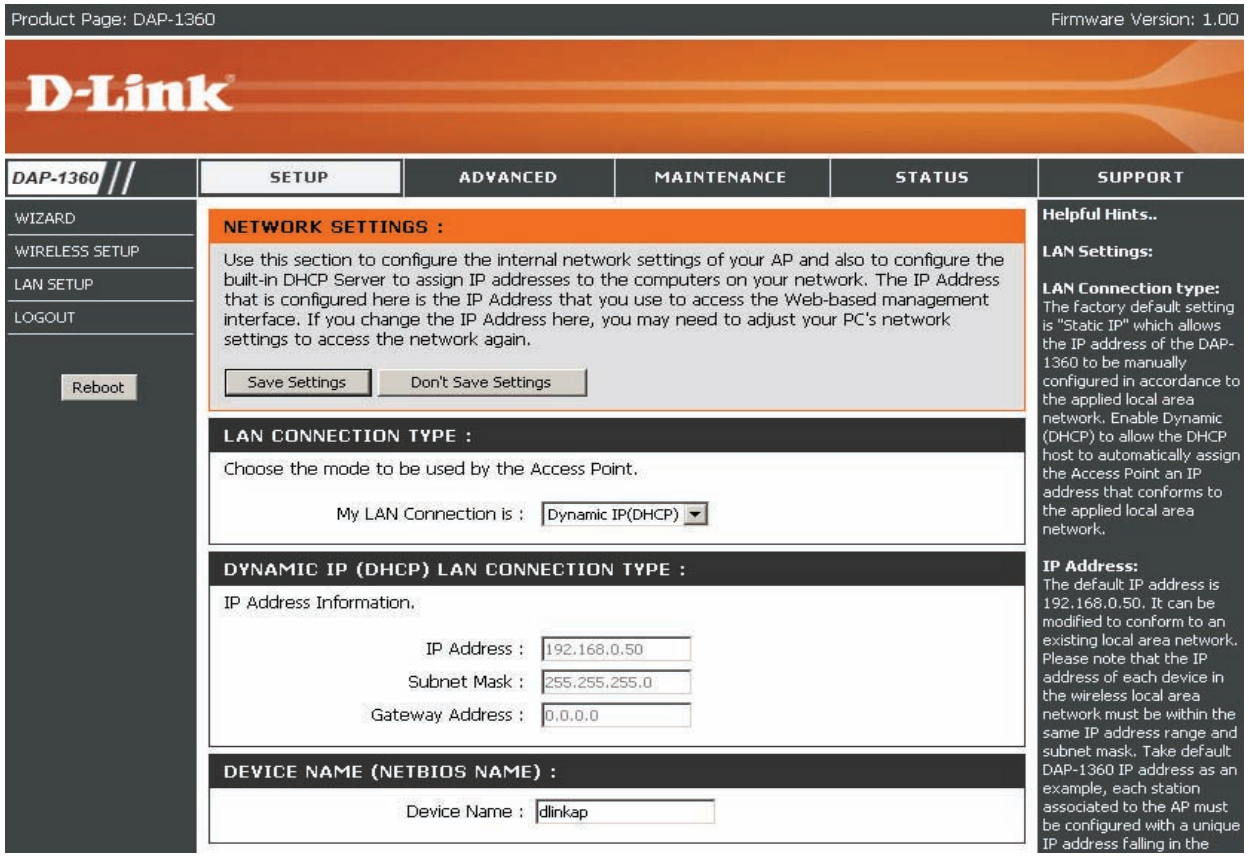
# LAN Setup

The LAN (Local Area Network) is your private, internal network. This page allows you to configure the IP settings of the LAN interface for the DAP-1360. The IP address can be changed to your current network IP range. This IP address cannot be seen from the Internet.



# LAN Settings

**My LAN Connection is:** The DAP-1360 is set to Dynamic IP by default. The IP address and subnet mask will fallback to 192.168.0.50 and 255.255.255.0, if don't get IP address from DHCP server exceed 30 seconds.

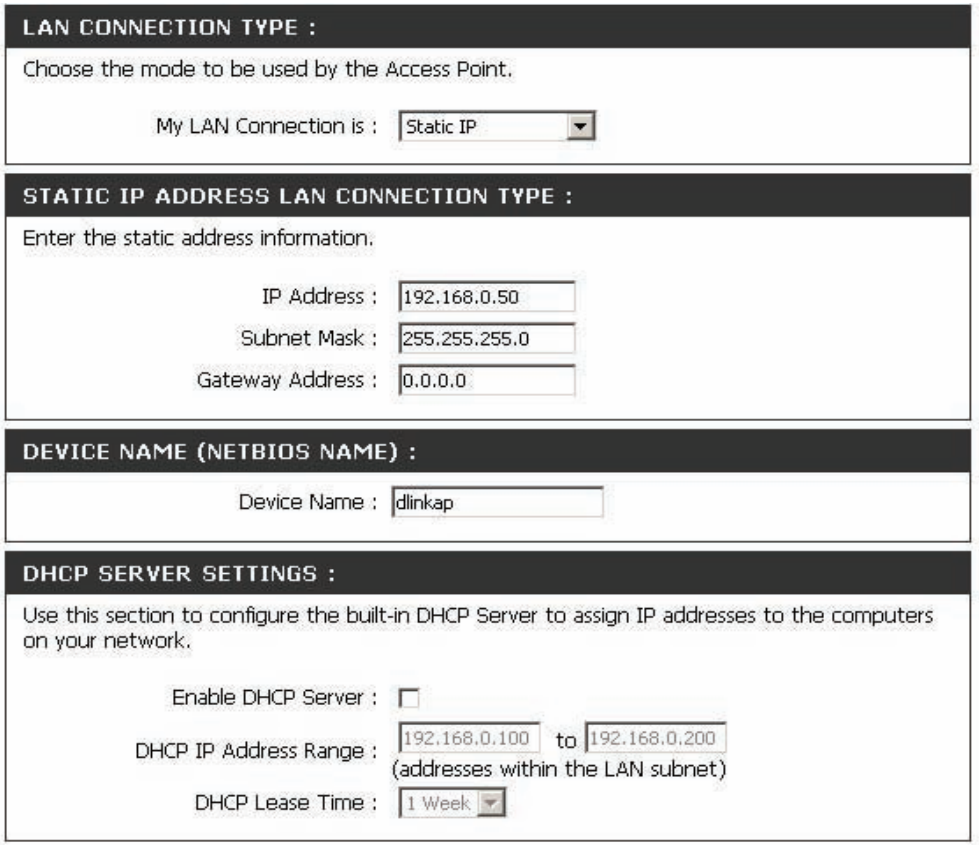
**Static IP:** Select this option if you are manually assigning an IP Address.

**Dynamic IP:** Select this option if you would like to have an IP Address automatically assigned to the DAP-1360 by a DHCP server in your network.

**IP Address:** Enter the IP address of the access point.

**Subnet Mask:** Enter the subnet mask of your access point.

**Gateway address:** Enter the IP Address of the router in your network.




**Device Name(NetBIOS Name):** It allows you to configure this device more easily when your network using TCP/IP protocol. You can enter the device name of the AP into your web browser to access the instead of ip address for configuration.

**Enable DHCP Server:** Select this to enable the DHCP server if static IP address is selected.

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

**Lease Time:** Enter the length of time for the IP address lease.

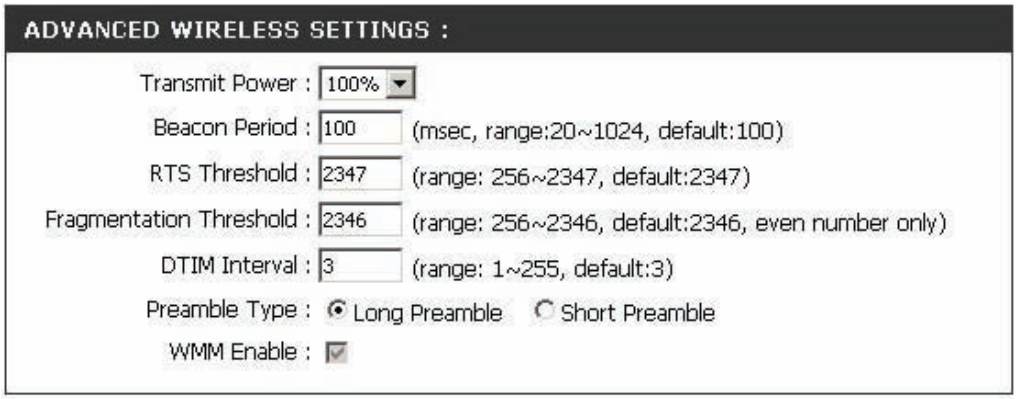
# Advanced Wireless

**TX Rates:** Select the transmission rate for the network.

**Transmit Power:** Choose **100%**, **50%**(-3dB), **25%** (-6dB), or **12.5%** (-9dB).

**Beacon Period:** Beacons are packets sent by an access point to synchronize a wireless network. Specify a beacon interval value. The default value 100 is recommended.

**RTS Threshold:** This value should remain at its default setting of 2,432. If you encounter inconsistent data flow, only minor modifications to the value range between 256 and 2,432 are recommended.




**Fragmentation:** This value should remain at its default setting of 2,346. If you experience a high packet error rate, you may slightly decrease your fragmentation threshold within the value range of 256 to 2,346. Setting the fragmentation threshold too low may result in poor performance.

**DTIM Interval (Beacon Rate):** A DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default vaule is 3 and the possible range of vaules is between 1 and 255.

**Preamble Type:** Select Short or Long Preamble. The default setting in Long Preamble. The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the access point and roaming wireless network adapters. **Note:** High network traffic areas should use the short preamble type.

**WMM:** WMM (Wi-Fi Multimedia) is only available in Access Point Mode. WMM provides basic QoS (Quality of Service) functions for wireless networks. WMM prioritizes traffic based on the 4 AC (Access Categories) of voice, video, best effort, and background. However, WMM does not provide guaranteed throughput.

# Access Control

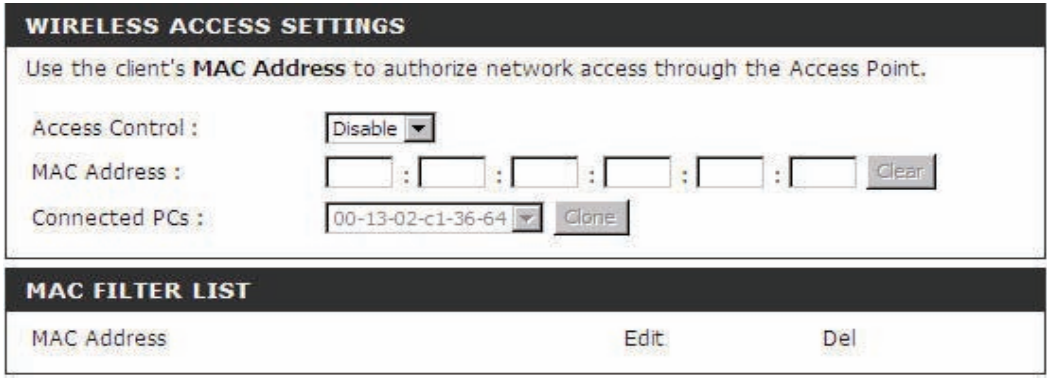
Use MAC Filters to allow or deny wireless clients, by their MAC addresses, from accessing the DAP-1360. You can manually add a MAC address or select the MAC address from the list of clients that are currently connected to the AP (Connected PCs). The default setting is Disable MAC Filters.

**Access Control:** Access control is set to **Disable** by default. Select **Reject** to deny access to the AP. Select **Accept** to allow access to the AP.

**MAC Address:** Enter the MAC address of the client that you want to allow or deny access to the AP.

**Connected PCs:** Select the MAC address of a computer from the drop-down menu and click **Clone** to fill in the MAC Address field with that computer.

**MAC Filter List:** This list will display the MAC addresses that are in the selected filter.



# User Limit

The D-Link DAP-1360 can set a limit upon the number of wireless clients. Using user limit, you can prevent scenarios where the DAP-1360 in your network shows performance degradation because it is handling heavy wireless traffic.

**Enable User Limit:** Click this to enable the User Limit options on this page.

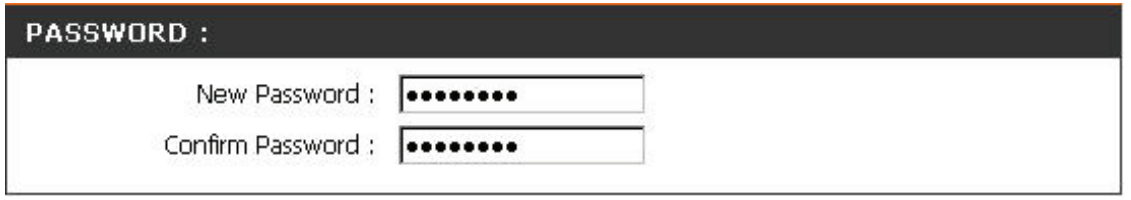
**User Limit (1 - 32):** Type the maximum number of wireless connections that can be made to the AP.

# Maintenance

## Device Administration

**New Password:** Enter a new password.

**Confirm Password:** Re-enter the password to confirm it.

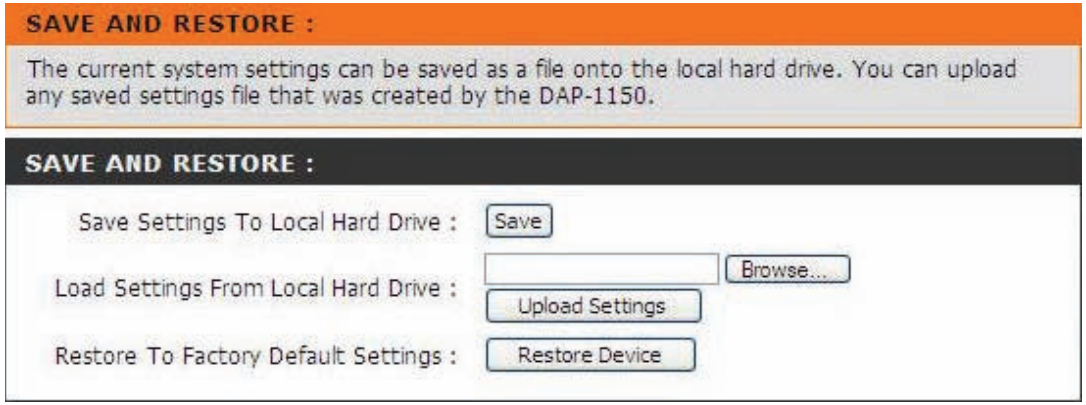



## Save and Restore

**Save Settings To Local Hard Drive:** Click **Save** to save the current system settings as a file onto your local hard drive.

**Load Settings From Local Hard Drive:** To load a system settings file, click on **Browse** to browse the local hard drive and locate the system settings file to be used. Click **Upload Settings** when you have selected the file to be loaded back onto the access point.

**Restore To Factory Default Settings:** You can reset the DAP-1360 back to the factory default settings by clicking on **Restore Device**. Make sure to save the current system settings before clicking on **Restore Device**. You will lose your current system settings after you click **Restore Device**.



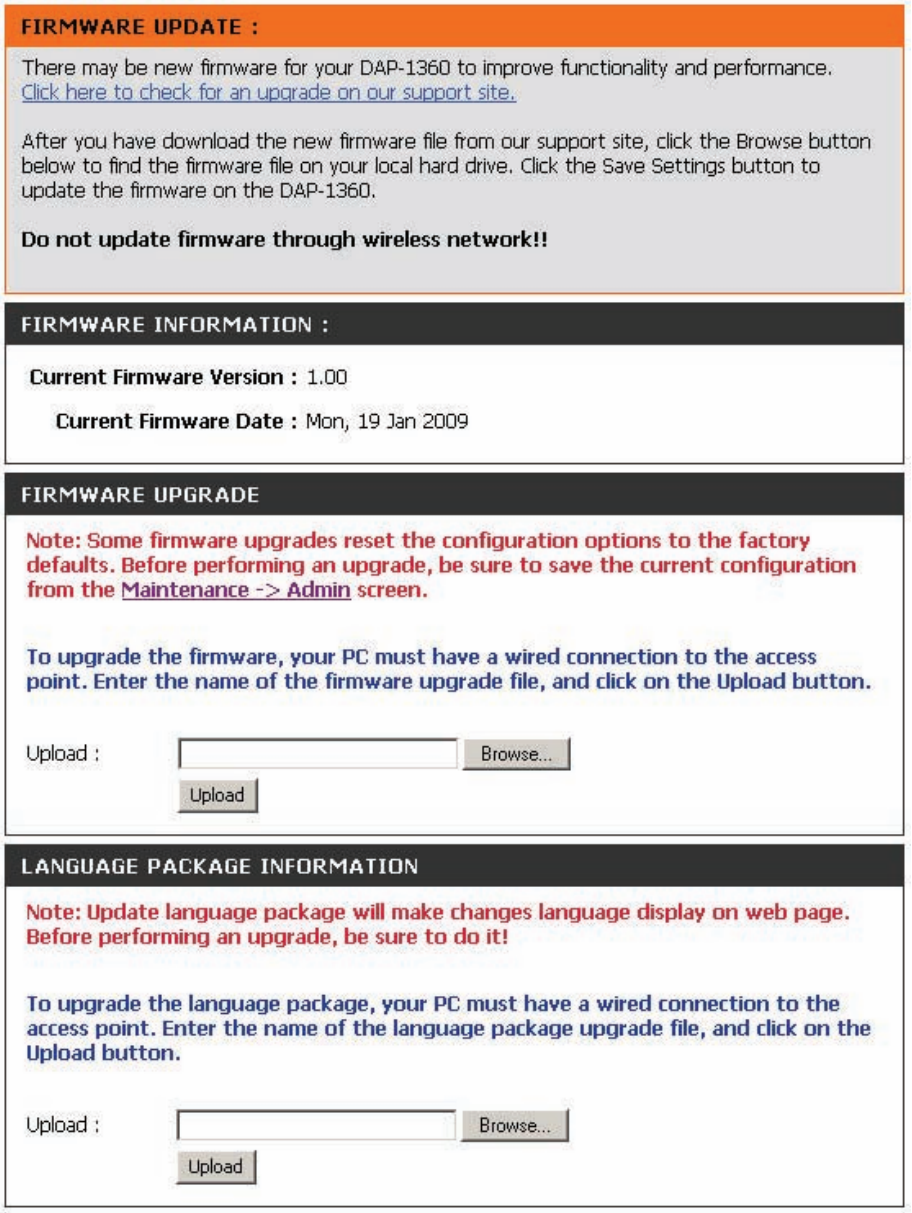
# Firmware

This feature is used to update the firmware of the DAP-1360. The current firmware version and firmware date are displayed here.

**Click here to check for an update on our support site:** Click this link and you will be connected to D-Link's support website where you can download the latest firmware version to your local hard drive.

**Current Firmware Info:** To update the firmware, click on **Browse** to browse the local hard drive and locate the updated firmware file. Click the **Upload** button after you have selected the updated firmware file.

**Language Package Information:** To change the web configurator language, click on **Browse** to browse locate the language package upgrade file and click the **Upload** button.



# Watchdog (Ping of Life)

The Watchdog feature pings a specified IP address. If the IP address stops responding to pings, your AP will be rebooted. You can also select an option to have the DAP-1360 send an e-mail alert if the specified IP address stops responding to pings.

**Enable Watchdog (Ping of Life):** Check this box to enable the Watchdog (Ping of Life) to check some host IP.

**Update Time Interval:** Enter the time interval of how often you would like the Watchdog to ping the response IP address.

**Watchdog Response IP:** Enter the IP address that the Watchdog will ping.

**Enable Mail Alert:** Check this box to enable e-mail notification for the Watchdog.

**SMTP Server:** Enter the SMTP server IP address.

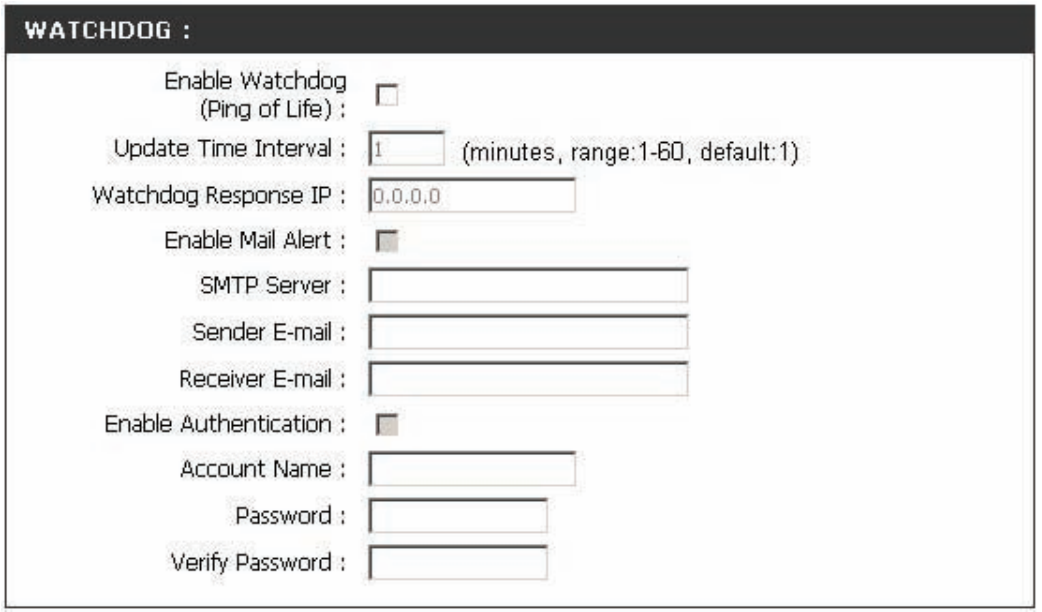
**Sender E-Mail:** Enter the e-mail address from which the notification will be sent.

**Receiver E-Mail:** Enter the e-mail address which the notification will be sent to.

**Enable Authentication:** Check the box to enable authentication that is used with the SMTP server.

**Account Name:** Enter your account name that is used with the SMTP server.

**Password:** Enter your password that is used with the SMTP server and re-enter it in the next box.



# Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.

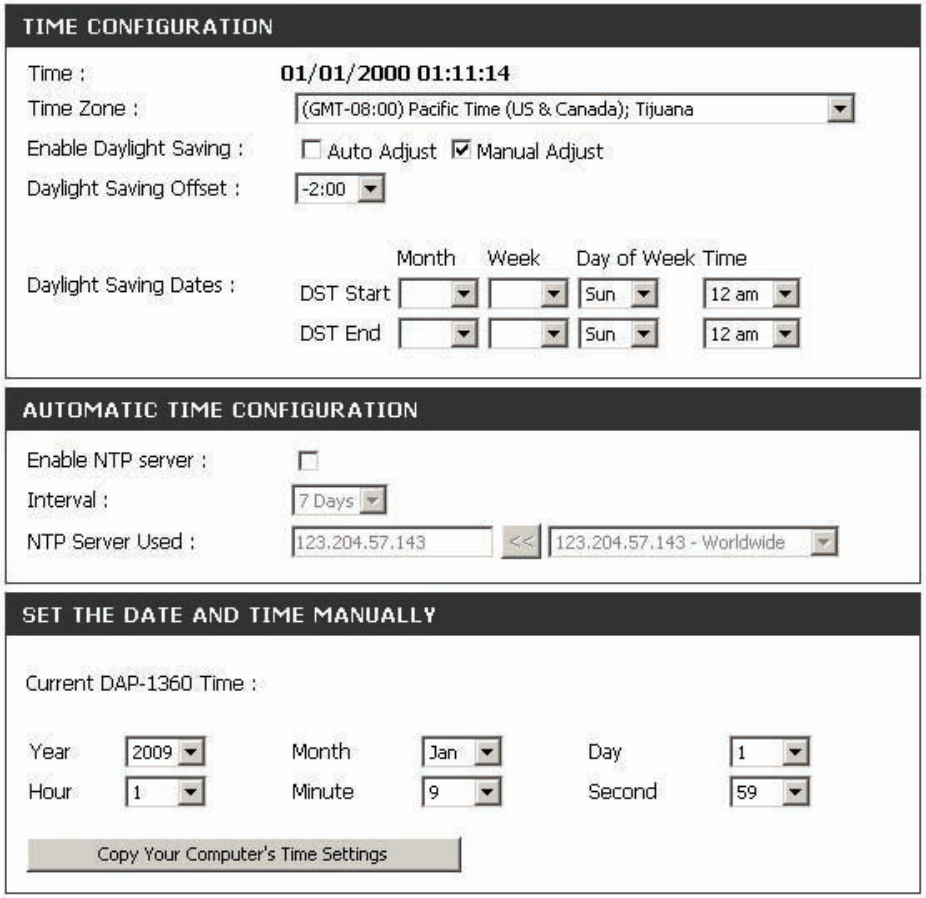
**Time Zone:** Select the Time Zone from the drop-down menu.

**Daylight Saving:** To select Daylight Saving time manually, select enabled or disabled, and enter a start date and an end date for daylight saving time.

**Enable NTP Server:** NTP is short for Network Time Protocol. NTP synchronizes computer clock times in a network of computers. Check this box to use a NTP server. This will only connect to a server on the Internet, not a local server.

**NTP Server Used:** Enter the NTP server or select one from the drop-down menu.

**Manual:** To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second and then click **Save Settings**. You can also click **Copy Your Computer's Time Settings**.



# Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm, you could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

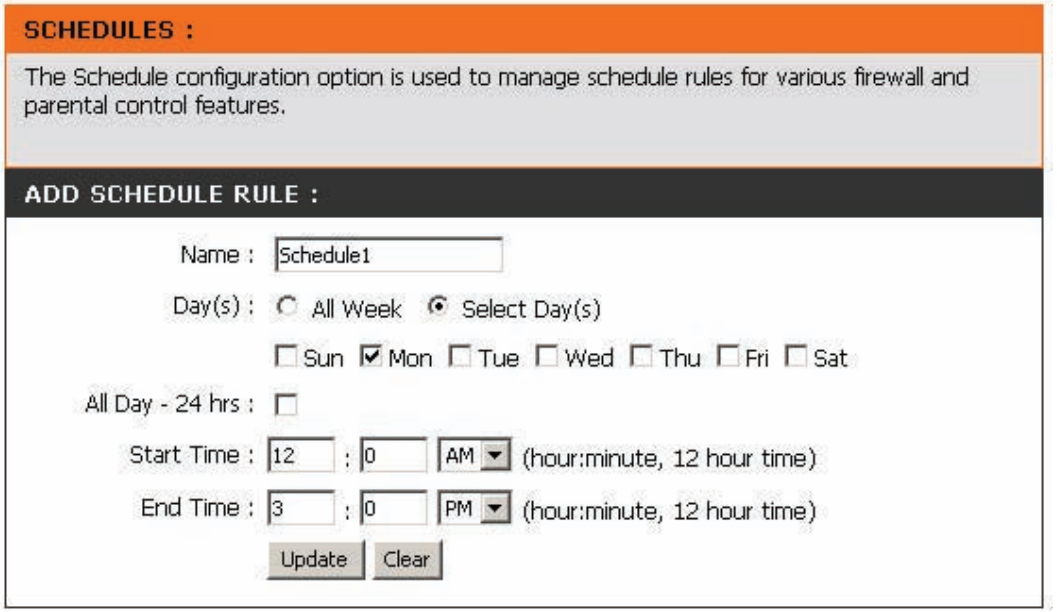
**Name:** Enter a name for your new schedule.

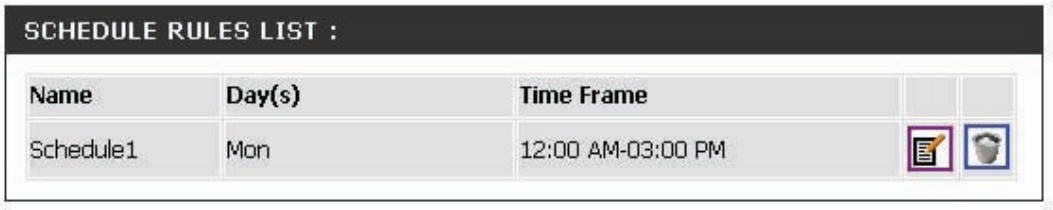
**Days:** Select a day, a range of days, or All Week to include every day.

**Time:** Check **All Day - 24hrs** or enter a start and end time for your schedule.

**Save:** Click **Save** to save your schedule. You must click **Save Settings** 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.

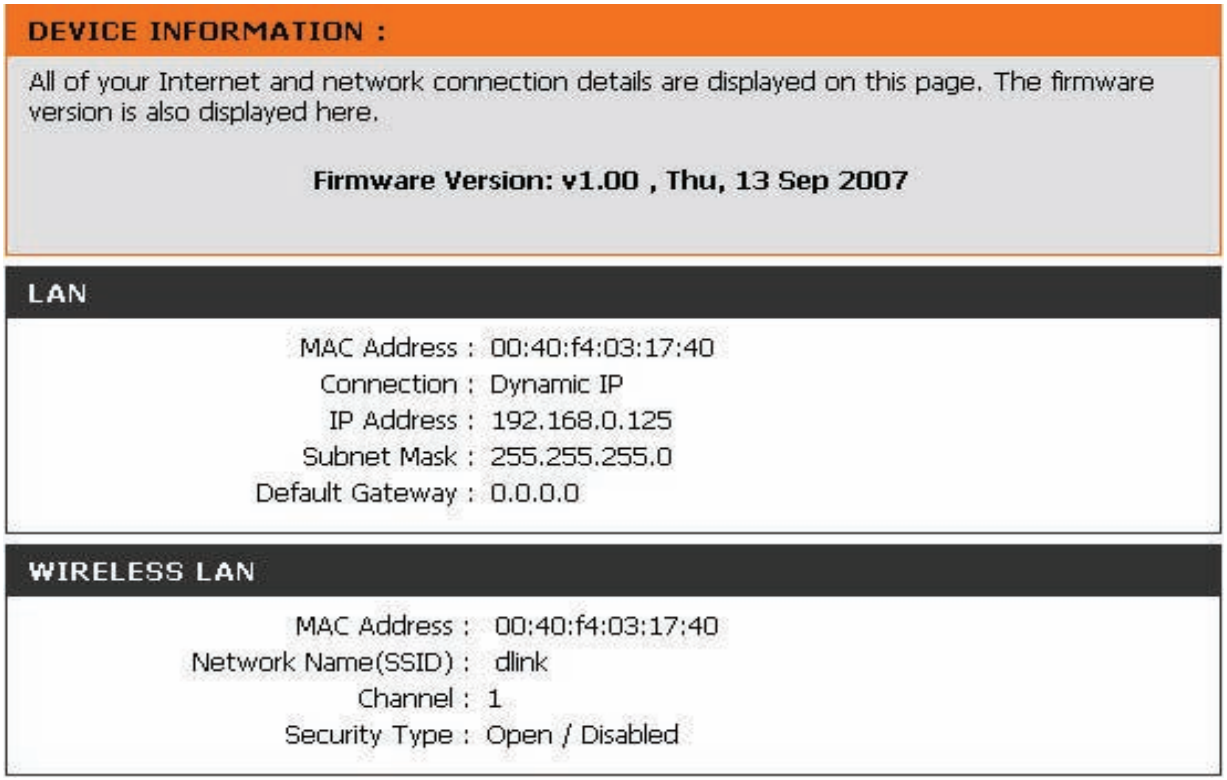


# Status

## Device Info

This screen displays the current firmware version and the current LAN, and Wireless LAN settings on your access point.



# Log

The DAP-1360 keeps a running log of events and activities occurring on the AP. If the AP is rebooted, the logs are automatically cleared. You can save the log files under Log Setting.

**First Page:** This button directs you to the first page of the log.

**Last Page:** This button directs you to the last page of the log.

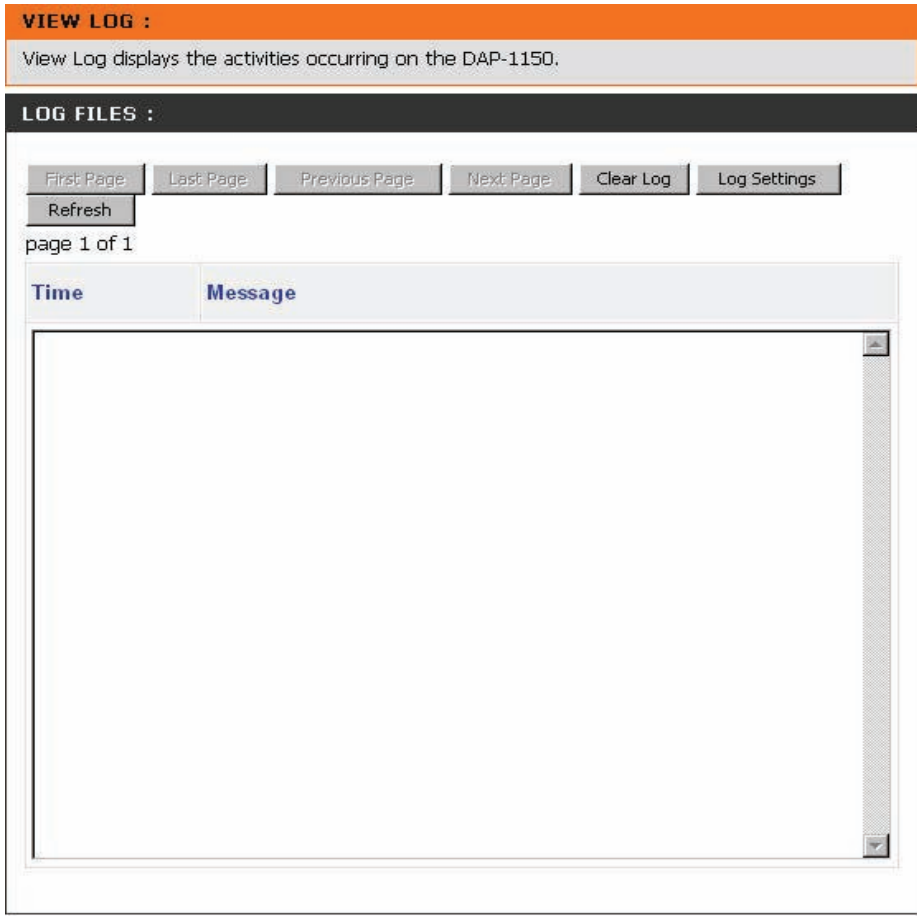
**Previous Page:** This button directs you to the previous page of the log.

**Next Page:** This button directs you to the next page of the log.

**Clear Log:** This button clears all current log content.

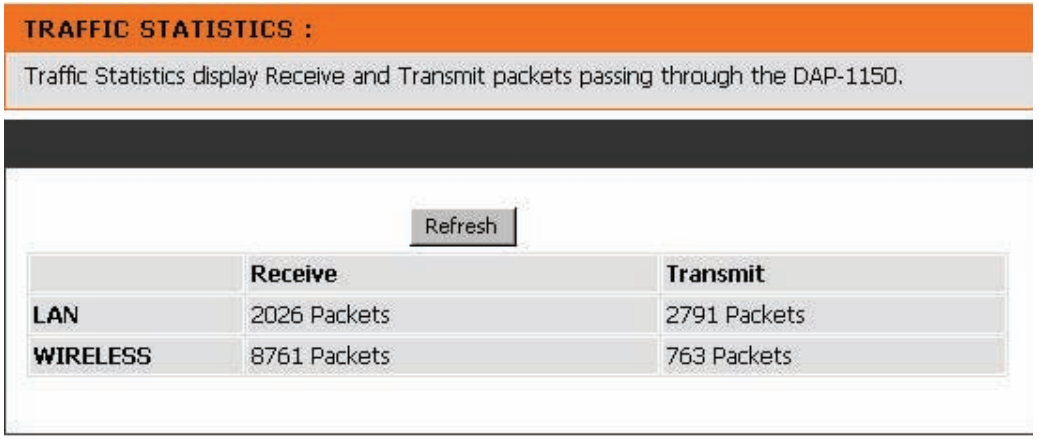
**Log Settings:** This button opens a new menu where you can configure the log settings.

**Refresh:** This button refreshes the log.



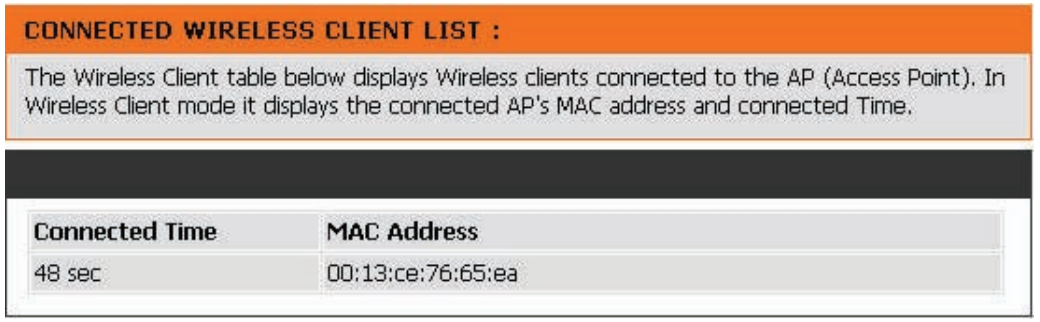
# Statistics

The DAP-1360 keeps statistics of the traffic that passes through it. You can view the amount of packets that pass through the LAN and wireless portions of the network. The traffic counter will reset if the access point is rebooted.



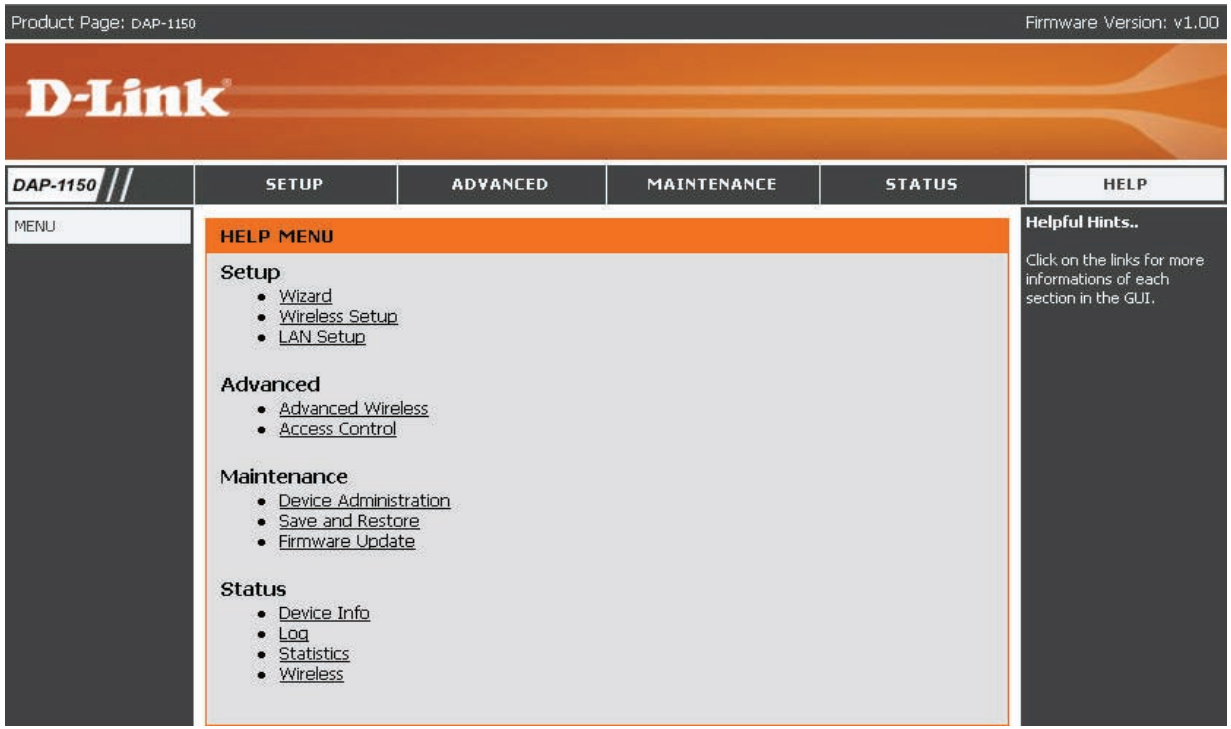

# Wireless

This list displays the MAC addresses of connected wireless clients and the length of time that they have been connected.



# Help

The Help menu contains an index of links to help topics for each feature of the DAP-1360.



# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-1360 offers the following types of security:

- WPA-Personal (Pre-Shared Key)
- WPA2-Personal (Pre-Shared Key 2)
- WPA2-Auto-Personal
- WEP (Wired Equivalent Privacy)
- WPA-Enterprise (Extensible Authentication Protocol)
- WPA2-Enterprise (Extensible Authentication Protocol 2)
- WPA2-Auto-Enterprise (Extensible Authentication Protocol 2 Auto)

# 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 access point 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 utility by opening a web browser and entering the device name of the access point (dlinkap). Click on **Wireless Setup** on the left side.

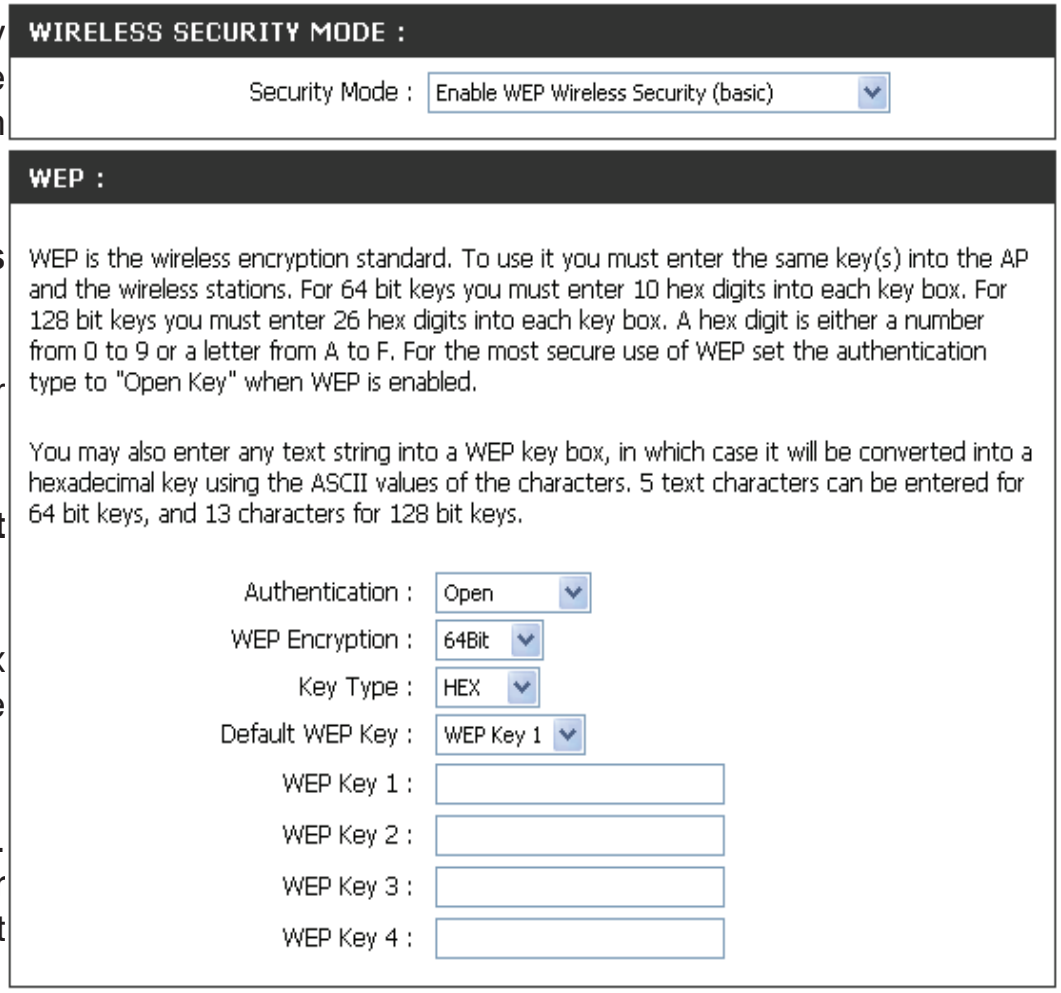
2. Next to Security Mode, select **Enable WEP Wireless Security (Basic)**.

3. Next to Authentication, select **Shared Key** or **Open**.

4. Next to WEP Encryption, select **64-bit** or **128-bit** encryption.

5. Next to Key Type, select either **Hex** or **ASCII**.Hex (recommended) - Letters A-F and numbers 0-9 are valid. ASCII - All numbers and letters are valid.

6. Next to Key 1, enter a WEP key that you create. Make sure you enter this key exactly on all your wireless devices. You may enter up to 4 different keys.




7. Click **Save Settings** to save your settings. If you are configuring the access point 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 access point.

# 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).

There are 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.

- User authentication, which is generally missing in WEP, is done 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.

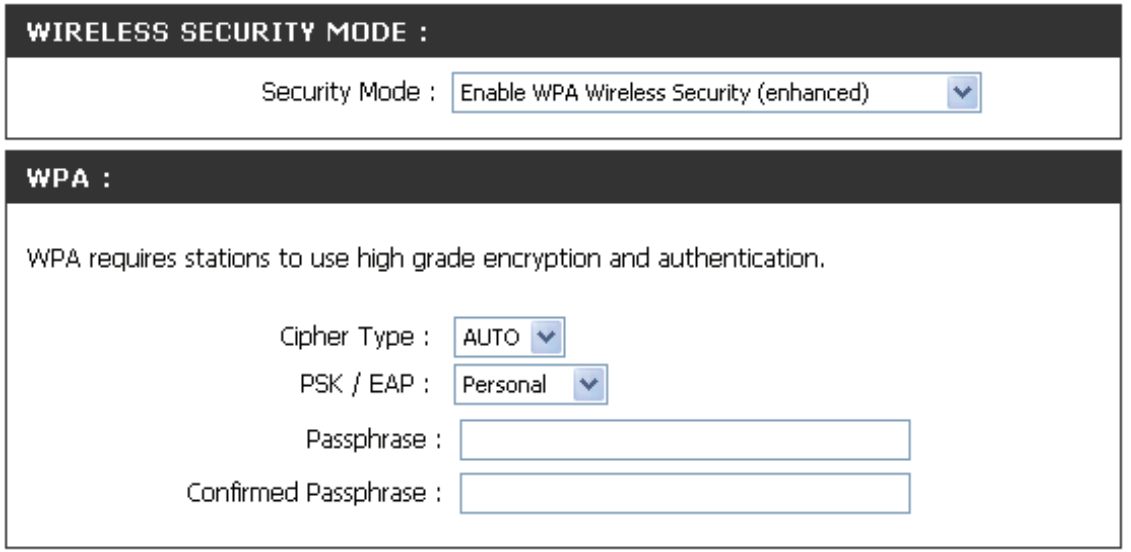
WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

WPA-EAP/WPA2-EAP 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.

WPA2-Auto-PSK/WPA2-Auto-EAP accepts wireless clients that use WPA or WPA2. Authentication is sill necessary.

# Configure WPA-PSK, WPA2-PSK, and WPA2-Auto-PSK (Personal)

It is recommended to enable encryption on your wireless access point 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 utility by opening a web browser and entering the device name of the access point (dlinkap). Click on **Wireless Setup** on the left side.

2. Next to Security Mode, select **Enable WPA Wireless Security**, **Enable WPA2 Wireless Security**, or **Enable WPA2-Auto Wireless Security**.

3. Next to Cipher Mode, select **TKIP, AES,** or **Auto**.

4. Next to PSK / EAP, select **Personal**.

5. Next to Passphrase, 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. Enter the passphrase again next to Confirmed Passphrase.

7. Click **Save Settings** to save your settings. If you are configuring the access point with a wireless adapter, you will lose connectivity until you enable WPA-Personal, WPA2-Personal, or WPA2-Auto-Personal on your adapter and enter the same passphrase as you did on the access point.

# Configure WPA-EAP, WPA2-EAP, and WPA2-Auto-EAP (Enterprise)

It is recommended to enable encryption on your wireless access point 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 utility by opening a web browser and entering the device name of the access point (dlinkap). Click on **Wireless Setup** on the left side.

2. Next to Security Mode, select **Enable WPA Wireless Security**, **Enable WPA2 Wireless Security**, or **Enable WPA2-Auto Wireless Security**.

3. Next to Cipher Mode, select **TKIP, AES,** or **Auto**.

4. Next to Personal / Enterprise, select **Enterprise**.

5. Next to RADIUS Server 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.

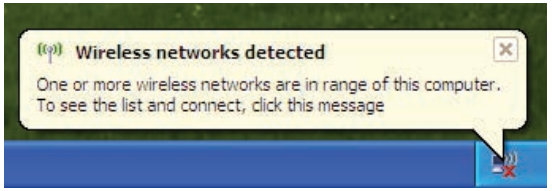
7. Next to Shared Secret, enter the security key.

8. Click **Save Settings** to save your settings.

# Connect to a Wireless Network Using Windows® XP

Windows® XP users can use the built-in wireless utility (Zero Configuration Utility) to connect to a wireless network. 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 shown below.

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

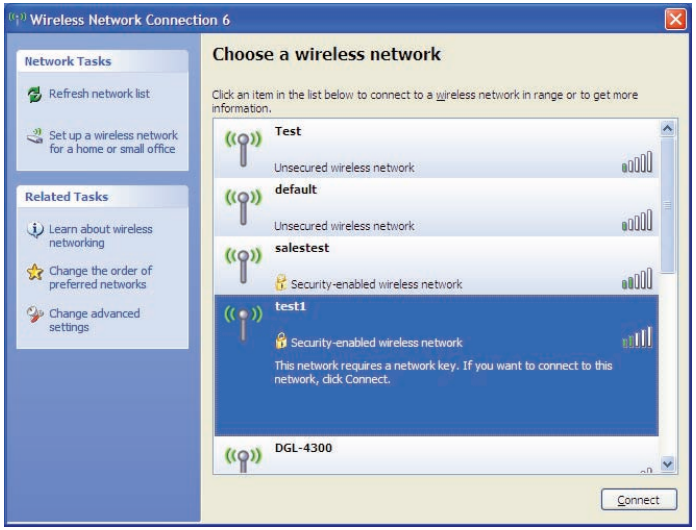



or

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 all available wireless networks in your area. Click on a network (displayed using the SSID) and click the **Connect** button.

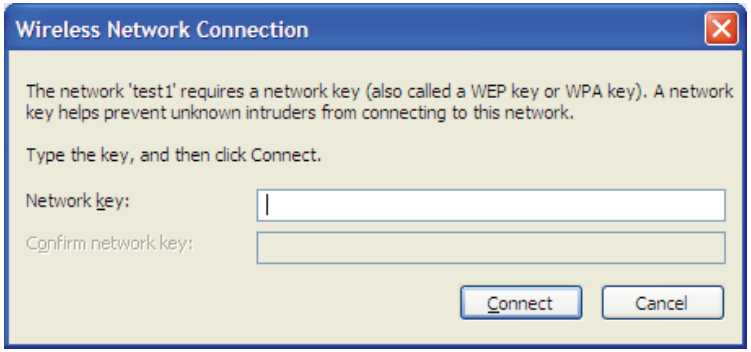
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



# Configure WEP/WPA-PSK

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

Follow the steps on the previous page to connect to a wireless network using Windows® XP. After you highlight a network and click **Connect**, the **Wireless Network Connection** box will appear if the network requires authentication. Enter the same WEP or WPA-PSK key that is on your access point and click **Connect**.

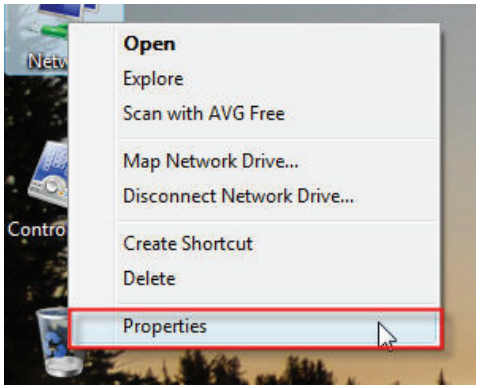



It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP or WPA-PSK settings are correct. The WEP or WPA-PSK key must be exactly the same as on the wireless access point.

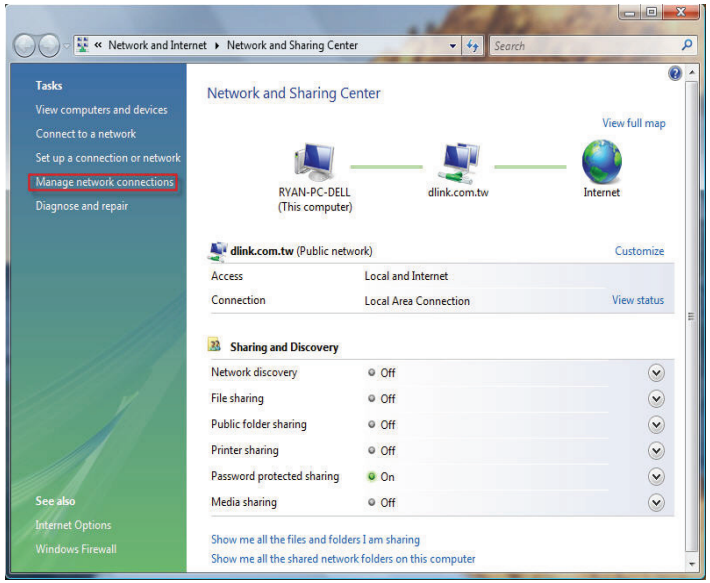
# Using Windows® Vista (Secured Network)

The following are step-by-step directions to connect to a secured wireless network using Windows® Vista.

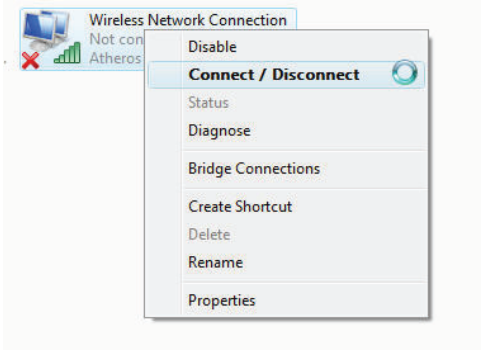
1. Right-click on **Network** and click on **Properties**.



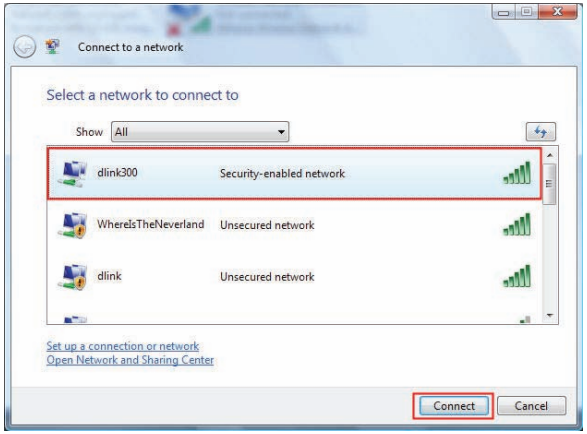

**2.** Click the **Manage network connections** link in the **Network and Sharing Center** window.



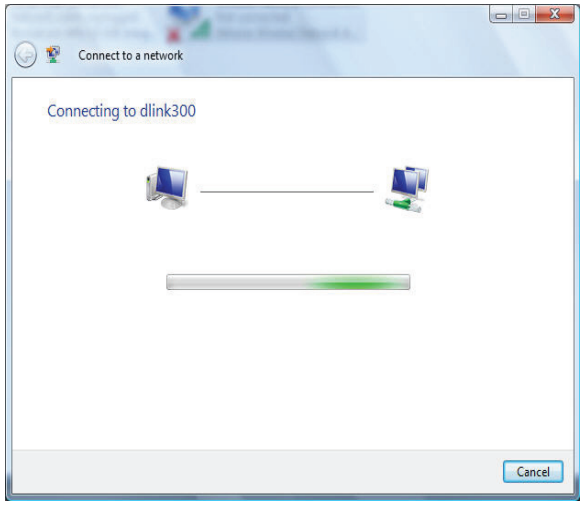
**3.** Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



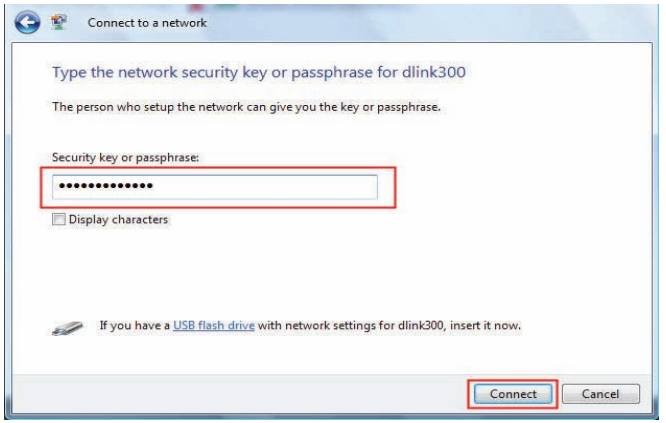

**4.** Select a network to connect to in the **Select a network to connect to** window and then click the **Connect** button.



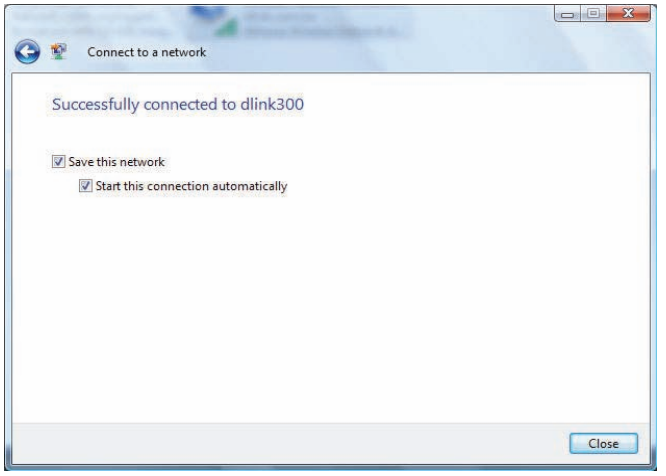

**5.** The following window displays connection progress.



**6.** Enter the network security key or passphrase for the AP in the textbox provided in the **Type the network security key or passphrase for [SSID name]** window. When you are finished, click the **Connect** button.



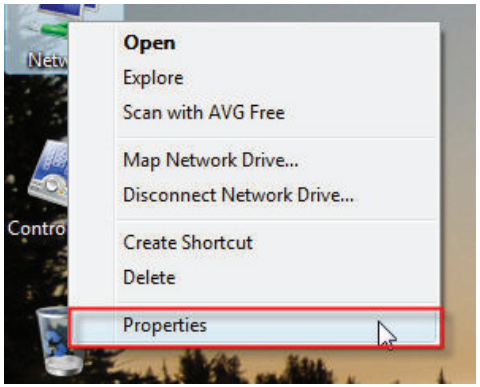

**7.** The following **Successfully connected to [SSID name]** window is displayed. Choose to save this network and/or start this new connection automatically. When you are finished, click the **Close** button.



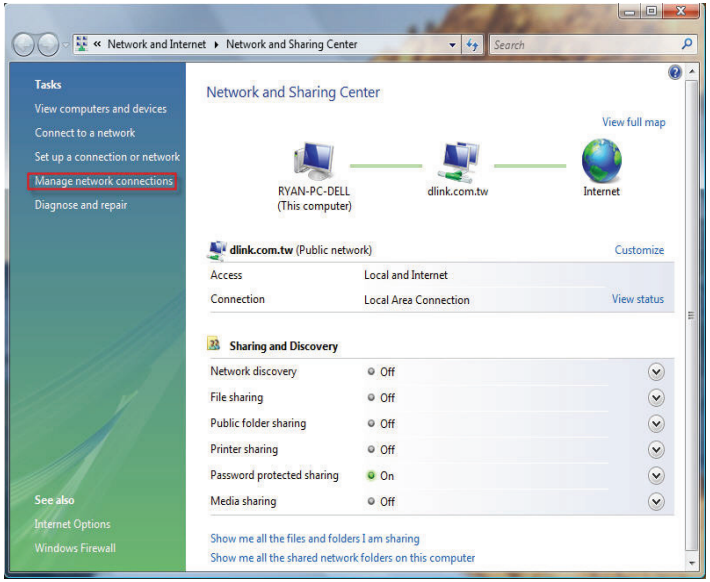
# Using Windows® Vista (Unsecured Network)

The following are step-by-step directions to set up a wireless connection on an unsecured network using Windows® Vista.

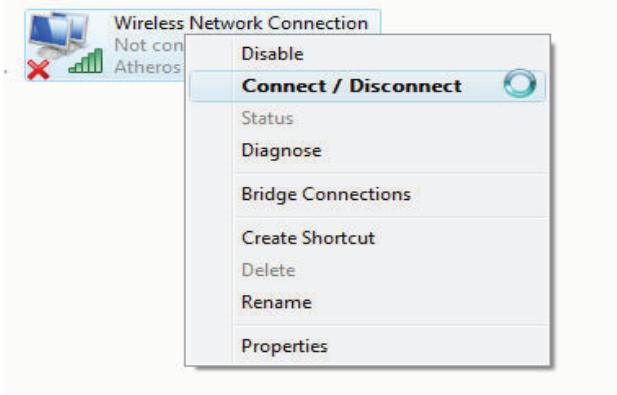
1. Right-click on **Network** and click on **Properties**.



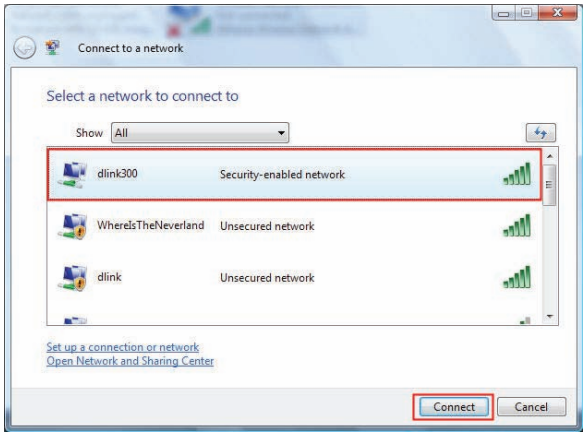

**2.** Go to the **Network and Sharing Center** window and click the **Manage Network Connections** link.



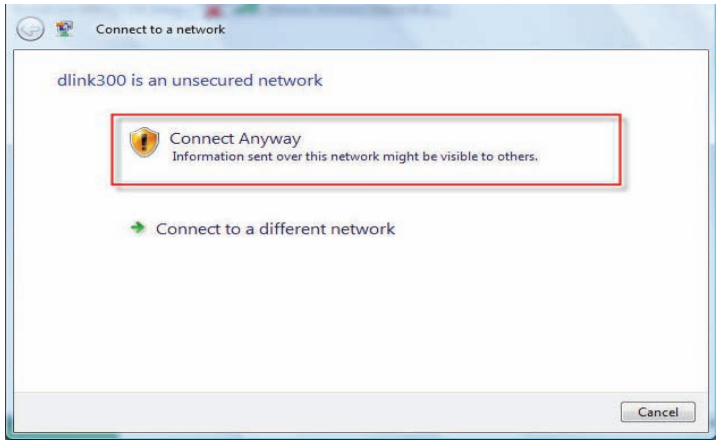
**3.** Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



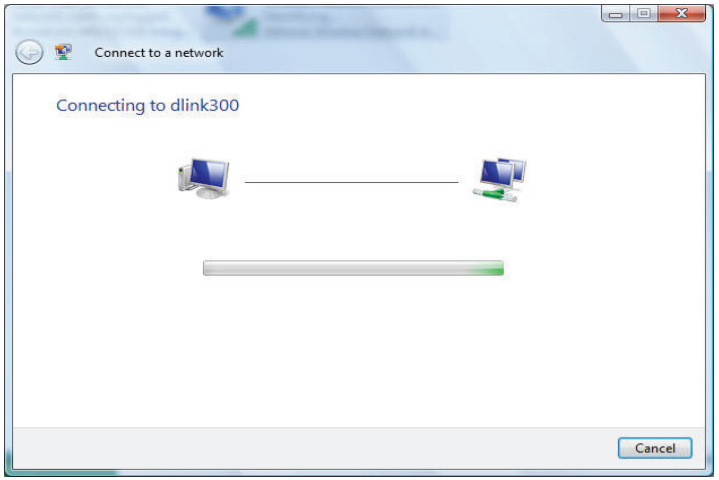

**4.** Select a network to connect to in the **Select a network to connect to** window and then click the **Connect** button.



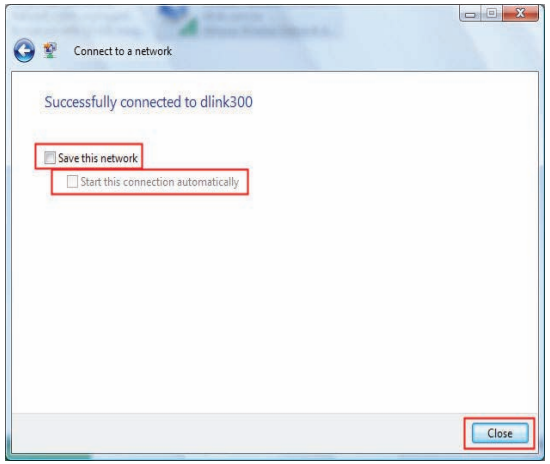

**5.** Confirm that you still want to connect on the following **Network Connection Status** window by clicking on **Connect Anyway**.



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




**7.** The following **Successfully connected to [SSID name]** window is displayed. Choose to save this network and/or start this new connection automatically. When you are finished, click the **Close** button.



# Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the DAP-1360. Read the following descriptions if you are having problems. The examples below use Windows® XP. If you have a different operating system, the troubleshooting steps may be different from the following examples.

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

When entering the IP address of the D-Link access point (for example, dlinkap), 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
    - 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-based configuration utility. Open your web browser and enter the IP address of your D-Link access point in the address bar. This should open the login page for your the web-based configuration utility.

- If you still cannot access the web-based configuration utility, unplug the power to the access point for 10 seconds and plug back in. Wait about 30 seconds and try accessing the web-based configuration utility. 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 access point. Unfortunately this process will change all your settings back to the factory defaults.

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

# Wireless Basics

D-Link wireless products are based on the latest industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business, or public wireless networks. Strictly adhering to IEEE standards, the D-Link wireless family of products allows 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 waves 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 a worldwide leader and an 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 a cordless phone works- using radio signals to transmit data from one point to another. However, 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: a Wireless Local Area Network (WLAN) and a Wireless Personal Area Network (WPAN).

### Wireless Local Area Network (WLAN)

In a WLAN, 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 AP, the signal can travel up to 300 feet. With an outdoor AP 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 WPANs. Bluetooth devices in WPANs operate in a range up to 30 feet away.

The speed and wireless operation range of a WPAN is less than of a WLAN, but it excels in its efficient consumption of power. WPANs are 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, at home and in the office.

**Home**

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

**Small Office and Home Office (SOHO)**

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

## Where is wireless used?

Wireless technology is quickly expanding beyond home and office use. The freedom of mobility it offers is becoming so popular that more and more public facilities are now providing wireless access to attract people. Public places that offer wireless access is usually called a “hotspot”.

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.

A wireless network is relatively 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 Access Point

Make sure you place the router/access point in a central 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 and 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 will significantly reduce any interference that the appliances might cause if operating on the same frequency.

### Security

Don't let your next-door neighbors or unwanted intruders connect to your wireless network. Secure your wireless network by turning on the WEP or WPA security feature on the access point. Refer to the section "Wireless Security" in this manual for detailed 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.

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

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.

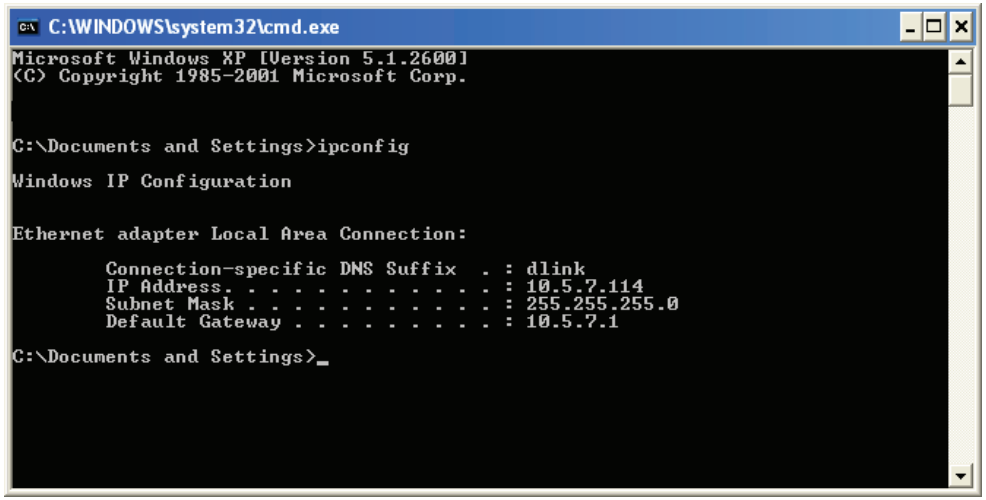
# Networking Basics

## Check your IP address

After you install your network 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 in a hotel, coffee shop, airport, or another public place, please contact an employee or administrator to verify their wireless network settings.

# Statically Assign an IP address

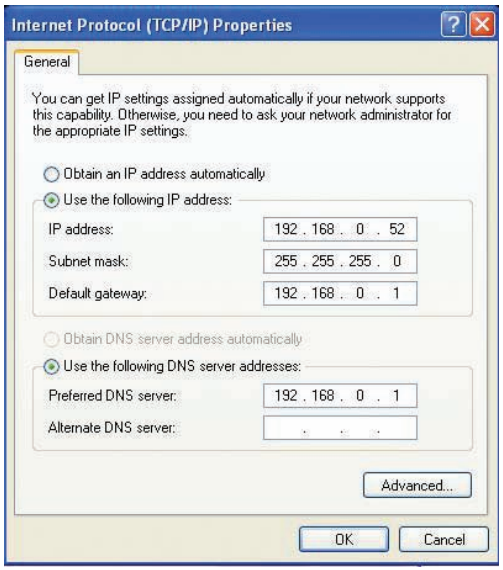
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

**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 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.

# FCC statement

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.

**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 NOTE:**

**FCC Radiation Exposure Statement:**

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

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

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

IC statement

**Industry Canada statement:**

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

**IMPORTANT NOTE:**
**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.

This device has been designed to operate with an antenna having a maximum gain of 5 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

**CE statement**
Europe – EU Declaration of Conformity
This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN60950-1: 2006
Safety of Information Technology Equipment

EN 50385: 2002
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1 (2006-10)

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 489-1 V1.8.1 (2008-04)
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

EN 301 489-17 V1.3.2 (2008-04)
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems , 5 GHz high performance RLAN equipment and 5,8GHz Broadband Data Transmitting Systems.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

| | |
|---|---|
| cs Česky [Czech] | *[Jméno výrobce]* tímto prohlašuje, že tento *[typ zařízení]* je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES. |
| da Dansk [Danish] | Undertegnede *[fabrikantens navn]* erklærer herved, at følgende udstyr *[udstyrets typebetegnelse]* overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF. |
| de Deutsch [German] | Hiermit erklärt *[Name des Herstellers]*, dass sich das Gerät *[Gerätetyp]* in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet. |
| et Eesti [Estonian] | Käesolevaga kinnitab *[tootja nimi = name of manufacturer]* seadme *[seadme tüüp = type of equipment]* vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. |
| en English | Hereby, *[name of manufacturer]*, declares that this *[type of equipment]* is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC. |
| es Español [Spanish] | Por medio de la presente *[nombre del fabricante]* declara que el *[clase de equipo]* cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE. |
| el Ελληνική [Greek] | ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *[name of manufacturer]* ΔΗΛΩΝΕΙ ΟΤΙ *[type of equipment]* ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ. |
| fr Français [French] | Par la présente *[nom du fabricant]* déclare que l'appareil *[type d'appareil]* est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. |
| it Italiano [Italian] | Con la presente *[nome del costruttore]* dichiara che questo *[tipo di apparecchio]* è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE. |
| lv Latviski [Latvian] | Ar šo *[name of manufacturer / izgatavotāja nosaukums]* deklarē, ka *[type of equipment / iekārtas tips]* atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. |
| lt Lietuvių [Lithuanian] | Šiuo *[manufacturer name]* deklaruoja, kad šis *[equipment type]* atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas. |
| nl Nederlands [Dutch] | Hierbij verklaart *[naam van de fabrikant]* dat het toestel *[type van toestel]* in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. |
| mt Malti [Maltese] | Hawnhekk, *[isem tal-manifattur]*, jiddikjara li dan *[il-mudel tal-prodott]* jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC. |
| hu Magyar [Hungarian] | Alulírott, *[gyártó neve]* nyilatkozom, hogy a *[... típus]* megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak. |
| pl Polski [Polish] | Niniejszym *[nazwa producenta]* oświadcza, że *[nazwa wyrobu]* jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC. |
| pt Português [Portuguese] | *[Nome do fabricante]* declara que este *[tipo de equipamento]* está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE. |
| sl Slovensko [Slovenian] | *[Ime proizvajalca]* izjavlja, da je ta *[tip opreme]* v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES. |
| sk Slovensky [Slovak] | *[Meno výrobcu]* týmto vyhlasuje, že *[typ zariadenia]* spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES. |
| fi Suomi [Finnish] | *[Valmistaja = manufacturer]* vakuuttaa täten että *[type of equipment = laitteen tyyppimerkintä]* tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. |
| sv Svenska [Swedish] | Härmed intygar *[företag]* att denna *[utrustningstyp]* står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG. |

# Technical Specifications

**NETWORK STANDARDS**
- 802.11n wireless LAN
- 802.11g wireless LAN
- 802.11b wireless LAN
- 802.3/802.3u 10BASE-T/100BASE-TX Ethernet
- ANSI/IEEE 802.3 NWay auto-negotiation

**DEVICE INTERFACES**
- 802.11n wireless LAN
- One 10/100BASE-TX Ethernet LAN port

**OPERATING FREQUENCY**
2.4 to 2.4835 GHz

**OPERATING CHANNELS**
- FCC: 11
- ETSI: 13

**RADIO & MODULATION SCHEMES**
DQPSK, DBPSK, CCK, OFDM

**OPERATION MODES**
- Access Point
- Repeater
- Wireless Client
- Bridge
- Bridge with AP
- WISP Client Router
- WISP Repeater

**ANTENNA**
Two 5dBi Gain detachable omni-directional antennas with RP-SMA connector

**SECURITY**
- 64/128-bit WEP data encryption
- WPA-PSK, WPA2-PSK
- WPA-EAP, WPA2-EAP
- TKIP, AES
- MAC address filtering
- SSID broadcast disable function

**QUALITY OF SERVICE (QoS)**
Wi-Fi Multimedia (WMM)

**DEVICE MANAGEMENT**
- Web-based management through Internet Explorer v.6 or later, Netscape Navigator v.6 or later or other Java-enabled browser

**Diagnostic LED**
- Power
- WLAN
- LAN

**POWER INPUT**
5VDC 2.5A
External power adapter

**DIMENSIONS**
144 (W) x 109 (D) x 30 (H) mm (5.67 x 4.29 x 1.18 inches)

**WEIGHT**
220grams (0.5lb)

**OPERATING TEMPERATURE**
0 to 55 C (32 to 131 F)

**STORAGE TEMPERATURE**
-10 to 70 C (14 to 158 F)

**OPERATING HUMIDITY**
10% to 90% non-condensing

**STORAGE HUMIDITY**
5% to 95% non-condensing

Maximum wireless signal rate based on IEEE Standard 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.

D-Link®

Building Networks for People

Version 1.00

2009/01/22