

DDNS

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

Enable Dynamic DNS: Check this box to enable DDNS updates.

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

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

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

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

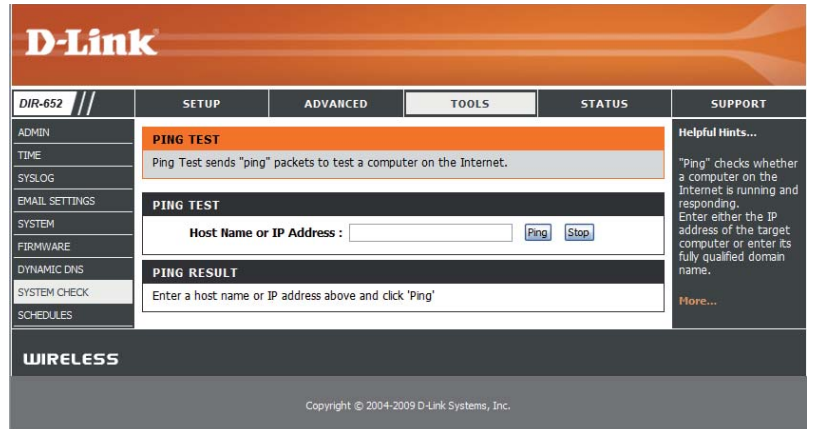
Timeout: Enter a time (in hours).

The screenshot shows the D-Link DIR-652 web interface. The top navigation bar includes 'D-Link', 'DIR-652 //', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists menu items: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS (highlighted), SYSTEM CHECK, and SCHEDULES. The main content area is titled 'DYNAMIC DNS' and contains the following text: 'The DDNS feature allows you to host a server (Web, FTP, Game Server, etc...) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter your host name to connect to your game server no matter what your IP address is. Sign up for D-Link's Free DDNS service at www.dlinkddns.com.' Below this text are two buttons: 'Save Settings' and 'Don't Save Settings'. The 'DYNAMIC DNS SETTINGS' section includes: 'Enable Dynamic DNS : ', 'Server Address : dlinkddns.com(Free) << Select Dynamic DNS Server', 'Host Name :', 'Username or Key :', 'Password or Key :', 'Verify Password or Key :', 'Timeout : 576 (hours)', and 'Status : Disconnected'. A 'Helpful Hints...' sidebar on the right states: 'To use this feature, you must first have a Dynamic DNS account from one of the providers in the drop down menu. More...'. The footer of the interface shows 'WIRELESS' and 'Copyright © 2004-2009 D-Link Systems, Inc.'

System Check

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

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



Schedules

Name: Enter a name for your new schedule.

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

Time: Enter a start and end time for your schedule, or check **All Day - 24hrs** to set the schedule to run all day (for the selected days).

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

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

The screenshot shows the D-Link DIR-652 web interface. The top navigation bar includes 'DIR-652', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'SUPPORT'. The left sidebar lists various configuration options: ADMIN, TIME, SYSLOG, EMAIL SETTINGS, SYSTEM, FIRMWARE, DYNAMIC DNS, SYSTEM CHECK, and SCHEDULES (which is currently selected). The main content area is titled 'SCHEDULES' and contains the following sections:

- SCHEDULES:** A brief description: "The Schedule configuration option is used to manage schedule rules for various firewall and parental control features."
- ADD SCHEDULE RULE:** A form with the following fields:
 - Name:** A text input field.
 - Day(s):** Radio buttons for 'All Week' and 'Select Day(s)'. Under 'Select Day(s)', there are checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, and Sat.
 - All Day - 24 hrs:** A checkbox.
 - Start Time:** A time selection field (12:00 AM) with a dropdown for AM/PM and a note "(hour:minute, 12 hour time)".
 - End Time:** A time selection field (12:00 AM) with a dropdown for AM/PM and a note "(hour:minute, 12 hour time)".
 - Buttons:** 'Save' and 'Clear' buttons.
- SCHEDULE RULES LIST:** A table with columns for 'Name', 'Day(s)', and 'Time Frame'. The table is currently empty.

The right sidebar contains 'Helpful Hints...' with the following text:

Schedules are used with a number of other features to define when those features are in effect.

Give each schedule a name that is meaningful to you. For example, a schedule for Monday through Friday from 3:00pm to 9:00pm, might be called "After School".

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

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

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

[More...](#)

At the bottom of the page, there is a 'WIRELESS' section and a copyright notice: "Copyright © 2004-2009 D-Link Systems, Inc."

Device Information

This page displays the current information for the DIR-652. It will display the LAN, WAN (Internet), and Wireless information.

If your Internet connection is set up for a Dynamic IP address then a **Release** button and a **Renew** button will be displayed. Use **Release** to disconnect from your ISP and use **Renew** to connect to your ISP.

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

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

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

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

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

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

IGMP Multicast Memberships: Displays the Multicast Group IP Address.

DIR-652	SETUP	ADVANCED	TOOLS	STATUS	SUPPORT
<ul style="list-style-type: none"> DEVICE INFO LOGS STATISTICS INTERNET SESSIONS WIRELESS IPV6 	<h3>DEVICE INFORMATION</h3> <p>All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.</p> <hr/> <h4>GENERAL</h4> <p>Time : Thursday, December 03, 2009 4:19:17 PM Firmware Version : 1.00 , Thu, 3, Dec, 2009</p> <hr/> <h4>WAN</h4> <p>Connection Type: DHCP Client Cable Status : Disconnected Network Status : Disconnected StreamEngine : N/A Connection Up Time : N/A</p> <p><input type="button" value="DHCP Release"/> <input type="button" value="DHCP Renew"/></p> <p>MAC Address : 00:18:e7:6a:27:93 IP Address : 0.0.0.0 Subnet Mask : 0.0.0.0 Default Gateway : 0.0.0.0 Primary DNS Server : 0.0.0.0 Secondary DNS Server : 0.0.0.0 Advanced DNS : Disabled</p> <hr/> <h4>LAN</h4> <p>MAC Address : 00:18:e7:6a:27:92 IP Address : 192.168.0.1 Subnet Mask : 255.255.255.0 DHCP Server : Enabled</p> <hr/> <h4>WIRELESS LAN</h4> <p>Wireless Radio : Enabled 802.11 Mode : Mixed 802.11n, 802.11g and 802.11b Channel Width : 20MHz Channel : 11 WPS : Active</p>				<p>Helpful Hints...</p> <p>All of your WAN and LAN connection details are displayed here.</p> <p>More...</p>

Logs

The router automatically logs (records) events of interest in its internal memory. If there isn't enough internal memory for all events, logs of older events are deleted, but logs of the most recent events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

Log Type: You can select the types of messages that you want to display from the log. System Activity, Debug Information, Attacks, Dropped Packets, and Notice messages can be selected.

Apply Log Settings Now: Will filter the log results so that only the selected message types appear.

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

Clear: Clears all of the log contents.

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

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

D-Link

DIR-652 // SETUP ADVANCED TOOLS STATUS SUPPORT

LOGS

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

LOG OPTIONS

Log Type: System Activity
 Debug Information
 Attacks
 Dropped Packets
 Notice

Apply Log Settings Now

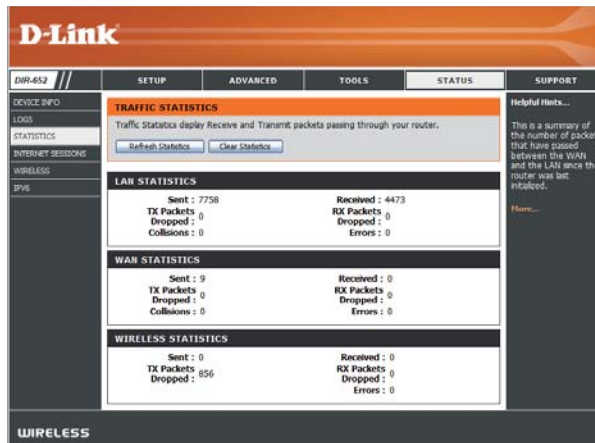
LOG DETAILS

1 / 12

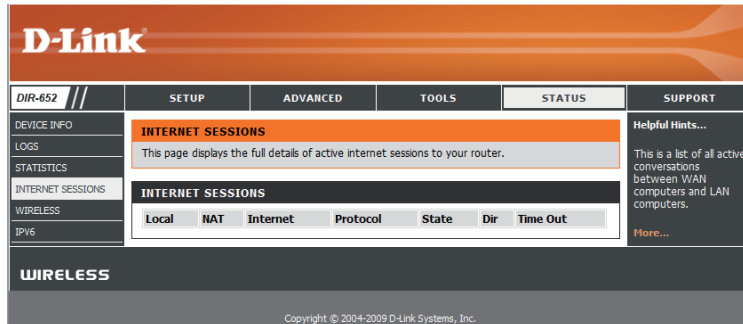
Priority	Time	Message
info	Dec 3 16:17:59	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:17:56	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:15:07	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:15:04	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:13:02	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:12:57	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:11:48	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:11:44	UDHCPD Inform: add_lease 192.168.0.101
info	Dec 3 16:11:15	[26.460000] br0: port 2(ath0) entering forwarding state
info	Dec 3 16:11:15	[26.460000] br0: topology change detected, propagating

Statistics

The screen below displays the Traffic Statistics. Here you can view the amount of packets that pass through the DIR-652 on both the Internet and the LAN ports. The traffic counter will reset if the device is rebooted.

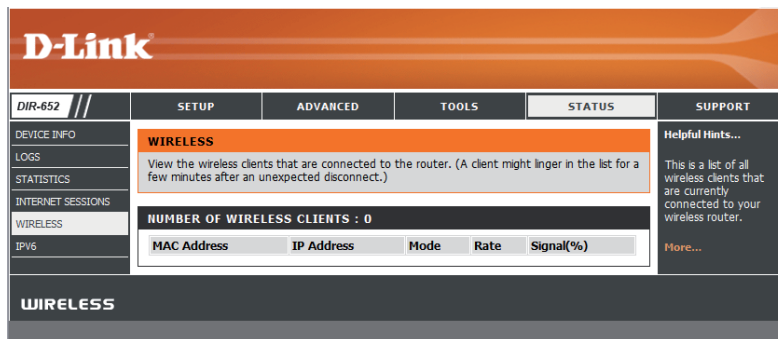


Internet Sessions



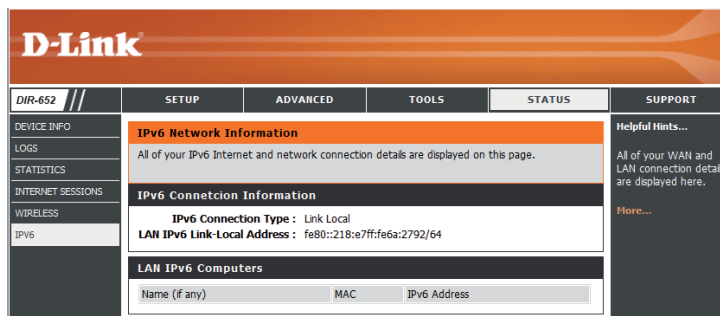
Wireless

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



IPv6

The IPv6 details page displays full details of IPv6 clients that are connected when IPv6 is enabled.



Support

D-Link

DIR-652 //

SETUP ADVANCED TOOLS STATUS **SUPPORT**

MENU
SETUP
ADVANCED
TOOLS
STATUS

SUPPORT MENU

- [Setup](#)
- [Advanced](#)
- [Tools](#)
- [Status](#)

SETUP HELP

- [Internet Connection](#)
- [WAN](#)
- [Wireless](#)
- [Network Settings](#)

ADVANCED HELP

- [Virtual Server](#)
- [Port Forwarding](#)
- [Application Rules](#)
- [QoS Engine](#)
- [Access Control](#)
- [Website Filter](#)
- [Network Filter](#)
- [Firewall Settings](#)
- [Routing](#)
- [Inbound Filter](#)
- [Advanced Wireless](#)
- [WISH](#)
- [Advanced Network](#)
- [GUEST_ZONE](#)
- [IPv6](#)

TOOLS HELP

- [Admin](#)
- [Time](#)
- [Syslog](#)
- [Email Settings](#)
- [System](#)
- [Firmware](#)
- [Dynamic DNS](#)
- [System Check](#)
- [Schedules](#)

STATUS

- [Device Info](#)
- [Logs](#)
- [Statistics](#)
- [Internet Sessions](#)

WIRELESS

Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DIR-652 offers the following types of security:

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

What is WPA?

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

The 2 major improvements over WEP:

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

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

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

Wireless Security Setup Wizard

To run the security wizard, click on Setup at the top and then click **Launch Wireless Security Setup Wizard**.

WIRELESS SETTINGS

The following Web-based wizards are designed to assist you in your wireless network setup and wireless device connection.

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

WIRELESS NETWORK SETUP WIZARD

This wizard is designed to assist you in your wireless network setup. It will guide you through step-by-step instructions on how to set up your wireless network and how to make it secure.

[Wireless Network Setup Wizard](#)

Note: Some changes made using this Setup Wizard may require you to change some settings on your wireless client adapters so they can still connect to the D-Link Router.

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

This wizard is designed to assist you in connecting your wireless device to your wireless router. It will guide you through step-by-step instructions on how to get your wireless device connected. Click the button below to begin.

[Add Wireless Device with WPS](#)

MANUAL WIRELESS NETWORK SETUP

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

[Manual Wireless Network Setup](#)

Click **Next** to continue.

WELCOME TO THE D-LINK WIRELESS SECURITY SETUP WIZARD

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

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

[Next](#) [Cancel](#)

Section 4 - Security

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

STEP 1: NAME YOUR WIRELESS NETWORK

Your wireless network needs a name so it can be easily recognized by wireless clients. For security purposes, it is highly recommended to change the pre-configured network name of [dlink].

Wireless Network Name (SSID):

Select the level of security for your wireless network:

- Best - WPA2 Authentication
- Better - WPA Authentication
- None - No security

Click **Next** to continue.

STEP 2: SECURE YOUR WIRELESS NETWORK

In order to protect your network from hackers and unauthorized users, it is highly recommended you choose one of the following wireless network security settings.

There are three levels of wireless security - Good Security, Better Security, AND Best Security. The level you choose depends on the security features your wireless adapters support.

BEST Select this option if your wireless adapters SUPPORT WPA2

BETTER Select this option if your wireless adapters SUPPORT WPA

GOOD Select this option if your wireless adapters DO NOT SUPPORT WPA

NONE Select this option if you do not want to activate any security features

For information on which security features your wireless adapters support, please refer to the adapters' documentation.

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

If you selected Best or Better, enter a password between 8-63 characters.

If you selected Good, enter 13 characters or 26 Hex digits.

Click **Next** to continue.

STEP 3: SET YOUR WIRELESS SECURITY PASSWORD

You have selected your security level - you will need to set a wireless security password.

Wireless Security Password:

(8 to 63 characters)

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

Section 4 - Security

If you selected Better, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

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



SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

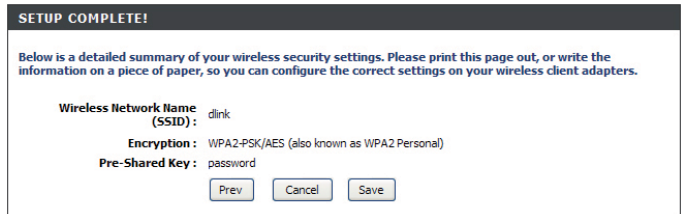
Wireless Network Name (SSID) : dlink

Encryption : WPA-PSK/TKIP (also known as WPA Personal)

Pre-Shared Key : password1M2Z

If you selected Best, the following screen will show you your Pre-Shared Key to enter on your wireless clients.

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



SETUP COMPLETE!

Below is a detailed summary of your wireless security settings. Please print this page out, or write the information on a piece of paper, so you can configure the correct settings on your wireless client adapters.

Wireless Network Name (SSID) : dlink

Encryption : WPA2-PSK/AES (also known as WPA2 Personal)

Pre-Shared Key : password

If you selected WPA-Enterprise, the RADIUS information will be displayed. Click **Save** to finish the Security Wizard.

Configure WPA-Personal (PSK)

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

Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1).

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WPA-Personal**.
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
5. Next to *Pre-Shared Key*, enter a key (passphrase). The key is entered as a pass-phrase in ASCII format at both ends of the wireless connection. The pass-phrase must be between 8-63 characters.
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 on your adapter and enter the same passphrase as you did on the router.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode : WPA-Personal ▼

WPA

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES (CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode : WPA Only ▼

Group Key Update Interval : 3600 (seconds)

PRE-SHARED KEY

Pre-Shared Key : ●●●●●●●●

Configure WPA-Enterprise (RADIUS)

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

1. Log into the web-based configuration by opening a web browser and entering the IP address of the router (192.168.0.1). Click on **Setup** and then click **Wireless Settings** on the left side.
2. Next to *Security Mode*, select **WPA-Enterprise**.
3. Next to *WPA Mode*, select **Auto**, **WPA2 Only**, or **WPA Only**. Use **Auto** if you have wireless clients using both WPA and WPA2.
4. Next to *Group Key Update Interval*, enter the amount of time before the group key used for broadcast and multicast data is changed (3600 is default).
5. Next to *Authentication Timeout*, enter the amount of time before a client is required to re-authenticate (60 minutes is default).
6. Next to *RADIUS Server IP Address* enter the IP Address of your RADIUS server.
7. Next to *RADIUS Server Port*, enter the port you are using with your RADIUS server. 1812 is the default port.
8. Next to *RADIUS Server Shared Secret*, enter the security key.
9. If the *MAC Address Authentication* box is selected then the user will need to connect from the same computer whenever logging into the wireless network.
10. Click **Advanced** to enter settings for a secondary RADIUS Server.
11. Click **Apply Settings** to save your settings.

WIRELESS SECURITY MODE

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option requires an external RADIUS server.

Security Mode: WPA-Enterprise

WPA

Use **WPA** or **WPA2** mode to achieve a balance of strong security and best compatibility. This mode uses WPA for legacy clients while maintaining higher security with stations that are WPA2 capable. Also the strongest cipher that the client supports will be used. For best security, use **WPA2 Only** mode. This mode uses AES (CCMP) cipher and legacy stations are not allowed access with WPA security. For maximum compatibility, use **WPA Only**. This mode uses TKIP cipher. Some gaming and legacy devices work only in this mode.

To achieve better wireless performance use **WPA2 Only** security mode (or in other words AES cipher).

WPA Mode: WPA Only

Group Key Update Interval: 3600 (seconds)

EAP (802.1X)

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

Authentication Timeout: 60 (minutes)

RADIUS server IP Address: 0.0.0.0

RADIUS server Port: 1812

RADIUS server Shared Secret: radius_shared

MAC Address Authentication:

Advanced >>

EAP (802.1X)

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

Authentication Timeout : (minutes)

RADIUS server IP Address :

RADIUS server Port :

RADIUS server Shared Secret :

MAC Address Authentication :

Optional backup RADIUS server:

Second RADIUS server IP Address :

Second RADIUS server Port :

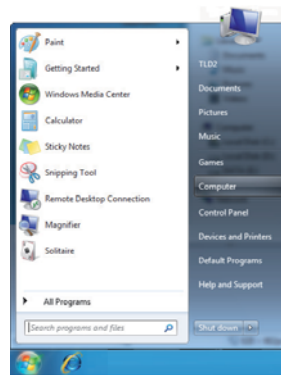
Second RADIUS server Shared Secret :

Second MAC Address Authentication :

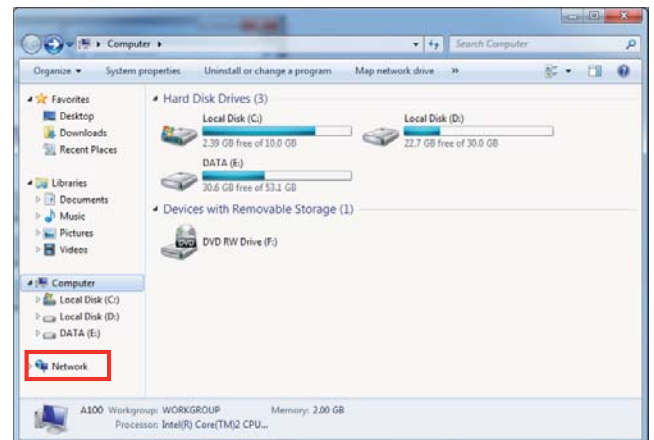
Using Windows® 7 and WPS for Wireless Configuration

The following steps allow you to configure your DIR-652 wireless network settings using Windows® 7 through WPS.

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

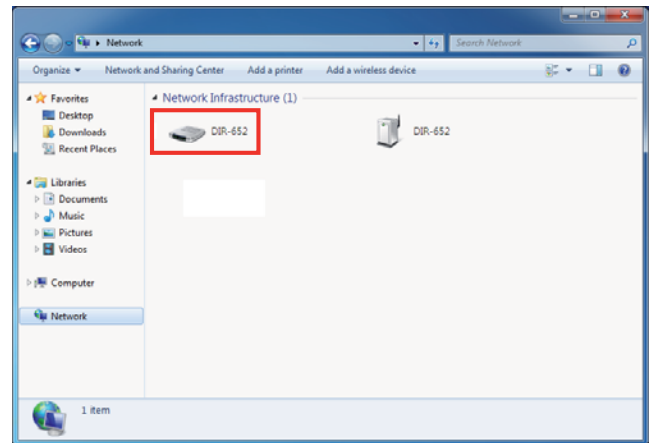


2. Click the **Network** option.

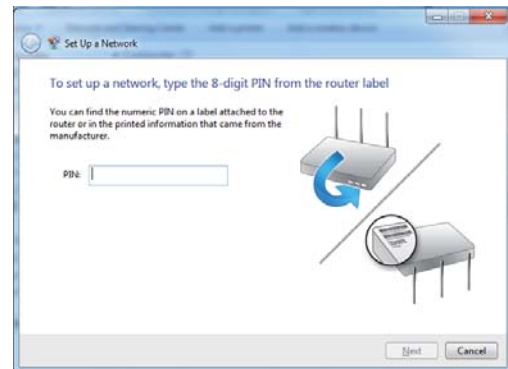


Section 5 - Connecting to a Wireless Network

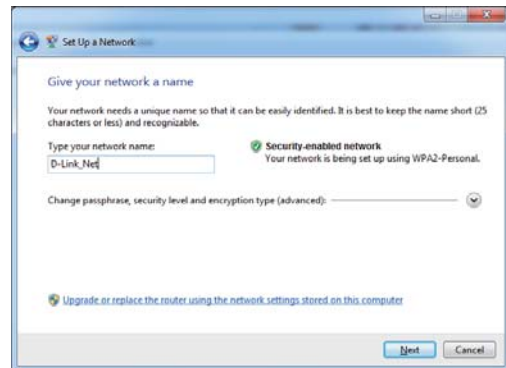
3. Double-click the DIR-652 router.




4. Input the WPS PIN number (displayed in the **Advanced > Wi-Fi Protected Setup** section in the Router's Web UI) and click **Next**.

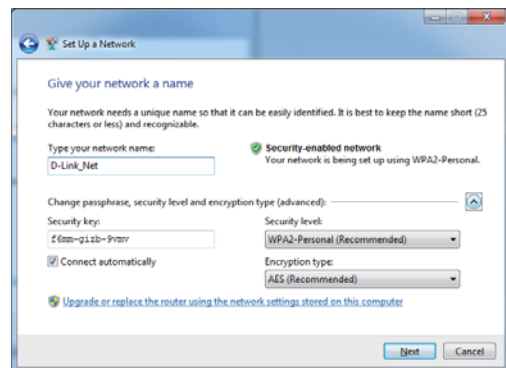


5. Type a name for your wireless network.



6. To configure advanced settings, click the  icon.

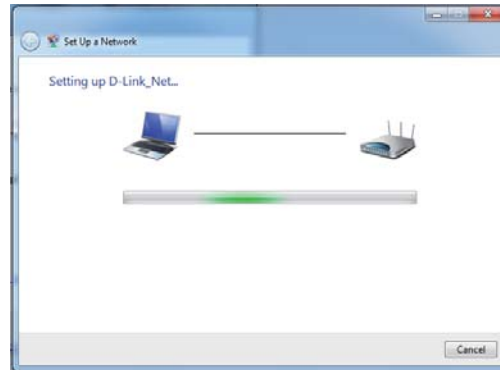
Click **Next** to continue.



Section 5 - Connecting to a Wireless Network

7. The following window will appear while the Router is being configured.

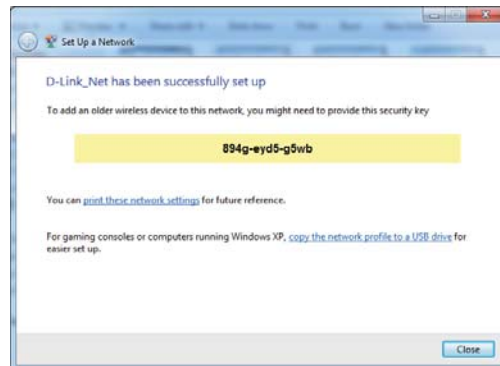
Wait for the configuration to complete.



8. After configuration is complete, a window will appear that your wireless network has been set up successfully.

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

Click **Close** to complete WPS setup.



Connecting to a Wireless Network Using Windows® 7

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

1. Click on the wireless icon in the system tray in the lower-right corner of your screen.



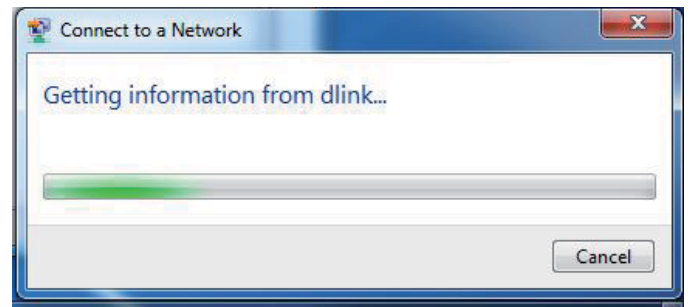
2. The utility will display any available wireless networks in your area.



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



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



Section 5 - Connecting to a Wireless Network

5. If your wireless network uses encryption such as WEP or WPA/WPA2, enter the encryption password/passphrase for your wireless network and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the key or passphrase is exactly the same as on the wireless router.



Connecting to a Wireless Network Using Windows Vista®

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

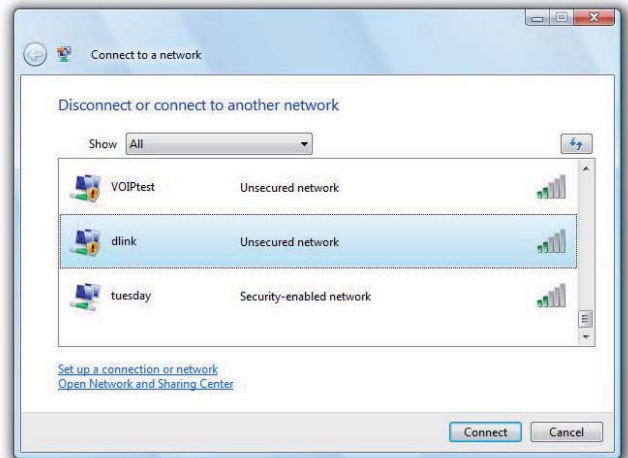
1. Open the Windows Vista® Wireless Utility by right-clicking on the wireless computer icon in the system tray in the lower right corner of the screen. Select **Connect to a network**.



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

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

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



Section 5 - Connecting to a Wireless Network

3. If your wireless network uses encryption such as WEP or WPA/WPA2, enter the encryption password/passphrase for your wireless network and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the key or passphrase is exactly the same as on the wireless router.



Connecting 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.

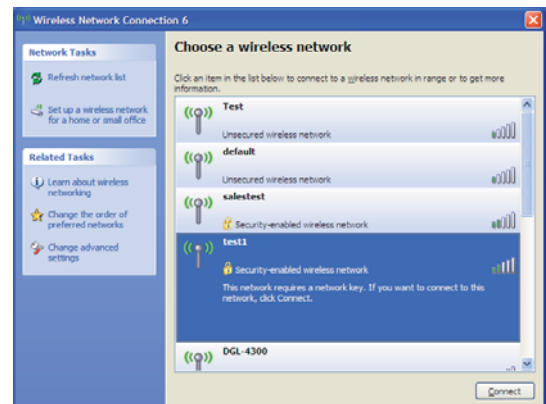
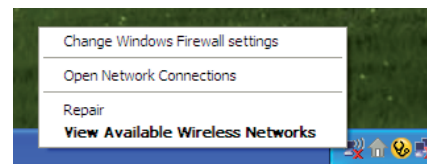
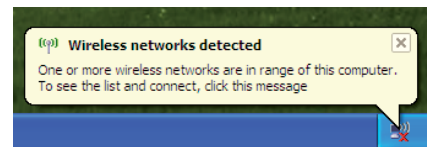
1. If you receive the **Wireless Networks Detected** bubble, click on the center of the bubble to access the utility.

or

Right-click on the wireless computer icon in the system tray in the lower-right corner of the screen. Select **View Available Wireless Networks**.

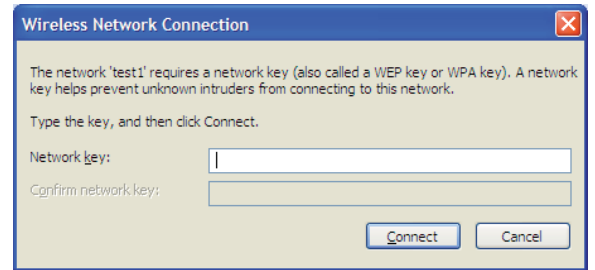
2. The utility will display any available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

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.



3. If your wireless network uses encryption such as WEP or WPA/WPA2, enter the encryption password/passphrase for your wireless network and click **Connect**.

It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the key or passphrase is exactly the same as on the wireless router.



Troubleshooting

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, XP and Vista® users type in **cmd**) and press **Enter** (or click **OK**).
- Once the window opens, you'll need to do a special ping. Use the following syntax:

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

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

```
C:\>ping yahoo.com -f -l 1482
Pinging yahoo.com [66.94.234.13] with 1482 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>ping yahoo.com -f -l 1472
Pinging yahoo.com [66.94.234.13] with 1472 bytes of data:
Reply from 66.94.234.13: bytes=1472 time=93ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=109ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=125ms TTL=52
Reply from 66.94.234.13: bytes=1472 time=203ms TTL=52
Ping statistics for 66.94.234.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 93ms, Maximum = 203ms, Average = 132ms
C:\>
```

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

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

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

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

Wireless Basics

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

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

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

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

What is Wireless?

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

Why D-Link Wireless?

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

How does wireless work?

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

Wireless Local Area Network (WLAN)

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

Wireless Personal Area Network (WPAN)

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

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

Who uses wireless?

Wireless technology 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.

Eliminate Interference

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

Security

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

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.
- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DIR-652 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.

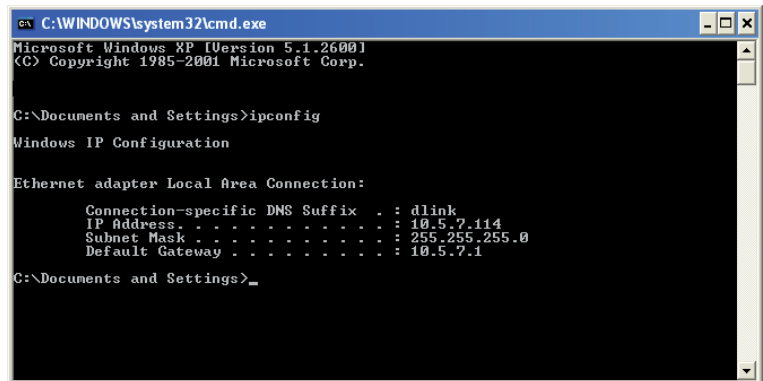
Click on **Start > Run**. In the run box type *cmd* and click **OK**. (Windows Vista® users type *cmd* in the **Start Search** box.)

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

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

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

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 Vista®: Click on **Start > Control Panel > Network and Internet > Network and Sharing Center > Manage Network Connections.**
Windows® XP: Click on **Start > Control Panel > Network Connections.**
Windows® 2000: From the desktop, right-click **My Network Places > Properties.**

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

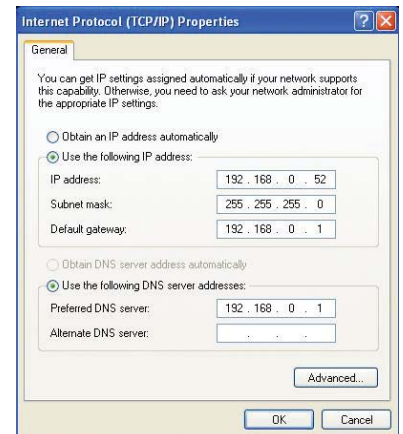
Step 3
Highlight **Internet Protocol (TCP/IP)** and click **Properties.**

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 802.11n
- IEEE 802.11g
- IEEE 802.3
- IEEE 802.3u

Security

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

Wireless Signal Rates*

IEEE 802.11n (HT20/40):

- 144.4Mbps (300)
- 117Mbps (243)
- 78Mbps (162)
- 58.5Mbps (121.5)
- 39Mbps (81)
- 19.5Mbps (40.5)
- 6.5Mbps (13.5)
- 130Mbps (270)
- 104Mbps (216)
- 66Mbps (135)
- 52Mbps (108)
- 26Mbps (54)
- 12Mbps (27)

IEEE 802.11g:

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

Frequency Range

- 2.4GHz to 2.483GHz

Transmitter Output Power (Average)

- 21.8 dBm

External Antenna Type

- Two (2) detachable reverse SMA Antennas

LEDs

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

Operating Temperature

- 32°F to 131°F (0°C to 55°C)

Humidity

- 95% maximum (non-condensing)

Safety & Emissions

- FCC
- CE

Dimensions

- L = 5.81 inches
- W = 4.6 inches
- H = 1.2 inches

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

Certifications

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 communication. 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 or more of the following measures:

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

FCC Caution:

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

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

IMPORTANT NOTICE:

FCC Radiation Exposure Statement:

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

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