# USER MANUAL

## DAP-1160

VERSION 1.30

D-Link®

WIRELESS

# Table of Contents

**Product Overview ..... 4**
Package Contents ..... 4
System Requirements ..... 4
Introduction ..... 5
Features ..... 6
Hardware Overview ..... 7
Connections ..... 7
LEDs ..... 8

**Configuration ..... 9**
Web-based Configuration Utility ..... 9
Setup Wizard ..... 10
Wireless Setup ..... 11
Access Point ..... 12
AP Client ..... 13
Bridge ..... 14
Bridge with AP ..... 15
Repeater ..... 16
WISP Client Router ..... 17
WISP Repeater ..... 17
WAN Settings ..... 18
Dynamic IP (DHCP) ..... 18
Static IP ..... 19
PPPoE ..... 20
PPTP ..... 21
LAN Setup ..... 22
LAN Settings ..... 23
Advanced ..... 25
Port Forwarding ..... 25
Port Filter ..... 26
Access Control ..... 27
DMZ ..... 28
Parental Control ..... 29
Advanced Wireless ..... 30
Advanced Network ..... 31
Traffic Management Settings ..... 32
Maintenance ..... 33
Device Administration ..... 33
Save and Restore ..... 33
Firmware Update ..... 34
Watchdog (Ping of Life) ..... 35
Status ..... 36
Device Info ..... 36
Log ..... 37
Stats ..... 38
Wireless ..... 38
Help ..... 39

**Wireless Security ..... 40**
What is WEP? ..... 40
Configure WEP ..... 41
What is WPA? ..... 42
Configure WPA-PSK (Personal) ..... 43

Configure WPA-EAP (Enterprise) ..... 44

**Connect to a Wireless Network ..... 45**
Using Windows® XP ..... 45
Configure WEP/WPA-PSK ..... 46
Using Windows® Vista (Secured Network) ..... 47
Using Windows® Vista (Unsecured Network) ..... 50

**Troubleshooting ..... 53**

**Wireless Modes ..... 55**
Access Point Mode ..... 55
AP Client Mode ..... 56
Bridge Mode ..... 57
Bridge with AP Mode ..... 58
Repeater Mode ..... 59
WISP Client Router Mode ..... 60
WISP Repeater Mode ..... 61

**Wireless Basics ..... 62**
What is Wireless? ..... 63
Tips ..... 65
Wireless Modes ..... 66

**Networking Basics ..... 67**
Check your IP address ..... 67
Statically Assign an IP address ..... 68

**Technical Specifications ..... 69**

# Package Contents

- D-Link DAP-1160 Wireless G Access Point
- Power Supply
- CD-ROM with User Manual and Quick Install Guide
- Quick Installation Guide
- Ethernet Cable

**Note:** Using a power supply with a different voltage rating than the one included with the DAP-1160 will cause damage.

# System Requirements

- A computer with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer or Netscape Navigator version 6.0 or above, with JavaScript enabled

# Introduction

D-Link, an industry leader in computer networking, introduces the new D-Link Wireless G Access Point (DAP-1160). With the ability to transfer files with a maximum wireless signal rate of up to 54Mbps[1], the DAP-1160 gives you high-speed wireless network access for your home or office.

The DAP-1160 is Wi-Fi IEEE 802.11g compliant, meaning that it can connect and interoperate with other 802.11g compatible wireless client devices. The DAP-1160 is also backwards compatible with 802.11b devices.

The DAP-1160 can be flexibly configured to operate as an Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router, or WISP Repeater. The DAP-1160 also includes an embedded DHCP server that can automatically assign IP addresses to wireless network clients.

The DAP-1160 Access Point features Wi-Fi Protected Access (WPA-PSK/WPA2-PSK) and 64/128-bit WEP Encryption to provide an enhanced level of security for wireless data communications. The DAP-1160 also includes additional security features to keep your wireless connection safe from unauthorized access.

With an easy-to-use Web-based management interface, the DAP-1160 Access Point is the right choice for setting up your first wireless network or extending the range of an existing wireless network.

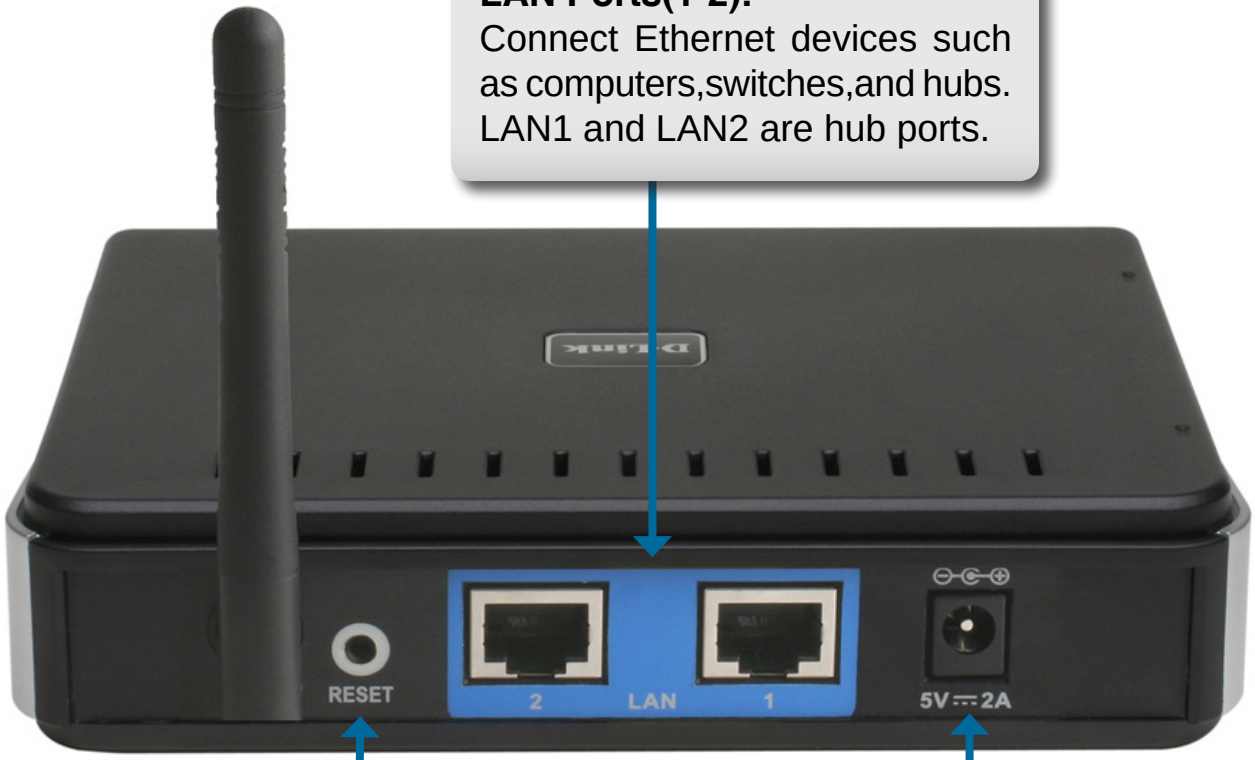
1 Maximum wireless signal rate based on IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower the actual data throughput rate.

# Features

- **Seven operation modes –** Can be flexibly configured to operate as an Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router or WISP Repeater.
- **Total security –** Complete set of security features including WEP encryption and WPA/WPA2 to protect your network from outside intruders.
- **Two integrated Ethernet ports –** Two Ethernet ports for ready connection to two computers, or to an Ethernet-enabled device (for example, a broadband router) and a PC.
- **Connect home and soho to a wireless network –** Create a wireless network for your home and office using the D-Link DAP-1160 Wireless Access Point. Connect this Access Point to a broadband modem and wirelessly share your Internet connection. Enjoy surfing the web, checking e-mail, and chatting with family and friends online.
- **Protect wireless network and data –** The DAP-1160 provides 64/128-bit WEP encryption and WPA/WPA2 security to protect your network and wireless data. In addition, it also provides MAC address filtering and the Disable SSID Broadcast function to limit outsiders' access to your home and office network.
- **Flexibly configure your AP for different applications –** The DAP-1160 can be configured to operate as (1) an Access Point to act as a central hub for wireless users, (2) an AP Client to connect to another Access Point, (3) a Bridge to join two wireless workgroups together, (4) a Bridge with AP to act as a wireless hub and a bridge at the same time, (5) a Repeater to extend the wireless coverage to cover all "dead" spots, (6) a WISP Client Router to let wireless Internet service subscribers share an Internet connection with home and office Ethernet-enabled computers without the need for an extra router, or (7) a WISP Repeater to let WISP subscribers share Internet connection with wireless computers without an extra router.

1 Maximum wireless signal rate based on IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower the actual data throughput rate.

# Hardware Overview
## Connections




**LAN Ports(1-2):**
Connect Ethernet devices such as computers,switches,and hubs. LAN1 and LAN2 are hub ports.

**RESET:** Pressing the Reset Button restores the access point to its original factory default settings.

**Power Socket:**
Connect the power adapter.

# Hardware Overview

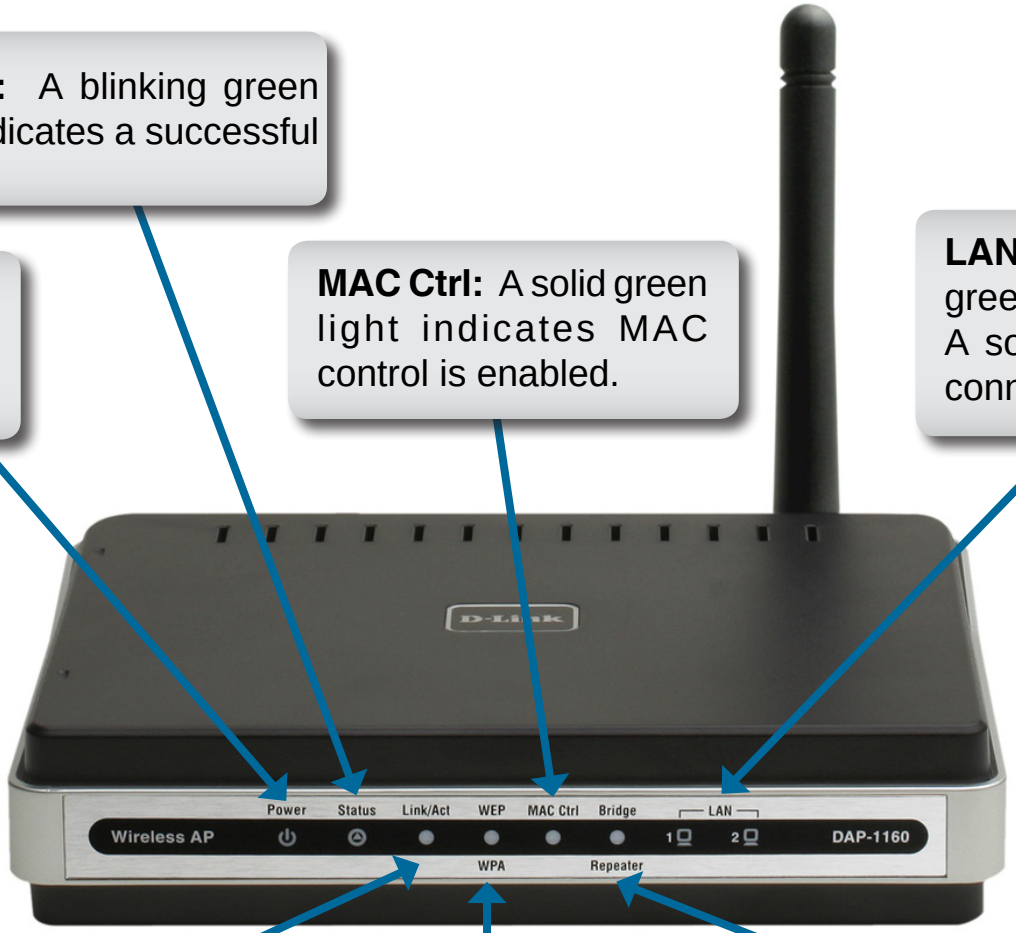
## LEDs

**Status:** A blinking green light indicates a successful boot.

**Power:** A solid green light indicates connection to a power source.

**MAC Ctrl:** A solid green light indicates MAC control is enabled.

**LAN Ports(1-2):** A blinking green light indicates activity. A solid green light indicates connection.




**Link/Act:** A blinking green light indicates wireless activity. A solid green light indicates connection.

**WEP/WPA:** A solid green light indicates when wireless security is enabled.

**Bridge/Repeater:** A solid green light indicates bridge or repeater is enabled.

# Configuration

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

# Web-based Configuration Utility

Use the Web-based Configuration Utility if you wish to change the default settings or optimize the performance of the DAP-1160. After you have completed the initial installation, you can access the configuration menu at any time by opening a web-browser and typing in the IP address of the DAP-1160. The DAP-1160's default IP address is 192.168.0.50. Follow the steps below to access the Web-based configuration utility.

1. Open a web browser

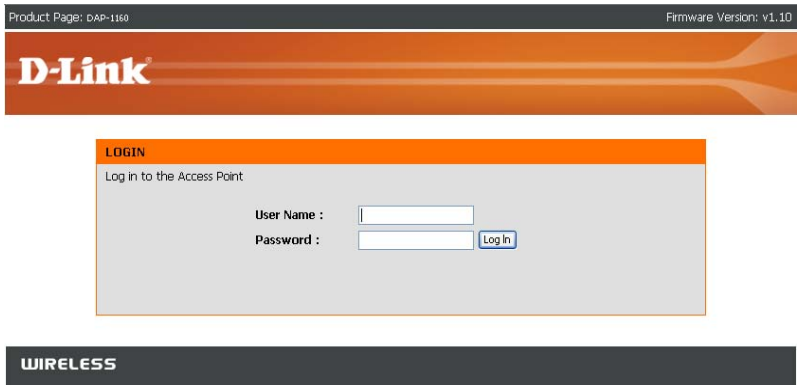
2. Type in the **IP address** of the DAP-1160 (192.168.0.50)

**Note:** If you have changed the default IP address assigned to the DAP-1160, make sure to enter the correct IP address.

3. Type **admin** in the **User Name** field

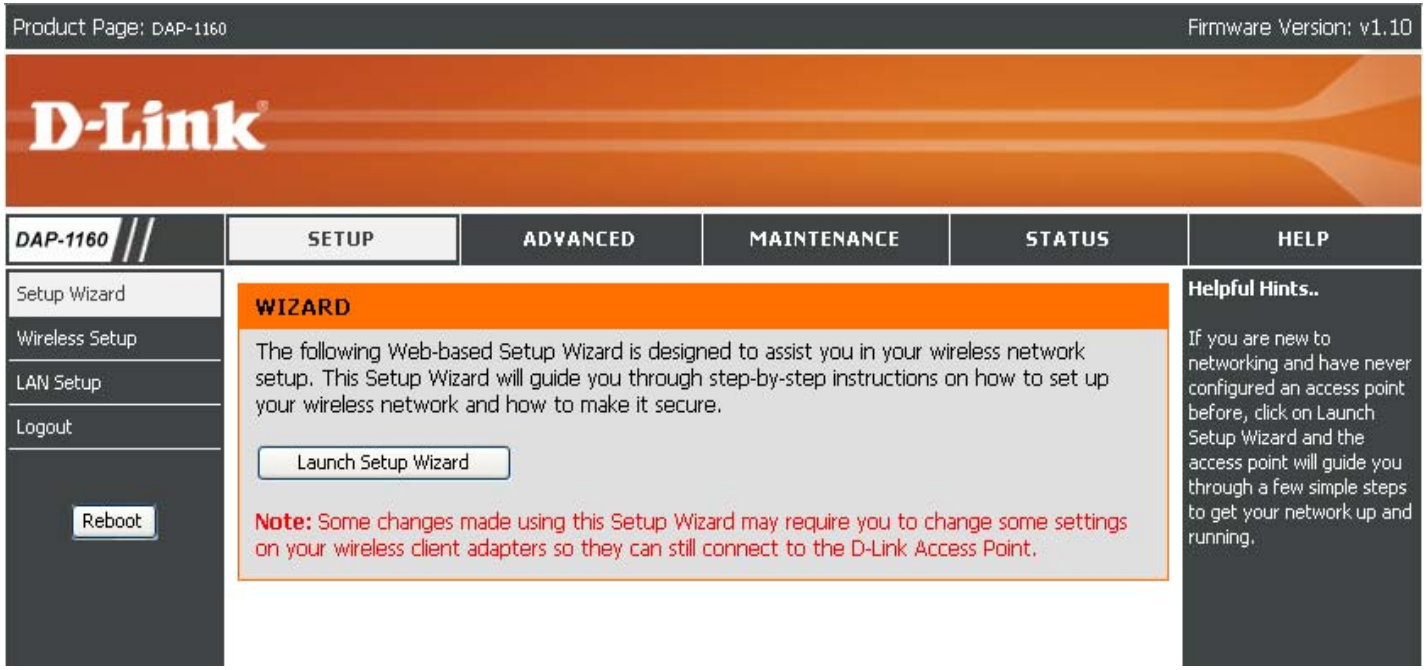
4. Leave the **Password** field blank

5. Click **OK**



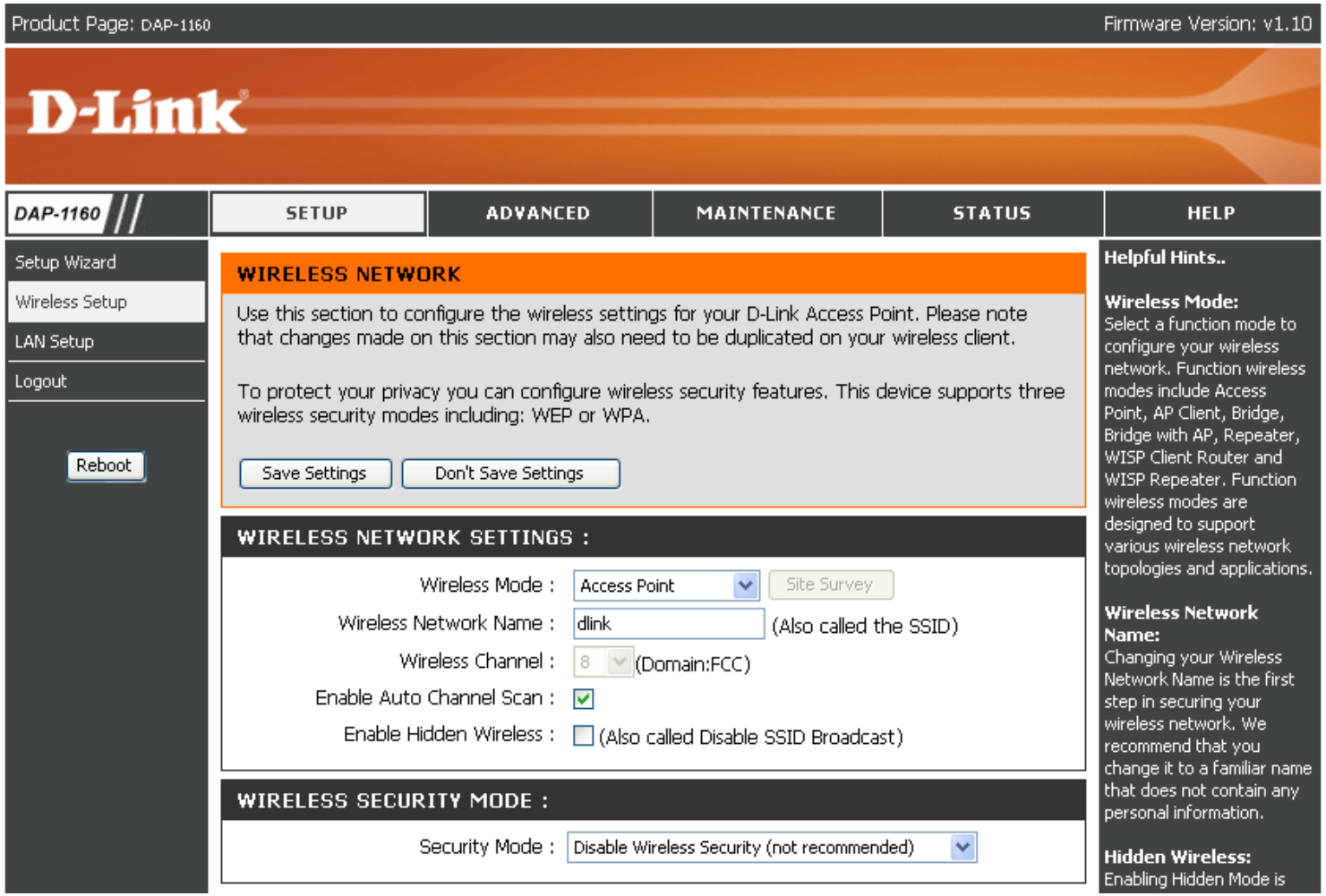
# Setup Wizard

After logging in, the **Setup > Setup Wizard** page will be displayed.Please refer to the Quick Installation Guide for more information regarding the Setup Wizard.



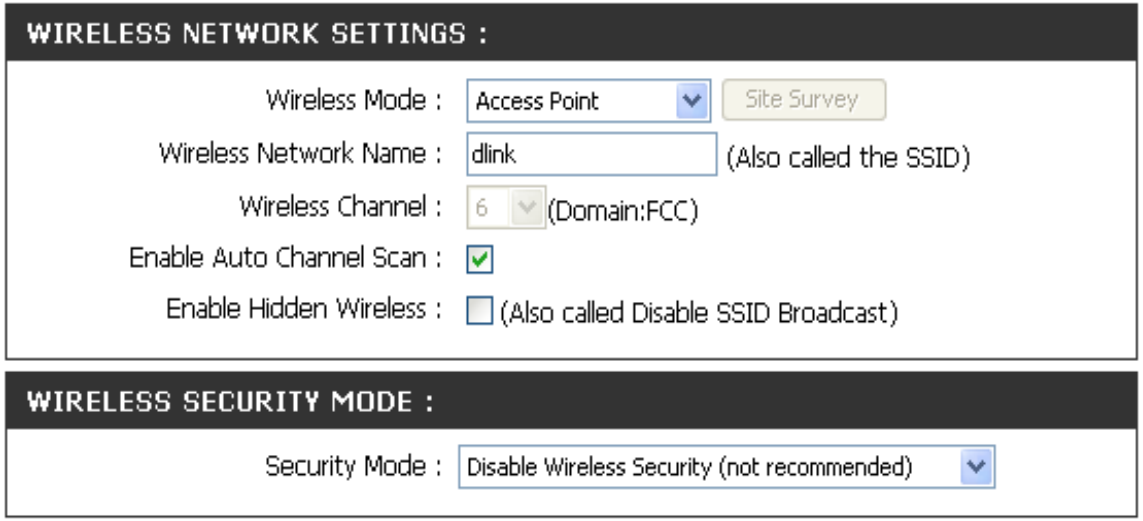
# Wireless Setup

The Wireless Setup page is used to configure the wireless settings for the access point. Wireless security settings can also be configured on this page. There are 7 possible wireless modes on the DAP-1160: Access Point, AP Client, Bridge, Bridge with AP, Repeater, WISP Client Router, and WISP Repeater. See Appendix A in this manual for more information about wireless modes. The first step is to select one of the 7 modes from the drop-down menu next to **Wireless Mode** under **Wireless Network Settings**.



# Access Point

In AP mode, the DAP-1160 acts as a central connection point for any computer (client) that has an 802.11g or backward-compatible 802.11b wireless network adapter and is within range of the AP.




**Wireless Network Name (also called the SSID):** The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

**Site Survey:** This button is unavailable in Access Point mode.

**Wireless Channel:** Auto channel selection is the default setting. First disable Auto Channel Scan (see below) and you will be able to select a wireless channel.

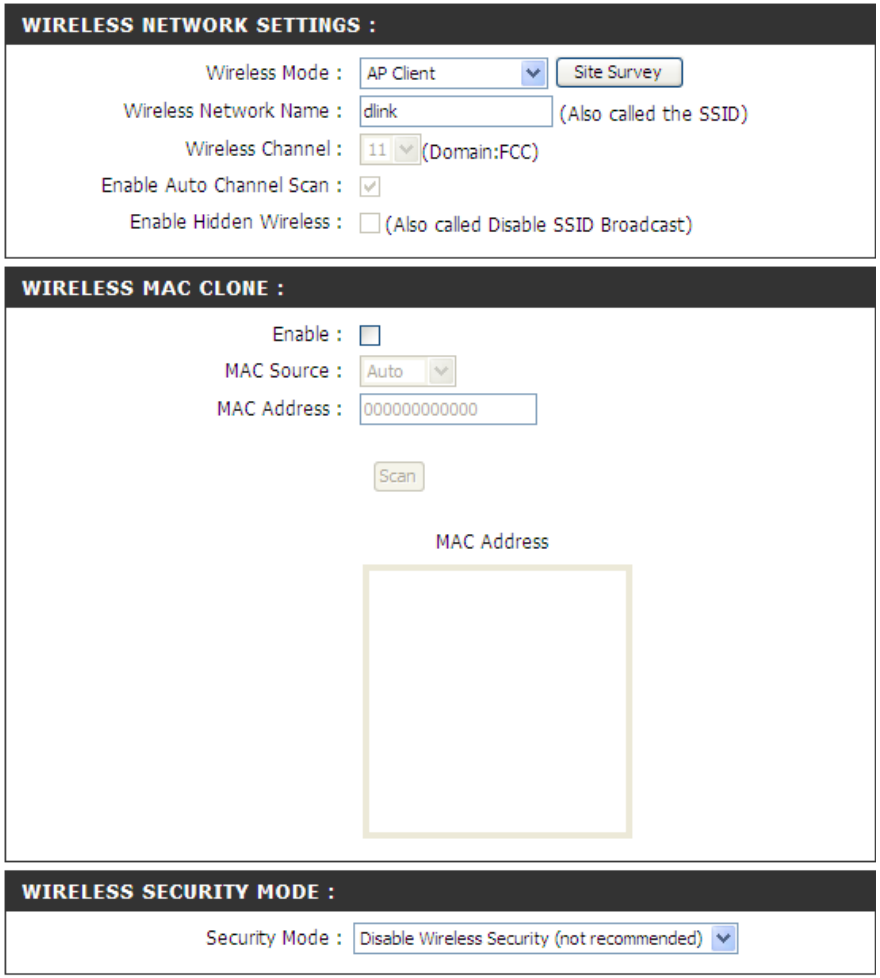
**Enable Auto Channel Scan:** Check the box to enable Auto Channel Scan. Enable this feature to auto-select the channel for the best wireless performance.

**Enable Hidden Wireless:** Check the box if you do not want the SSID to be broadcast by the DAP-1160. This prevents the SSID from being seen by site survey utilities, so any wireless clients will have to be pre-configured with the SSID of the DAP-1160 in order to connect to it.

**Wireless Security Mode:** Select a wireless security setting. Options are **None**, **WEP**, **WPA**, **WPA2,** or **WPA2-Auto**. See p.38 of this manual for a detailed explanation of the wireless security options.

# AP Client

In AP Client wireless mode, the DAP-1160 acts as a wireless network adapter for your Ethernet-enabled device (such as a game console or a TV set-top box).




**Wireless Network Name (also called the SSID):** You can input the wireless network name of the root AP or click the **Site Survey** button to find the root AP.

**Site Survey:** Click this button to choose the root AP from an available connection list.

**Wireless Channel:** The channel used will be displayed. The channel will follow the root AP.

**Enable Auto Channel scan:** This option is unavailable in AP Client mode.

**Enable Hidden Wireless:** This option is unavailable in AP Client mode.

**Wireless MAC Clone:** Enabling this option allows the user to manually assign the source MAC address to packets forwarded by the DAP-1160. If not manually assigned, the packet's source MAC address field will be automatically selected as the DAP-1160's MAC address.

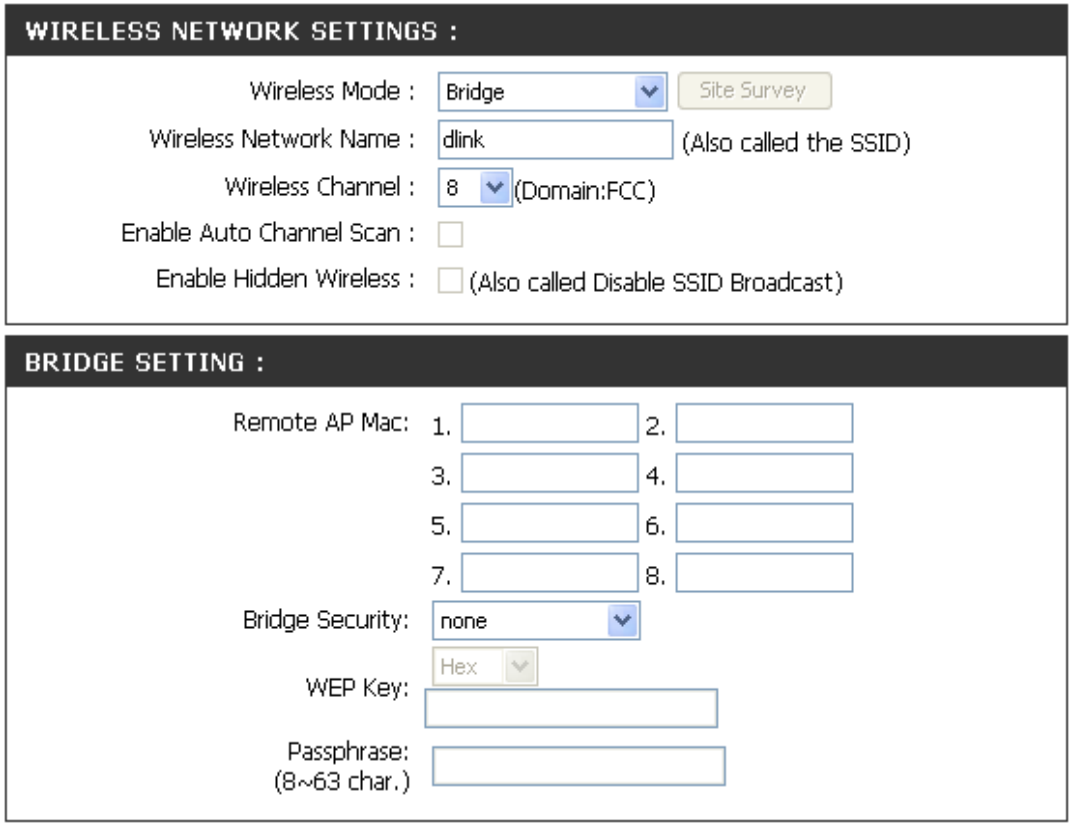
**MAC Address:** Enter the desired MAC address connected to your DAP-1160 to enable the clone function.

**Scan:** Click the **Scan** button to search for all available devices connected to your DAP-1160's Ethernet ports.

**Wireless Security Mode:** Select a wireless security setting. Options are **None**, **WEP**, **WPA**, or **WPA2**. See p.38 of this manual for a detailed explanation of the wireless security options.

# Bridge

Bridge wireless mode connects 2 LANs together.




**Wireless Network Name (also called the SSID):** The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

**Site Survey:** This button is unavailable in Bridge mode.

**Wireless Channel:** All devices on the network must share the same channel.

**Enable Auto Channel scan:** This option is unavailable in Bridge mode.

**Enable Hidden Wireless:** This option is unavailable in Bridge mode.

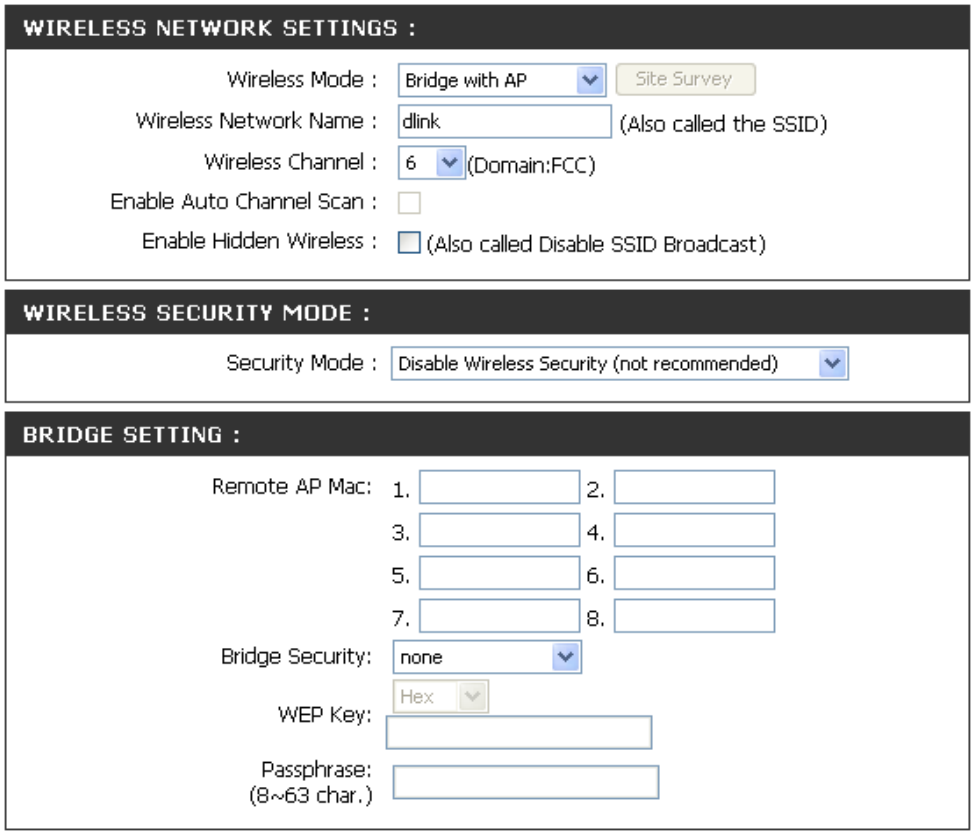
**Remote AP MAC:** Enter the MAC addresses of the APs in your network that will serve as bridges to wirelessly connect multiple networks.

**Bridge Security:** Select **None** to disable encryption to across the network. Select **WEP 64bits** or **WEP 128bits** to limit communication to only those devices that share the same WEP settings. Select **WPA-PSK** or **WPA2-PSK** to secure your network using a password and dynamic key changes (No RADIUS server required).

**Note:** Bridge Mode is not completely specified in WiFi or IEEE standards. It can work with other DAP-1160 units. Communication with other APs (even other D-Link APs) is not guaranteed.

# Bridge with AP

Bridge with AP wireless mode connects 2 LANs, while still functioning as a wireless AP for local wireless clients.




**Wireless Network Name (also called the SSID):** The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

**Site Survey:** This button is unavailable in Bridge with AP mode.

**Wireless Channel:** Input a new number if you want to change the default setting. All devices on the network must be set to the same channel to communicate on the network.

**Enable Auto Channel scan:** This option is unavailable in Bridge mode.

**Enable Hidden Wireless:** Check the box if you do not want the SSID to be broadcast by the DAP-1160. This prevents the SSID from being seen by Site Survey utilities, so any wireless clients will have to be pre-configured with the SSID of the DAP-1160 in order to connect to it.

**Wireless Security Mode:** Select a wireless security setting. Options are **None**, **WEP**, **WPA**, **WPA2,** or **WPA2-Auto**. See p.34 of this manual for a detailed explanation of the wireless security options.

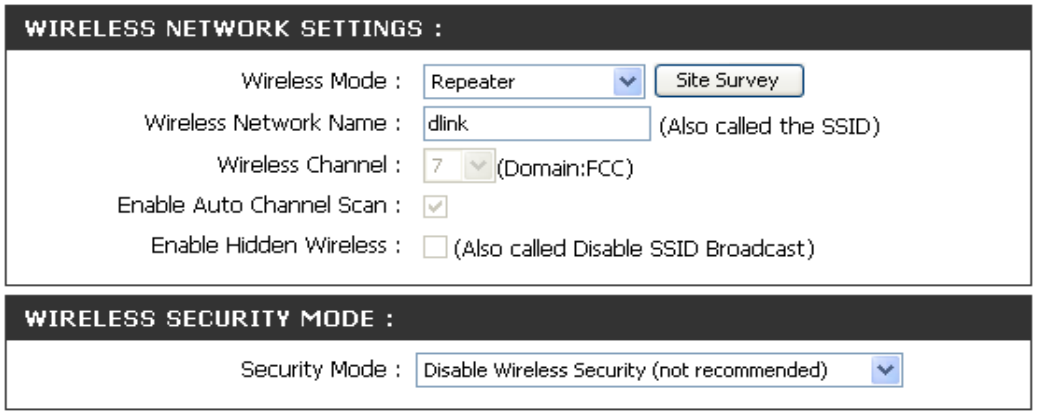
**Remote AP Mac :** Enter the MAC addresses of the APs in your network that will serve as bridges to wirelessly connect multiple networks.

**Bridge Security:** Select **None** to disable encryption to across the network. Select **WEP 64bits** or **WEP 128bits** to limit communication to only those devices that share the same WEP settings. Select **WPA-PSK** or **WPA2-PSK** to secure your network using a password and dynamic key changes (No RADIUS server required).

**Note:** Bridge with AP mode is not completely specified in WiFi or IEEE standards. It can work with other DAP-1160 units. Communication with other APs (even other D-Link APs) is not guaranteed.

# Repeater

Repeater wireless mode extends the wireless coverage of another wireless AP or wireless router.




**Wireless Network Name (also called the SSID):** The Wireless Network Name is a unique name that identifies a network. All devices on a network must share the same wireless network name in order to communicate on the network. If you decide to change the wireless network name from the default setting, enter your new wireless network name in this field.

**Site Survey:** Click this button to choose the root AP from an available connection list.

**Wireless Channel:** The channel will follow the root AP. The channel used will be displayed.

**Enable Auto Channel scan:** This option is unavailable in Repeater mode.

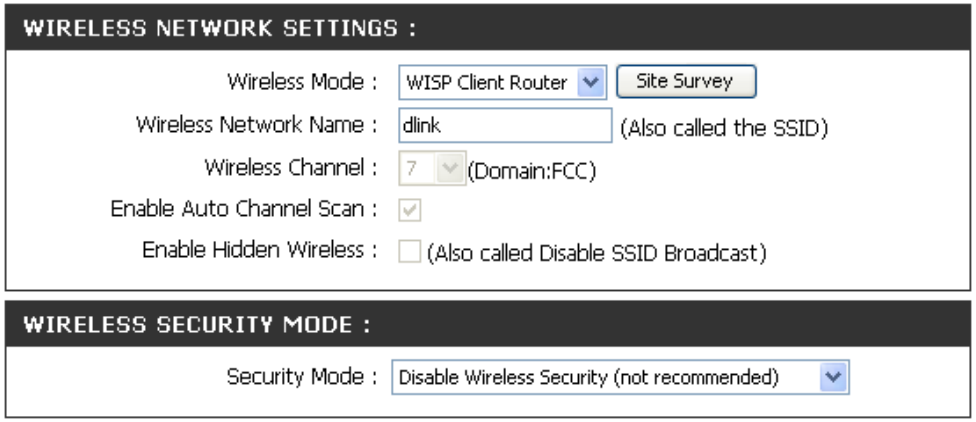
**Enable Hidden Wireless:** This option is unavailable in Repeater mode.

**Wireless Security Mode:** Select a wireless security setting. Options are **None**, **WEP**, **WPA**, or **WPA2**. See p.38 of this manual for a detailed explanation of the wireless security options.

# WISP Client Router and WISP Repeater

In WISP Router Client mode, the DAP-1160 wirelessly connects to a WISP (Wireless Internet Service Provider) AP. In this mode, the DAP-1160 also acts as a router for wired clients on your LAN and provides NAT (Network Address Translation) and a DHCP server to generate IP addresses for wired clients. NAT and the DHCP server allow many computers to share the same wireless Internet connection.

WISP Repeater wireless mode acts the same as WISP Client Router wireless mode, with the addition of a wireless signal for any wireless clients on the LAN.




**Wireless Network Name:** You can input the wireless network name of the root AP or click the **Site Survey** button to find the root AP.

**Site Survey:** Click this button to choose the root AP from an available connection list. If the root AP has wireless encryption, you have to use the same wireless security mode to connect the root AP.

**Wireless Channel:** The channel used will be displayed. The channel will follow the root AP.

**Enable Auto Channel Scan:** This option is unavailable in WISP Client Router and WISP Repeater mode.

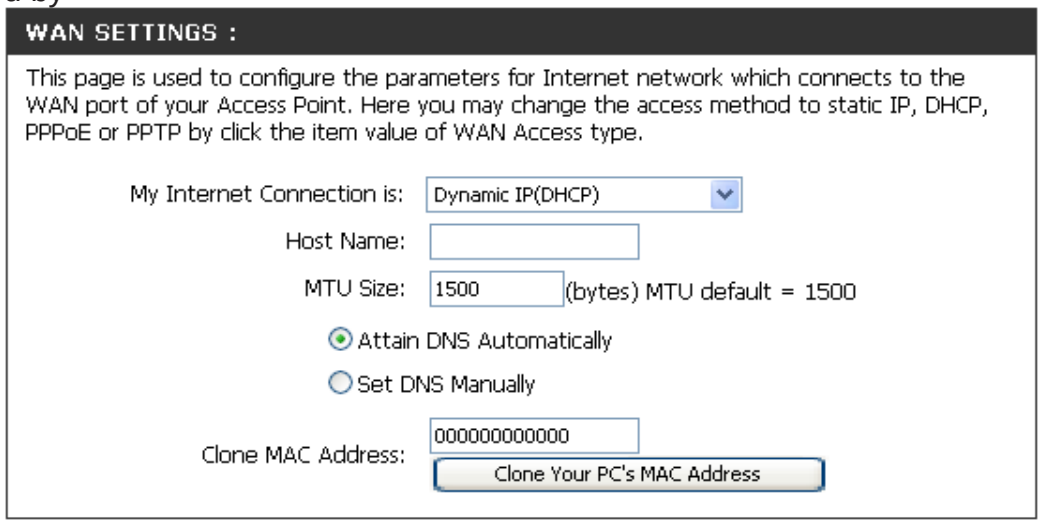
**Enable Hidden Wireless:** This option is unavailable in WISP Client Router and WISP Repeater mode.

**Wireless Security Mode:** Select a wireless security setting. Options are **None**, **WEP**, **WPA**, or **WPA2**. See p.38 of this manual for a detailed explanation of the wireless security options.

# WAN Settings

## Dynamic IP (DHCP)

WAN Settings are only used with WISP Client Router wireless mode and WISP Repeater wireless mode. Choose Dynamic IP(DHCP) to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services.




**Host Name:** The Host Name is optional but may be required by some ISPs.

**MTU Size:** You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The default MTU size is 1500.

**Attain DNS automatically:** Select this option if you want the DAP-1160 to get the DNS (Domain Name System) server IP address automatically.

**Set DNS manually:** Select this option if you want to manually enter the DNS Server IP address(es). Fields to enter the Primary and Secondary DNS server IP addresses will appear after you select this option.

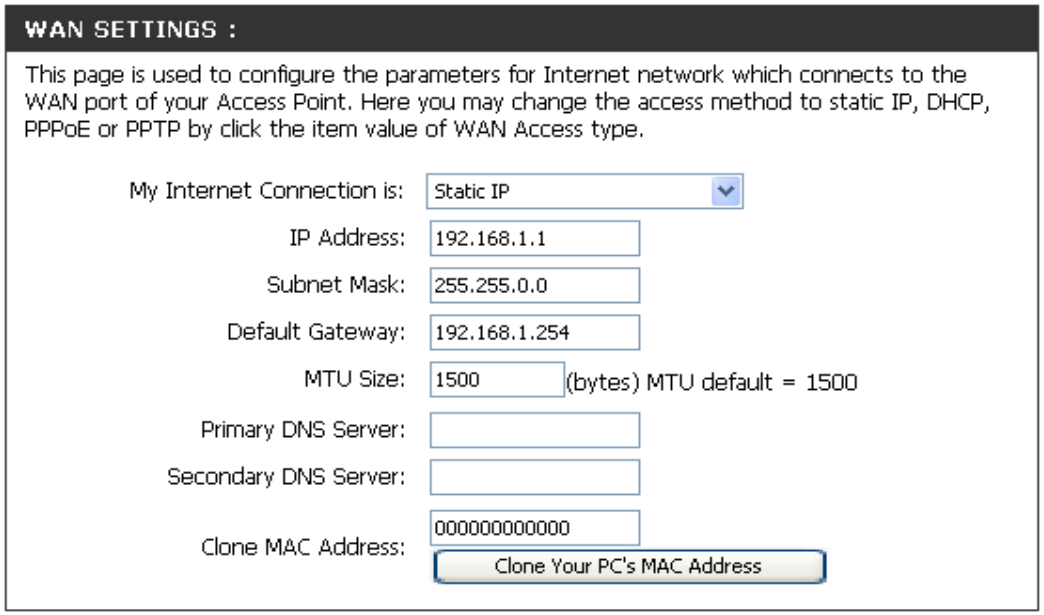
**Primary DNS Server:** Enter the Primary DNS server IP address assigned by your ISP.

**Secondary DNS Server:** This is optional.

**Clone MAC address:** The default MAC address is set to the MAC address on the AP (Access Point). You can click the **Clone Your PC's MAC Address** button to replace the AP's MAC address with the MAC address of your Ethernet card. It is not recommended that you change the default MAC address unless required by your ISP.

# Static IP

Select Static IP if all WAN IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP.




**IP Address:** 192.168.1.1 is the default WAN IP Address of the DAP-1160.

**Subnet Mask:** 255.255.255.0 is the default subnet mask. All devices on the network must have the same subnet mask to communicate on the network.

**Default Gateway:** Enter the IP Address of the gateway in your network. The default setting is 192.168.1.254.

**MTU Size:** You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The default MTU size is 1500.

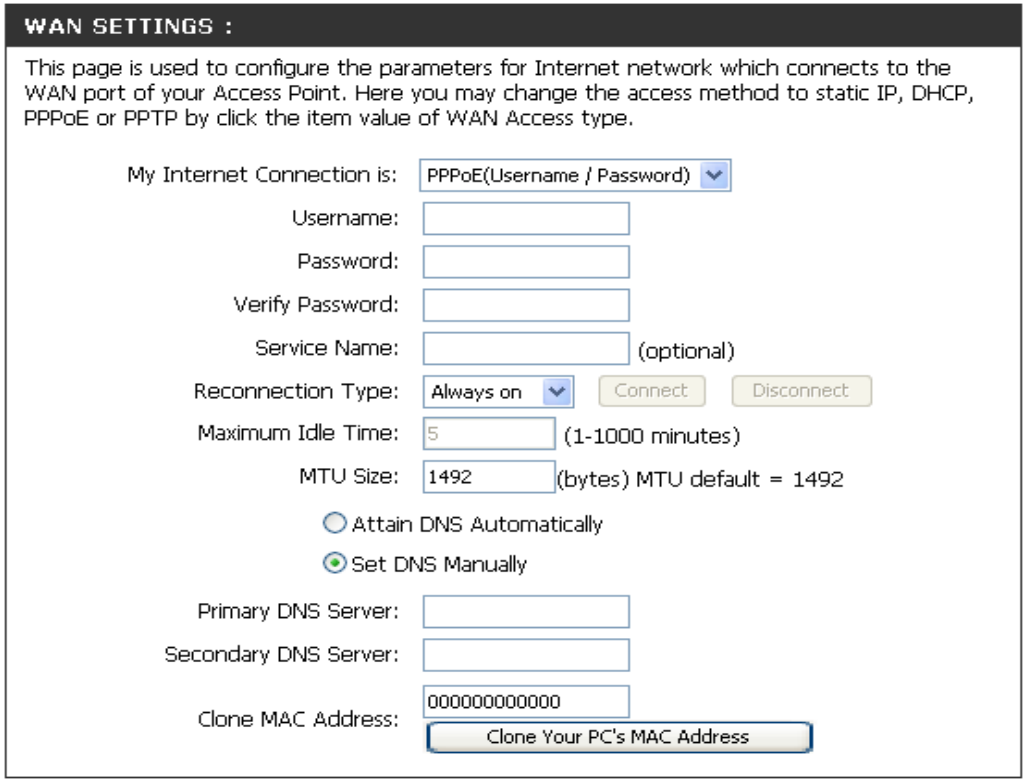
**Primary DNS Server:** Enter the Primary DNS (Domain Name System) server IP address assigned by your ISP.

**Secondary DNS Server:** This is optional.

**Clone MAC address:** The default MAC address is set to the MAC address on the AP (Access Point). You can click the **Clone Your PC's MAC Address** button to replace the AP's MAC address with the MAC address of your Ethernet card. It is not recommended that you change the default MAC address unless required by your ISP.

# PPPoE

Choose PPPoE (Point-to-Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Make sure to remove your PPPoE software from your computer. The software is no longer needed and will not work through the DAP-1160.




**User Name:** Enter your PPPoE user name.

**Password:** Enter your PPPoE password and then retype the password in the next box.

**Service Name:** Enter the ISP Service Name (optional).

**Reconnection Type:** Select **Always on**, **On demand**, or **Manual**.

**Maximum Idle time:** Enter a maximum idle time during which the Internet connection is maintained during inactivity.

**MTU Size:** You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The default MTU size is 1492.

**Attain DNS Automatically:** Select this option if you want the DAP-1160 to get the DNS (Domain Name System) server IP address automatically.

**Set DNS Manually:** Select this option if you want to manually enter the DNS Server IP address(es). Fields to enter the Primary and Secondary DNS server IP addresses will appear after you select this option.

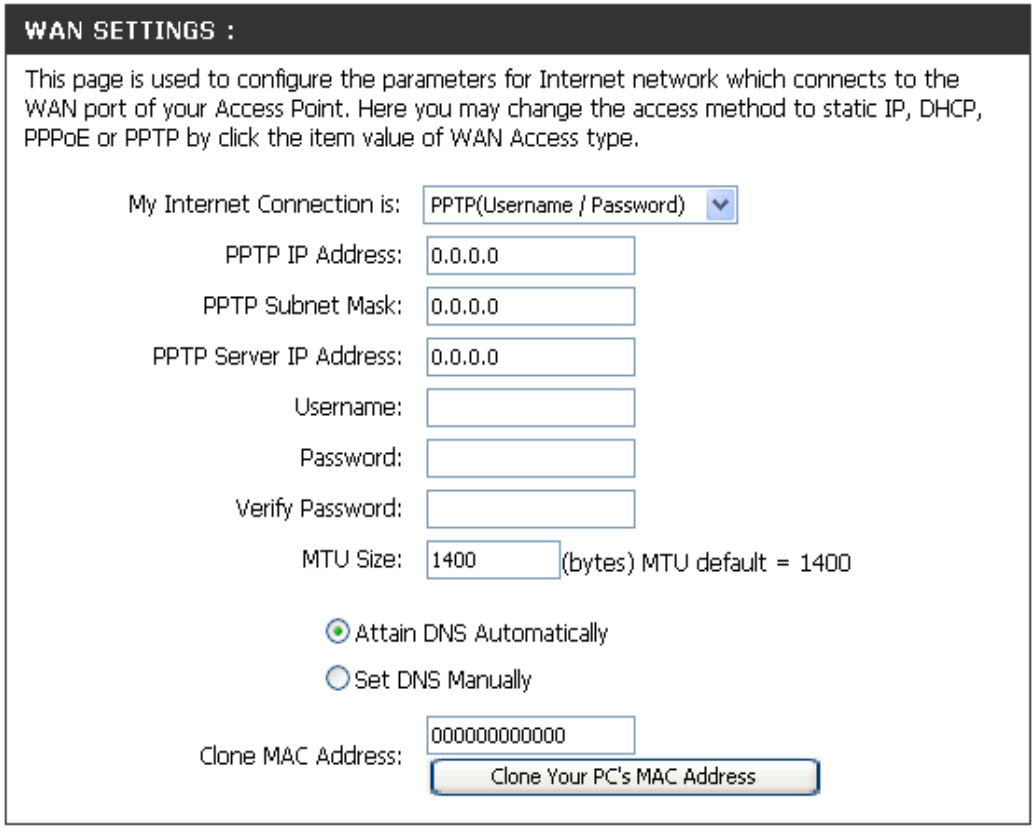
**Primary DNS Server:** Enter the Primary DNS server IP address assigned by your ISP.

**Secondary DNS Server:** This is optional.

**Clone MAC Address:** The default MAC address is set to the MAC address on the AP (Access Point). You can click the **Clone Your PC's MAC Address** button to replace the AP's MAC address with the MAC address of your Ethernet card. It is not recommended that you change the default MAC address unless required by your ISP.

# PPTP

Choose PPTP (Point-to-Point Tunneling Protocol) if your ISP uses a PPTP connection. Your ISP will provide you with a username and password. This option is typically used for DSL services.




**PPTP IP Address:** Enter the IP address (Static PPTP only).

**PPTP Subnet Mask:** Enter the subnet mask.

**PPTP Server IP Address:** Enter the Server IP Address provided by your ISP.

**Username:** Enter your PPTP account name.

**Password:** Enter your PPTP password and then retype the password in the next box.

**MTU Size:** You may need to change the MTU (Maximum Transmission Unit) for optimal performance with your specific ISP. The default MTU size is 1400.

**Attain DNS automatically:** Select this option if you want the DAP-1160 get DNS server IP address automatically.

**Set DNS Manually:** Select this option if you want to manually enter the DNS Server IP address(es). Fields to enter the Primary and Secondary DNS server IP addresses will appear after you select this option.

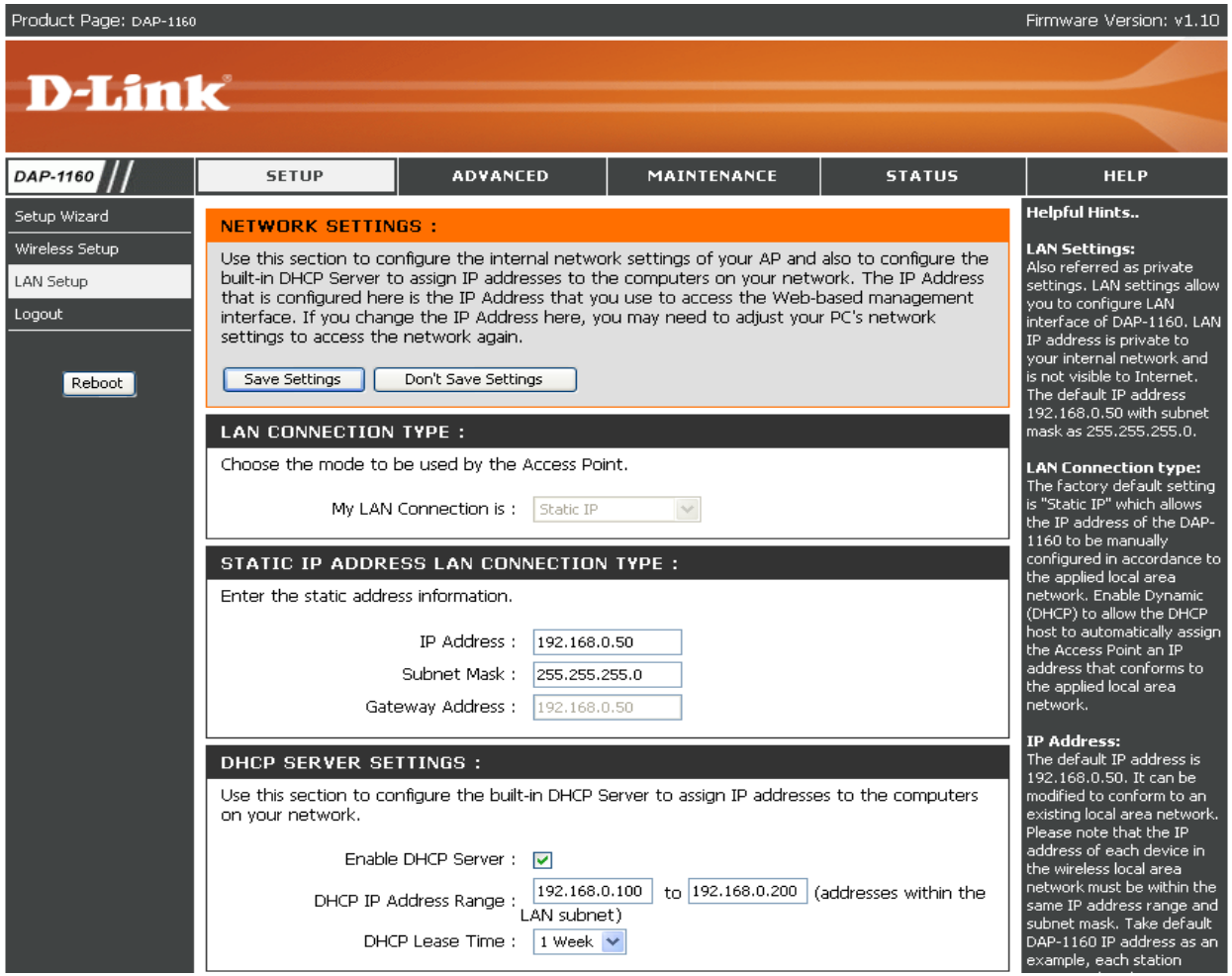
**Primary DNS Server:** Enter the Primary DNS (Domain Name System) server IP address assigned by your ISP.

**Secondary DNS Server:** This is optional.

**Clone MAC address:** The default MAC address is set to the MAC address on the AP (Access Point). You can click the **Clone Your PC's MAC Address** button to replace the AP's MAC address with the MAC address of your Ethernet card. It is not recommended that you change the default MAC address unless required by your ISP.

# 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-1160. 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-1160 is set to Static IP by default. Select this option if you do not have a DHCP server on your network, or if you wish to assign a static IP address to the DAP-1160.

**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-1160 by a DHCP server in your network.

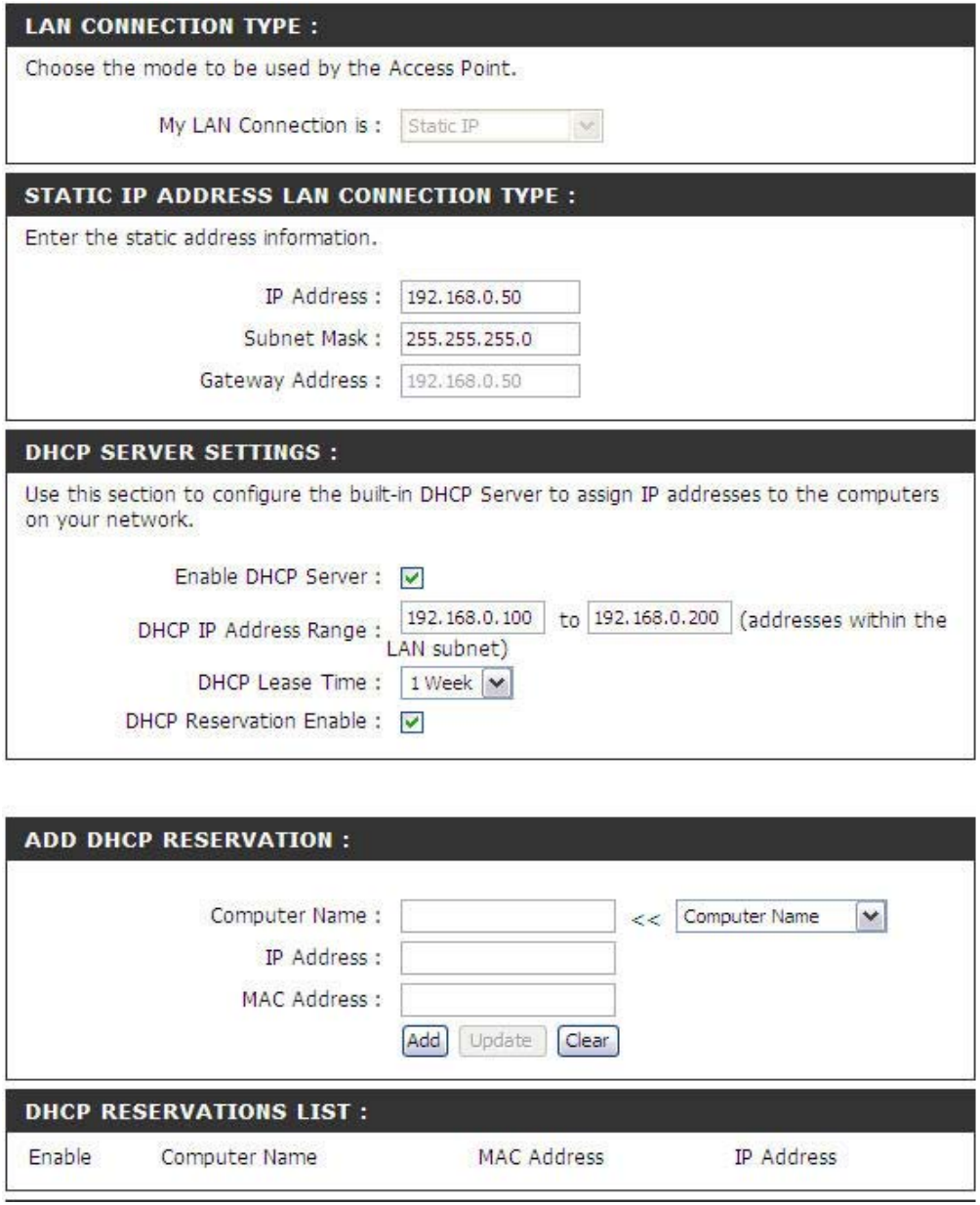
**IP Address:** 192.168.0.50 is the default LAN IP Address of the Access Point.

**Subnet Mask:** 255.255.255.0 is the default subnet mask. All devices on the network must have the same subnet mask to communicate on the network.

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

**Enable DHCP Server:** The default setting is disabled. Check this box if you want to use the DAP-1160 as a DHCP server to automatically assign dynamic IP addresses on the network.

**DHCP IP Address Range:** If you have enabled the DHCP server function, enter the starting and Ending point of the IP address range for your network.



**DHCP Lease Time:** Choose the length of time during which the DHCP function of the DAP-1160 automatically regenerates the IP addresses to the devices in your network.

**Dynamic DHCP Client List:** This section lists the devices on your network that are receiving dynamic IP addresses from the DAP-1160.

**DHCP Reservation:** DHCP Reservation allows you to manually assign and reserve specific IP addresses to computers connected on your network. This is useful when also using other network management features, such as firewall rules and port forwarding. After entering a reservation, click on the **Save Settings** button to save the changes of your settings.

**Computer Name:** Enter a name for the computer you want to reserve the IP address for.

**IP Address:** Enter the IP address that you want assigned to your desired computer.

**MAC Address:** Enter the MAC address of the computer that you want to reserve the IP address for. To find the MAC address on a computer, please refer to the Networking Basics section in this manual.
You can also use the dropdown box (Computer Name) to automatically enter the computer name, current IP address, and MAC address of a computer currently connected to the router; to do so, select a computer from the dropdown box, then click the << button.

**DHCP Reservation List:** This section lists the devices on your network that are using DHCP reservation.

**Dynamic DHCP Client List:** This section lists the devices on your network that are receiving dynamic IP addresses from the DAP-1160.

# Advanced
## Port Forwarding

This function is available if the DAP-1160 is in WISP Client Router or WISP Repeater mode. This feature allows you to open a single port or a range of ports. Click **Save Settings** and the port forwarding rule will be put into the Port Forwarding List.

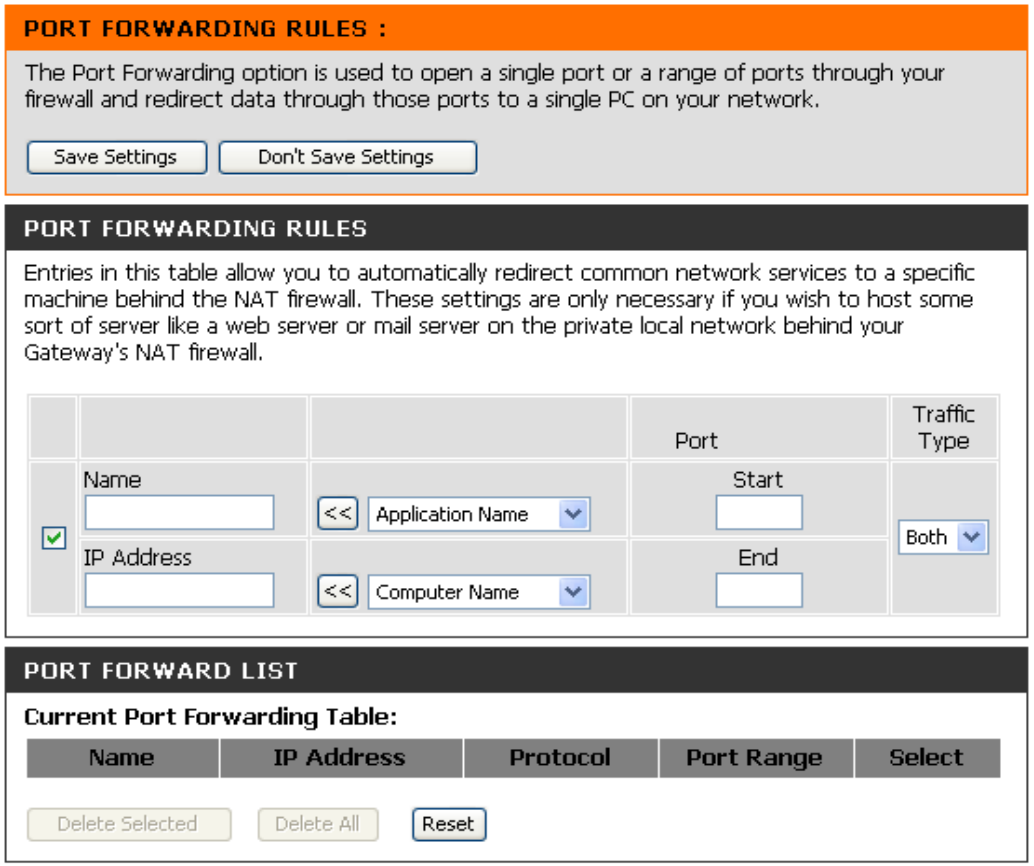
**Port Forwarding Rules:** Check the box to configure a port forwarding rule.

**Name:** Enter a name for the rule. You can select an application name from the Application Name drop-down menu. Click the **<<** button to fill in the Name field with the application name that you selected.

**IP Address:** Enter the IP address of the computer on your local network that you want to allow the incoming service to.

**Start Port/End Port:** Enter the port or ports that you want to open. If you want to open one port, enter the same port in both boxes.

**Traffic Type:** Select **TCP**, **UDP**, or **Both**.



# Port Filter

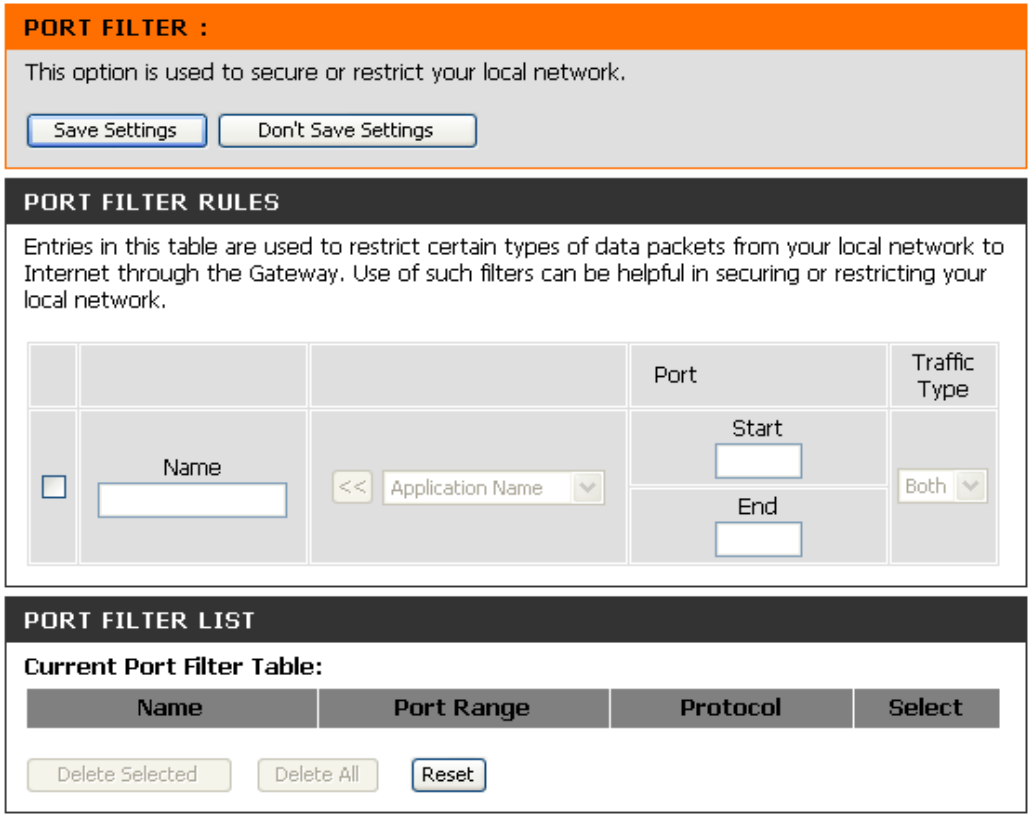
This function is available if the DAP-1160 is in WISP Client Router or WISP Repeater mode. This feature is used to secure or restrict your local network. It will deny the ports that you enter from the local network to the Internet. Click **Save Settings** and the port filter rule will be put into the Port Filter List.

**Port Filter Rules:** Check the box to configure a port filter rule.

**Name:** Enter a name for the rule. You can select an application name from the Application Name drop-down menu. Click the **<<** button to fill in the Name field with the application name that you selected.

**Start Port/End Port:** Enter the port or ports that you want to open. If you want to open one port, enter the same port in both boxes.

**Traffic Type:** Select **TCP**, **UDP**, or **Both**.



# Access Control

Use MAC Filters to allow or deny wireless clients, by their MAC addresses, from accessing the DAP-1160. 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.

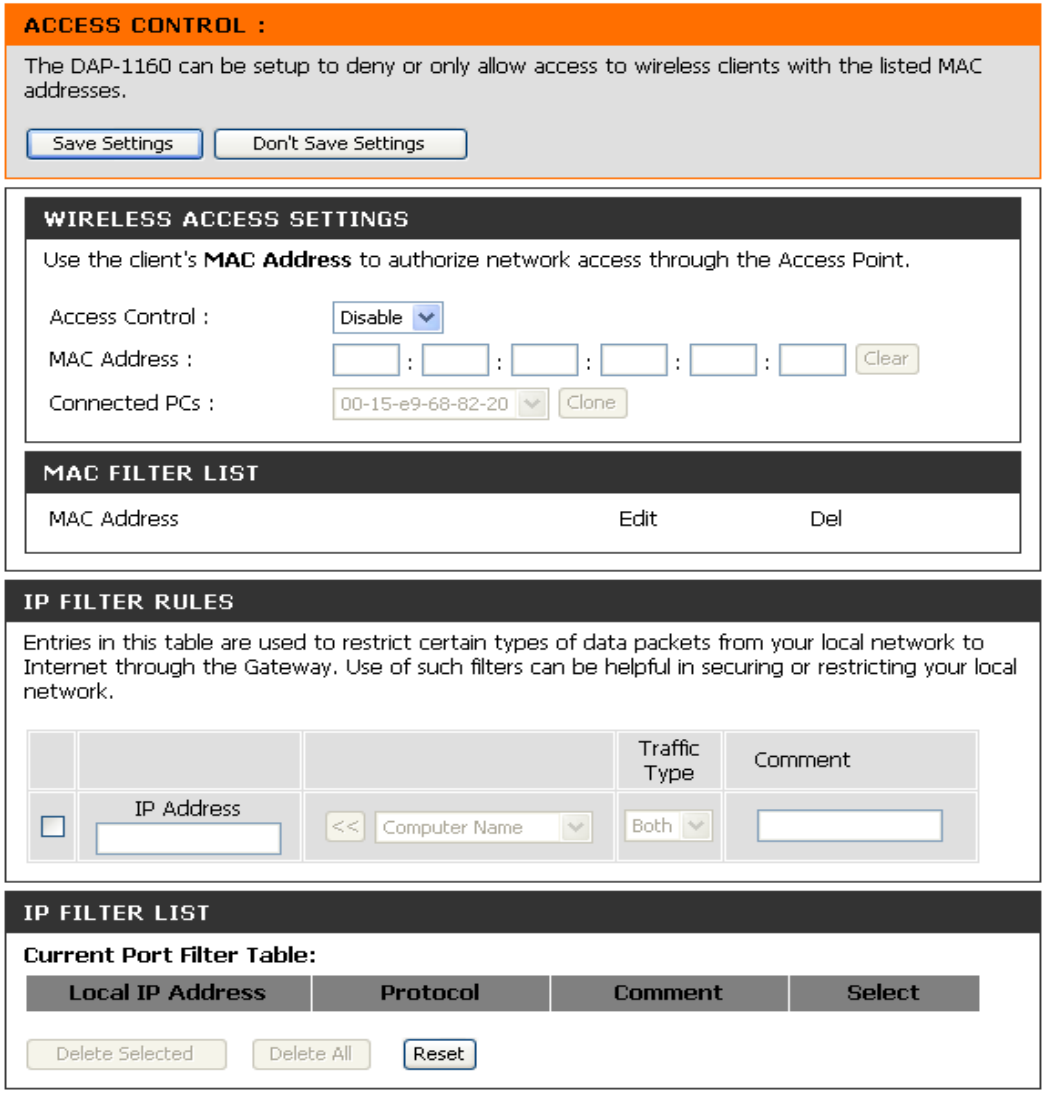
**Connected PCs:** Select the MAC address of a computer from the drop-down menu and click **Clone** to fill in the MAC Address field with that computer.

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

**IP Filter Rules:** This function is available if the DAP-1160 is in WISP Client Router or WISP Repeater mode.
IP filter rules are used to secure or restrict your local network. It will deny wireless clients by their IP Addresses from the local network to the Internet. Click **Save Settings** and the IP filter rule will be put into the Port Filter List.

**IP Address:** Enter the IP address of the computer on your local network that you want to deny the outgoing traffic to.

**Traffic Type:** Select **TCP**, **UDP**, or **Both**.

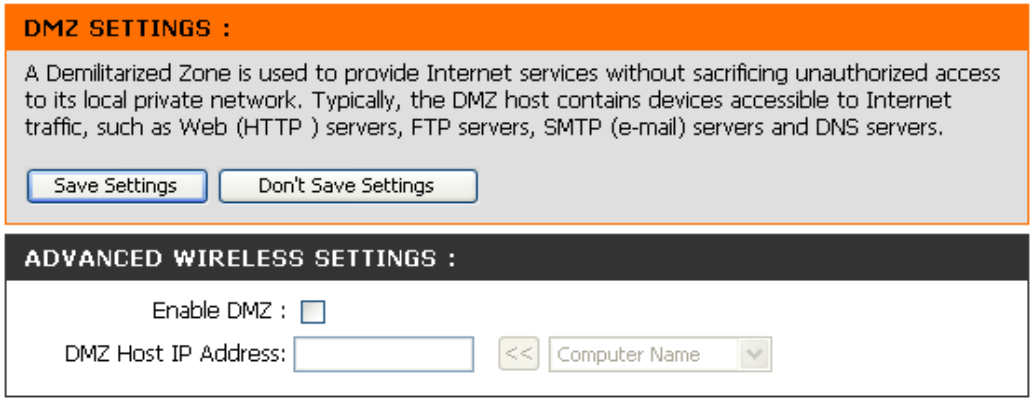


# DMZ

This function is available if the DAP-1160 is in WISP Client Router or WISP Repeater mode. This feature allows you to set up a DMZ (Demilitarized Zone) host. If you have a client PC that cannot run Internet applications properly from behind the DAP-1160, then you can set the client up for unrestricted Internet access. The DMZ allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP address of the computer that will be the DMZ host. Adding a client to the DMZ may expose your local network to a variety of security risks, so only use this option as a last resort.

**Enable DMZ:** Check this box to enable DMZ.

**DMZ Host IP Address:** Enter the IP address of the computer you would like to open all ports to. You can select a computer from the Computer Name drop-down menu and click **<<** to enter the computer name into the DMZ Host IP Address field.

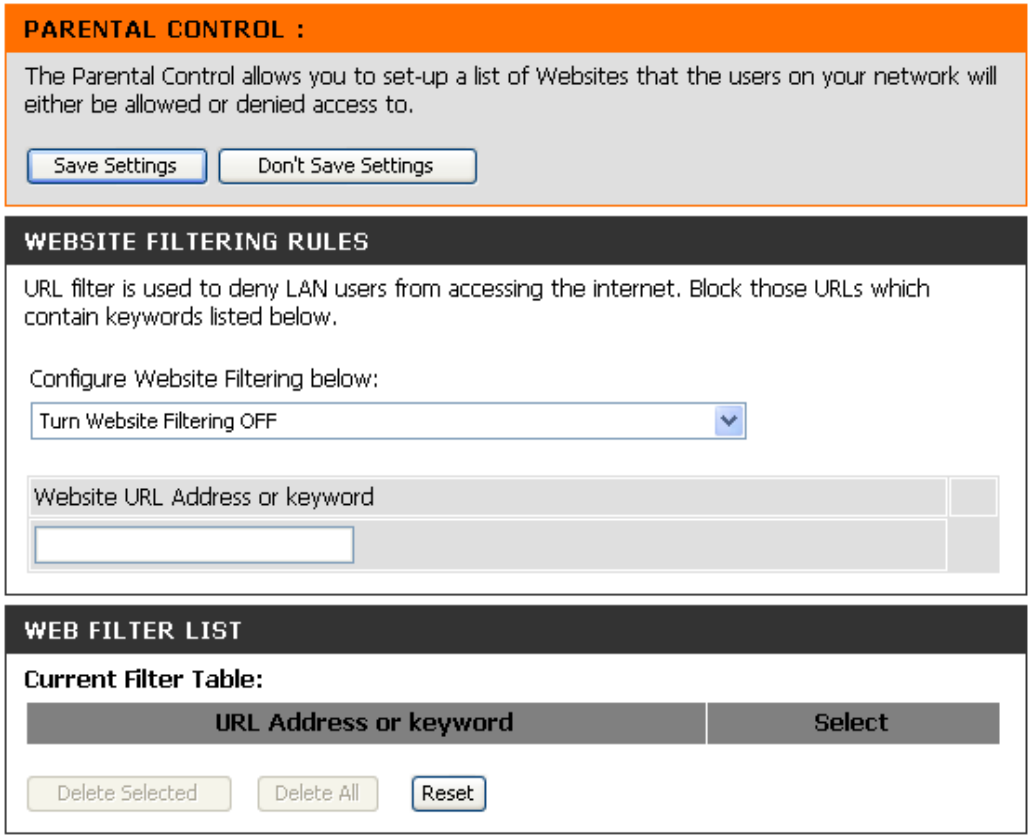


# Parental Control

This function is available if the DAP-1160 is in WISP Client Router or WISP Repeater mode. This feature allows you to create a list of websites that you want to deny users access.

**Configure Website Filtering below:** Select **Turn Website Filtering OFF** or **Turn Website Filtering ON and DENY computers access to ONLY these sites**.

**Website URL Address:** Enter a keyword or URL that you want to block and click **Save Settings**. Any URL that contains the keyword will be blocked.



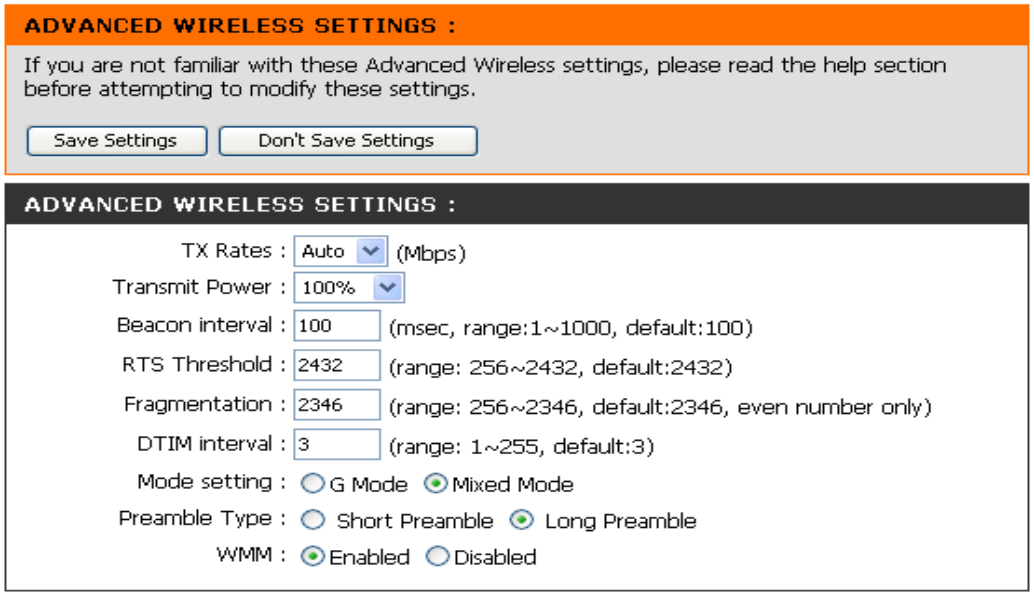
# Advanced Wireless

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

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

**Beacon Interval:** 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.

**Mode Setting:** For the fastest speed, select **G Mode** to include only 802.11g devices in your network. Select **Mixed Mode** to include 802.11g and 802.11b devices in your network.

**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.

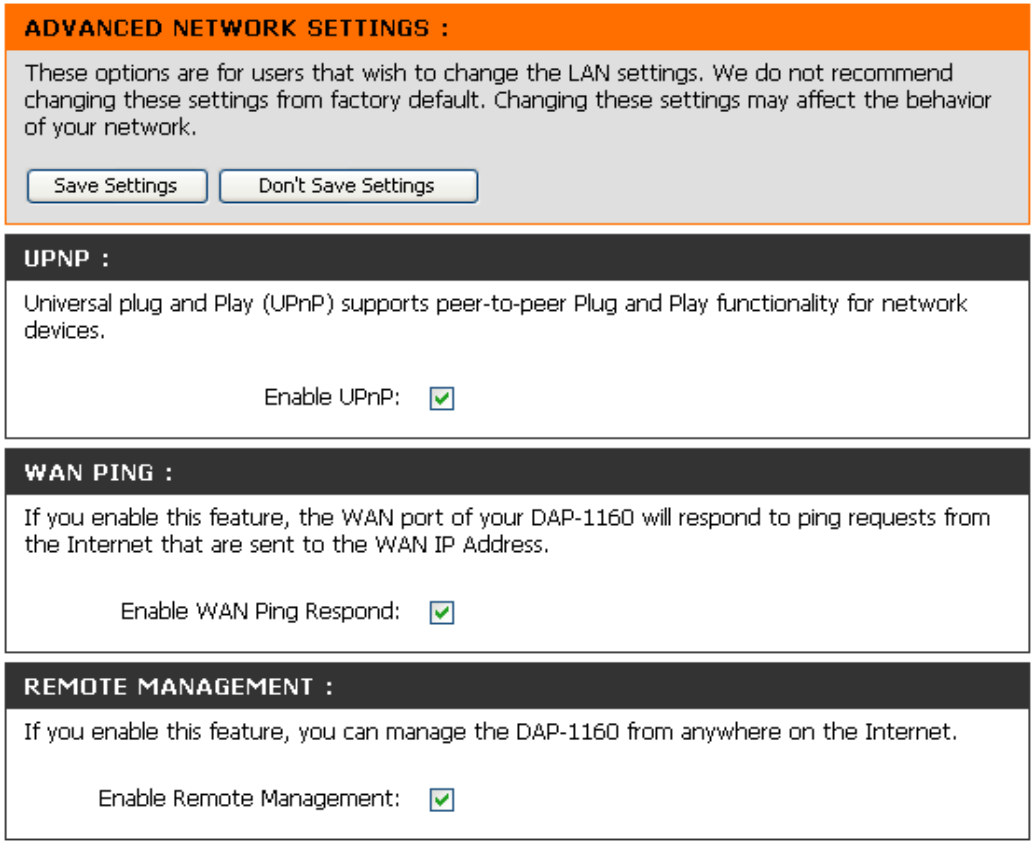
# Advanced Network

This function is available if the DAP-1160 is in WISP Client Router or WISP Repeater mode. This feature allows you to change the LAN settings. Please be aware that any changes to the factory default settings may affect the behavior of your network.

**Enable UPnP:** Check this box to use the Universal Plug and Play (UPnP™) feature. UPnP provides compatibility with networking equipment, software and peripherals.

**Enable WAN Ping Respond:** Check this box to allow the WAN port of the DAP-1160 to be pinged. Unchecking the box will not allow the DAP-1160 to respond to pings. Blocking ping response may provide some extra security from intruders.

**Remote Management:** Remote management allows the DAP-1160 to be configured from the Internet by a web browser. A username and password are still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform Administrator tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.



# Traffic Management Settings

Traffic management settings allow you to specify rules to control a client's maximum bandwidth. This function is available in WISP Client Router and WISP Repeater mode. To enable this feature, you must first enable the DAP-1160 DHCP server and make a DHCP reservation. Remember that client has not in DHCP reservation list will auto bypass this system. You can refer to the setup example below.

**Setup Example:** You want to set the bandwidth limit for the PC, with 00:FF:08:90:11:3A as its MAC address, to a maximum uplink and downlink speed of 1024kbps.

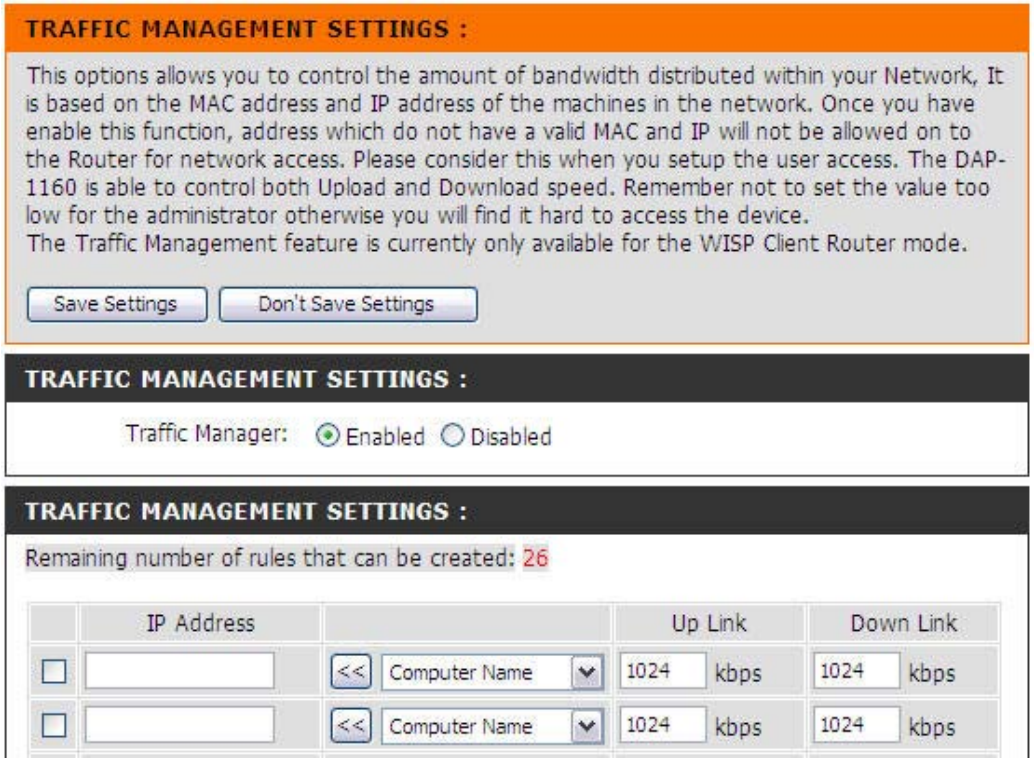
1. Enable the DAP-1160 DHCP server.
2. Make a DHCP reservation (192.168.0.120 reserved for 00:FF:08:90:11:3A).
3. Enable Traffic Manager.
4. Create traffic management rules, select the computer which you reserved the IP address for, then enter the maximum uplink and downlink speed to 1024kbps. Check the box on the left of the IP address to enable this rule.

**Traffic Manager:** Select Enabled or Disabled.

**IP Address:** Enter the IP address that you wish to limit the maximum bandwidth.

**Uplink:** Enter the maximum uplink value of this PC.

**Downlink:** Enter the maximum uplink value of this PC.

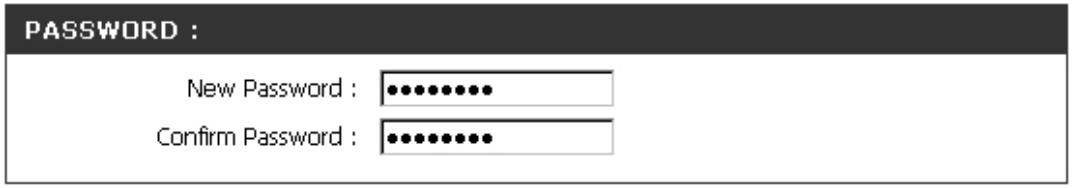


# Maintenance

## Device Administration

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

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

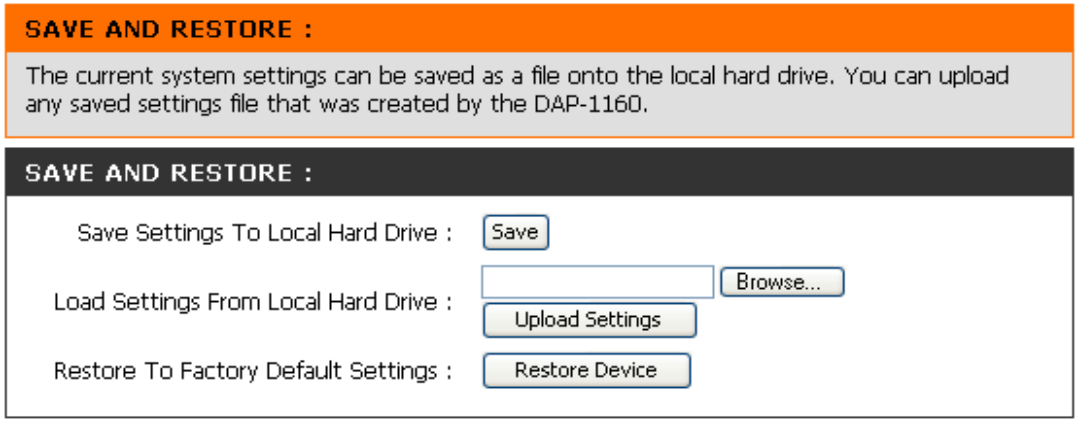



## Save and Restore

**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-1160 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 Update

This feature is used to update the firmware of the DAP-1160. 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 **Save Settings** button after you have selected the updated firmware file.

# 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-1160 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.

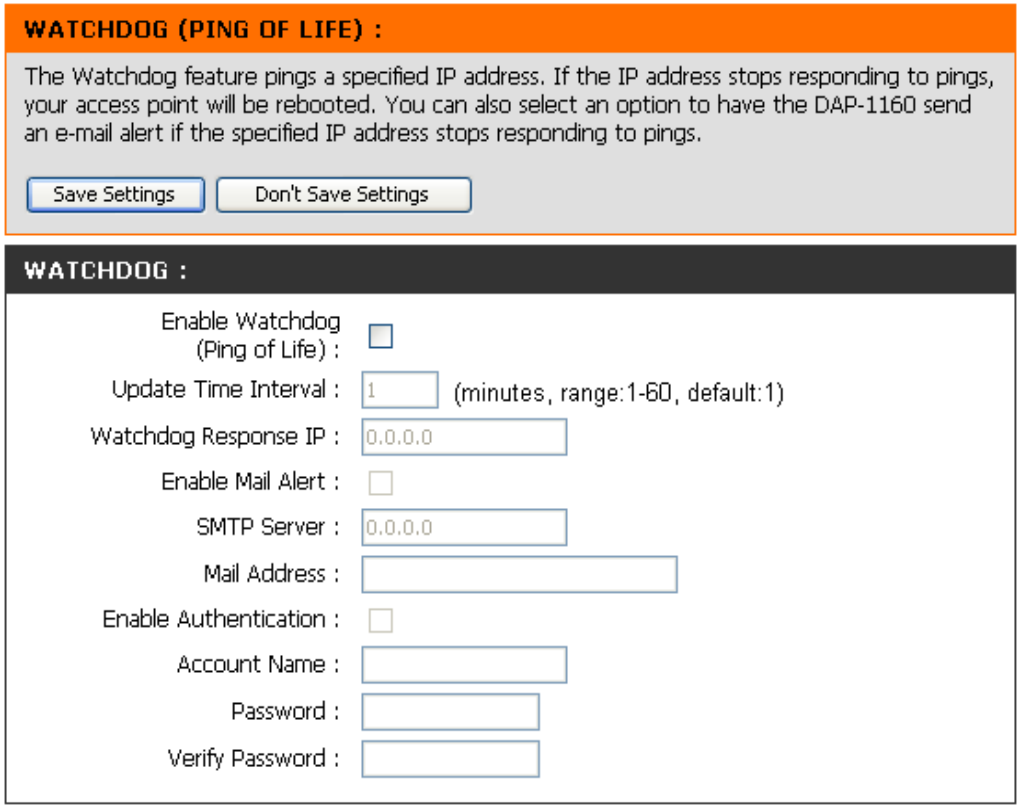
**SMTP Server:** Enter the SMTP server IP address.

**Mail Address:** 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.

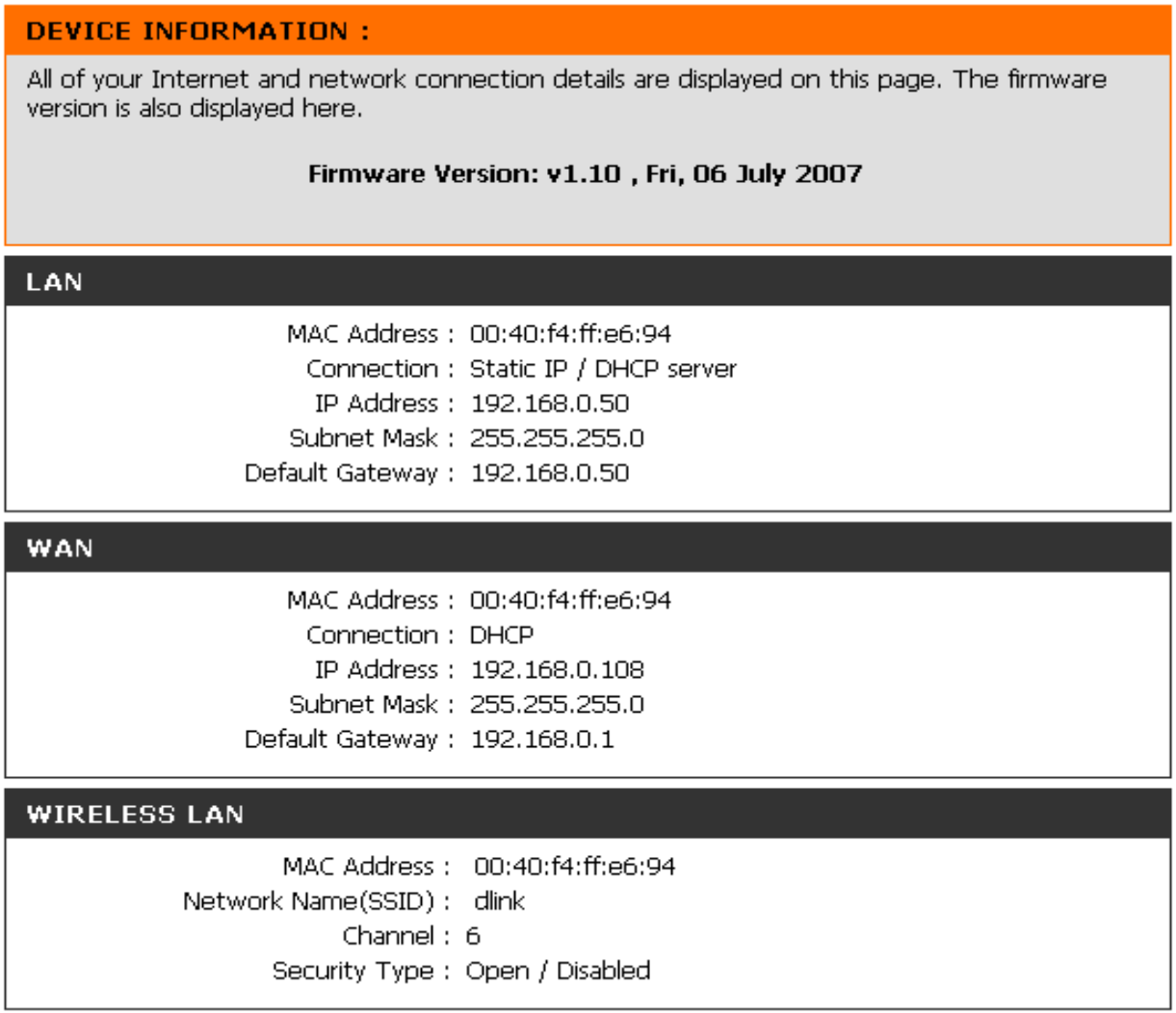
**Password:** Enter your password that is used with the SMTP server and re-enter it in the next box.



# Status

## Device Info

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



# Log

The DAP-1160 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.

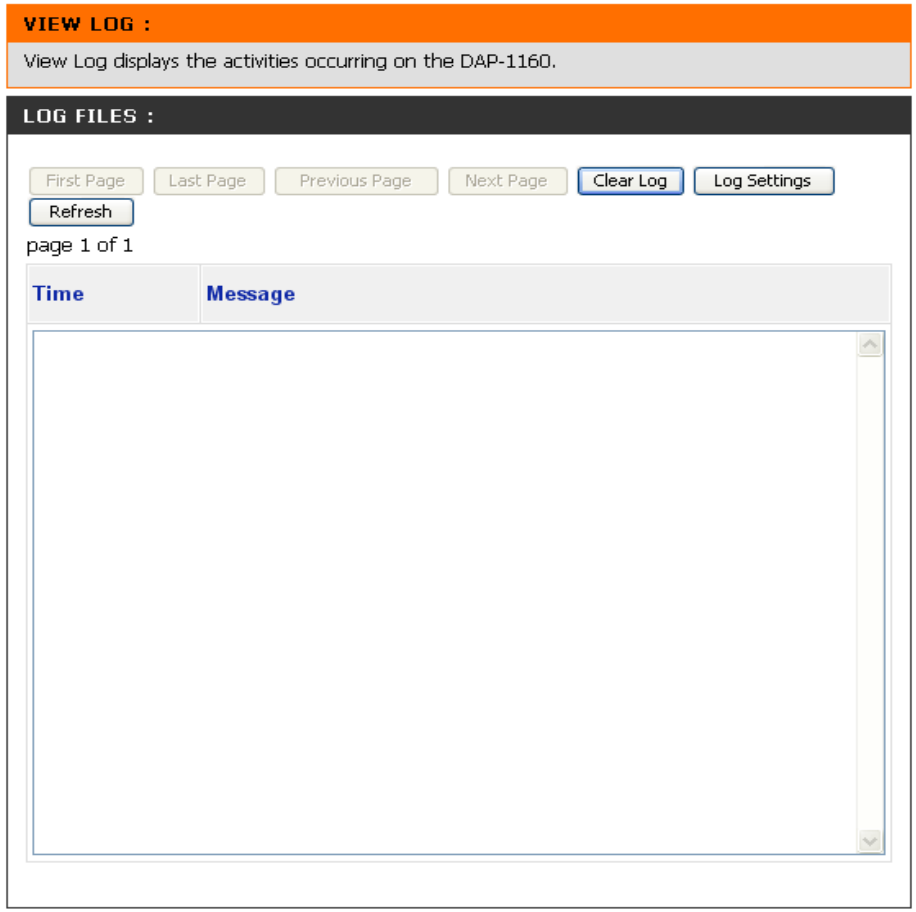
**Previous Page:** This button directs you to the previous page of the log.

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

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

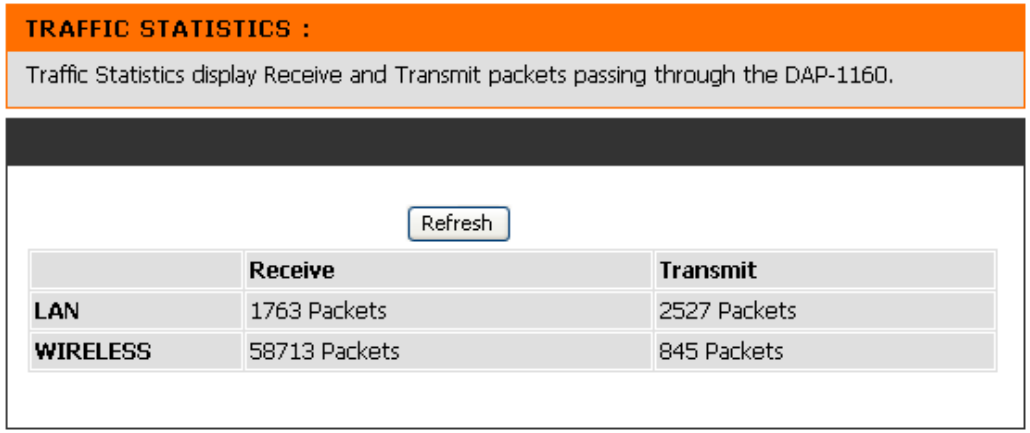
**Log Settings:** This button opens a new menu where you can configure the log settings.

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



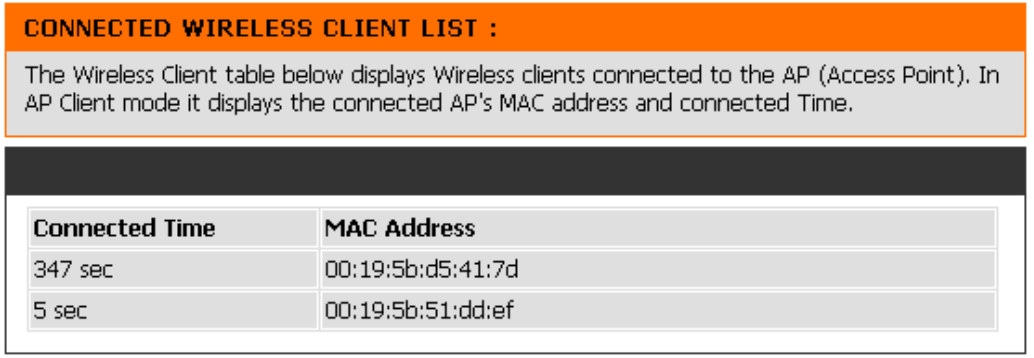
# Statistics

The DAP-1160 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.



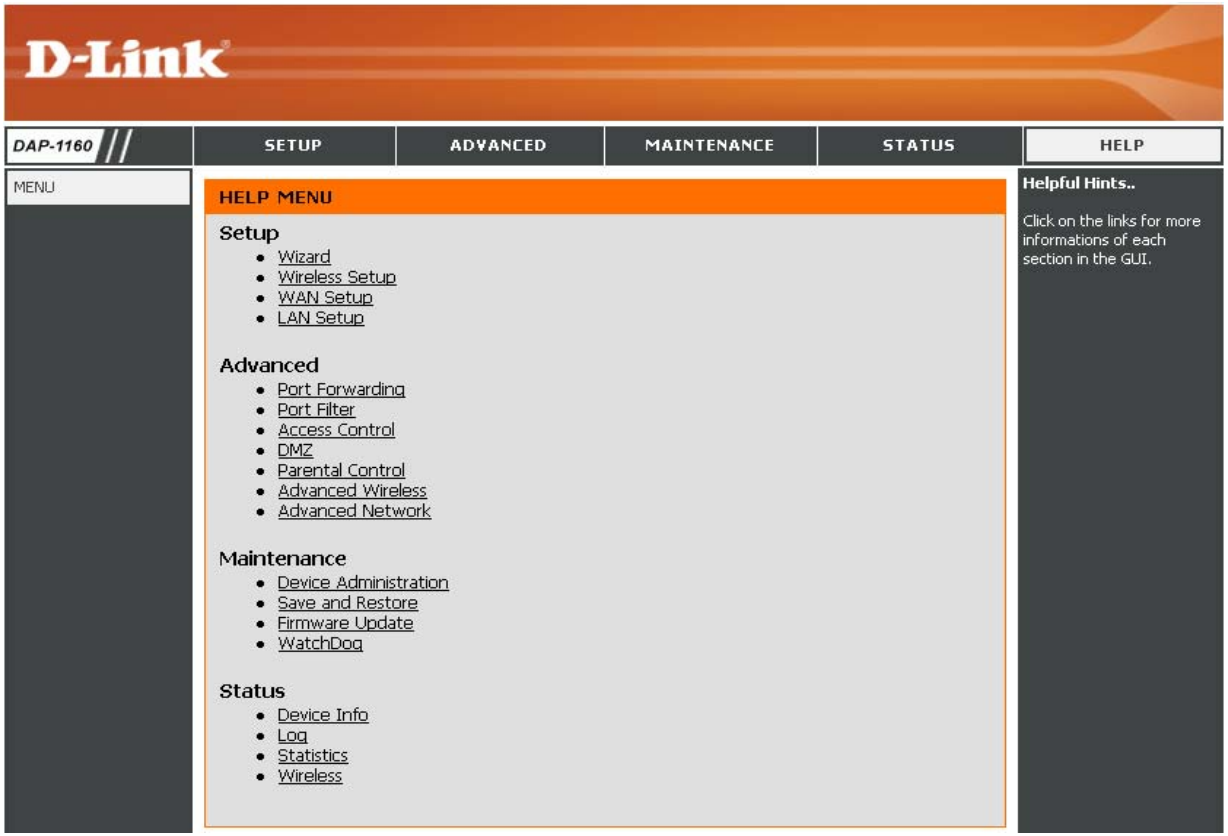

# Wireless

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-1160.



# Wireless Security

This section will show you the different levels of security you can use to protect your data from intruders. The DAP-1160 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 IP address of the access point (192.168.0.50). Click on **Wireless Settings** on the left side.

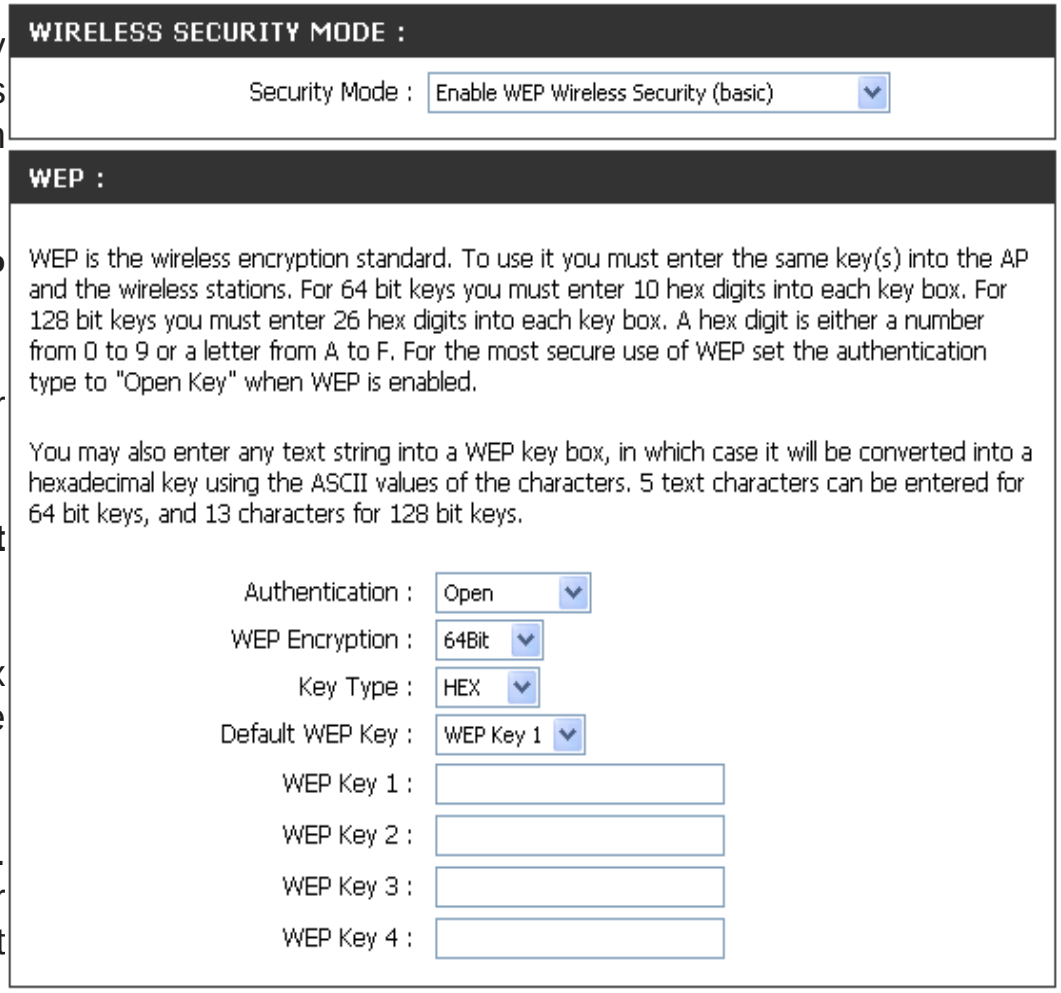
2. Next to Security Mode, select **Enable WEP Security**.

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.

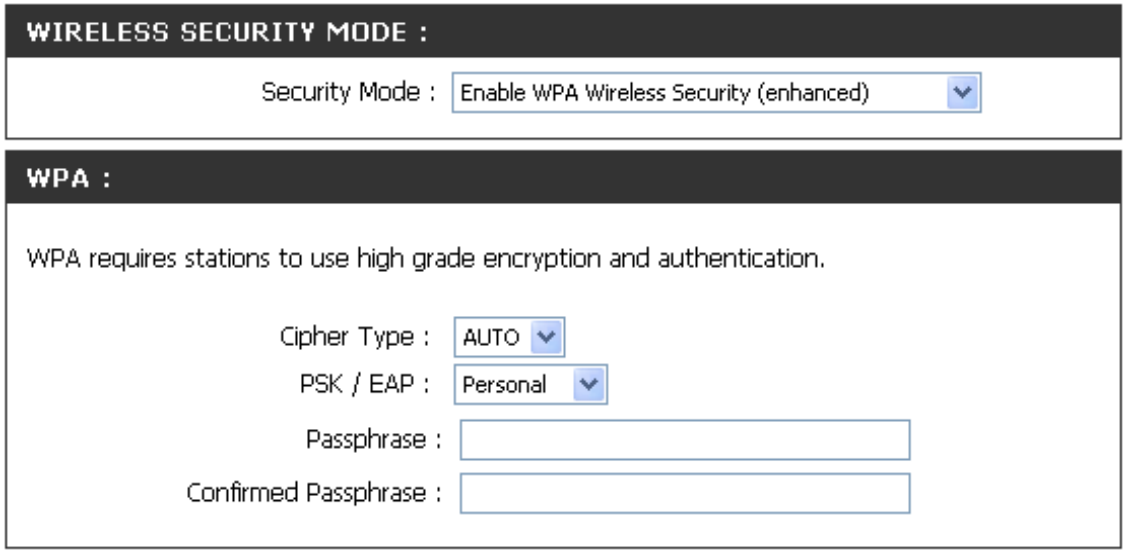
WPA-PSK/WPA2-PSK uses a passphrase or key to authenticate your wireless connection. The key is an alpha-numeric password between 8 and 63 characters long. The password can include symbols (!?*&_) and spaces. This key must be the exact same key entered on your wireless router or access point.

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 IP address of the access point (192.168.0.50). Click on **Wireless Settings** 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 IP address of the access point (192.168.0.50). Click on **Wireless Settings** 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.

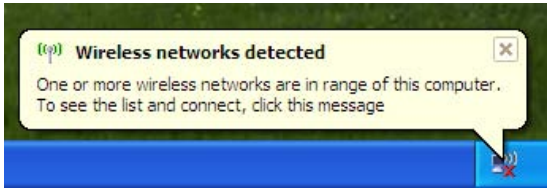
7. Next to Shared Secret, enter the security key.

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

# Connect to a Wireless Network Using Windows® XP

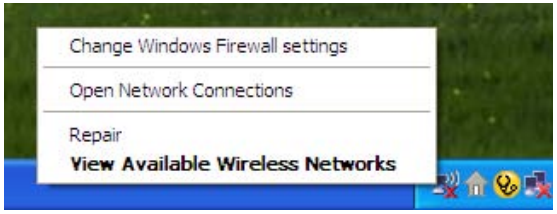
Windows® XP users can use the built-in wireless utility (Zero Configuration Utility) to connect to a wireless network. The following instructions are for Service Pack 2 users. If you are using another company's utility or Windows® 2000, please refer to the user manual of your wireless adapter for help 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.



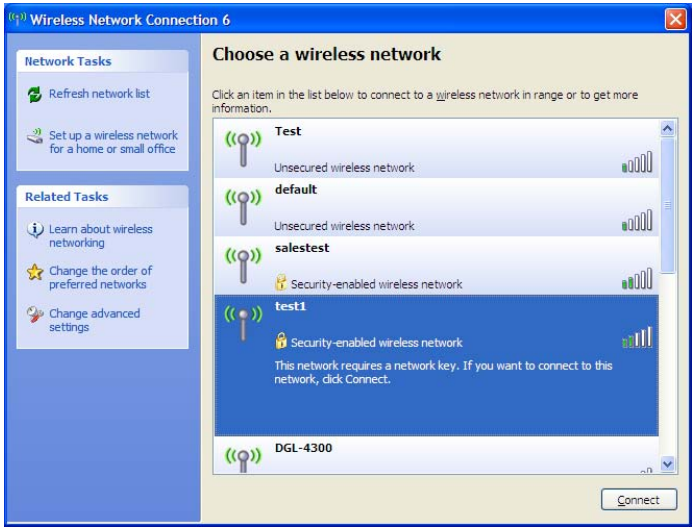

or

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.

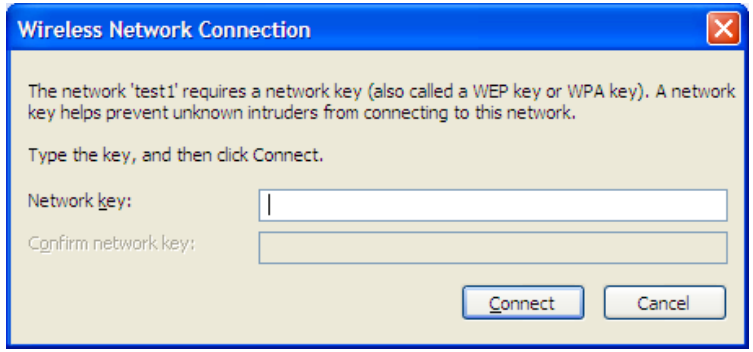
If you get a good signal but cannot access the Internet, check the TCP/IP settings for your wireless adapter. Refer to the **Networking Basics** section in this manual for more information.



# 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**.

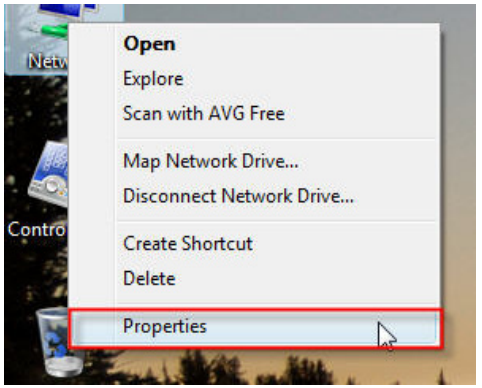



It may take 20-30 seconds to connect to the wireless network. If the connection fails, please verify that the WEP or WPA-PSK settings are correct. The WEP or WPA-PSK key must be exactly the same as on the wireless access point.

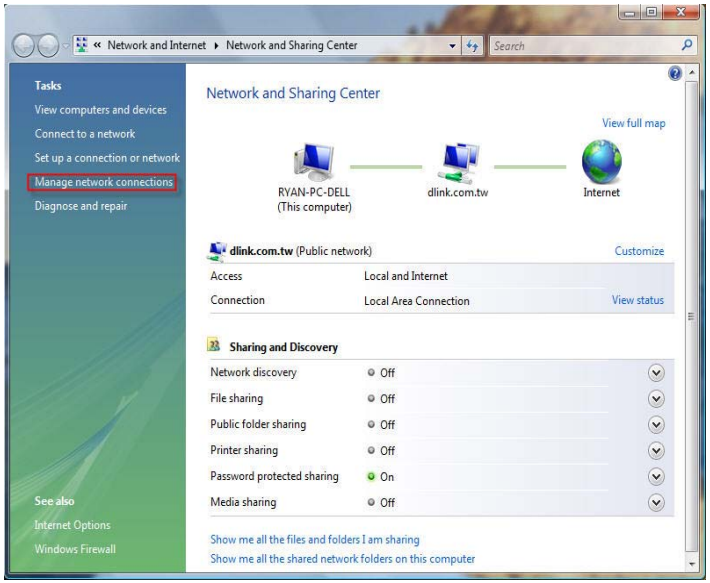
# Using Windows® Vista (Secured Network)

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

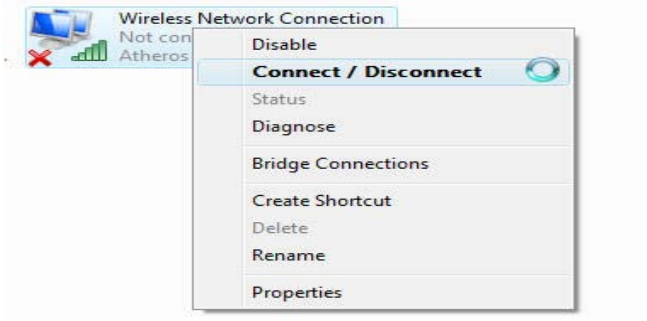
1. Right-click on **Network** and click on **Properties**.



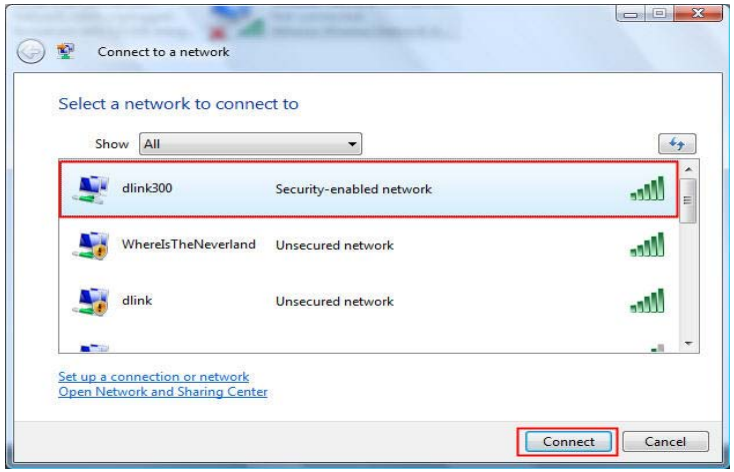

**2.** Click the **Manage network connections** link in the **Network and Sharing Center** window.



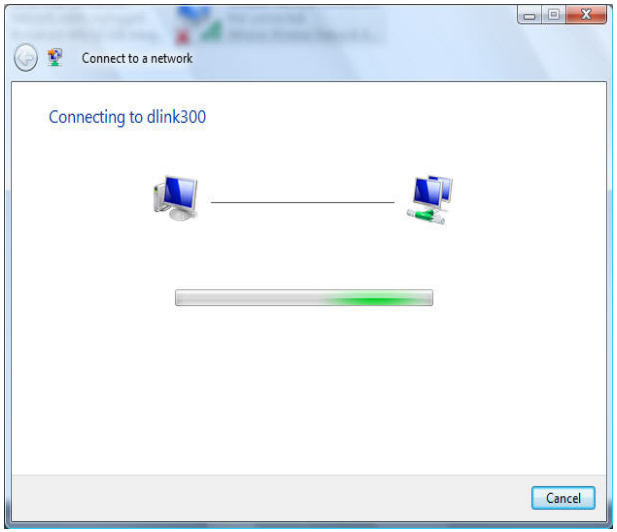
**3.** Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



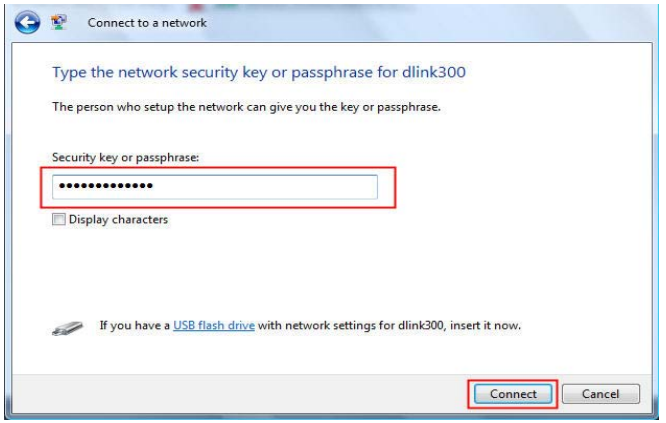

**4.** Select a network to connect to in the **Select a network to connect to** window and then click the **Connect** button.



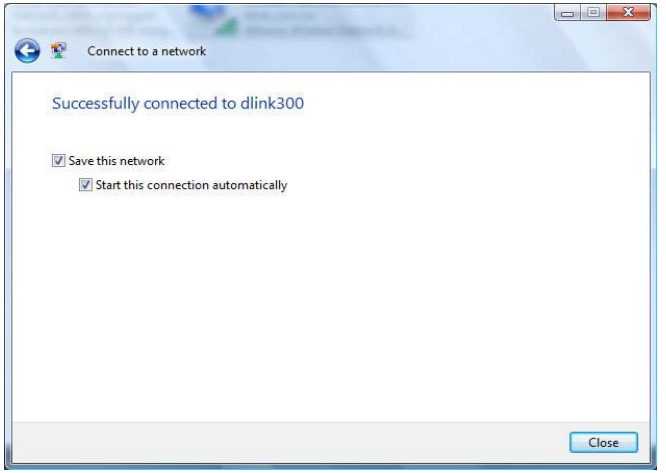

**5.** The following window displays connection progress.



**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.



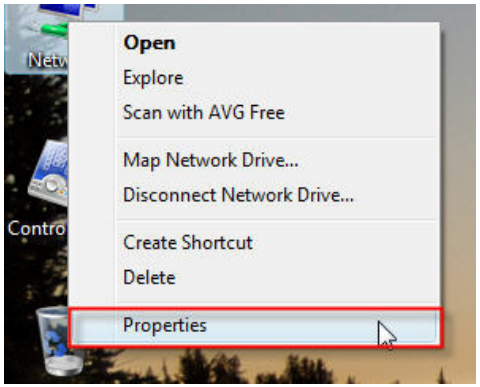

**7.** The following **Successfully connected to [SSID name]** window is displayed. Choose to save this network and/or start this new connection automatically. When you are finished, click the **Close** button.



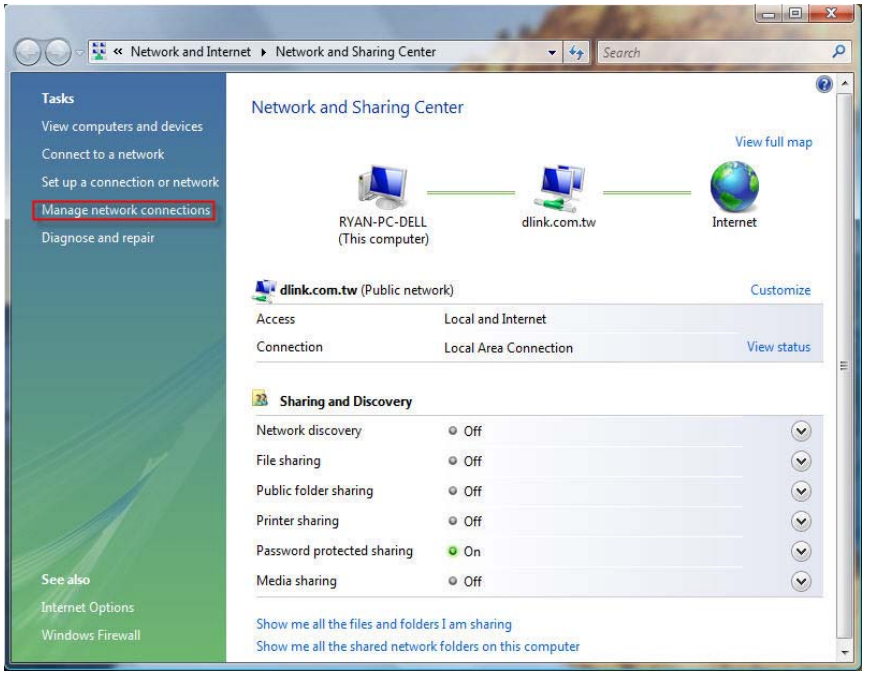
# Using Windows® Vista (Unsecured Network)

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

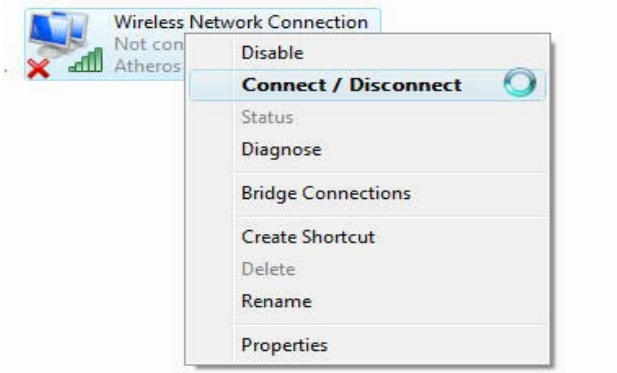
1. Right-click on **Network** and click on **Properties**.



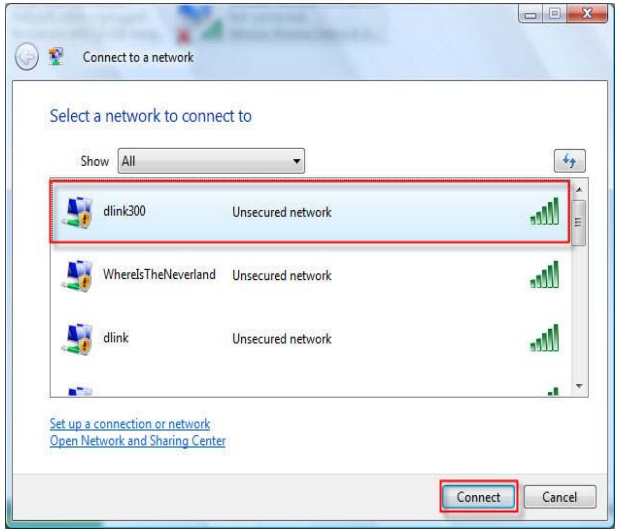

**2.** Go to the **Network and Sharing Center** window and click the **Manage Network Connections** link.



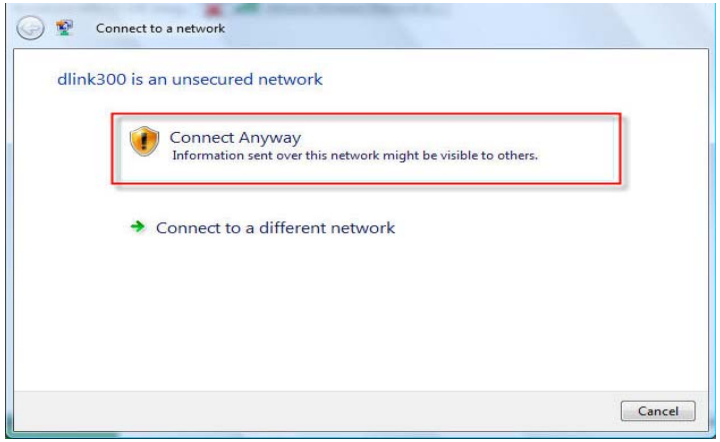
**3.** Right-click the **Wireless Network Connection** entry and then select **Connect/Disconnect** from the drop-down menu.



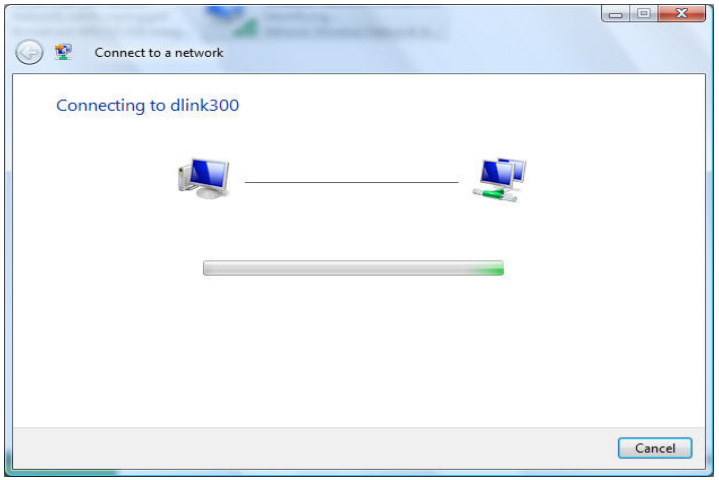

**4.** Select a network to connect to in the **Select a network to connect to** window and then click the **Connect** button.



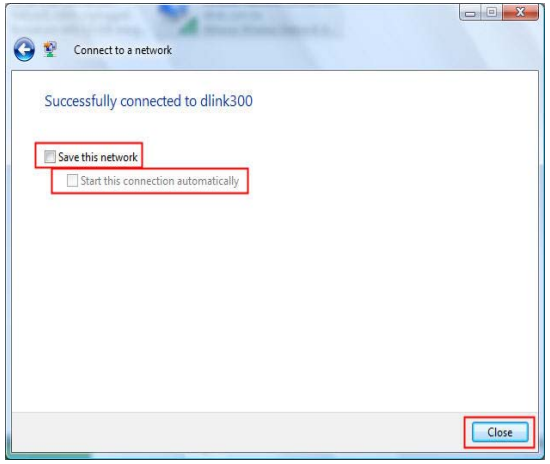

**5.** Confirm that you still want to connect on the following **Network Connection Status** window by clicking on **Connect Anyway**.



**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-1160. 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, 192.168.0.50), 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.

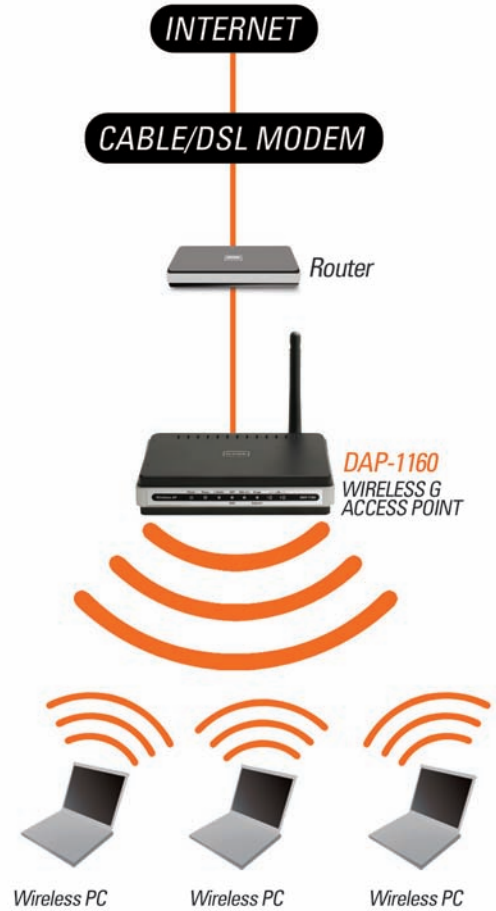
**2. What can I do if I forgot my password?**

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 192.168.0.50. When logging in, the username is **admin** and leave the password box empty.

# Wireless Modes
# Access Point Mode

In Access Point mode, the DAP-1160 acts as a central connection point for any computer (client) that has a 802.11g or backward-compatible 802.11b wireless network adapter and is within range of the AP. Clients must use the same SSID (wireless network name) and channel as the AP in order to connect. If wireless security is enabled on the AP, the client will need to enter a password to connect to the AP. Multiple clients can connect to the AP at the same time in Access Point mode.




**Wireless PCs Using the DAP-1160 as a Central Connection Point**

# AP Client Mode

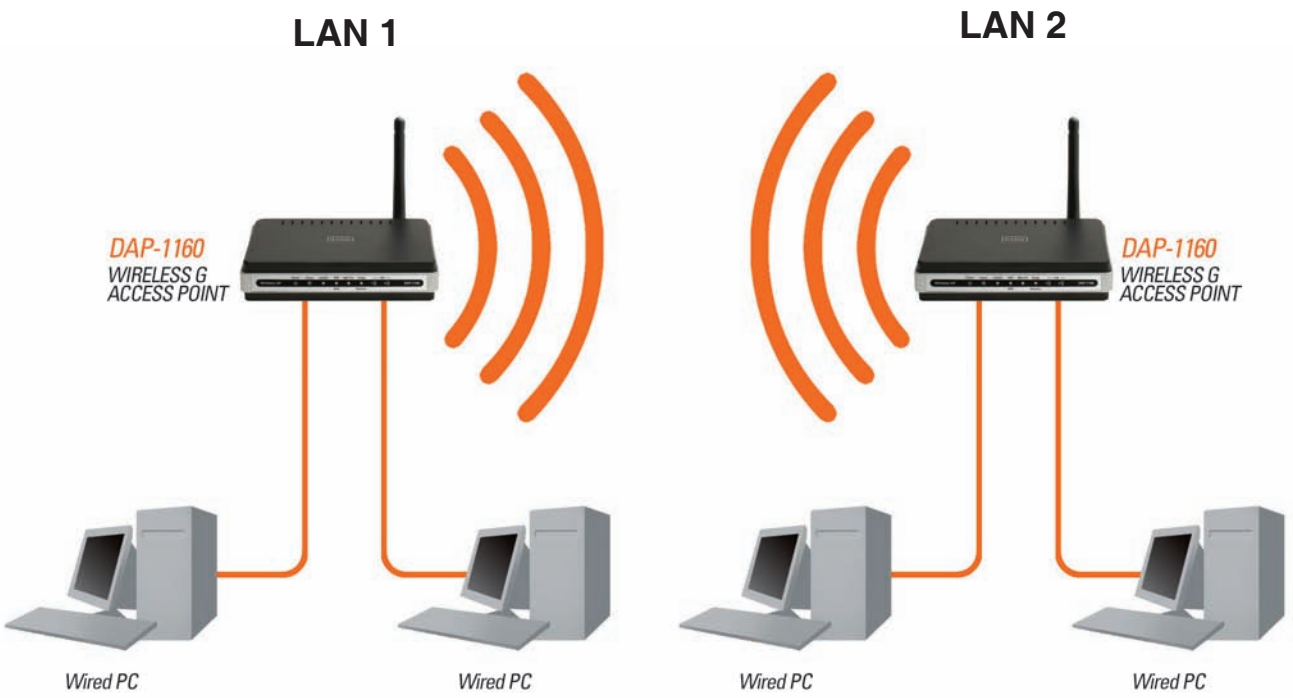
In AP Client mode, the DAP-1160 acts as a wireless network adapter for your Ethernet-enabled device (such as a game console or a TV set-top box). Connect your Ethernet-enabled device to the AP using an Ethernet cable. AP Client mode can support multiple wired clients.

**Ethernet-enabled Gaming Console Using the DAP-1160 as a Wireless Interface to Access the Internet**

# Bridge Mode

In Bridge mode, the DAP-1160 wirelessly connects seperate LANs that can't easily be connected together with a cable. For example, if there are wired LANs separated by a small courtyard, it would be expensive to bury cable between the two sides. A better solution is to use two DAP-1160 units to wirelessly connect the two LANs. In Bridge mode, both DAP-1160 units do not act as APs.

**Note:** Bridge Mode is not completely specified in Wi-Fi or IEEE standards. It can only work using other DAP-1160 units. Communication with other APs (even other D-Link APs) is not guaranteed.

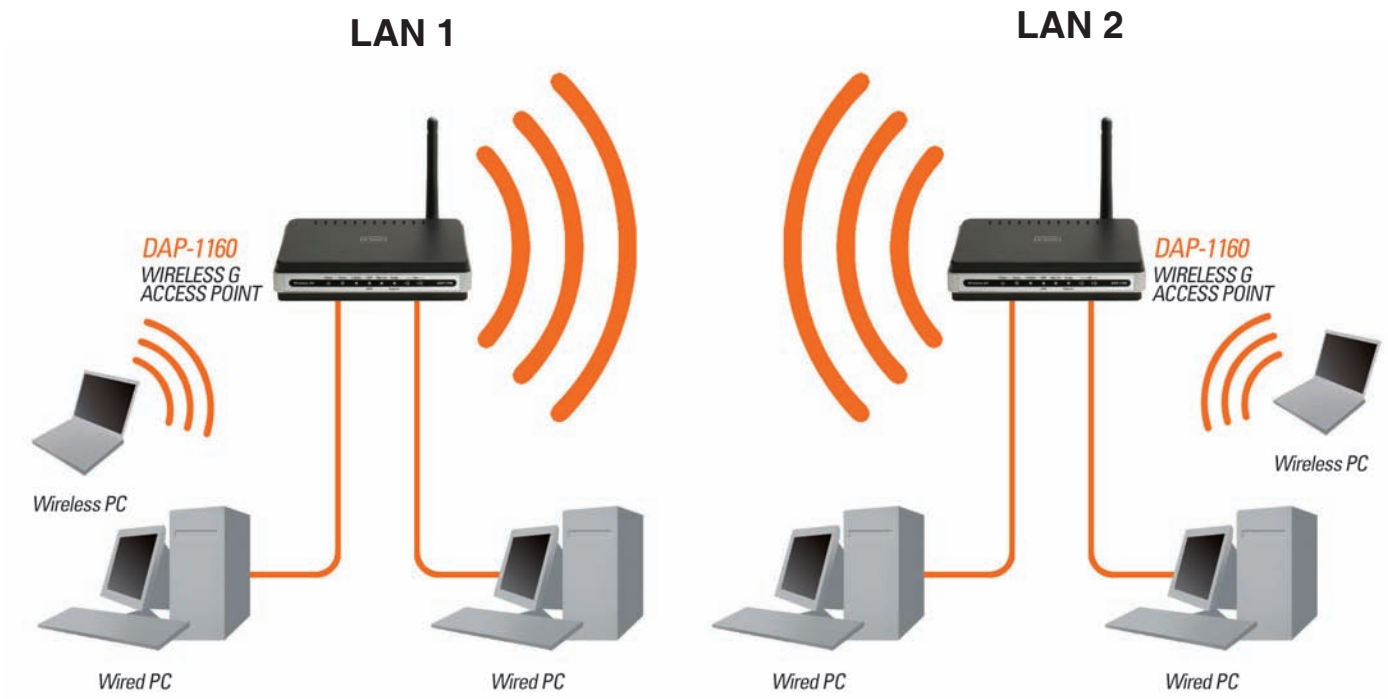



**Connecting Two Separate LANs Together Through Two DAP-1160 Units (Wireless PCs Cannot Access the DAP-1160 Units)**

# Bridge with AP Mode

Bridge with AP mode is the same as Bridge mode, but it also acts as an AP. Clients with wireless network adapters can wirelessly connect to the AP and then connect to the other LAN that the DAP-1160 bridges to.

**Note:** Bridge with AP Mode is not completely specified in WiFi or IEEE standards. It can only work using other DAP-1160 units. Communication with other APs (even other D-Link APs) is not guaranteed.




**Connecting Two Separate LANs Together Through Two DAP-1160 Units (Wireless PCs Can Access the DAP-1160 Units)**

# Repeater Mode

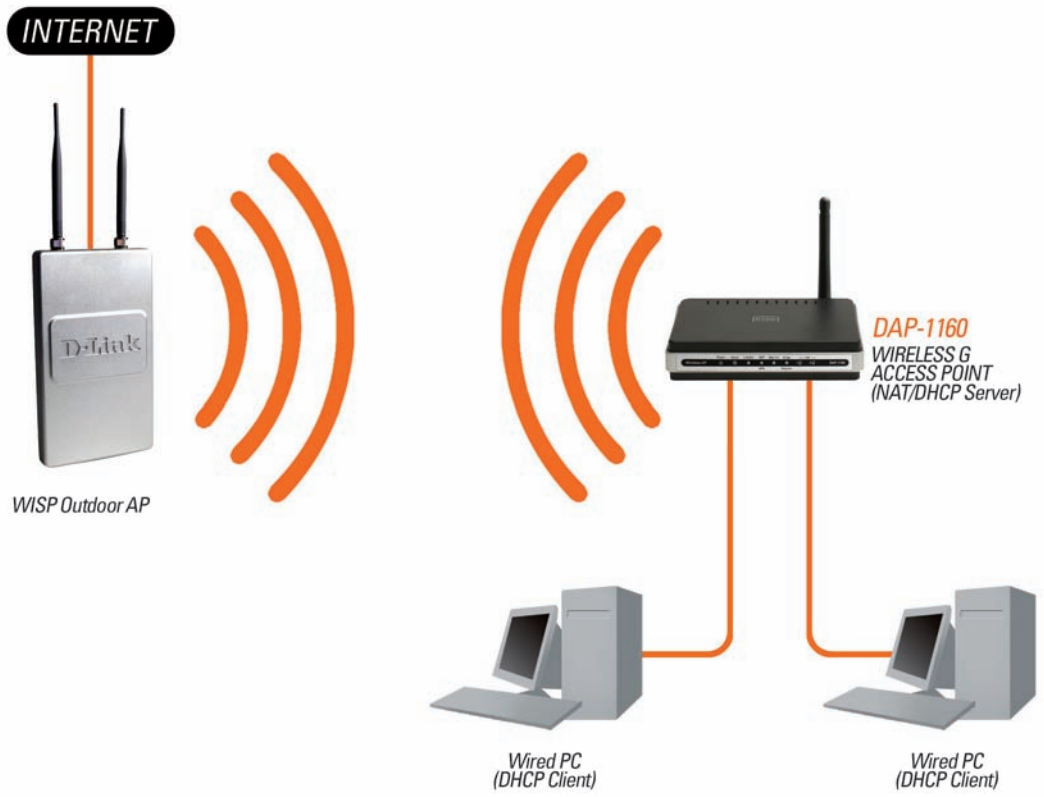
Repeater mode increases the range of your wireless network by extending the wireless coverage of another AP or wireless router. The APs and wireless router (if used) must be within range of each other. Make sure that all clients, APs, and the wireless router all use the same SSID (wireless network name) and channel.

**Extending the Wireless Coverage of a Wireless Router Using the DAP-1160**

# WISP Client Router Mode

In WISP Client Router mode, the DAP-1160 wirelessly connects to a WISP (Wireless Internet Service Provider) AP. In this mode, the DAP-1160 also acts as a router for wired clients on your LAN and provides NAT (Network Address Translation) and a DHCP server to generate IP addresses for wired clients. NAT and the DHCP server allow many computers to share the same wireless Internet connection.

An example scenario is a WISP subscriber that wants to access their WISP account using wired computers. The wired computers connect to the DAP-1160, which provides NAT, and then connects to the WISP AP.

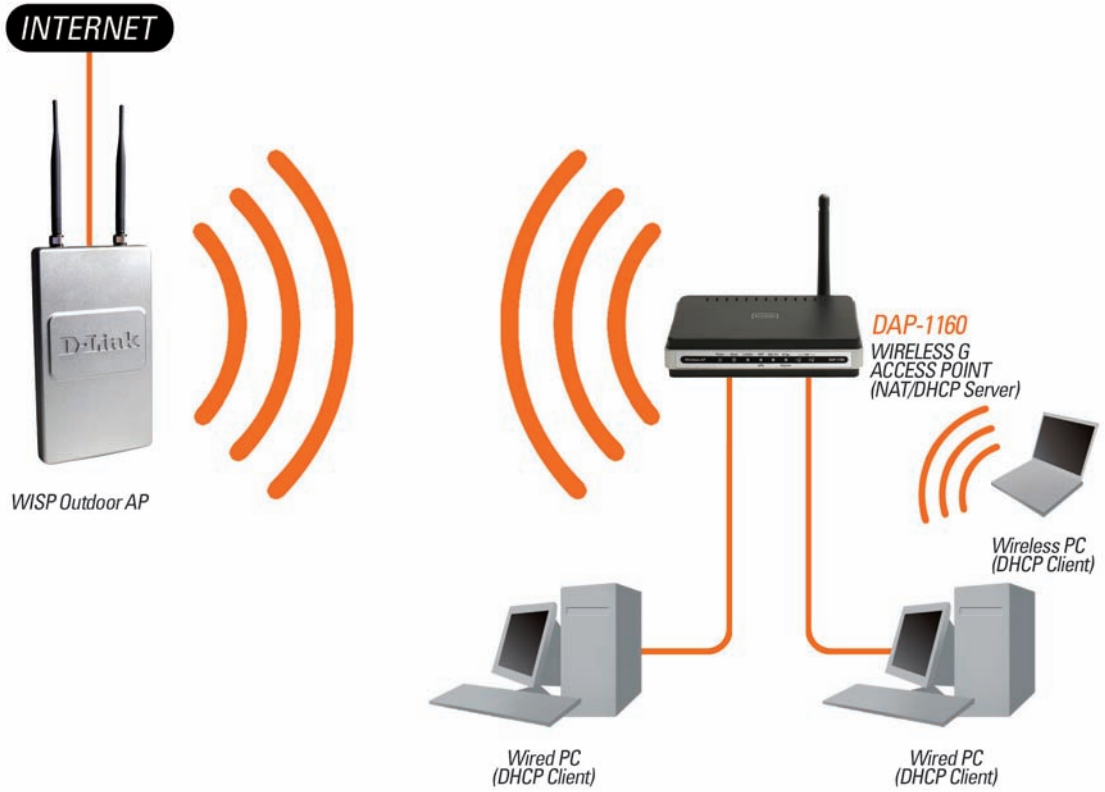



**Connecting Wired PCs to the Internet Using the DAP-1160**

# WISP Repeater Mode

In WISP Repeater mode, the DAP-1160 wirelessly connects to a WISP (Wireless Internet Service Provider) AP. In this mode, the DAP-1160 also acts as a router for both wireless and wired clients on your LAN. WISP Repeater mode provides NAT (Network Address Translation) and a DHCP server to generate IP addresses for both wireless and wired clients. NAT and the DHCP server allow many computers to share the same wireless Internet connection.

An example scenario is a WISP subscriber that wants to use their WISP account in their house, but the signal from the outdoor WISP AP isn't strong enough to reach all of the areas in the house. The DAP-1160 can extend the signal from the outdoor WISP AP and provide access for any wireless clients in the house. In addition, wired clients can connect to the DAP-1160, thus accessing the outdoor WISP AP.




**Connecting Wired and Wireless PCs to the Internet Using the DAP-1160**

# 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 a WLAN, but it doesn't use nearly as much 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 expanding everywhere not just at home or the 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 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 you next-door neighbors or 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.

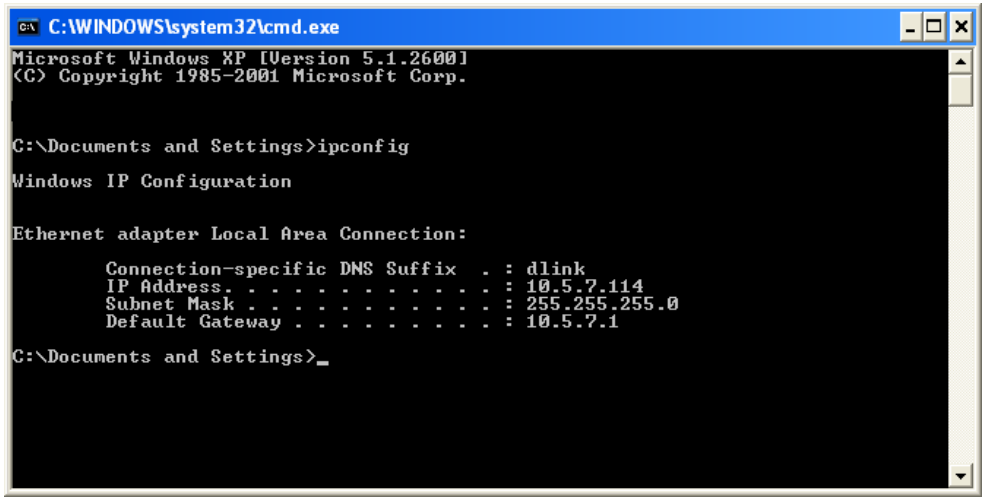
# Networking Basics

## 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

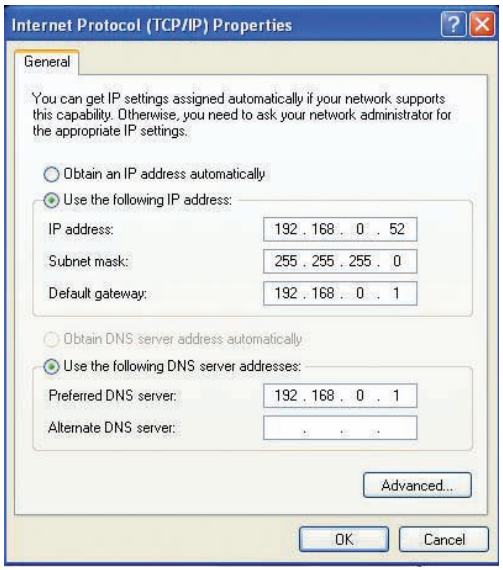
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

**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.

# Technical Specifications

**NETWORK STANDARDS**
- 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**
- 802.11g wireless LAN
- 2 10/100BASE-TX Ethernet LAN ports

**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
- AP Client
- Bridge
- Bridge with AP
- Repeater
- WISP Client Router
- WISP Repeater

**ANTENNA**
2dBi Gain detachable omni-directional antenna with RP-SMA connector

**RECEIVE SENSITIVITY**
+For 802.11b, at 8% PER:
- 11Mbps: -80dBm
- 5.5Mbps: -84dBm
- 2Mbps: -87dBm
- 1Mbps: -88dBm

+ For 802.11g, at 10% PER:
- 54Mbps: -65dBm
- 48Mbps: -66dBm
- 36Mbps: -70dBm
- 24Mbps: -74dBm
- 18Mbps: -77dBm
- 12Mbps: -79dBm
- 9Mbps: -81dBm
- 6Mbps: -82dBm

**Transmit Output Power**
+ For 802.11b:
16dBm (typical)
+ For 802.11g:
14dBm (typical)

**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
- Status
- Link/Act
- WEP/WPA
- MAC Ctrl
- Bridge/Repeater
- LAN1
- LAN2

**POWER INPUT**
5VDC 2A
External power adapter

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

**WEIGHT**
229grams (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

**CERTIFICATION**
- FCC Class B
- CE
- C-Tick
- Wi-Fi

54Mbps maximum wireless signal rate derived from IEEE standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, may lower actual throughput rate. Environmental factors will adversely affect wireless signal range, maximum throughput based on 802.11g devices.

D-Link®

Building Networks for People

Version 1.30

Jan 22, 2009