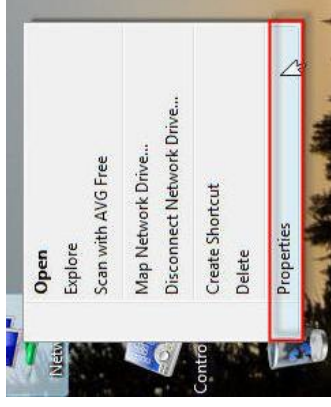




# Connecting to an Unsecured Wireless Network

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.



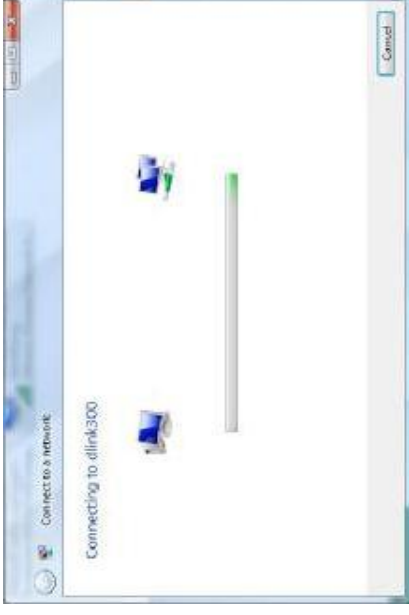
4. Select a network to connect to in the **Select a network to connect to** window in the **Connect to a network** wizard and then click the **Connect** button.



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



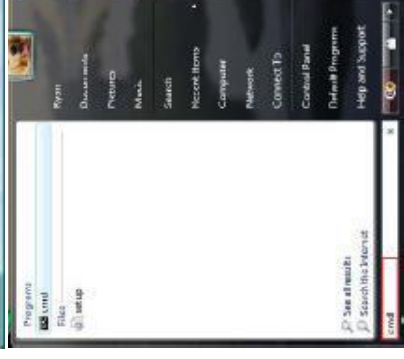
6. The following **Connect to a network** wizard window displays the system progress.



7. The following **Successfully connected to link300** 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.



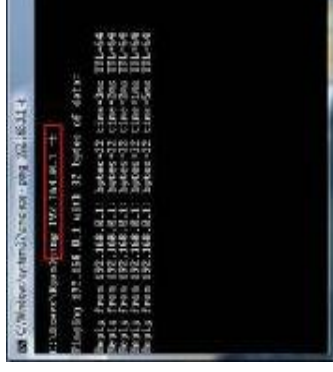
8. The successful connection is displayed at the bottom of the Windows start up menu.



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.



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DIR-605. 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.
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).

## **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.

# 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**.

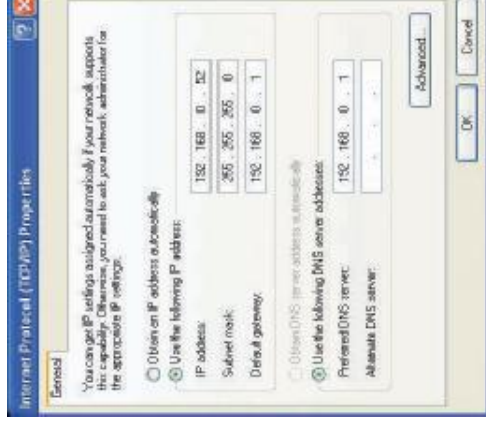
**Step 3**  
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

**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
- IEEE 802.3
- IEEE 802.3u
- IEEE 802.3x

## Wireless Signal Rates\*

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

## Security

- WPA - Wi-Fi Protected Access (TKIP, MIC, IV Expansion, Shared Key Authentication)
- 802.1x
- 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

## Receiver Sensitivity

- 11b -- 1Mbps, 2Mbps, 5.5Mbps, 11Mbps
- 11g -- 6Mbps, 9Mbps, 12Mbps, 18Mbps, 24Mbps, 36Mbps, 48Mbps, 54Mbps
- HT20 MCS0~7 (800NS GI): 6.5Mbps, 13Mbps, 19.5Mbps, 26Mbps, 39Mbps, 52Mbps, 58.5Mbps, 65Mbps
- HT20 MCS8~15 (800NS GI): 13Mbps, 26Mbps, 39Mbps, 52Mbps, 78Mbps, 104Mbps, 117Mbps, 130Mbps
- HT40 MCS0~7 (800NS GI): 13.5Mbps, 27Mbps, 40.5Mbps, 54Mbps, 81Mbps, 108Mbps, 121.5Mbps, 135Mbps
- HT40 MCS8~15 (800NS GI): 27Mbps, 54Mbps, 81Mbps, 108Mbps, 162Mbps, 216Mbps, 243Mbps, 270Mbps
- HT20 MCS0~7 (400NS GI): 7.2Mbps, 14.4Mbps, 21.7Mbps, 28.9Mbps, 43.3Mbps, 57.8Mbps, 65.0Mbps, 72.2Mbps
- HT20 MCS8~15 (400NS GI): 14.444Mbps, 28.889Mbps, 43.333Mbps, 57.778Mbps, 86.667Mbps, 115.556Mbps, 130.000Mbps, 144.444Mbps
- HT40 MCS0~7 (400NS GI): 15.0Mbps, 30.0Mbps, 45.0Mbps, 60.0Mbps, 90.0Mbps, 120.0Mbps, 135.0Mbps, 150.0Mbps
- HT40 MCS8~15 (400NS GI): 30.0Mbps, 60.0Mbps, 90.0Mbps, 120.0Mbps, 180.0Mbps, 240.0Mbps, 270.0Mbps, 300.0Mbps

## VPN Pass Through/ Multi-Sessions

- PPTP
- IPSec

## 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**

2400~2483.5MHz

**Safety and Emissions**

1.FCC Part 15B/ 15C/ MPE 2.IC RSS-210 3.NCC LP0002

**LEDs**

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

**Wireless Operating Range<sup>2</sup>**

- 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 MHF external antenna

**Dimensions**

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

**Advanced Firewall Features**

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

**Weight**

0.246kg

**Warranty**

1 Year

**Operating Temperature**

32°F to 129 °F ( 0°C to 40°C)

**Humidity**

95% maximum (non-condensing)

\* 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.

# Contacting Technical Support

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product. U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

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

- Model number of the product (e.g. DIR-605)
- Hardware Revision (located on the label on the bottom of the router (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the router).

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

## For customers within the United States:

**Phone Support:**  
(877) 453-5465

24 hours a day, seven days a week.

**Internet Support:**  
<http://support.dlink.com>  
[support@dlink.com](mailto:support@dlink.com)

## For customers within Canada:

**Phone Support:**  
(800) 361-5265

Monday to Friday 7:30am to 9:00pm EST

**Internet Support:**  
<http://support.dlink.ca>  
[email:support@dlink.ca](mailto:support@dlink.ca)

# Warranty

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

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

## **Limited Warranty:**

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

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

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

**Limited Software Warranty:**

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

**Non-Applicability of Warranty:**

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

**Submitting A Claim:**

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at <https://rma.dlink.com/>.

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

**What Is Not Covered:**

The Limited Warranty provided herein by D-Link does not cover:

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

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

**Disclaimer of Other Warranties:**

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



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

**Limitation of Liability:**

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

**Governing Law:**

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

**Trademarks:**

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

**Copyright Statement:**

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

Copyright ©2005-2007 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

**CE Mark Warning:**

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

**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.

# Registration



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

Version 1.0  
09/04/2008

## **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 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. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

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。